第 54 卷 第 3 期
2021 年 3 月

中国电力
ELECTRIC POWER

Vol. 54, No. 3
Mar. 2021

馈线功率控制下的主动配电网信息物理风险演化分析

翁嘉明，刘东，安宇，殷浩洋，黄植，秦汉

(上海交通大学 电力传输与功率变换控制教育部重点实验室，上海　200240)

摘　要：在主动配电网信息物理系统中，信息系统与物理网架之间存在强耦合关系。在电网复杂的信息物理交互作用下，信息系统的异常或故障会直接影响并降低电力系统的运行水平，甚至引发严重的连锁故障。且相对于传统电力系统，电网信息物理系统的风险致因因素更多，交互机理更复杂，监测识别更困难。电网信息物理系统的安全风险问题已成为当前亟待解决的基础问题之一。以主动配电网为研究对象，对信息侧架构与信息物理交互机理进行分析，建立了信息攻击下的风险传递模型，揭示了故障在配电网信息物理系统中的演化机理。最后，在 DIgSILENT 中搭建仿真算例进行实例分析，验证了所提出模型的正确性，并对未来配电网如何抵御信息侧风险，加强安全风险防护水平提出了建议。

关键词：主动配电网；信息物理系统；馈线功率控制；风险演化；信息攻击

DOI：10.11930/j.issn.1004-9649.202009100

0　引言

信息物理系统（CPS）是实现计算、通信以及控制技术深度融合的系统，硬件上融合物理设备、计算平台、网络结构；功能上由计算机和网络通过反馈回路监视并控制物理过程；在反馈回路中物理过程与计算相互影响[1]。随着信息技术的深度应用，电网已成为典型的信息物理系统，而现有分析控制方法主要关注信息空间或物理系统本身，难以揭示二者交互影响所诱发的叠加风险，未能挖掘二者融合作用带来的能力提升。

电力系统运行涉及复杂的电气物理过程，包含大量实时数据的产生与传递，无论是单一设备元件、设备组，还是全系统范围，其单独控制工作或是系统联动，都需要准确的物理模型和信息模型实现协调控制。文献 [2-3] 针对包含电源、负荷、输电系统的完整电网按照功能化、模块化和统一建模思想，建立了信息物理模型，分析并设计信息传递的过程，运用建立的模型论证了分层分区控制以及统一控制的可行性，并判断系统的稳定性。文献 [4] 基于混合系统理论，构建了一种分析和设计电力系统动态行为的方法，用于判断系统的稳定性，保障电网安全。安全是电网可靠稳定运行的首要前提。对于信息物理系统的电网而言，安全性与风险性问题的范畴已远远超过传统的系统暂态稳定和供电安全层面[5]。由于信息物理过程的深度交织耦合，信息空间的通信、计算、时序配合、动态逻辑以及运算性能，和信息空间面临的病毒、恶意代码、攻击破坏、窃密篡权等严重问题，共同作用于电网物理系统而产生客观存在、不可忽视的直接影响，进而和物理系统的连续过程叠加发展、连锁传导，会造成难以想象的严重后果[6]。

因此，电网信息物理系统的安全风险问题更为复杂且求解难度更大，因而也在这一背景下凸显出计及信息空间与物理网络因素叠加交互影响的电网安全风险评估方法的重要价值和意义。当前已有较多成果研究电网信息系统安全对物理系统安全性的影响，以及如何加强电网信息安全、提高其应对风险威胁和恶意攻击的防御水平[7-10]。文献 [11] 全面总结论述了电力二次系统的风险因素来源，讨论了风险因素的作用形式和对一次系统的影响。文献 [12] 建立了一种双元素相对模糊

收稿日期：2020-09-15；**修回日期：**2021-01-14。

基金项目：国家重点研发计划资助项目 (2017YFB0903000)；国网江苏省电力有限公司科技项目 (适应高可靠性配电网的分布式馈线自动化协同运维及控制技术研究与应用，J2019061)。

评估方法以及一套风险评估框架体系用以提高电力系统应对信息空间安全攻击的坚强性。文献 [13-15] 对于变电站通信安全问题，考虑了软件失效造成的定量安全风险评估，建立了入侵检测防御系统的模型并对其进行安全性评估，开发了试验环境用于研究观察信息系统和电网物理系统之间的交互对电网性能和可靠性的影响。此外，文献 [16-18] 对电网信息物理系统的关键信息网络节点和重要环节的脆弱性进行了研究，如通信系统的故障对电网非正常运行造成的影响，威胁入侵和电网自身防御相互对抗即攻防博弈下的脆弱性等。文献 [19] 阐述了电力 CPS 安全风险跨空间传播的基本形式，根据细胞自动机理论的特征建立了信息物理安全风险的传播模型，通过仿真计算分析了风险跨空间传递概率、故障细胞治愈概率等因素对风险传播的影响。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信息物理系统电力系统连锁故障模型，综合考虑物理层电网潮流、在脆弱度指标中的拓扑完整度、信息层延时增量进行连锁故障仿真研究。文献 [21-25] 均针对信息空间的网络攻击带来的电网风险进行了研究。

基于上述需求，本文分析配电网信息侧架构与信息物理交互机理，建立信息攻击下的配电网信息物理系统风险传递模型，揭示了故障在配电网信息物理系统中的演化机理，并以配电网量测信息被篡改的场景为例，模拟仿真验证所提模型的可行性。

