DOI:10.12158/j.2096-3203.2022.03.001

# 基于事件驱动的配电信息物理连锁故障演化机理

黄植，刘东，陈冠宏，翁嘉明，殷浩洋，王臻
（电力传输与功率变换控制教育部重点实验室（上海交通大学），上海 200240）

**摘　要**：随着通信与控制技术在配电系统中的迅速发展，配电系统逐渐呈现出信息物理系统的典型特征，这既带来了崭新的发展机遇，也将信息系统中的多类型风险引入到了电力系统。多类型风险易使电网中信息物理连锁故障频发，导致严重事故。因此，分析与研究信息物理连锁故障的演化过程与故障后果，探索信息物理连锁故障演化的内在机理具有重要的理论与现实意义。文中基于事件驱动模型提出配电信息物理系统架构，分析物理与信息系统的交互机理，提出信息物理连锁故障演化机理研究框架。然后，对信息系统内部节点重要度进行研究，综合考虑系统总风险值与防御资源，计算信息节点被攻击成功概率等相关参数并建立相关矩阵。最后，在算例上进行信息物理连锁故障演化机理的仿真计算，得出了发生信息物理连锁故障时系统会承受更大的风险且可能导致更大损失的结论，验证了所提机理在故障过程推演和后果计算上的有效性。

**关键词**：事件驱动；配电信息物理系统；信息物理系统架构；交互机理；信息物理连锁故障；连锁故障演化机理
**中图分类号**：TM71　　**文献标志码**：A　　**文章编号**：2096-3203（2022）03-0002-12

## 0　引言

随着通信技术在电力系统中的迅速发展，电力系统逐渐呈现出信息物理系统（cyber-physical system，CPS）的典型特征[1—4]。配电 CPS 作为整个电力 CPS 发展的关键环节，是一个多层异构复杂系统。当电力系统与信息系统相互关联融合后，原本存在于信息系统中的各类安全风险也有可能被引入电力系统中，甚至严重影响电力系统的安全可靠运行[5—7]。近年来电网信息物理连锁故障频繁发生[8]，严重影响了电力用户的正常工作生产与电力系统的正常运行。因此，分析信息物理连锁故障的演化过程并对其机理进行理论研究具有重要意义。

目前，针对信息物理连锁故障的研究主要集中在两方面：一方面是分析其带给电力 CPS 的安全风险与故障危害，并相应提出提升安全性的方法；另一方面是在特定场景下对其演化与传播过程进行分析和研究。对第一类研究，文献[9]分析了信息系统监测与控制功能失效对连锁故障演化的影响；文献[10—13]对电力 CPS 架构存在的安全缺陷及其可能面临的安全风险进行了探讨，并提出了若干针对信息物理连锁故障的防护策略；文献[14]对因信息系统节点遭受攻击而导致物理系统故障引发大规模停电事故的可能性进行了论证；文献[15]对电力 CPS 运行过程中物理与信息空间的交互机理进行了初步探索研究；文献[16]提出了一种配电网信息物理故障的耦合度计算方法，从故障带来的危害程度方面对故障进行评价。文献[17—18]建立了信息物理连锁故障脆弱度评估体系，量化了连锁故障的危害性。对第二类研究，文献[19—22]从具体应用场景出发，设想几类典型的信息物理连锁故障并推演其发展过程，试图归纳总结演化机理。

无论是对于电力 CPS 安全风险与故障危害的分析[23—24]，还是对信息物理连锁故障演化过程的推演与总结，大多是从几类具体的连锁故障出发展开分析与研究，并试图从中总结出演化机理。但这种由某几类具体故障总结抽象而得出的成果缺少泛用性，无法证明其对其他故障也适用，研究成果可扩展性不强。

为进一步阐明配电 CPS 中连锁故障机理及故障对系统安全稳定运行的危害，文中做了如下工作：（1）基于事件驱动模型建立配电 CPS 架构，以符号化语言定义 CPS 事件，分析物理与信息系统的交互机理。（2）基于此提出了信息物理连锁故障演化机理，通过分析与计算信息节点重要度与被攻击成功概率等多项指标建立信息矩阵，完善了机理内容。（3）由所提出的机理对实际算例进行研究，量化计算信息物理连锁故障相比于物理连锁故障对电力系统的额外风险与损失，验证了机理的合理性与其在故障过程推演和后果计算上的有效性。

## 1　基于事件驱动的系统架构与机理框架

### 1.1　基于事件驱动的配电 CPS 架构

事件驱动是指在系统中，由于某一事件的出现或须要被处理，驱动系统整体或部分的状态发生改

收稿日期：2022-02-11；修回日期：2022-04-17
基金项目：国家自然科学基金资助项目（U2166210）

变。事件驱动性是 CPS 的一种本征运行机制:物理层、信息层设备的工作状态与系统的运行状态变化,会在具体 CPS 事件触发后依序执行控制命令,从而形成 CPS 节点或组件间的交互。

在配电 CPS 中,信息系统可由下至上归纳为 3 个层级:接入层、汇聚层和核心层。在不同层级中,存在不同的信息设备,其可靠性也不同。文中提出基于事件驱动的配电 CPS 架构,如图 1 所示。图中,信息事件代指以信息传输或影响其过程为形式的各类事件;物理事件代指以物理元件或设备动作或影响其物理实体为形式的各类事件,具体到不同元件之间其形式各有不同。图 1 中基于事件驱动模型对配电网中故障演化过程进行了描述,其中 $E_1$—$E_8$代指各类 CPS 事件。

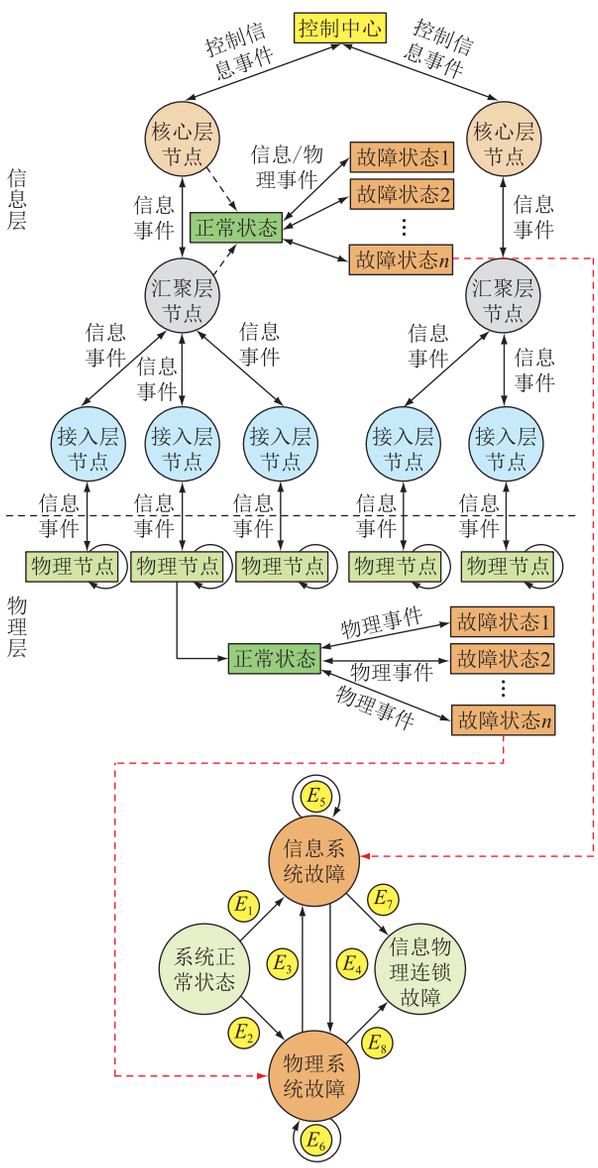


**图 1　基于事件驱动模型的配电 CPS 架构**

Fig.1　Distribution CPS architecture based on event-driven model

因此,在事件驱动框架的视角下,配电 CPS 中各对象交互的基本单元是 CPS 事件,事件驱使各个 CPS 对象状态发生演变。为了更准确地描述配电 CPS 演化过程中的交互逻辑与约束关系,文中采用符号化语言定义的 CPS 事件描述 CPS 协同动作的同步机制和时间约束机制。一个 CPS 事件可以定义为:

$$\langle pr\rangle \mapsto \xi_{\mathrm{CPS}} :=$$
$$\Gamma\langle a\rangle \oplus \langle t_{\mathrm{g}}, o_{\mathrm{g}}\rangle \oplus \langle t_{\mathrm{r}}, o_{\mathrm{r}}\rangle$$
$$t_{\mathrm{g}}, t_{\mathrm{r}} := [t_1, t_2]$$
$$o_{\mathrm{g}}, o_{\mathrm{r}} \in O_{\mathrm{CPS}}$$
$$t_1, t_2 \in \mathbf{R}^+$$

