Applied Physics 应用物理, 2024, 14(9), 629-639
Published Online September 2024 in Hans. https://www.hanspub.org/journal/app
https://doi.org/10.12677/app.2024.149067

Hans汉斯

面向网络攻击的电力信息物理系统风险量化评估研究综述

张五一[1,2]，李圣泉[1,2]，彭承宗[3,4]，田　叶[1,2]

[1]国电南京自动化股份有限公司，江苏　南京
[2]南京南自数安技术有限公司，江苏　南京
[3]成都信息工程大学网络空间安全学院(芯谷产业学院)，四川　成都
[4]先进微处理器技术国家工程研究中心(工业控制与安全分中心)，四川　成都

收稿日期：2024年7月8日；录用日期：2024年8月29日；发布日期：2024年9月6日

摘　要

针对网络攻击严重威胁电力系统安全运行的现状，文中对面向网络攻击的电力信息物理系统风险量化评估问题展开分析。本文从由网络攻击造成的典型停电事故出发，阐述电力信息物理系统的风险来源及传播机理。然后对比传统信息系统及电力系统，对电力信息物理系统风险量化评估的特点展开讨论，并进一步基于节点风险概率、风险传播概率和物理量损失量三个方面，对电力系统风险量化计算方法进行分析总结。最后，面向网络攻击的发展方向，对未来研究提出建议和展望。

关键词

电力信息物理系统，网络攻击，风险量化评估，风险传播

A Review on Quantitative Risk Assessment of Cyber-Physical Power Systems for Cyber Attacks

Wuyi Zhang[1,2], Shengquan Li[1,2], Chengzong Peng[3,4], Ye Tian[1,2]

[1]Nanjing SAC Power Grid Automation Co., Ltd., Nanjing Jiangsu
[2]Nanjing SAC Power Grid Automation Cyber Securtiy Technology Co., Ltd., Nanjing Jiangsu
[3]School of Cybersecurity (Xin Gu Industrial College), Chengdu University of Information Technology, Chengdu Sichuan

文章引用: 张五一, 李圣泉, 彭承宗, 田叶. 面向网络攻击的电力信息物理系统风险量化评估研究综述[J]. 应用物理, 2024, 14(9): 629-639. DOI: 10.12677/app.2024.149067

[4]SUGON Industrial Control and Security Center, Chengdu Sichuan

Received: Jul. 8th, 2024; accepted: Aug. 29th, 2024; published: Sep. 6th, 2024

Abstract

In view of the current situation that cyber attacks pose a serious threat to the safe operation of power systems, this paper analyzes the quantitative risk assessment of cyber-physical power systems for cyber attacks. Based on the typical power outages caused by cyber attacks, the sources of risk and the mechanisms of risk propagation within cyber-physical power systems is elucidated. Then, compared with traditional information systems and power systems, the distinctive characteristics of risk quantification assessment for cyber-physical power systems are discussed. Furthermore, based on nodal risk probability, risk propagation probability, and physical quantity loss, the quantitative risk calculation methods for power systems is summarized. Finally, facing the development direction of network attacks, suggestions and prospects for future research are proposed.

Keywords

Cyber-Physical Power Systems, Cyber Attacks, Quantitative Risk Assessment, Risk Propagation

1. 引言

传统电力系统风险评估主要侧重于电网在物理域的设备失效风险，这些设备失效的机理通常具有清晰明确的物理特性，现有研究已经建立了相对完善的电力系统设备失效模型及风险指标体系，形成了较为成熟的电力系统风险分析理论。随着科技的飞速发展，电力系统的运行和管理方式发生了深刻变革，随着电网的信息化水平不断提高，信息域和物理域之间的耦合变得日益紧密，电力系统逐渐演变为一个典型的信息物理系统(Cyber-physical system, CPS)，电力系统的控制与决策对于信息系统愈发依赖[1]。2012年的伊朗震网蠕虫攻击事件、2015 年的乌克兰大停电事件及 2019 年的委内瑞拉大停电事件等典型由网络攻击导致的电网安全事件表明，信息域的安全风险已经对电力系统物理域的运行安全构成了极大的威胁[2]。2024 年国家发展改革委和国家能源局联合发布的《关于加强电网调峰储能和智能化调度能力建设的指导意见》中进一步明确指出“推动“云大物移智链边”、5G 等先进数字信息技术在电力系统各环节广泛应用”，未来我国电力系统信息域对物理域的影响将进一步加深，在对电力系统进行安全风险评估时必须考虑信息域的安全风险。