1 主动配电网信息物理交互机理

1.1 主动配电网系统信息侧架构

在讨论主动配电网信息物理融合风险的交互机理之前，要明确主动配电网系统信息侧的组织架构。主动配电网系统信息侧各组织层的功能、链路及信息流关系如图 1 所示。数据采集系统采集配电网各节点的实时运行数据，如母线的电压、有功等量测量及断路器的开关状态量等，为主站控制系统各高级应用的计算与评估提供数据基础。通信系统一方面负责将本地采集的量测量和状态量传送至主站控制系统，另一方面提供通信链路为主站控制系统下发各种控制信号命令。此外，各控制中心和控制器之间的协同配合控制也需要基于通信系统完成。主站控制系统负责处理来自测量设备的数据，并评估电力系统状态。状态估计作为主站系统中最为重要的监视工具，基于实时测量，伪测量和网络拓扑，提供可靠、完整的电力网络状态。主站中的各种应用分析工具基于状态估计的输出来检测潜在的越限情况，提醒操作员采取预防或者校正措施。人机交互界面是操作员了解并收集有关系统状态信息的主要手段，显示各高级应用的分析计算结果，在检测到异常事件时生成警报，并为操作员访问系统所有信息提供便利。

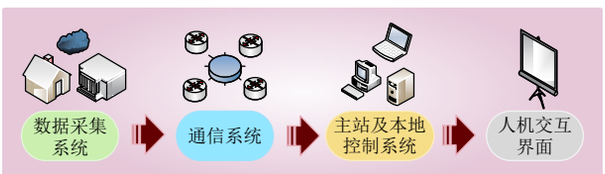

图 1 主动配电网信息侧组织架构

Fig. 1 Cyber-side infrastructure of active distribution network

操作员在对电力系统当前状态进行评估时，是基于人机交互界面所显示的数据结果进行分析的，而显示的电力系统的实时运行状态则通过各种高级应用程序计算得到。但是，此“状态”并不代表电力系统的“实际状态”，而是电网信息系统基于采集、传输、计算、分析后提供的“感知状态”。“实际状态”是指电力系统所有组件在给定时刻下的状态。为获得系统的“实际状态”，需要完善而准确的信息系统。所谓“感知状态”是指电力系统各种应用分析工具基于当前信息系统所提供的数据所描述的系统状态。从某种意义上说，信息物理系统充当了电力系统“实际状态”和“感知状态”之间的过滤器。

1.2 配电网故障信息物理交互机理

如图 2 所示，信息基础架构中的局限性、设计缺陷或故障会导致系统的“感知状态”与“实际状态”之间出现差异。例如：主站系统从各配电终端接收不完整、不正确甚至矛盾的信息；采集的信息遭到攻击和篡改，误导或迷惑了主站系统的判断；当前系统状态变化过快或当前感知状态比较少见等。在这些情况下，“感知状态”可能与“实际状态”有较大差异。一方面，物理系

统的“实际状态”经信息系统“过滤”后，变成“感知状态”，作为主站控制系统控制决策依据。若“感知状态”与“实际状态”有较大偏差，则主站控制系统有可能下发错误的控制指令，导致物理系统故障。另一方面，当发生电力系统故障时，控制中心需要收集大量数据，包括节点电压、传输线上的功率流、分布式电源和柔性负载状态等，通信网络的性能将受到通信流量激增的影响，从而发生数据包丢失、传输速率降低、传输延迟增加等现象，最终造成信息系统故障。由此可见，主动配电网信息系统与物理系统紧密融合，相辅相成，物理系统或信息系统中任何一环故障，都会对配电网的稳定运行造成影响，甚至导致连锁故障的发生。

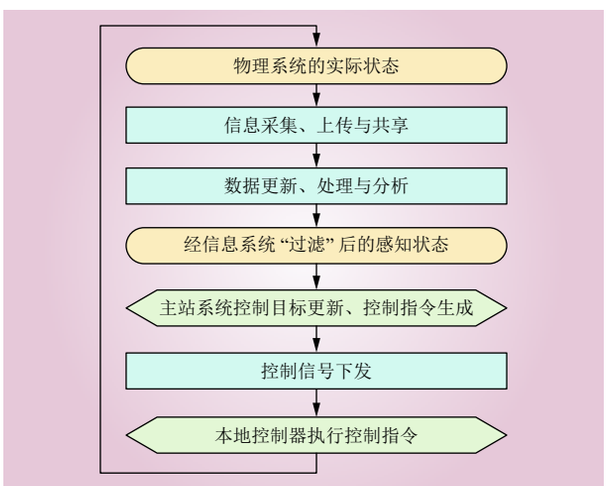

图 2　电网信息物理故障演化
Fig. 2　Failure evolution of active distribution network cyber-physical system

2　信息攻击下的电力系统

配电网 CPS 系统中信息空间元件与电力系统元件紧密融合、协同工作，使得原本孤立于两个空间的各类安全风险（如信息攻击、系统及硬件可靠性缺陷、电力二次设备故障和电力系统扰动等）有可能跨越原有的空间界限，并将其危害传播到另一空间中，从而形成跨空间故障。

跨空间故障的一种典型过程为：因遭受网络攻击导致信息空间元件工作异常，可能导致与之连接的电力二次设备出现异常（或以隐性故障形态存在），比如网络攻击会引发配电终端量测数据篡改、通信中断、通信延迟等故障。进而电力二次设备异常工作后将有可能诱使电力一次设备出现非正常操作或者处于异常工况，从而使信息风险的破坏作用从信息空间向电力系统投影。

形成故障的原因可分为两大类：一类为客观可靠性因素，即信息系统自身设备老化、低效或外界环境影响导致的数据丢失、通信延迟及终端设备不可控等；另一类为主观因素，即精心设计的信息攻击行为，通过破坏、削弱电网二次系统的部分功能或通过篡改数据内容以误导控制决策生成，从而达到影响整个电网稳定运行的目的。