在符号化语言中,“:=”表示“定义为”;“↦”表示判据触发后将会进行的 CPS 事件;$[t_1, t_2]$ 标定了时标 $t_{\mathrm{g}}$和 $t_{\mathrm{r}}$的取值范围,为闭集;$O_{\mathrm{CPS}}$ 为 CPS 中所有对象的集合;$\mathbf{R}^+$为正实数集合;触发判据 $\langle pr\rangle$ 的形式为逻辑命题表达式,其决定了事件 $\xi_{\mathrm{CPS}}$ 是否产生;$\Gamma$ 为 CPS 事件实例的类型标识符,指示了该事件的类型;$a$ 为值向量,用于传递事件类型对应的物理量值/信息量值;$\langle t_{\mathrm{g}}, o_{\mathrm{g}}\rangle$ 为内部属性组,$t_{\mathrm{g}}$ 为事件发生的时间,$o_{\mathrm{g}}$ 为事件发生的对象;$\langle t_{\mathrm{r}}, o_{\mathrm{r}}\rangle$ 为外部属性组中,$t_{\mathrm{r}}$ 为事件处理对象接收到事件的时间,$o_{\mathrm{r}}$ 为事件处理对象。

该事件驱动模型实现了状态迁移事件、信息交互事件的统一建模。文中将使用该模型对各 CPS 事件进行定义与表示。

### 1.2　基于事件驱动的信息物理连锁故障演化机理研究框架

#### 1.2.1　配电 CPS 物理与信息系统交互机理分析

在建立配电信息物理连锁故障演化机理的研究框架之前,应先分析物理系统与信息系统之间的交互机理。而在分析交互机理之前,首先应明确系统的整体架构及各部分功能。由所提出的配电 CPS 架构可知,信息系统一方面负责采集物理系统各节点的实时运行数据并将其逐级向上传输,为控制中心的系统状态评估与调度指令发布提供必要的数据基础;一方面将控制中心发布的调度指令下传,使得物理系统执行相关指令以调整电力系统运行状态,完成对电力系统的控制。一旦控制中心通过所收到的数据判断电力网络存在故障,就会对故障的位置与类型进行准确判断,并基于内嵌算法或人工下发调度指令切除故障使得损失降到最小。

由以上分析可知,控制中心对电力系统当前状态进行评估时,是基于数据采集系统收集到的各量测信息进行的;物理系统依据指令进行动作时,是

基于信息系统传来的控制信息进行的。因此控制中心的判断状态并不是电力系统的真实状态，而是基于采集数据分析得来的感知状态；物理系统执行的控制命令也不是控制中心实际产生的真实指令，而是通过信息系统传递的传输指令。物理系统与信息系统的交互作用见图 2。

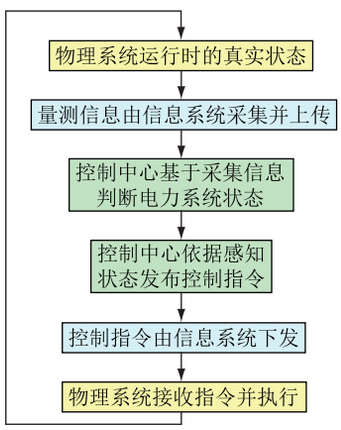


**图 2　物理系统与信息系统的交互作用**

Fig.2　Interaction between physical system and cyber system

因此，若由于信息系统存在设计缺陷或遭受网络攻击而导致信息的采集或传输出现故障时，一方面可能使得控制中心对于电力系统状态的判断与电力系统的真实状态出现较大差异，另一方面也可能使得控制中心实际产生的调度指令与物理系统接收到的传输指令不同，从而导致严重后果。由此可见，配电 CPS 中物理系统与信息系统紧密耦合、相互影响，物理或信息系统中任意一个故障，都可能对配电 CPS 的稳定运行造成影响，甚至可能导致信息物理连锁故障的发生。

1.2.2　信息物理连锁故障演化机理研究框架

由上节分析可知，产生信息物理连锁故障的根源可能是信息系统元件与电力系统元件，亦或二者同时引发。而使得电力系统与信息系统紧密耦合的关键点就是存在于二者之间的信息流。信息流可分为上行信息流与下行信息流。前者指由物理层发往信息层的信息流，通常是各类电力二次设备与一次设备交互产生的各类状态信息等；后者指由信息层发往物理层的信息流，通常是控制中心产生的各类用以调整电力系统运行状态的控制指令。因此，产生信息物理连锁故障的根本原因是信息系统与电力系统的紧密耦合，使得以往孤立存在于各自系统中的安全风险与故障通过信息流对对方网络甚至整个系统产生影响。

引起配电 CPS 连锁故障演化的机理是信息流不断地在物理与信息系统之间来回传递并产生影响，使得物理与信息系统自身的状态不断变化，该过程不断反复，使得故障状态不断演化。文中将信息物理连锁故障演化机理的研究重点放在导致故障形成的上行与下行信息流上，对其在信息与物理空间之间传递并产生影响的过程进行描述并以矩阵形式量化分析，以体现电力系统与信息系统的交互过程。文中基于事件驱动模型建立的机理研究框架如图 3 所示。

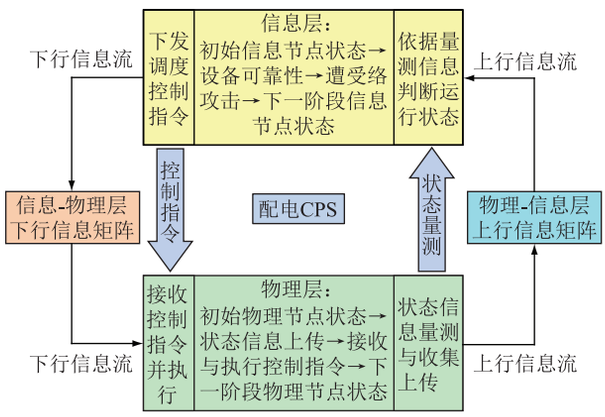


**图 3　信息物理连锁故障机理研究框架**

Fig.3　Research framework of cyber-physical cascading failure mechanism

## 2　信息物理连锁故障演化机理

### 2.1　信息节点重要度分析与计算

与一般的电力系统不同，对于信息与物理系统紧密耦合的配电 CPS 而言，评价信息节点的重要度不仅应考虑单侧网络的特性，还应考虑 2 个系统的耦合性。鉴于此，文中提出从信息节点在拓扑中的重要性，在信息业务中的重要性与所在信息层级重要性 3 个方面来综合评价其重要性。

2.1.1　信息节点拓扑重要度计算

基于复杂网络理论将信息系统抽象为一个无向无权网络，将馈线终端装置（feeder terminal unit，FTU）、数据传输单元（data transfer unit，DTU）、交换机、路由器等均视为节点，信息通信线路视为边，使用复杂网络理论中的统计特征从拓扑结构方面评价其重要度，使用邻接矩阵 $\boldsymbol{M}_c$ 来描述网络中各个节点之间的连接关系。假设信息层节点数目为 $m$，则邻接矩阵 $\boldsymbol{M}_c$ 中各元素的数值定义如下：

$$m_c(i,j)=m_c(j,i)=\begin{cases}1 & 1\leqslant i,j\leqslant m;i\neq j;j\in\varphi(i)\\0 & 1\leqslant i,j\leqslant m;i\neq j;j\notin\varphi(i)\\0 & 1\leqslant i,j\leqslant m;i=j\end{cases}\tag{1}$$