相对于物理域风险，信息域的安全风险除了受设备失效等物理因素的影响，而互联网的开放性、匿名性、互联性也使信息域更容易遭受人为攻击。虽然网络攻击、防御及安全漏洞等都有比较明确的数学模型，但攻击和防御的模式众多，安全漏洞五花八门，新的攻击模式和防御模式层出不穷，且信息域的安全性依赖于攻击与防御的博弈，导致信息域的风险机理非常复杂[3]。而信息域的安全问题也并不必然导致电网物理域的安全事故，因此电力信息物理系统的风险评估不仅需要考虑物理域和信息域各自的风险机理，还需要考虑风险从信息域到物理域的传导机制。由此电力信息物理系统风险评估成为电网风险

评估领域的重要研究课题。为此，本文面向网络攻击场景对电力信息物理系统风险评估研究展开综述。

2. 电力信息物理系统风险分析

2.1. 典型事件分析

由表 1 可知，近年来已发生多次由信息系统风险导致的电力系统事故。其中，早期美加大停电事件中的信息系统风险主要来自于设备自然故障导致的设备失效。而近期典型事件中，信息系统风险主要来自网络攻击，信息系统的风险特征在发生明显的变化。在乌克兰大停电事件，网络攻击导致信息系统设备失效，使物理系统设备丧失感知和控制能力。虽然同样是信息系统设备失效，但美加大停电事件中的信息系统设备失效风险由设备本身的失效概率进行表征，而乌克兰大停电事件中的信息系统设备失效风险则应由网络攻击的成功概率进行表征。而在伊朗布什尔核电站事故事件中，网络攻击并没有使设备失效，而是在信息传递过程中篡改了数据，一方面使物理系统获得了错误的指令，另一方面运行人员由于错误的信息未能感知风险并及时干预，相对于直接使设备失效更具有隐蔽性。由此可见，不同形式的网络攻击，对电力信息物理系统的影响机理不同，风险概率模型和风险传播模式也不相同，由此面向网络攻击风险的电力信息物理系统风险评估也成了近年来研究的主流。

Table 1. Typical events of blackout accidents caused by information system risks
表 1. 信息系统风险导致电力事故的典型事件

事件	信息系统风险
2003 年美加大停电事件	状态估计器未能提供正确的系统信息。[4]
2010 年伊朗布什尔核电站事故事件	震网病毒入侵离心机后，首先记录离心机的正常转速。然后一方面控制离心机的速度周期性异常变化，另一方面向监控设备发送正常数据，使异常不被察觉。[5]
2015 年乌克兰大停电事件	病毒植入 EMS 系统，使底层发电机或变电站的控制服务器关机，丧失对相应物理设备的感知与控制能力。[6]
2019 年委内瑞拉大停电事件	水电站的计算机系统中枢遭受网络攻击。[7]

2.2. 风险来源分析

通常可以将信息物理系统简单分为三层，分别是信息层、通信层(耦合层)和物理层。目前通信层和物理层主要考虑的风险来源仍是设备故障、操作失误等传统设备失效因素。由典型事件分析可知，信息层的风险来源除了传统设备失效因素，还需要进一步考虑网络攻击的影响。如前文所述，网络攻击风险是目前电力信息物理系统风险研究的重点内容[8]。网络攻击的目标和形式丰富多样，但最终都是通过破坏网络安全性，进而使电力物理系统丧失感知和控制能力。因此依据网络安全三要素，又可以将网络攻击风险分为破坏信息保密性风险、破坏信息可用性风险和破坏信息完整性风险[9] [10]，下面对以上三类风险进行具体分析。