如图 3 所示，网络攻击、系统或硬件可靠性故障、电力二次设备故障和暂态稳定节点扰动之间存在明显的因果逻辑关系，正是由于信息空间与电力系统的紧密耦合，它们在电力 CPS 中顺序爆发形成了配电网 CPS 跨空间故障。

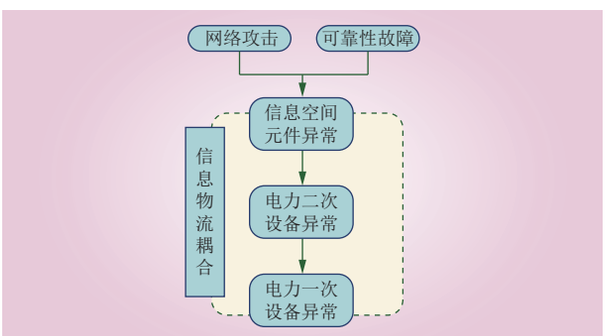

图 3　跨空间级联故障形成过程
Fig. 3　Formation process of cross-space cascading failure

电力二次设备作为电力 CPS 信息空间与物理空间的联动接口，实现了离散信息流与连续能量流之间的交互。但是信息空间与物理空间的紧密耦合也使得信息空间的安全风险可以通过电力二次设备扩散到电力物理系统中，诱发跨空间级联故障。

在电力 CPS 中常见的网络攻击[24]中，不是所有的信息风险均可引发电力系统故障，比如电力企业的内外网采用安全隔离，虚假消息攻击难以直接引发电力二次设备故障。同理，不是所有的电力系统故障均是由信息风险造成的。

所有客观因素造成的信息侧风险均可以由主观的信息攻击模拟完成，比如信息元件由于可靠性出现故障而导致其无法正常工作的情形，可由 DoS 攻击进行模拟，两者对二次设备的危害性相

同。因此，为了分析信息侧风险对物理侧系统的传递作用，有必要从信息攻击者的角度定义主动配电网信息侧风险模型。

电网控制系统主要采用分层分布的控制方式。如图 4 所示，主站系统基于当前电网各节点提供的实时运行信息，对整个电网进行监视、调控和优化，并为各区域控制器和本地控制器提供控制目标。区域控制器、本地控制器及终端量测相互配合，一方面跟踪主站下发的控制指令；另一方面在特殊情况下对现场的可控设备（如可控 DG、柔性负荷等）进行本地控制。智能电子设备、控制单元以及通信链路的大量增加，给电网控制系统带来了更多的信息安全漏洞。

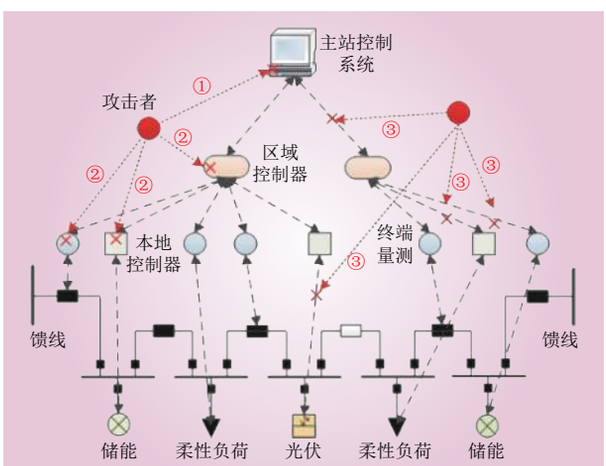

图 4 电网信息侧风险来源

Fig. 4 Cyber risk sources of active distribution networks

由信息攻击引发的跨空间连锁故障与传统电力系统故障的显著区别在于，其故障源头在信息空间并按照攻击者的意图在电网 CPS 中发展演化，且其危害影响涉及信息空间与电网物理系统。因此剖析跨空间连锁故障的爆发全过程，需要充分考虑攻击者因素并从信息空间发掘故障根源。针对电网 CPS 的信息攻击方式包括 3 种：（1）窃取控制中心的控制权限；（2）篡改控制参数或整定值；（3）通信延迟、数据篡改、数据丢失以及拒绝服务等。

第 1 种信息攻击的目标一般为主站监控系统，若主站系统的控制权限丢失，则会造成调度功能失效以及产生恶意操控指令。因此主站系统控制权限的丢失会给整个配电网信息物理系统带来极大风险。另外，针对主站监控系统部署的信息安全保护资源也使得信息攻击成本高，成功率低。

第 2 种攻击方式涉及 DG 的控制参数。定参数是指如控制 DG 动态行为的比例-积分-微分（proportion integration differentiation，PID）参数，这类参数一般厂家设定的固定值，攻击难度较大。可控参数包括 DG 的有功、无功功率设定值和馈线终端单元（feeder terminal unit, FTU）过流保护定值等，存在被信息攻击的风险。相比入侵主站系统，对于控制器参数的攻击难度较低，但可选择的攻击路径仍然较少，大多数攻击者一般选择对通信内容中的可控参数进行攻击。

第 3 种信息攻击均可以通过攻击通信系统或终端量测设备实现。主动配电网中信息交互复杂且安全环境较低，因此针对通信系统和终端量测系统的信息攻击更易实施。信息攻击者除了通过注入虚假测量数据误导主站控制决策以外，还可以通过发送大量伪造的数据包到目标服务器或网络，占用通信带宽、消耗缓存资源，以造成通信系统中断或终端设备拒绝服务等。