式中：$\varphi(i)$ 为信息节点 $i$ 的连接边集合。信息节点 $i$ 的拓扑重要度计算方式如下：

$$I_{\mathrm{dt}i}=\sum_{j=1}^{m}\frac{m_{\mathrm{c}}(i,j)}{k^2} \tag{2}$$

式中:$k$ 为平均度值;$I_{\mathrm{dt}i}$ 为信息节点 $i$ 的拓扑重要度,与该点相连接的节点越多,该值越大。

2.1.2 信息节点业务重要度分析与计算

将信息层的信息节点分为 2 类:与物理层设备有信息交换,存在耦合关系的信息节点称为混合信息节点;仅与信息层设备有信息交换的信息节点称为纯信息节点。设配电 CPS 中信息层节点的集合 $E_{\mathrm{c}}=E_{\mathrm{h}}\cup E_{\mathrm{p}}=\{E_1,E_2,\cdots,E_m\}$,混合信息节点集合 $E_{\mathrm{h}}=\{e_1,e_2,\cdots,e_{m_{\mathrm{h}}}\}$,$m_{\mathrm{h}}$ 为混合信息节点数量;$E_{\mathrm{p}}=\{e_1,e_2,\cdots,e_{m_{\mathrm{p}}}\}$ 为纯信息节点集合,$m_{\mathrm{p}}$ 为纯信息节点数量;$m=m_{\mathrm{h}}+m_{\mathrm{p}}$。

(1) 混合信息节点。该类信息节点一般位于信息网络接入层的最底端,承担采集、发送物理设备相关参数,接收控制指令等任务。混合信息节点在信息业务上的重要度主要由与其耦合的物理节点的重要度决定。定义 $\delta_{\mathrm{uh}}=\{\delta_{\mathrm{uh1}},\delta_{\mathrm{uh2}},\cdots,\delta_{\mathrm{uh}m_{\mathrm{h}}}\}$ 为混合信息节点业务重要度系数集合,其与各耦合物理节点的物理后果成正比。混合信息节点耦合物理节点的物理后果计算流程如图 4 所示,各点业务系数计算方法如式(3)所示。

$$\delta_{\mathrm{uh}i}=\frac{L_{\mathrm{loss}i}-\min L_{\mathrm{loss}}}{\max L_{\mathrm{loss}}-\min L_{\mathrm{loss}}} \tag{3}$$

式中:$\delta_{\mathrm{uh}i}$ 为混合信息节点业务重要度系数;$L_{\mathrm{loss}}=\{L_{\mathrm{loss1}},L_{\mathrm{loss2}},\cdots,L_{\mathrm{loss}m_{\mathrm{h}}}\}$ 为各耦合物理节点负荷期望损失值集合;$\max L_{\mathrm{loss}}$,$\min L_{\mathrm{loss}}$ 分别为集合 $L_{\mathrm{loss}}$ 中最大值和最小值。

(2) 纯信息节点。该类信息节点大多数位于信息网络汇聚层与核心层,承担连接多个信息设备,进行信息传输与交换等任务。纯信息节点业务重要度系数集合 $\delta_{\mathrm{up}}=\{\delta_{\mathrm{up1}},\delta_{\mathrm{up2}},\cdots,\delta_{\mathrm{up}m_{\mathrm{p}}}\}$,其由各纯信息节点承载的信息量决定。纯信息节点承载信息量计算流程如图 5 所示,其业务系数计算方法如式(4)所示。

$$\delta_{\mathrm{up}i}=\frac{I_{\mathrm{gather}i}-\min I_{\mathrm{gather}}}{\max I_{\mathrm{gather}}-\min I_{\mathrm{gather}}} \tag{4}$$

式中:$\delta_{\mathrm{up}i}$ 为纯信息节点业务重要度系数;$I_{\mathrm{gather}}=\{I_{\mathrm{gather1}},I_{\mathrm{gather2}},\cdots,I_{\mathrm{gather}m_{\mathrm{p}}}\}$ 为各纯信息节点承载信息量集合;$\max I_{\mathrm{gather}}$,$\min I_{\mathrm{gather}}$ 分别为集合 $I_{\mathrm{gather}}$ 中最大值和最小值。

$\delta_{\mathrm{u}}=\delta_{\mathrm{uh}}\cup\delta_{\mathrm{up}}=\{\delta_{\mathrm{u1}},\delta_{\mathrm{u2}},\cdots,\delta_{\mathrm{u}m}\}$ 为信息层信息节点业务重要度系数集合。

2.1.3 信息节点重要度计算

文中节点重要度由 3 个表征不同方面但数值相差较大的分项组成,不宜采用加法而宜采用乘法运算。当信息节点业务重要度 $\delta_{\mathrm{u}i}$ 值为 0 时,其实际意义为节点 $i$ 的 $\delta_{\mathrm{u}}$ 值在所有信息节点中最低,此时定义该项将使得节点整体重要度值维持不变。考虑

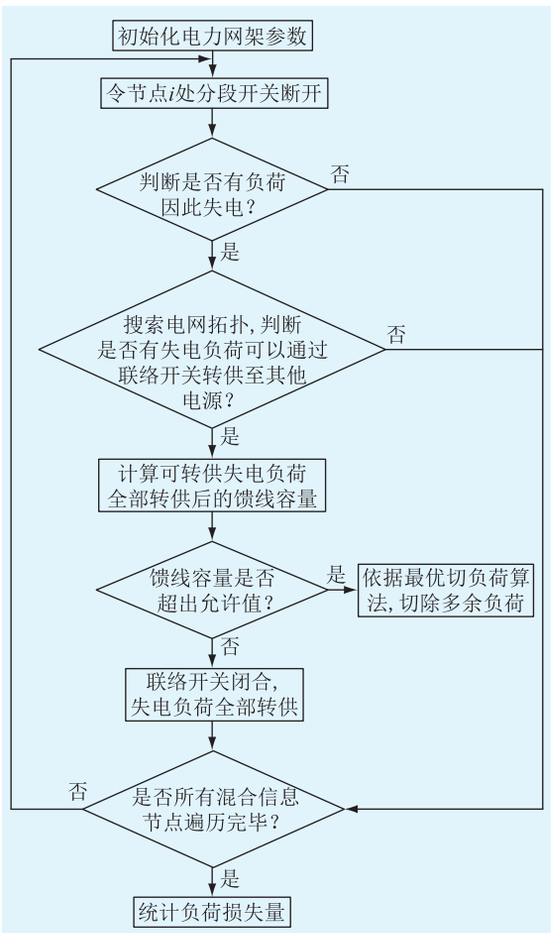


**图 4 混合信息节点业务系数计算流程**

Fig.4 Flow chart for calculating business coefficients of mixed information nodes

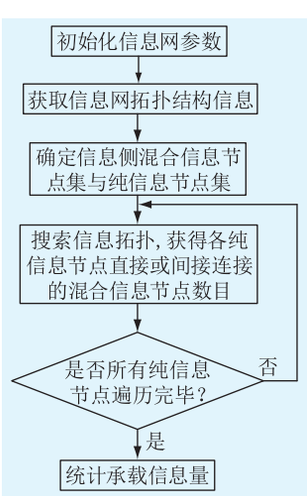


**图 5 纯信息节点业务系数计算流程**

Fig.5 Flow chart for calculating business coefficients of pure information nodes

到文中信息节点重要度值为相对值，更关注不同节点值的相对大小，因此在信息节点重要度计算式中对业务重要度系数做+1 处理既可体现上述分析意义，也不会由于其影响了值的绝对大小而使得结果出现错误。定义信息节点重要度计算如下：

$$I_{di}=(1+\delta_{ui})I_{dti}\delta_{Li}=(1+\delta_{ui})\sum_{j=1}^{m}\frac{m_c(i,j)}{k^2}\delta_{Li} \tag{5}$$

式中：$I_{di}$ 为信息节点 $i$ 重要度；$\delta_{ui}$ 为信息节点 $i$ 的业务重要度系数；$\delta_{Li}$ 为信息节点 $i$ 的信息层级系数，表示节点所在信息层级的相对重要度，层级越高，其值越大。

### 2.2 信息节点被攻击成功概率分析与计算

#### 2.2.1 系统风险评估模型

兰德公司于 2004 年提出了适用于恶意攻击的风险评估模型[25]：

$$R=TVC \tag{6}$$

式中：$T$ 为目标被攻击的概率；$V$ 为若目标被攻击，其被攻击成功的概率；$C$ 为若目标被攻击成功，其带来的损失大小，代表攻击后果；$R$ 为攻击目标最终损失的期望值，代表风险。