破坏信息保密性的攻击并不会直接威胁物理系统安全，但该类攻击一方面可能使攻击者获得更多的权限，另一方面可能使攻击者掌握更加全面的物理系统信息，从而提高以破坏物理系统安全为目标的网络攻击成功概率，因此破坏信息保密性的攻击同样会影响电力信息物理系统安全风险[3]。

破坏信息可用性会使得物理系统失去感知和控制能力，其破坏效果类似于信息系统设备失效；破坏信息完整性会使得物理系统得到错误的信息从而做出错误的控制决策，或者使得正确的控制指令被篡改，从而导致控制系统错误动作。破坏信息可用性攻击相对简单粗暴，不需要掌握太多的物理系统知识和信息，但攻击的隐蔽性较弱，更容易被检测和防御。破坏信息完整性攻击相对于破坏信息可用性攻击具有

更强的隐蔽性，一个对物理系统足够了解的攻击者可以在不改变数据外部特征的情况下对数据进行修改从而使攻击不易被察觉，这也就意味着破坏信息完整性攻击对攻击者的物理系统知识和信息掌握的全面性提出了更高的要求。这也就意味着在风险分析时，针对破坏信息可用性攻击需侧重考虑防御对攻击成功率的影响，而针对破坏信息完整性攻击则需侧重考虑攻击者信息掌握程度对攻击成功率的影响。

2.3. 风险跨域传播分析

电力物理系统是一个连续系统，其风险会依据基尔霍夫电压电流定律等固有物理定律向整个系统传播。而信息系统则是一个离散系统，其风险传播特性主要依赖于风险传播路径的特征。目前电力 CPS 风险评估主要考虑的是信息系统失效对物理系统的影响，因此电力 CPS 的风险传播分析主要关注的是风险因素从信息系统到物理系统边界的传播特性，即主要考虑风险的传播路径特征。基于此，目前在风险传播研究中，电力 CPS 常被抽象成一个由信息节点、物理节点、信息边、物理边及节点关联关系的系统(如图 1 所示)，由此可基于图论和相依性分析等理论方法研究风险传播路径特征。以上理论方法可普遍用于电力 CPS 风险传播的研究，但由于系统过度简化，难以保留具体系统元件特性。

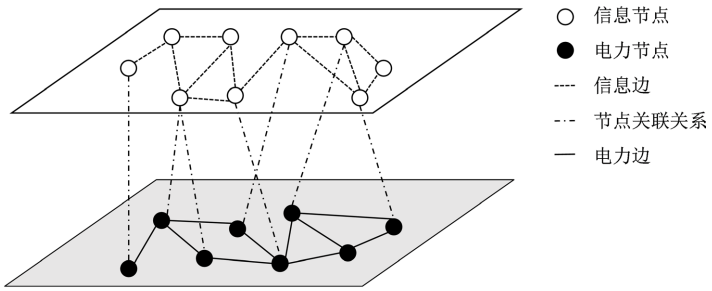

Figure 1. The structure figure of cyber physical power systems
图 1. 电力 CPS 结构图

也有文献通过仿真模拟对风险传播机理进行分析，该类方法能够更加详细地考虑信息物理系统元件特性，更符合实际运行需求，但所得结论通常是针对某一具体对象，难以得到一般性结论。同时建模所需信息量也更加庞大，实现难度较高。但随着信息技术的快速发展，数据获取、收集与储存越来越容易，构建高精度模拟实际系统的仿真平台是未来研究的发展趋势。通过仿真平台分析得到的具体结论也可以进一步指导理论方法的完善。