3 主动配电网信息物理故障演化机理

由于大量可控式 DG 和柔性负荷的存在，电网信息物理系统与传统电力系统相比，自动控制属性更高，电力元件与信息元件之间的融合更紧密，交互作用更强，信息空间风险也更容易传递到物理网络中。在大量通信设备和智能终端的紧密组织下，一方面，信息侧的控制决策系统基于实时量测数据，计算分析得到当前电网的“感知状态”，并向电网物理侧各可控设备下发控制指令或更新控制目标；另一方面，物理侧的各可控设备执行收到的控制指令，改变电网潮流甚至拓扑，使电网“实际状态”发生变化，并由数据采集装置反馈至控制决策系统。由此可见，主动配电网信息侧的控制决策系统与物理侧的各可控设备之间形成了控制闭环，而信息物理风险依此传递。

电网信息风险传递过程由电力系统连续动态过程、通信过程和信息系统控制决策过程组成，如图 5 所示。电力系统的连续动态过程包括同步机转子运动方程，逆变器、调速器的自动控制过程以及间歇式能源、负荷的波动变化等。信息系

统控制决策过程主要包括主站控制系统及其配套的区域控制器、本地控制器、各种传感量测设备以及智能终端之间的协同配合等。

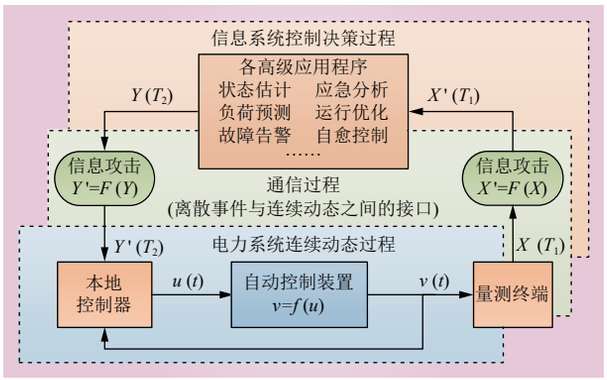

图 5　电网信息物理故障传递过程

Fig. 5　Failure transfer process of active distribution network cyber-physical system

通信过程作为 2 个异构系统之间的接口，包括各种实时数据的上传、共享以及控制指令的下发。其中，$v=f(u)$表示可控设备的自动控制过程；$u(t)$和$v(t)$分别为控制器的输入、输出量；$X'=F(X)$和$Y'=F(Y)$表示信息攻击者建立的信息攻击模型；$X(T_1)$和$Y(T_2)$分别为信息系统在T_1时刻采集的实际运行数据和在T_2时刻下发的实际控制目标；$X'(T_1)$和$Y'(T_2)$分别为修饰后的采集数据和控制目标。实时量测数据$X(T_1)$可以是当前物理系统各节点的电压、有功（无功）功率、系统频率等量测量，也可以是各断路器、开关或可控 DG 运行模式等状态量。控制目标$Y(T_2)$一般为本地各可控设备的控制参数，如 DG 的有功（无功）功率设定值、电压参考点、控制模式等，或各断路器、开关的分合闸控制指令等。信息系统的控制决策过程基于当前量测终端采集得到的实时量测数据，通过调用主站内的各种高级程序对电网当前运行状态进行监视和分析，并实时更新本地控制器的控制目标；在紧急情况下（如频率失稳或电压、电流越限等）本地控制器也会就地实施故障保护。

在通信系统的支持下，电网的离散信息处理系统和连续物理动态系统形成了控制闭环。电力系统的连续动态过程可以依次通过传感量测设备采集、数据上送、主站计算分析的方式得到。同时，电力系统运行方式的改变也可以通过主站决策系统下发控制目标，改变本地控制器的控制输入或控制参数而实现。因此，在信息物理风险的交互传递中，对本地的传感量测终端进行损害或对通信链路内的数据信息进行篡改，同样可以起到破坏电力系统安全运行的作用。精心设计的信息攻击可以通过修饰某些原始数据信息，使主站控制系统计算得到错误的电网“感知状态”，下发错误的控制指令，导致系统偏离正常运行状态，甚至造成电网的连锁故障。针对状态量的信息攻击，一般是将当前的实际状态量取反，或屏蔽主站对某些状态量的观测。针对量测量的信息攻击，则根据当前控制系统的算法，对某些关键节点的量测进行篡改，以误导监控系统对当前系统状态的评估。

对量测量篡改的一般形式可表示为

$$X'(T)=X(T)+B(T) \tag{1}$$

式中：$X(T_1)$和$X'(T)$分别为在T时刻的实际量测值和被篡改后的量测值；$B(T)$为信息攻击者设置的量测数据偏移量。

4　馈线功率控制下的主动配电网信息物理风险演化分析

基于所提出的主动配电网信息物理风险传递模型，以针对主动配电网馈线功率控制的信息攻击为例，分析信息物理风险的传递演化过程及其产生的影响。

4.1　主动配电网馈线功率控制原理

在主动配电网中，大量 DG 和柔性负荷的接入，一方面有助于降低输电损耗，另一方面也为配电网增加了更灵活的运行方式，如微网自治或紧急情况下的孤岛运行等。配电网一般通过升压变压器接入输电网。由于潮流的双向性，主动配电网对于输电网相当于一座虚拟电厂，既能作为一个负荷，也可以作为一个聚合的电源，为上级电网输送有功功率。因此，配电网和上级电网之间的交换功率一般被要求在一定范围内。由于 DG 的容量较小，一般情况下同一片区域或同一条馈线上会聚集大量的 DG，以积累更高的可控容量。分布式电源这种“既分散又集中”和“即插即用”的特点，需要较高的通信带宽和灵活的