式(6)所示的风险值算法同时考虑了目标的脆弱性与重要程度，其评估结果更贴近实际。文中采用该模型评估配电 CPS 的风险大小。

#### 2.2.2 信息节点被攻击成功概率计算

基于上述模型与一定假设，对该风险值算法中的各参数进行量化。在以该模型计算风险值时，文中假设攻击者对所有目标发动随机攻击，即所有攻击目标的 $T$ 值大小相同。同时，一个节点的重要度越高，其被攻击成功后带来的损失越大，即二者成正比关系。因此，将 2.1 节计算出的各信息节点重要度作为式(6)中的 $V$ 值。将对各信息设备的投资情况抽象描述为防御资源，其对信息攻击的抵御能力称为防御效果[26]，攻击者须破坏目标的防御才能攻击成功。实际情况中，防御者的总防御资源数有限，且对目标的防御资源投入越多，其防御效果越好，即被攻击成功概率越低。

采用倒数关系描述防御效果与被攻击成功概率间的联系[25]，并且考虑到文献[25]与[27]中所提出的对于不同安全级别要求的区域存在防御设备种类、数目和固有防御效果上的差异与资源换算系数，引入安全系数的概念：对于安全级别要求越高的区域，其安全系数越大，表示对该区域的资源投入能够起到更强的防护效果。

通过上述分析，建立防御方的数学模型，防御方通过对各可能被攻击的目标分配防御资源，以期将整个系统的总风险降至最低，其数学表达式如式(7)所示。

$$\begin{cases}\min\limits_{\lambda_{di}} R_{st}=\min\limits_{\lambda_{di}}\sum\limits_{i=1}^{m}\left(\dfrac{\delta_{Li}\delta_{ui}}{1+\delta_{di}\lambda_{di}}\sum\limits_{j=1}^{m}\dfrac{m_c(i,j)}{k^2}\right)\\ \text{s.t.}\ \sum\limits_{i=1}^{m}\lambda_{di}=\lambda_D\end{cases} \tag{7}$$

式中：$R_{st}$ 为系统总风险；$\delta_{di}$ 为信息节点 $i$ 的安全系数；$\lambda_{di}$ 为分配给信息节点 $i$ 的防御资源；$\lambda_D$ 为防御资源总数。

通过求解该最优化问题，即可得到信息系统中，分配给各信息节点的防御资源数目，进而求得信息节点 $i$ 被攻击成功的概率值 $P_{si}$，如式(8)所示。

$$P_{si}=\frac{1}{1+\delta_{di}\lambda_{di}} \tag{8}$$

定义信息节点被攻击成功概率矩阵为：

$$\boldsymbol{M}_{as}=\begin{bmatrix}P_{s11} & P_{s12} & \cdots & P_{s1m}\\ P_{s21} & P_{s22} & \cdots & P_{s2m}\\ \vdots & \vdots & & \vdots\\ P_{sm1} & P_{sm2} & \cdots & P_{smm}\end{bmatrix} \tag{9}$$

其中，矩阵元素为：

$$P_{sij}=\begin{cases}0 & i\neq j\\ P_{si} & i=j\end{cases} \tag{10}$$

至此，完成了对配电 CPS 中信息节点重要度与信息节点被攻击成功概率的计算与模型建立。

### 2.3 配电 CPS 信息矩阵描述与量化计算

将信息设备的功能依据“三遥”技术进行划分。将信息设备的遥信与遥测功能定义为信息设备的信息上行功能，将信息设备的遥控功能定义为信息设备的信息下行功能。

定义 $\boldsymbol{V}_c=[v_{c1}\ v_{c2}\ \cdots\ v_{cm}]$ 为信息节点功能状态向量，其值为 0-1 变量，1 为功能状态正常，0 为功能状态故障。需要时可将其扩充为 $1\times 2m$ 维向量 $\boldsymbol{V}_{ce}=[v_{ce1}\ v_{ce2}\ \cdots\ v_{cem}\ v_{ce(m+1)}\ \cdots\ v_{ce(2m)}]$，其中前 $1\times m$ 维表征信息节点的遥控功能状态，后 $1\times m$ 维表征信息节点的遥信遥测功能状态。定义信息上行矩阵 $\boldsymbol{M}_{pc}$ 与信息下行矩阵 $\boldsymbol{M}_{cp}$ 如式(11)所示。

$$\begin{cases}\boldsymbol{M}_{pc}=\begin{bmatrix}s_{u11} & s_{u12} & \cdots & s_{u1m}\\ s_{u21} & s_{u22} & \cdots & s_{u2m}\\ \vdots & \vdots & & \vdots\\ s_{um1} & s_{um2} & \cdots & s_{umm}\end{bmatrix}\\ \boldsymbol{M}_{cp}=\begin{bmatrix}s_{d11} & s_{d12} & \cdots & s_{d1m}\\ s_{d21} & s_{d22} & \cdots & s_{d2m}\\ \vdots & \vdots & & \vdots\\ s_{dm1} & s_{dm2} & \cdots & s_{dmm}\end{bmatrix}\end{cases} \tag{11}$$

各矩阵中元素值如式(12)所示。

$$\begin{cases} s_{uij}= \begin{cases} 0 & 1\leqslant i,j\leqslant m;i\neq j \\ v_{cet} & 1\leqslant i,j\leqslant m;m+1\leqslant t\leqslant 2m;i=j \end{cases} \\ s_{dij}= \begin{cases} 0 & 1\leqslant i,j\leqslant m;i\neq j \\ v_{cet} & 1\leqslant i,j,t\leqslant m;i=j \end{cases} \end{cases} \tag{12}$$

扩充信息节点功能状态向量,其中前 $1\times m$ 维值与后 $1\times m$ 维值分别为信息下行矩阵与信息上行矩阵中对角元素。提出信息节点功能状态向量在一次信息系统内部风险传播中的具体演化步骤如图 6 所示。

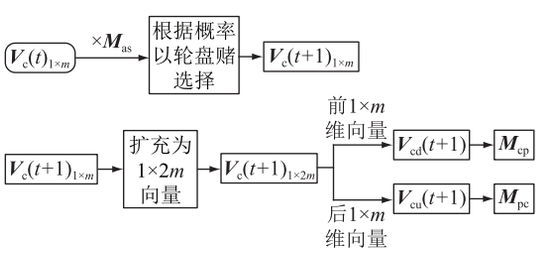


**图 6　信息节点状态转换步骤示意**

Fig.6　Schematic diagram of the transition steps of the information node status

图中,向量 $\boldsymbol{V}_c(t)$ 为 $t$ 时刻向量 $\boldsymbol{V}_c$ 的值;向量 $\boldsymbol{V}_c(t+1)$ 为 $t+1$ 时刻(即下一时刻)向量 $\boldsymbol{V}_c$ 的值;$\boldsymbol{V}_{cd}$ 为信息节点的上行功能状态向量;$\boldsymbol{V}_{cu}$ 为信息节点的下行功能状态向量。根据图 6 中步骤,可由前一时刻的信息节点状态通过各类参数与矩阵运算得到下一时刻信息节点状态,进而形成下一时刻的信息上行与下行矩阵。

至此,上行信息矩阵与下行信息矩阵建立完毕。上行信息矩阵反映了信息节点接收所上传物理节点量测状态信息的能力,下行信息矩阵反映了信息节点向物理节点发送控制指令的能力,体现了配电 CPS 中信息系统与物理系统交互的能力。

当物理系统发生故障,且信息系统发生故障后,根据所提信息节点状态转换步骤计算并判断信息节点状态,形成上行与下行信息矩阵;然后,根据上行信息矩阵,即信息节点上行功能状态,将各物理节点状态上传至控制中心,控制中心根据感知状态判断并处理故障,下发调度控制指令;最后,根据下行信息矩阵,即信息节点下行功能状态,将调度指令下发至各物理节点,物理节点根据传输指令进行动作。至此,结束本轮运算,进行下一轮运算,直至系统故障清除。