3. 电力信息物理系统风险量化评估

3.1. 电力信息物理系统风险量化评估的特点

风险量化计算主要依赖于失效概率 P 与损失 C，风险值 R 的计算公式如下：

$$R = \sum PC \tag{1}$$

传统信息系统的风险量化评估主要研究网络攻击导致信息节点失效的概率，包括信息节点被成功攻击的概率以及风险在信息节点传播，进而推导计算每个节点的失效概率。在传统电力系统风险量化评估中，主要考虑的是物理节点失效(电力元件失效)概率以及电力元件失效导致的电力系统损失，除了连锁故障的风险评估，一般较少考虑风险在节点间的传播。

而电力 CPS 系统需要考虑的是信息节点失效对电力系统的影响，因此对其进行量化评估时，需要考虑三部分内容：一是信息系统网络攻击导致信息节点失效的概率，二是信息节点导致物理节点失效的概

率，三是物理节点失效导致的电力系统损失。总体可分为四个步骤：分别是信息节点被成功攻击、风险在信息系统传播、风险从信息系统向物理系统传播、造成物理系统损失。当信息系统和物理系统都抽象为节点网络时，风险在信息系统内部节点传播和从信息节点向物理节点传播在进行数学建模时并无本质区别。因此，本文将从信息节点被成功攻击的概率、风险传播分析和物理损失量三个方面对现有文献进行总结(图 2)。

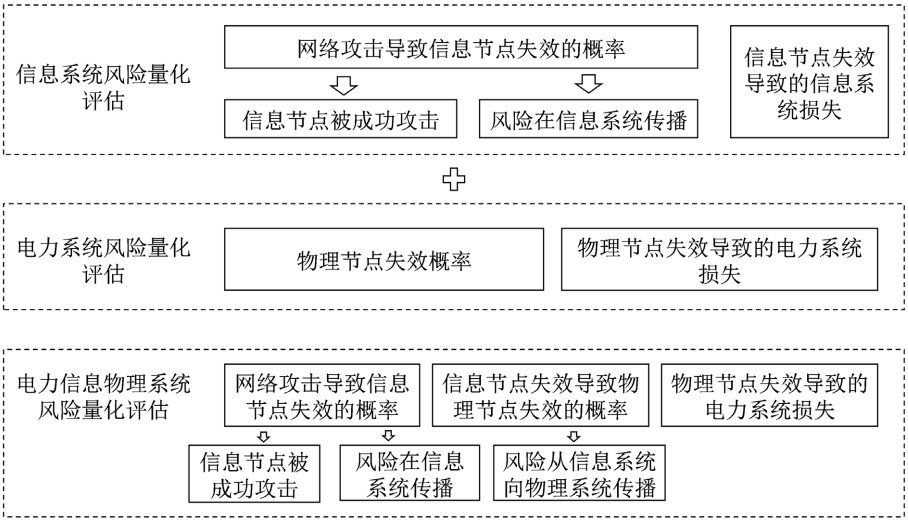

Figure 2. Characteristic analysis of risk quantification assessment of cyber physical power systems
图 2. 电力 CPS 风险量化评估的特点分析图

3.2. 单个信息节点失效概率

单个信息节点失效主要包括两个方面：一是元件失效，元件失效又包括硬件失效和软件失效[11]，该类失效概率主要由元件的失效模型获得，其重点在于研究元件的失效机理；二是网络攻击，网络攻击成功则认为信息节点失效，信息节点的失效概率也可认为是漏洞被攻击的成功概率。网络攻击的成功概率主要与信息节点的脆弱性和威胁性相关，表达函数形式不唯一，典型计算公式有[12]：

$$P_i = \begin{cases} 1-e^{-k\lambda_i}, & x_i \geq y_i \\ 1, & x_i < y_i \end{cases} \tag{2}$$