通信链路，并不适用于传统的集中式实时控制。因此，在主动配电网中，一般会在存在大量DG的馈线或区域设置一个区域控制器，通过与量测终端、各DG控制器之间通信，实现对该区域的实时自治控制，如图6所示[26]。

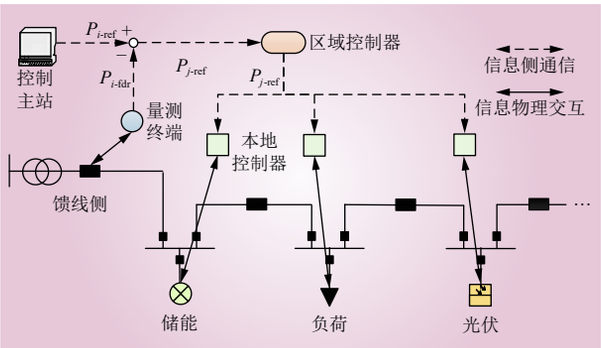

图 6 主动配电网区域自治控制

Fig. 6 Regional autonomous control in active distribution networks

在图6中，$P_{i-\mathrm{ref}}$表示馈线i的参考交换功率（发出功率为正，吸收功率为负），$P_{i-\mathrm{fdr}}$表示馈线i的当前实际交换功率值，$P_{j-\mathrm{ref}}$表示分布式电源j的有功功率参考值。由于配网内DG一般采用恒功率控制（即PQ控制），区域控制器可以基于当前馈线交互功率及其参考功率，通过调整区域内可控DG的有功功率参考值，使馈线交换功率趋于给定的馈线交换功率参考值。

4.2 针对馈线功率控制的信息攻击模型

区域自治控制是一个典型的信息物理控制过程。区域控制器、本地控制器、量测终端和通信系统构成了信息物理系统的信息层，DG、负荷以及馈线构成了信息物理系统的物理层。物理层的动态连续潮流以离散的量测数据形式上传至信息层，信息层的区域控制器再经过控制算法的计算迭代，为本地控制器更新控制目标，从而使物理层的配电网系统趋于目标运行状态。

然而，相较于主站的集中式控制，区域自制控制具有较低的信息安全等级，且自动控制响应更快，因此有更高的信息物理交互风险。若区域控制器无法获得实时更新DG状态或收到有误的量测数据，这将有可能导致DG有功功率贡献率的计算出现偏差，使DG偏离目标运行状态，甚至造成配电网系统的不稳定，触发相应的紧急控制或故障保护等举措。

针对终端量测的信息攻击可表示为

$$P'_{i-\mathrm{fdr}}(T_k)=P_{i-\mathrm{fdr}}(T_k)+B(T_k) \tag{2}$$

式中：$P'_{i-\mathrm{fdr}}(T_k)$为T_k时刻遭篡改后的馈线交换功率量测值；$P_{i-\mathrm{fdr}}(T_k)$为T_k时刻实际的馈线交换功率值；$B(T_k)$为信息攻击者在T_k时刻设置的数据偏移值。

信息攻击者的目的是通过篡改馈线交换功率量测值，误导区域控制器对各DG的调节，最终使实际馈线交互功率偏离其目标值。

这种信息攻击为配电网系统带来的后果，轻则影响上级电网对电价分配的公平性，重则影响整个配电网甚至上级电网的安全稳定。尤其在馈线可调节容量较低的情况下，DG的异常运行有可能导致馈线过载，造成频率下降，触发低频减载保护。当系统频率低于最低频率限值，且频率变化率达到启动门槛值时，区域控制器将依据式（3）切除部分负荷来弥补当前系统的功率缺额。

$$\Delta P_{\mathrm{load}}=\frac{2H}{f_0}\cdot\frac{f(T)-f(T+\Delta T)}{\Delta T} \tag{3}$$

当且仅当

$$\frac{f(T)-f(T+\Delta T)}{\Delta T}>\omega \tag{4}$$

$$f(T)<f_{\min} \tag{5}$$

式中：ΔP_{load}为需要切除的负荷功率值；$f(T)$和$f(T+\Delta T)$分别为T时刻和$T+\Delta T$时刻的系统频率采样值；ΔT为系统的采样间隔；f_0为系统额定频率，$H>0$为系统转动惯量；$\omega>0$为频率变化率门槛值；$f_{\min}$为系统最低频率限值。本文中，ω=0.08 Hz/s，$f_{\min}$=49.5 Hz。

4.3 基于馈线功率控制的信息物理风险演化

基于主动配电网信息物理风险传递模型，仿真分析在主动配电网区域自治控制下，馈线出口处量测遭篡改对系统造成的动态影响。在DIgSILENT（也称PowerFactory）仿真软件中搭建主动配电网馈线结构及其相应的控制模型，如图7所示。信息侧模型包括量测采集、信息攻击模型、区域控制器和DG控制器等。其中，量测采集模块分别在馈线出口处和DG处采集实时量测信息；信息攻击模块连接了馈线出口处量测终端和区域控制器，以实现对上传量测数据的篡改；区域控制器包括保护控制和调度控制模块，前者负责低频减载，后者则实现DG有功功率参考值