## 3　配电信息物理连锁故障演化算例分析

### 3.1　算例介绍

以某配电系统衍生出的算例为对象进行研究。算例物理系统包含 3 个子网,3 个子网通过联络开关相互联系,相互备用。PV2、PV3 为光伏电源,DFIG2、DFIG3 为双馈风机,BAT1、BAT2、BAT3 为电池储能装置,GAS 为燃气轮机,Water 为水轮机。算例信息系统中包含若干交换机、路由器、终端设备与主站服务器。算例物理系统如图 7 所示,信息系统如图 8 所示。

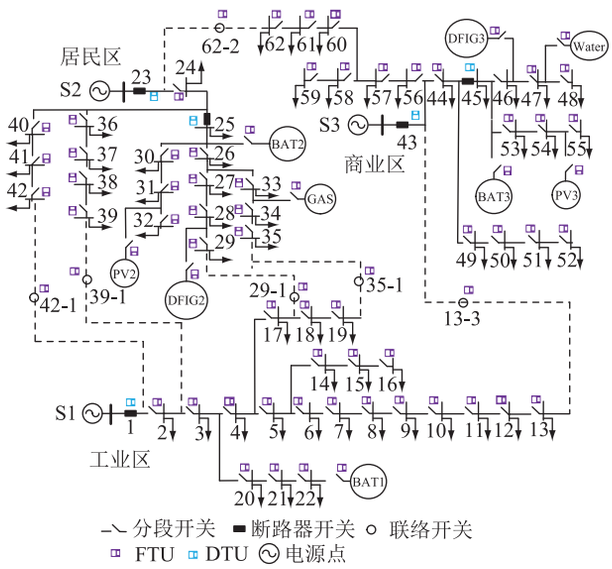


**图 7　算例物理系统**

Fig.7　Physical system of case

信息系统中主站服务器作为控制中心,内嵌集中式馈线自动化算法与最优切负荷算法,可实现对故障线路的自动隔离与负荷转供;各测控终端设备既可对对应物理节点的电压、电流、潮流等数据信息与分段开关等状态信息进行量测并逐级上传至主站服务器,也可接收来自上级的控制指令并控制对应分段开关或断路器作出相应动作。

### 3.2　信息网络攻击分析与概率计算

配电 CPS 中信息与物理系统的深度耦合使得各类信息安全风险可能严重影响到物理系统的安全可靠运行[28]。因此,信息网络攻击、信息设备故障和电力网络扰动与故障之间存在因果逻辑关系,选取典型的故障后果、网络攻击方式与网络攻击类型[29]。所选取的典型故障后果中包含了信息篡改、停止收发与拒绝执行,形成了故障后果的全集;在全网络攻击方式与类型中选择了能够直接导致电力二次设备故障的攻击,体现了网络攻击对信息系统的直接影响。文中假设网络攻击者以各类攻击

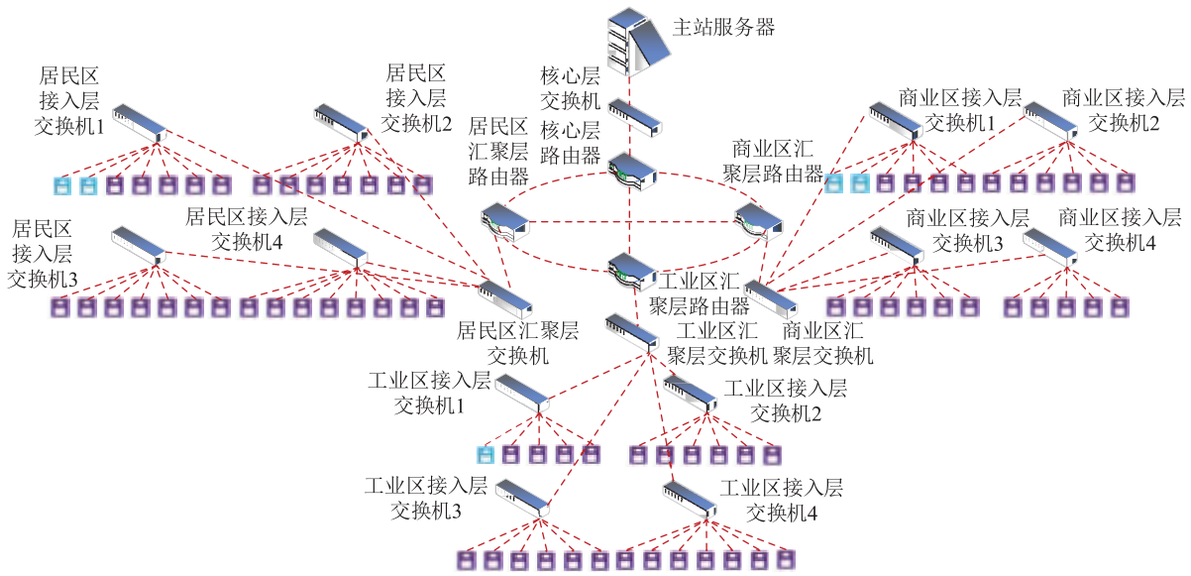


**图 8　算例信息系统**

Fig.8　Information system of case

方式发动攻击的概率相同，并以此计算每类攻击后果出现的概率。

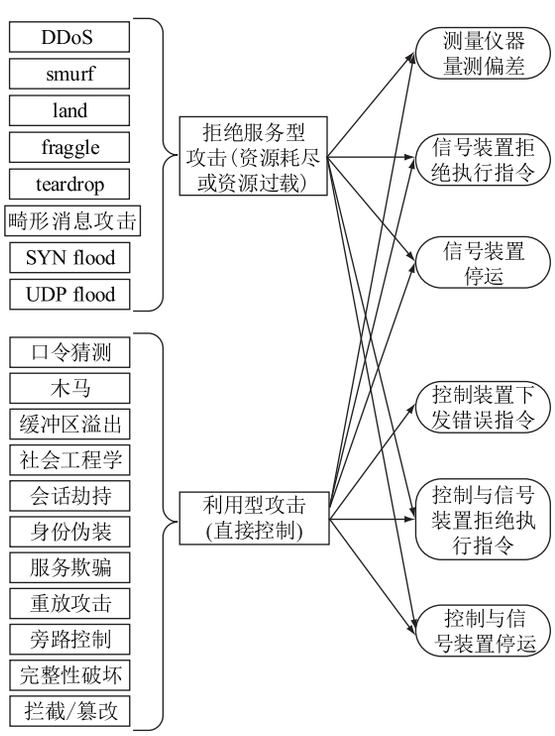


**图 9　典型网络攻击方式和类型及后果**

Fig.9　Typical cyber attack methods, types and consequences

图 9 为典型网络攻击方式和类型及后果。造成每一类典型攻击后果的典型网络攻击发生概率计算方式如式(13)所示。

$$p_r = \sum_{\beta}^{N_\beta} \frac{f_\beta}{N_\mathrm{f}} \frac{1}{\sum_{r=1}^{N_r} r_\beta} \tag{13}$$

式中：$p_r$ 为造成攻击后果 $r$ 的典型网络攻击发生概率；$N_r$ 为网络攻击后果总数；$r$ 为网络攻击后果编号，$r = 1,2,\cdots,N_r$；$N_\beta$ 为网络攻击类型总数；$\beta$ 为网络攻击类型编号，$\beta = 1,2,\cdots,N_\beta$；$N_\mathrm{f}$ 为网络攻击方式总数；$f_\beta$ 为在第 $\beta$ 类网络攻击类型下的网络攻击方式数目；$r_\beta$ 为 0-1 变量，其定义见式(14)。

$$r_\beta = \begin{cases} 1 & r \in \varphi(g_\beta,\beta) \\ 0 & r \notin \varphi(g_\beta,\beta) \end{cases} \tag{14}$$

式中：$\varphi(g_\beta,\beta)$ 为第 $\beta$ 类网络攻击类型可能导致的网络攻击后果的集合。

### 3.3　信息物理连锁故障期望失负荷量计算步骤

由于规程《电力安全事故应急处置和调查处理条例(国务院令第 599 号)》中明确了系统的减供负荷比例是划分电力安全事故等级的标准，且已有多篇高水平文献使用了系统失负荷量来衡量攻击或故障对电力系统的危害程度[16,25—26,30—31]，因此，采用故障后的系统失负荷量作为评估故障对系统的危害程度已是较为普遍的方法。文中同样采用系统失负荷量作为评估信息物理连锁故障对配电 CPS 危害性的标准。