式中，P_i 为第 i 个信息节点攻击成功概率；λ_i 为第 i 个信息节点的脆弱性系数，脆弱性系数越大，则攻击的成功概率越大；x_i 为第 i 个信息节点的防御强度；y_i 为第 i 个信息节点的攻击强度；k 为威胁性系数，与攻击强度正相关，与防御强度负相关，威胁性系数越大，则攻击的成功概率越大。$P_i = 1$ 表示第 i 个信息节点无法抵抗网络攻击，信息节点失效。

3.2.1. 脆弱性

脆弱性评估是信息系统风险评估的重要内容，脆弱性是系统自身的属性，与网络环境安全性、通信协议安全性及加密措施等多个网络安全指标有关。

脆弱性分析往往需要先对系统进行渗透测试[13]、网络扫描测试[14] [15]、仿真模拟[16] [17]等，以识别系统漏洞并获得系统漏洞的基本指标参数。然后需要进一步通过综合评估方法对各项指标进行整合。

其中公共漏洞评分系统(Common Vulnerability Scoring System, CVSS) [18]是进行信息系统脆弱性指

标量化分析最常用的方法之一，被认为是标准化的评价体系。其主要从基础评价、生命周期评价和环境评价三个方面对系统漏洞风险进行评估。其所对应的访问向量(access vector, AV)、访问复杂度(access complexity, AC)、认证(authentiation, Au)等指标即可用来计算脆弱性评价系数。文献[19]基于以上三个子项，给出了漏洞利用成功率的概率计算公式：

$$P(V_I) = 2I^{AV} I^{AC} I^{Au} \tag{3}$$

式中，$P(V_I)$为漏洞 V_I 的可利用率，I^{VA}、I^{AC}、I^{Au} 分别表示访问向量、访问复杂度、认证的指标赋值。

文献[20]、[21]则认为漏洞利用成功概率还与漏洞暴露时间有关，漏洞暴露时间越长越容易被攻击成功。因此需要进一步在时间尺度上对漏洞利用成功概率进行分析，采用帕累托分布描述时间对于漏洞可利用概率的影响，从而式(3)被改写为：

$$P(V_I) = \left(1 - \frac{k}{t}\right)^{\alpha} 2I^{AV} I^{AC} I^{Au} \tag{4}$$

式中，k 和 α 为帕累托分布的参数，t 为漏洞暴露时间。

另一方面，针对不同的实体，现有文献进一步梳理资产类型及其层次结构，考虑可能的外部威胁，提出考虑不同实体特点的风险评价指标并构建指标体系，通过指标赋值计算脆弱性系数。同时基于多采用层次分析法(AHP) [22] [23]和逼近理想解排序法(TOPSIS) [24]还可以对系统脆弱性进行综合评估。文献[25]-[31]分别对发电系统、输电系统、虚拟电厂等对象进行了脆弱性评估。

文献[25]将电力 CPS 抽象为感知层、网络层、平台层和应用层，从信息的获取、传输、处理及应用四个角度构建了风险评价指标体系。文献[26]从终端网络安全、移动应用网络安全、云端网络安全、终端运行特性四个方面构建了配电网用户侧的风险评估指标体系。文献[27]和[28]研究了发电系统 CPS 的指标体系。从信息安全风险的可用性、完整性和保密性构建指标，同时考虑了环境因素和人为因素的威胁、技术和管理的脆弱性及安全措施。文献[29]构建了虚拟电厂的 CPS 风险指标体系，其在静态风险评估中主要考虑了网络、管理平台、终端和重要数据四个对象。文献[30]则针对电网边缘计算这一具体业务构建了风险评估指标体系，主要考虑了网络设备安全、通道安全和协议安全三个方面的指标。

由上述文献可知，不同研究对象对应了不同设备，且所涉及的因素众多，研究者通常是根据自身需求选择一部分进行考虑。因此，对于指标的设定并没有统一的规则，到底选择哪些指标进行体系构建具有一定的随机性。考虑的指标不同，脆弱性评估结果也不同。文献[31]针对 SCADA 系统从管理指标和技术指标两个方面构建了含 83 个指标的风险安全指标体系，并通过 Autoencoder 方法从高维度的复杂数据中提取低维的数据特征，从而提取关键指标，通过先建立全面指标再进行指标筛选的思路在一定程度上增强了指标体系构建的科学性。