的计算与下发；DG 控制器根据区域控制器下发的控制目标更新逆变器输入变量或控制参数。物理侧的动态元件包括同步机动态模型和基于 PQ 控制的逆变器动态控制模型，前者为配电网提供频率和电压支撑，后者则作为 DG 控制器的执行器，实现 DG 的恒功率控制。物理侧模型的其他参数包括：馈线交流侧电压等级为 10 kV；DG 的直流侧电压等级为 0.35 kV；光伏（photovoltaic，PV）容量为 90 kW，电池储能（battery energy storage，BES）最大充放电功率为±100 kW（放电为正，充电为负）；馈线可承受的最大负载（即同步发电机最大容量）为 450 kW。

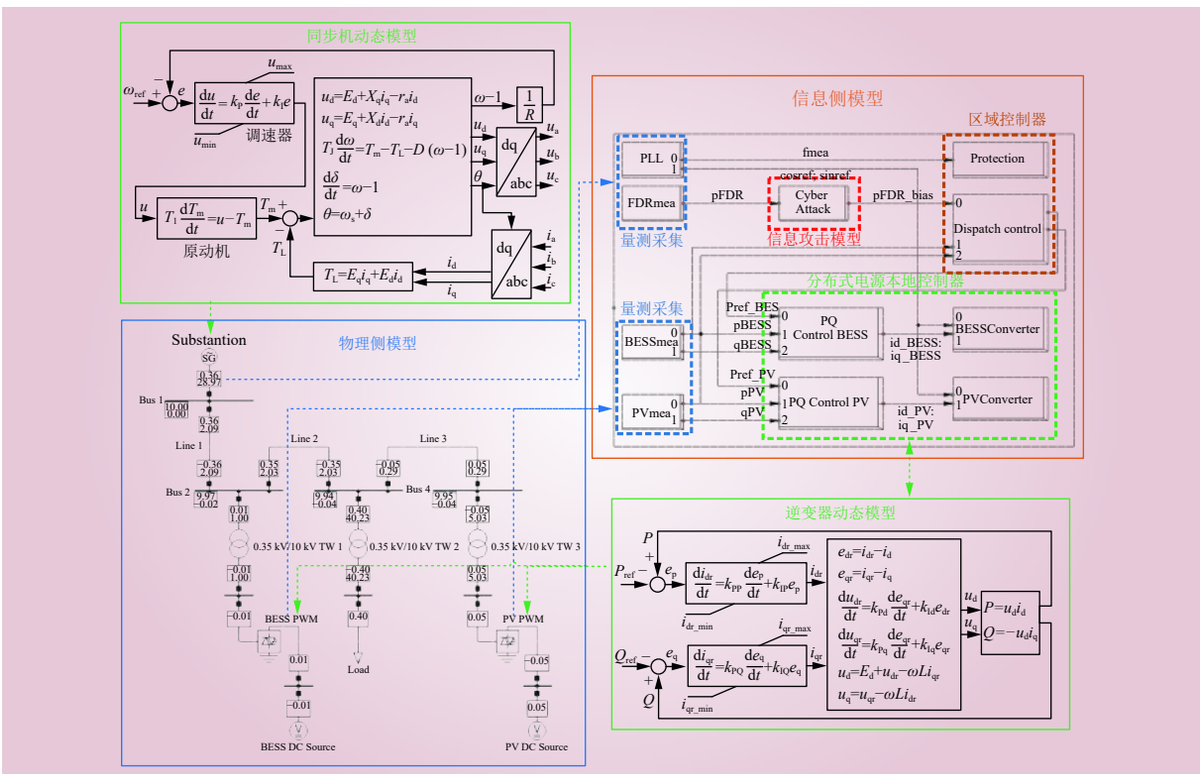

图 7　基于 DIgSILENT 的信息物理风险传递仿真模型

Fig. 7　DIgSILENT-based cyber-physical risk transfer simulation model

初始状态下，储能以 10 kW 充电，光伏以最大功率跟踪控制有功出力为 50 kW，当前馈线交换功率为 360 kW（向馈线侧注入功率），馈线交换功率参考值为 350 kW，控制死区δ设置为 10 kW。仿真中考虑 1 min 内连续 2 次的信息攻击：第 1 次信息攻击发生在 10 s 时刻，将馈线出口处的有功功率量测值增加 50 kW；第 2 次信息攻击发生在 30 s 时刻，将馈线出口处的有功功率量测值减少 100 kW。由于仿真时间为 60 s，在仿真过程中不考虑光伏和负荷受外界环境变化而发生的功率突变。仿真结果如图 8 所示。

第 1 次信息攻击后，区域控制器认为当前馈线交换功率已偏离了目标值，于是对储能和光伏的有功功率参考值进行重新分配，逐步迭代更新（增加）各分布式电源的有功功率贡献率。由于光伏已经处于最大功率跟踪状态，无法继续增加有功功率的输出，只有储能从原来的充电模式转为放电模式，并逐渐增加放电功率，直至区域控制器收到的馈线交换功率量测值回到目标区间（350±10 kW）内，如图 8 所示。第 1 次信息攻击虽然没有造成大的频率波动，但它使馈线的交换功率偏离了目标值 50 kW，且使原本处于充电模式的储能被调整至放电模式，这会对配电网的经济运行以及灵活容量储备造成不良影响。

第 2 次信息攻击发生后，在区域自治控制下，储能的发电功率首先被调整下降，这是因为当前光伏的有功功率贡献率（$\alpha = 50.0\%$）低于当前储能的有功功率贡献率（$\alpha = 72.5\%$）。当储能由放电模式转到充电模式后（$\alpha < 50\%$），光伏的有功功率开始同步下降。随着储能充电功率的增