当配电 CPS 发生信息物理连锁故障时，应用之前所提出的信息物理连锁故障机理对其故障过程进行推演，并对其负荷损失情况进行计算与分析。连锁故障其失负荷量计算流程如图 10 所示。

由图 10 可以计算出每次发生信息物理连锁故障后，系统清除故障时的负荷损失量。考虑到信息设备拥有多种信息故障类型且其发生概率各不相同，因此对于某一线路来说，其上可能发生多类信息物理组合故障。要量化该线路上信息物理连锁

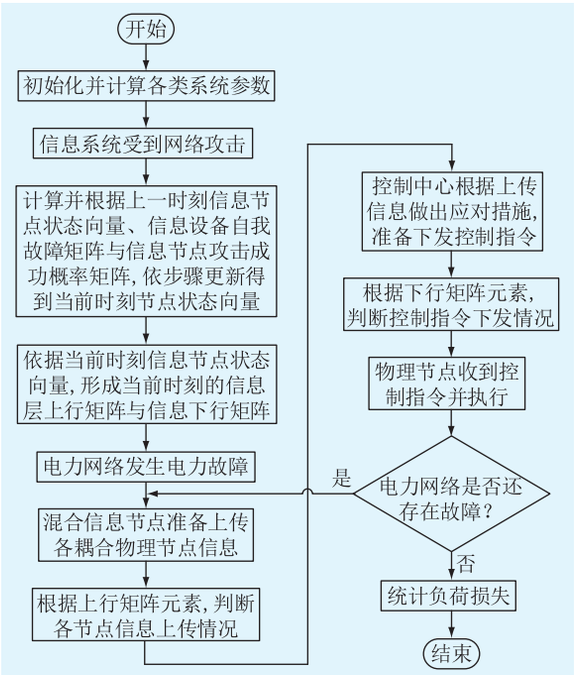


**图 10　发生信息物理连锁故障时失负荷量计算流程**

Fig.10　Flow chart of calculation of loss of load in cyber-physical cascading failures

故障的危害性,不应采用单个信息物理组合故障下的负荷损失量,而应采用能全面反映所有故障组合下故障后果的期望失负荷量。

为简化分析,假设仅故障输电线路两端物理节点对应的信息节点可能发生各类故障。期望失负荷量具体计算步骤如下:首先,依据前述所得各类典型网络攻击发生概率计算可能导致的各类攻击后果出现概率;然后,依据所提机理分别计算各类攻击后果出现致使信息节点发生各类故障时,其与物理侧故障相叠加而导致的失负荷量;最后,先列举该线路两端物理节点其对应的信息节点之间所有可能发生的信息物理连锁故障组合,分别计算组合中各故障出现的概率和其导致失负荷量值的乘积并求总和;再求取该线路仅发生物理单侧故障的概率与故障导致的失负荷量的乘积;将二者相加作为该线路的期望失负荷量。

设第 $i$ 段输电线路其左物理节点对应的信息节点为 $L_i$,相应右信息节点为 $R_i$。则发生信息物理连锁故障情况下其期望失负荷量 $E_{\mathrm{losscp}}(i)$ 计算如式(15)所示。

$$E_{\mathrm{losscp}}(i)=\sum_{r=1}^{N_r}p_r\left(P_{\mathrm{s}L_i}E_{\mathrm{losscpr}L_i}+P_{\mathrm{s}R_i}E_{\mathrm{losscpr}R_i}+P_{\mathrm{s}Li}P_{\mathrm{s}R_i}E_{\mathrm{losscpr}L_iR_i}\right)+\left(1-\sum_{r=1}^{N_r}p_rE_{\mathrm{loss}}(i)\right)\tag{15}$$

式中:$E_{\mathrm{losscpr}L_i}$,$E_{\mathrm{losscpr}R_i}$ 分别为信息节点 $L_i$ 和 $R_i$ 发生第 $r$ 类网络攻击后果后故障线路的期望失负荷量。

### 3.4　算例计算

#### 3.4.1　信息节点重要度计算

依据信息侧拓扑结构,将其抽象为由节点与边构成的图,首先构建信息层邻接矩阵 $\boldsymbol{M}_{\mathrm{c}}$,其中信息层节点数目 $m=88$。依序计算各信息节点拓扑重要度 $I_{\mathrm{dt}i}$、各混合信息节点与纯信息节点业务重要度 $\delta_{\mathrm{uh}i}$ 与 $\delta_{\mathrm{up}_i}$,并设信息层层级系数 $\delta_{\mathrm{L}i}=\{3^0,3^1,3^2\}$,3 个值分别代表信息侧接入层、汇聚层、核心层系数,其大小为相对值,仅起说明作用,并不代表实际数据。计算得到混合信息节点重要度与纯信息节点重要度值如图 11 所示。

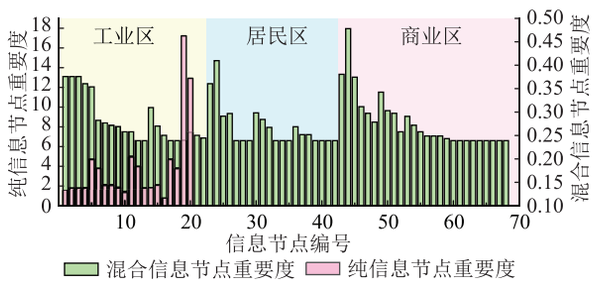


**图 11　信息节点重要度**

Fig.11　Importance of information nodes

由结果可知,纯信息节点重要度远大于混合信息节点重要度。这是因为其在信息层中都是起到汇聚并转发大量信息的作用,若某纯信息节点失效,则与其相关的大片区域的物理节点信息收发都将失效,造成严重后果;相比起来,单个混合信息节点的失效往往仅影响对应物理节点的信息收发。

#### 3.4.2　信息节点被攻击成功概率计算

根据上节计算所得的各信息节点重要度,本节采用 2.2 节所提最优化算法计算各信息节点在遭受信息攻击时被攻击成功的概率 $P_{si}$ 并建立相应矩阵 $\boldsymbol{M}_{\mathrm{as}}$。设防御资源总数 $\lambda_{\mathrm{D}}=1\ 000$ 份。计算结果如图 12 所示。

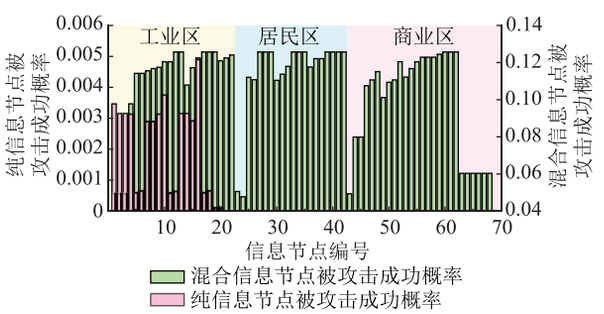


**图 12　信息节点被攻击成功概率**

Fig.12　The probability of an information node being successfully attacked

由结果可知,尽管各纯信息节点重要度较高,

但因为防御者同样倾向于对其进行较高程度的防御资源投入且固有防御效果更好，因此其被攻击成功概率很低。而在混合信息节点中，相对而言各联络开关处物理节点所对应信息节点被攻击成功概率较低。计算所得各混合信息节点被攻击成功概率较高，是因为文中防御资源为抽象概念，其大小并不代表实际数据，同时设定的防御资源总数有限且较少，致使对应节点无法分配到充足防御资源。

3.4.3　信息物理连锁故障危害评估

在算例线路上发生某具体物理故障（以三相短路故障为例），同时线路两端物理节点对应的信息节点发生各类信息故障时，应用之前所提出的信息物理连锁故障演化机理，对算例中所有线路的期望失负荷量进行计算。另外，再计算仅物理侧输电线路发生三相短路故障时系统的期望失负荷量，并将二者进行对比分析。计算结果如图 13 所示。