3.2.2. 威胁性

除了脆弱性，在网络攻击环境下的信息节点失效概率还要考虑网络攻击的威胁性。网络攻击的威胁性与系统脆弱性紧密相关，威胁性更侧重于攻击和防御条件和强度。

文献[32]-[34]主要采用分级量化思路对威胁性系数进行分析。基于指数函数提出了攻击成功率经验公式，通过攻击所需前提条件与节点漏洞信息之间的匹配度以及目标节点采用安防措施强度对信息系统威胁性进行量化。

文献[35]则更加详细地考虑了攻击行为特性，基于实现攻击的花销，技术难度，发现难度，运用多属性效用论对威胁性概率风险进行量化计算。

文献[36]则考虑了攻防资源对威胁性的影响。基于攻防动态博弈三层数学规划模型对电力 CPS 攻防

资源进行分配，构建了元件失效概率和防御资源的关系，面向攻防资源分配实现了节点攻防强度的量化。文献[38]认为不同元件对于相同攻防策略的资源转换效率不同，因此在文献[36]的基础上进一步考虑不同元件的攻防资源转换效率，建立了攻防资源和被成功攻击概率的关系表达式，增强了模型的适应性。

文献[38] [39]在威胁性量化中考虑了攻击者和防御者对系统了解程度的影响。文献[39]基于攻击者和防御者对漏洞的理解程度，依据泊松分布构建了漏洞被成功入侵的概率计算公式，其中对漏洞的理解程度用投入的资源和学习所需时间进行量化。文献[39]在漏洞攻击成功概率中考虑了攻击者知识和攻击数理程度作为威胁性的量化指标。

3.3. 节点间风险传播量化

传统电力系统的风险评估考虑的是物理元件失效直接导致电力系统损失，一般仅在考虑连锁故障时研究节点间的关系，否则认为各节点失效相互独立，较少考虑风险在系统内的传播。

而在电力 CPS 系统中，被攻击的对象是信息节点，被攻击的节点失效并不能直接造成物理量损失，而是沿着攻击路径将信息节点失效风险传导至物理节点，因此在获得单个节点失效概率之后，还需要进一步考虑风险在节点间的传播。风险在节点间传播的量化依赖于对节点间关联关系的描述，主要描述方法有矩阵和图。

3.3.1. 矩阵方法

文献[40]定义了每个节点被成功感染的概率和每个节点对周围任一节点的感染概率以构建传递概率矩阵来表征风险在电力 CPS 中的传递。文献[41]基于故障节点对正常节点的影响概率(使正常节点变为故障节点的概率)，构建风险状态依存矩阵来反映系统故障传播过程。其风险状态依存矩阵的元素不再是给定的值，而是依据节点状态实测值和估计值，通过优化模型反推风险状态依存矩阵取值，再依据风险状态依存矩阵推演风险传播过程。

依托状态转移矩阵，隐马尔可夫模型(Hidden Markov Model, HMM) [42] [43]也是一种常用的系统风险传播量化方法，其在识别系统隐藏状态序列方面有优势，常用于基于攻击检测的网络系统安全评估中。一个完整的 HHM 主要包括 5 项元素，分别是状态空间集合 $\boldsymbol{S}$，观测矩阵 $\boldsymbol{V}$，状态转移矩阵 $\boldsymbol{A}$，观测矩阵 $\boldsymbol{B}$ 和初始状态矩阵 $\boldsymbol{p}$。基于初始状态矩阵 $\boldsymbol{p}$ 和状态转移矩阵 $\boldsymbol{A}$、观测矩阵 $\boldsymbol{B}$ 即可获得风险传播过程中状态节点(非被攻击节点)失效的概率，典型计算公式如下[44]：

$$p_k(i+j) = p_v B_{i+j,k} \prod_{l=i+1}^{i+j} A_{l-1,l} \tag{4}$$

式中 p_v,$A_{l\text{-}1,l}$，$B_{i+j,k}$ 分别为初始状态矩阵 $\boldsymbol{p}$ 和状态转移矩阵 $\boldsymbol{A}$、观测矩阵 $\boldsymbol{B}$ 中的元素。