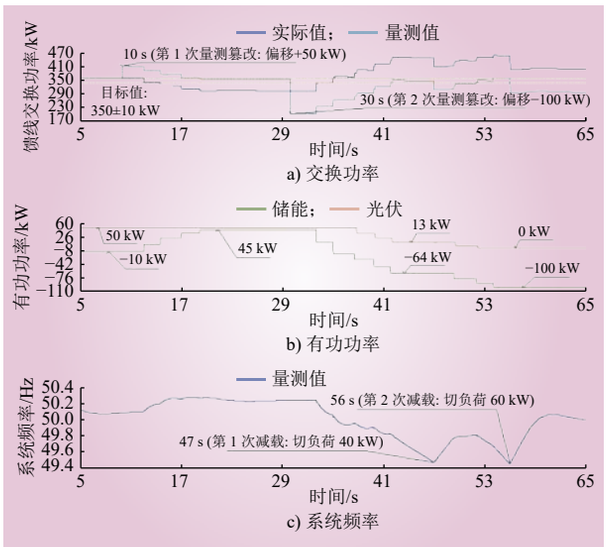

图 8 量测篡改信息攻击对主动配电网区域控制影响的 DIgSILENT 仿真结果

Fig. 8 DIgSILENT-based simulation results for tampered measurements impact on regional control of active distribution networks

加和光伏输出功率的降低，馈线侧实际的净负荷逐渐达到了馈线可承受负载的上限，系统频率逐渐下降。在 47 s 时刻，低频减载保护自动切除 40 kW 的负荷，系统频率停止下降，开始回升。然而，在 56 s 时刻，低频减载第 2 次被触发，再次切除了 60 kW 负荷。在第 1 次低频减载保护后，区域控制器观测到馈线交换功率量测值再一次低于目标值，于是进一步增加储能的充电功率、降低光伏的输出功率，导致馈线侧实际净负荷再次升高，系统频率又一次下降。最终，储能达到了最大充电功率，光伏的有功功率则降低至 0，损失 100 kW 负荷后，系统恢复稳定运行。

算例表明，对配电网系统关键量测节点的网络恶意攻击可以扰乱控制中心对电网运行状态的感知，下发错误的控制指令，引发连锁故障。因此应该采取建立冗余量测体系、提升系统对数据信息的甄别能力、探究信息缺失下的自愈控制算法等措施来抵御信息侧网络安全给主动配电网安全稳定运行带来的风险。

5 结语

本文首先对主动配电网信息物理交互机理进行了研究，并针对信息攻击引发的配电网跨空间连锁故障进行了分类讨论。在此基础上，建立了配电网信息物理风险传递过程，分析了配电网信息物理故障演化机理。最后，依据馈线功率控制原理，建立了针对馈线控制的信息攻击模型并在 DIgSILENT 中搭建了相应算例进行仿真分析，结果表明，当主动配电网信息系统与物理系统间存在强耦合关系时，网络恶意攻击造成的数据篡改扰乱了电网当前运行状态的正确感知，会导致控制中心下发错误的控制指令，最终引发主动配电网系统的连锁故障。本文结论对于今后配电网应对信息攻击所需采取的防御策略具有指导性意义，未来还可继续对主动配电网冗余量测体系，信息缺失下的自愈控制算法、信息安全等级强化策略等进行深入研究以期能够进一步提升配电网防护水平。

参考文献：

[1] 薛禹胜, 李满礼, 罗剑波, 等. 基于关联特性矩阵的电网信息物理系统耦合建模方法 [J]. 电力系统自动化, 2018, 42(2): 11–19.
XUE Yusheng, LI Manli, LUO Jianbo, *et al*. Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix[J]. Automation of Electric Power Systems, 2018, 42(2): 11–19.

[2] XIN S J, GUO Q L, SUN H B, *et al*. Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems[J]. IEEE Transactions on Smart Grid, 2015, 6(5): 2375–2385.

[3] XU L, GUO Q L, SUN H B, *et al*. A routing optimization model for EMS of power systems considering cyber-physical interdependence [C]//2017 IEEE Conference on Energy Internet and Energy System Integration (EI2). Beijing, China. IEEE, 2017: 1–5.

[4] DRIOUICH Y, PARENTE M, TRONCI E. Modeling cyber-physical systems for automatic verification[C]//2017 14th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD). Giardini Naxos, Italy. IEEE, 2017: 1–4.

[5] OYEWOLE P A, JAYAWEERA D. Power system security with cyber-physical power system operation[J]. IEEE Access, 2020, 8: 179970–179982.

[6] 高崇, 曾广璇, 张俊潇, 等. 基于成功流法的配电信息物理系统可靠性评估 [J]. 电力建设, 2020, 41(5): 58–64.
GAO Chong, ZENG Guangxuan, ZHANG Junxiao, *et al*. Reliability

assessment of distribution network cyber-physical system using goal-oriented method[J]. Electric Power Construction, 2020, 41(5): 58–64.

[7] HE H B, YAN J. Cyber-physical attacks and defences in the smart grid: a survey[J]. IET Cyber-Physical Systems: Theory & Applications, 2016, 1(1): 13–27.

[8] LIANG G Q, ZHAO J H, LUO F J, *et al*. A review of false data injection attacks against modern power systems[J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1630–1638.

[9] 周霞, 杨洲, 倪明, 等. 考虑信息-物理组合预想故障筛选的配电网 CPS 安全性评估 [J]. 中国电力, 2020, 53(1): 40–48.
ZHOU Xia, YANG Zhou, NI Ming, *et al*. Security evaluation of distribution network CPS considering cyber-physical combinations for anticipated fault screening[J]. Electric Power, 2020, 53(1): 40–48.