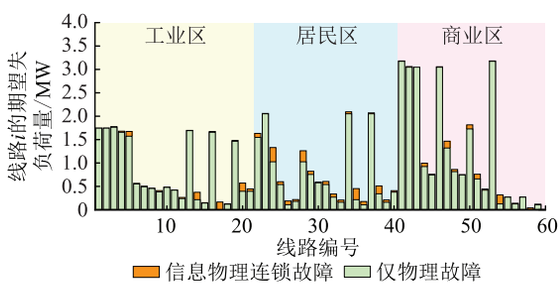


**图 13　线路期望失负荷量**

Fig.13　Expected load loss of the line

由图 13 可知：

（1）发生信息物理连锁故障时，各输电线路发生三相短路故障后的期望失负荷量均高于或等于信息系统不发生故障时的期望失负荷量，最高的期望值约升高了 33.9%，这表明信息物理连锁故障会带来更高的风险与更大的损失。

（2）部分线路发生信息连锁故障与仅发生物理故障下期望失负荷量相同，如线路 57—58。这是因为节点 58 处于无法转供的辐射状输电线上，其发生故障后一定损失；且与节点 57 相连的另外 2 个节点上无负荷，因此发生信息故障时也不会额外损失，使得期望失负荷量不变。但若不仅考虑线路两端对应信息节点发生故障，也考虑其他信息节点故障情况时，其负荷损失区域可能会进一步扩大至其他输电线路处，此时期望失负荷量必然会增大，符合上述结论。

（3）部分线路发生信息连锁故障与仅发生物理故障下期望失负荷量差距较大，如线路 17—18、线路 25—26 等。线路 17—18 由 0 上升至 0.17 MW，对其分析可知，其原期望负荷损失量为 0 是因为当此处仅发生物理故障时，该线路可以完全转供至另一电源处；而当发生信息故障时，其可能出现故障误判、开关误动或不动等情况，导致负荷无法转供或负荷损失区域扩大。

取线路 8—9 段发生三相短路故障，且节点 8 遭受信息攻击，使得该点处发生信息无法上传故障为例，基于事件驱动模型分析其事件交互与状态迁移过程，如图 14 所示。

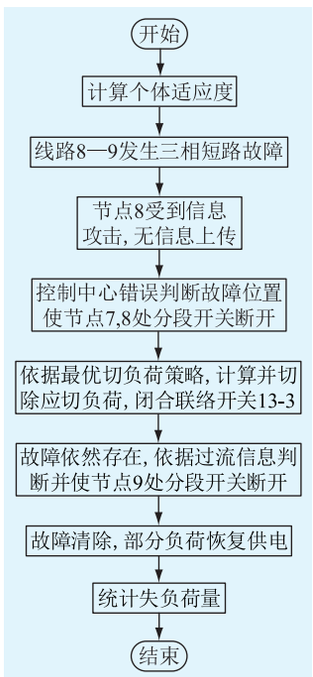


**图 14　线路 8—9 事件交互与状态迁移过程**

Fig.14　Line 8-9 event interaction and state transition process

符号化语言描述如下，其中 CC 为控制中心：

$$\langle \delta_{\mathrm{f}}=1\rangle \mapsto \xi_i:=\mathrm{Failure}\langle a\rangle \oplus \langle t_{\mathrm{g}},\mathrm{Line}_{8-9}\rangle \oplus \langle t_{\mathrm{r}},\mathrm{Line}_{8-9}\rangle$$

$$\downarrow$$

$$\langle |t_{\mathrm{g}}-t_{\mathrm{gref}}|\leqslant \varepsilon\rangle \wedge \langle \delta_{\mathrm{State}}=1\rangle \mapsto \xi_i:=\mathrm{State}\langle p_i,q_i\rangle \oplus \langle t_{\mathrm{g}},N_8\rangle \oplus \langle t_{\mathrm{r}},\mathrm{CC}\rangle$$

$$\downarrow$$

$$\langle \delta_{\mathrm{Control}}=1\rangle \mapsto \xi_i:=\mathrm{Mode\_alter1}\langle \delta_7=0,\delta_8=0\rangle \oplus \langle t_{\mathrm{g}},\mathrm{CC}\rangle \oplus \langle t_{\mathrm{r}},[N_7,N_8]\rangle$$

$$\downarrow$$

$$\langle \delta_{\mathrm{Control}}=1\rangle \mapsto \xi_i:=\mathrm{Control}\langle \delta_{13\text{-}3}=1\rangle \oplus \langle t_{\mathrm{g}},\mathrm{CC}\rangle \oplus \langle t_{\mathrm{r}},N_{13\text{-}3}\rangle$$

$$\downarrow$$

$$\langle \delta_{\mathrm{Control}}=1\rangle \mapsto \xi_i:=\mathrm{Mode\_alter2}\langle \delta_9=0\rangle \oplus \langle t_{\mathrm{g}},\mathrm{CC}\rangle \oplus \langle t_{\mathrm{r}},N_9\rangle$$

由图 14 可知，初始时该配电 CPS 物理侧发生了三相短路故障，且由于信息侧受到网络攻击后发

生信息上传故障,两侧故障相互叠加形成连锁故障使得控制中心误判故障位置而导致物理侧开关的误动,并可能进一步引起物理侧其他装置的错误动作,导致故障区域扩大,造成更大损失。

由文中所提机理可知,发生物理或信息故障时,故障会改变上行或下行信息流内容,进而导致故障状态演化。而物理系统某处发生故障时,若信息系统无故障,则控制中心能够通过所采集的各类信息进行判断并处理。对于其他类型的物理故障,仍然是通过采集节点处的各类信息上传,控制中心通过收集到的信息对故障进行判断处理,并下传控制指令至物理系统进行调度处理,其流程与上述一致。所提方法与机理对其他类型的故障同样适用。

综上可知,发生信息物理连锁故障时系统会承受更大的风险且可能导致更大的损失。文中所提机理能够有效反映发生信息物理连锁故障时的演化过程,并能计算故障发生时的负荷损失,验证了文中方法的有效性。

## 4 结语

目前对配电网中连锁故障演化机理的研究大多仅针对单一系统连锁故障展开,对信息物理连锁故障演化机理的研究还比较初步。在此背景下,文中对配电 CPS 的架构、交互机理与节点各参数等进行了分析,并对配电信息物理连锁故障进行了研究,通过算例进行了仿真。结果显示,发生信息物理连锁故障时配电 CPS 会承受更大的风险,进而可能造成更大的损失。文中方法在故障过程演化与后果分析上具有有效性和合理性。

在后续研究中,将对文中所提连锁故障演化机理中的内容进行精细化与补充,以进一步提高所提机理的准确性与适用性。同时,文中研究内容可对未来配电 CPS 的风险计算进行支撑,为电力 CPS 的进一步发展作出贡献。

**参考文献:**

[1] 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.

[2] 王海,曾飞,杨雄. 基于区块链的配电物联网数据安全防护方法[J]. 电力工程技术,2021,40(5):47-53.
WANG Hai,ZENG Fei,YANG Xiong. Blockchain-based data security protection for distribution Internet of Things[J]. Electric Power Engineering Technology,2021,40(5):47-53.

[3] 魏震波,刘梁豪,高红均,等. 考虑可观测性的电力信息物理系统级联故障分析方法[J]. 供用电,2020,37(4):39-45,51.
WEI Zhenbo,LIU Lianghao,GAO Hongjun,et al. Cascade failure analysis method for power information physical system considering observability[J]. Distribution & Utilization,2020,37(4):39-45,51.

[4] 李龙,李振文,刘颖,等. 基于改进结构熵的电力信息物理系统脆弱性分析[J]. 电力信息与通信技术,2021,19(2):1-6.
LI Long,LI Zhenwen,LIU Ying,et al. Vulnerability analysis of power cyber physical system based on improved structural entropy[J]. Electric Power Information and Communication Technology,2021,19(2):1-6.

[5] 许鹏程,林建森,林缔,等. 改进严重度模型下计及二次系统影响的电网风险评估[J]. 电力工程技术,2021,40(2):212-219.
XU Pengcheng,LIN Jiansen,LIN Di,et al. Grid risk assessment based on the improved severity model considering the influence of secondary system[J]. Electric Power Engineering Technology,2021,40(2):212-219.

[6] 蔡星浦,王琦,黄建业,等. 电力系统网络攻击信息物理双层协同紧急控制方法[J]. 全球能源互联网,2020,3(6):560-568.
CAI Xingpu,WANG Qi,HUANG Jianye,et al. Double-layered cyber-physical cooperative emergency control-strategy-adjustment method to prevent power-system cyber attacks[J]. Journal of Global Energy Interconnection,2020,3(6):560-568.

[7] 常鹏,吴泽群,孙文仲,等. 基于 PMU 优化部署的电网 CPS 线下攻击保护[J]. 智慧电力,2021,49(6):60-66.
CHANG Peng,WU Zequn,SUN Wenzhong,et al. Offline attack protection of power grid CPS based on PMU optimized deployment[J]. Smart Power,2021,49(6):60-66.

[8] 何连杰,亢超群,孙志达,等. 配电物联网边缘物联代理网络安全防护研究[J]. 供用电,2021,38(2):12-18.
HE Lianjie,KANG Chaoqun,SUN Zhida,et al. Research on security protection of edge IoT agent on the power distribution IoT[J]. Distribution & Utilization,2021,38(2):12-18.

[9] 遆宝中,李庚银,王剑晓,等. 计及监测与控制功能的电力信息物理系统关键输电线路辨识方法[J]. 中国电机工程学报,2022,42(7):2556-2566.
TI Baozhong,LI Gengyin,WANG Jianxiao,et al. Identification of critical transmission lines in cyber-physical power system considering monitoring function and control function[J]. Proceedings of the CSEE,2022,42(7):2556-2566.

[10] 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.

[11] 李稳国,邓曙光,李加升,等. 智能电网中信息网与物理电网间连锁故障的防御策略[J]. 高电压技术,2013,39(11):2714-2720.
LI Wenguo,DENG Shuguang,LI Jiasheng,et al. Defense strategy of cascading failures between information network and physical power grid[J]. High Voltage Engineering,2013,39

(11):2714-2720.

[12] 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.

[13] 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.

[14] ROSATO V,ISSACHAROFF L,TIRITICCO F,et al. Modelling interdependent infrastructures using interacting dynamical models[J]. International Journal of Critical Infrastructures,2008,4(1/2):63.

[15] 高昆仑,王宇飞,赵婷. 电网信息物理系统运行中信息-物理交互机理探索[J]. 电网技术,2018,42(10):3101-3109.
GAO Kunlun,WANG Yufei,ZHAO Ting. Exploration of cyber-physical interaction mechanism in power grid cyber-physical systems operation[J]. Power System Technology, 2018, 42(10):3101-3109.

[16] 秦汉,刘东. 配电网信息物理故障的耦合度计算方法[J]. 电力系统自动化,2021,45(3):76-82.
QIN Han,LIU Dong. Calculation method for coupling degree of cyber-physical fault in distribution networks[J]. Automation of Electric Power Systems,2021,45(3):76-82.

[17] 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.

[18] 郭嘉. 考虑连锁故障的电网信息物理系统脆弱性评估方法研究[D]. 杭州:浙江大学,2017.
GUO Jia. Research on cyber-physical power system (CPPS) vulnerability assessment methods considering cascading failures[D]. Hangzhou:Zhejiang University,2017.

[19] 郭经,刘文霞,张建华,等. 孤岛微网信息物理系统可靠性建模与评估[J]. 电网技术,2018,42(5):1441-1450.
GUO Jing,LIU Wenxia,ZHANG Jianhua,et al. Reliability modeling and assessment of islanded cyber physical microgrid system[J]. Power System Technology, 2018, 42(5): 1441-1450.

[20] LAW Y W,ALPCAN T,PALANISWAMI M. Security games for risk minimization in automatic generation control[J]. IEEE Transactions on Power Systems,2015,30(1):223-232.

[21] 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[J]. 电网技术,2021,45(1):235-242.
LIANG Ying,WANG Yaokun,LIU Keyan,et al. CPS fault simulation of distribution network considering network information security[J]. Power System Technology, 2021, 45(1): 235-242.

[22] 王振刚,陈渊睿,曾君,等. 面向完全分布式控制的微电网信息物理系统建模与可靠性评估[J]. 电网技术,2019,43(7):2413-2421.
WANG Zhengang,CHEN Yuanrui,ZENG Jun,et al. Modeling and reliability assessment of completely distributed microgrid cyber physical system[J]. Power System Technology,2019,43(7):2413-2421.

[23] 计丽妍,李存斌,贾雪枫,等. 多证据融合下电力信息物理系统风险评估研究[J]. 智慧电力,2021,49(10):23-29.
JI Liyan,LI Cunbin,JIA Xuefeng,et al. Risk assessment of cyber-physical power system based on multi-evidence fusion[J]. Smart Power,2021,49(10):23-29.

[24] 朱炳铨,郭逸豪,郭创新,等. 信息失效威胁下的电力信息物理系统安全评估与防御研究综述[J]. 电力系统保护与控制,2021,49(1):178-187.
ZHU Bingquan,GUO Yihao,GUO Chuangxin,et al. A survey of the security assessment and security defense of a cyber physical power system under cyber failure threat[J]. Power System Protection and Control,2021,49(1):178-187.

[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] 陈武晖,陈文淦,薛安成. 面向协同信息攻击的物理电力系统安全风险评估与防御资源分配[J]. 电网技术,2019,43(7):2353-2360.
CHEN Wuhui,CHEN Wengan,XUE Ancheng. Security risk assessment and defense resource allocation of power system under synergetic cyber attacks[J]. Power System Technology, 2019,43(7):2353-2360.

[27] KNAPP E D,LANGILL J. Industrial network security:securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems[M]. 2014:402-407.

[28] NEZAMODDINI N,MOUSAVIAN S,EROL-KANTARCI M. A risk optimization model for enhanced power grid resilience against physical attacks[J]. Electric Power Systems Research, 2017,143:329-338.

[29] 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.

[30] 韩宇奇,郭嘉,郭创新,等. 考虑软件失效的信息物理融合电力系统智能变电站安全风险评估[J]. 中国电机工程学

报,2016,36(6):1500-1508.
HAN Yuqi,GUO Jia,GUO Chuangxin,et al. Intelligent substation security risk assessment of cyber physical power systems incorporating software failures[J]. Proceedings of the CSEE,2016,36(6):1500-1508.
[31] 丁伟,唐洁瑶,曹扬,等. 电网信息物理系统网络安全风险分析与防护对策[J]. 电力信息与通信技术,2018,16(9):33-38.
DING Wei,TANG Jieyao,CAO Yang,et al. Network security risk analysis and protection countermeasures of power grid cyber-physical system [J]. Electric Power Information and Communication Technology,2018,16(9):33-38.

作者简介:


黄植

黄植(1996),男,硕士在读,研究方向为配电信息物理系统(E-mail:hz961218@sjtu.edu.cn);

刘东(1968),男,博士,教授,博士生导师,研究方向为智能配电网、信息物理系统;

陈冠宏(1997),男,博士在读,研究方向为电网信息物理系统。

## The evolution mechanism of the cyber-physical cascading failure of power distribution system based on event-driven

HUANG Zhi, LIU Dong, CHEN Guanhong, WENG Jiaming, YIN Haoyang, WANG Zhen
(Key Laboratory of Control of Power Transmission and Conversion,Ministry of Education
(Shanghai Jiao Tong University),Shanghai 200240,China)

**Abstract**:With the rapid development of communication and control technology in power distribution system,it has gradually shown the typical characteristics of cyber-physical systems,which not only brings new opportunities for development,but also brings multiple types of risks in the information system to the power system. As a result,cyber-physical cascading failures in the power system have occurred frequently,leading to serious accidents. Therefore,analyzing and studying the evolution process and failure consequences of cyber-physical cascading failures and exploring the internal mechanism of cyber-physical cascading failures have important theoretical and practical significance. Based on the event-driven model,an architecture of power distribution cyber-physical system is proposed to analyze the interaction mechanism between physical and information systems,and a research framework for the evolution mechanism of cyber-physical cascading failures is proposed. Then,the importance of the internal nodes of the information system is studied,the total risk value of the system and the defense resources are comprehensively considered,and the relevant parameters such as the probabilities of the information nodes being successfully attacked are calculated and the correlation matrices are established. Finally,a simulation of the evolution mechanism of cyber-physical cascading failures is carried out on a case,which verifies the rationality of the proposed mechanism and its validity in the deduction of the failure process and the calculation of the consequences.

**Keywords**:event-driven;power distribution cyber-physical system;cyber-physical system architecture;interaction mechanism;cyber-physical cascading failure;cascading failure evolution mechanism

(编辑 方晶)