[10] ALHAIDARI F A, AL-DAHASI E M. New approach to determine DDoS attack patterns on SCADA system using machine learning [C]//2019 International Conference on Computer and Information Sciences (ICCIS). Sakaka, Saudi Arabia. IEEE, 2019: 1–6.

[11] 郭创新, 陆海波, 俞斌, 等. 电力二次系统安全风险评估研究综述 [J]. 电网技术, 2013, 37(1): 112–118.
GUO Chuangxin, LU Haibo, YU Bin, *et al*. A survey of research on security risk assessment of secondary system[J]. Power System Technology, 2013, 37(1): 112–118.

[12] YAN J, GOVINDARASU M, LIU C C, *et al*. Risk assessment framework for power control systems with PMU-based intrusion response system[J]. Journal of Modern Power Systems and Clean Energy, 2015, 3(3): 321–331.

[13] HONG J, CHEN Y, LIU C C, *et al*. Cyber-physical security testbed for substations in a power grid[M]//Cyber Physical Systems Approach to Smart Electric Power Grid. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 261-301.

[14] CHEN Y, HONG J, LIU C C. Modeling of intrusion and defense for assessment of cyber security at power substations[J]. IEEE Transactions on Smart Grid, 2018, 9(4): 2541–2552.

[15] 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.

[16] WANG Q, PIPATTANASOMPORN M, KUZLU M, *et al*. Framework for vulnerability assessment of communication systems for electric power grids[J]. IET Generation, Transmission & Distribution, 2016, 10(2): 477–486.

[17] 汤奕, 韩啸, 吴英俊, 等. 考虑通信系统影响的电力系统综合脆弱性评估 [J]. 中国电机工程学报, 2015, 35(23): 6066–6074.
TANG Yi, HAN Xiao, WU Yingjun, *et al*. Electric power system vulnerability assessment considering the influence of communication system[J]. Proceedings of the CSEE, 2015, 35(23): 6066–6074.

[18] 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.

[19] 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.

[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] 陈霖, 许爱东, 蒋屹新, 等. 基于动态增量聚类分析的电力信息网络攻击模式识别算法 [J]. 南方电网技术, 2020, 14(8): 25–32.
CHEN Lin, XU Aidong, JIANG Yixin, *et al*. Attack pattern recognition algorithm of power information network based on dynamic incremental cluster analysis[J]. Southern Power System Technology, 2020, 14(8): 25–32.

[22] 王电钢, 黄林, 刘捷, 等. 考虑负荷虚假数据注入攻击的电力信息物理系统防御策略 [J]. 电力系统保护与控制, 2019, 47(1): 28–34.
WANG Diangang, HUANG Lin, LIU Jie, *et al*. Cyber-physical system defense strategy considering loaded false data injection attacks[J]. Power System Protection and Control, 2019, 47(1): 28–34.

[23] 李晓, 李满礼, 倪明. 配电信息物理系统分析与控制研究综述 [J]. 中国电力, 2020, 53(1): 11–21.
LI Xiao, LI Manli, NI Ming. A review of analysis and control of cyber physical distribution system[J]. Electric Power, 2020, 53(1): 11–21.

[24] 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.

[25] LIU X D, SHAHIDEHPOUR M, LI Z Y, *et al*. Power system risk assessment in cyber attacks considering the role of protection systems[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 572–580.

[26] 于文鹏, 刘东, 余南华. 馈线控制误差及其在主动配电网协调控制中的应用 [J]. 中国电机工程学报, 2013, 33(13): 108–115.
YU Wenpeng, LIU Dong, YU Nanhua. Feeder control error and its application in coordinate control of active distribution network[J]. Proceedings of the CSEE, 2013, 33(13): 108–115.

作者简介：

翁嘉明 (1986—)，男，博士，讲师，从事能源互联网、信息物理系统、主动配电网、智能电网研究，E-mail：wrzx_5@sjtu.edu.cn；

刘东 (1968—)，男，通信作者，博士，教授，从事能源互联网、信息物理系统、主动配电网、智能电网研究，E-mail：dongliu@sjtu.edu.cn。

（责任编辑　李博）

Cyber-Physical Risk Evolution Analysis of Active Distribution Network under Feeder Control Error

WENG Jiaming, LIU Dong, AN Yu, YIN Haoyang, HUANG Zhi, QIN Han

(Key Laboratory of Control of Power Transmission and Conversion, Ministry of Education, Shanghai Jiao Tong University, Shanghai 200240, China)

Abstract: In the active distribution network cyber-physical system exists a strong coupling relationship between the cyber system and the physical grid. Under the complex cyber-physical interaction, the cyber system anomalies or failures will directly affect and reduce the operation level of the power grids, and even cause serious cascading failures. Compared to the traditional power system, the risk incentives of the power cyber-physical system are more diversified, the interaction mechanisms are more complicated, and the identification are more difficult. The power system cyber-physical security risk has become one of the fundamental issues in the power system operation. By taking the active distribution network as an example, we establish a risk transfer model for active distribution networks under cyber-attacks to reveal the evolution mechanism of failures in the distribution network cyber-physical system. Finally, a simulation case study is carried out with DIgSILENT to verify the correctness of the proposed model, and some suggestions are proposed on how to prevent cyber-side risks in the future distribution network and improve the level of security risk protection.

The work is supported by the National Key Research and Development Program of China (No.2017YFB0903000), the Science and Technology Project of State Grid Jiangsu Electric Power Company (Research and Application of Distributed Feeder Automation Collaborative Operation and Control Technology for High Reliability Distribution Network, No.J2019061).

Keywords: active distribution network; cyber physical system; feeder control error; risk evolution; cyber attack