3.3.2. 图方法

攻击路径和贝叶斯网络是比较主流的两种通过图形式分析节点间风险传播的方法。基于攻击路径的方法相对比较简单直观，最简单的一种方式就是将风险传播过程看作攻击路径上的风险累积[45]-[47]。

基于贝叶斯网络的攻击图方法[48] [49]利用了叶斯网络量化处理不确定性信息和因果关联的优势，具有不确定性推理能力，能够比较准确地量化网络风险概率[50]。在得到单个节点失效概率之后，通过引入条件概率来表征节点间的关系，主要包括局部条件概率、先验概率和后验概率[51]。局部条件概率反映了某个状态节点受到威胁的可能性，该条件概率与状态节点和其父节点的依赖关系有关[52]。每个状态节点的先验概率等于当前节点与其父节点的条件概率之积。由于网络中的安全条件、安全因素等都可能影响各个状态节点的先验概率，利用贝叶斯网络推理方法还可以进一步计算评估在攻击时间条件下的安全风险，即后验概率[53]。因此，基于贝叶斯网络的攻击图方法还可以实现风险的动态评估[54]。

除了以上比较主流的一些方法，现有文献还基于细胞自动机理论、病毒传播理论及渗透流理论对风险在电力 CPS 中的传播进行了描述和量化。

文献[55]和[56]基于细胞自动机理论对电力 CPS 的风险传播机理展开研究。信息节点和电力节点对应信息细胞和物理细胞，基于信息细胞被攻击后导致其他信息细胞被攻击的概率及信息细胞故障导致物理细胞故障的概率构建矩阵，量化节点间的关联关系。依据设定的节点状态演变规则，通过仿真模拟推演故障传播过程，并获得风险值。在以上研究中认为构建矩阵的相关概率均为已知数，研究的重点是在既定概率下故障的演变过程。

文献[57]将网络攻击的风险传播过程看作病毒传播过程，通过求解进化博弈的演化动力学方程分析所有网络节点的稳定感染率，并通过模拟网络节点在博弈过程中的随机状态转移来评估网络节点的感染概率。

文献[58]和[59]则基于渗透流理论提出电力 CPS 的风险传播动力学模型。渗透流理论认为节点或边发生故障，则认为该节点或边被占据，故障会以一定概率导致其他点或边发生故障，进而导致风险向图中其他节点传播的行为。该方法重点研究了信息系统和物理系统的相互影响，可通过动力学递归方程的求解获得电力 CPS 被攻击后的平衡状态，以获得风险阈值。

前述文献大部分仅考虑了风险在信息系统内部的传播和信息系统向物理系统的传播，文献[60]则进一步考虑了电力 CPS 系统的连锁故障，即风险在电力系统的传播。针对单个物理节点，考虑了与老化因素相关的线路故障概率，并进一步讨论了由初始故障引发的其他线路故障概率以量化风险在物理系统内的传播。

3.3. 物理损失量

目前针对电力 CPS 的风险评估主要集中在针对信息可用性攻击方面。该类攻击对物理系统的主要影响仍是使物理系统元件失效，在电力系统分析中引入的干扰是 0-1 变量，即元件是否退出运行，因此在物理损失量计算方面与传统的电力系统风险分析方法基本一致。物理量损失主要考虑了电力系统物理量(电压、频率、负载)偏离[61] [62]，其中研究最多的是切负荷量。物理量偏移的来源可能是电力系统动态失稳和系统 $N-1$ 故障等。

随着近年来虚假数据注入攻击研究的逐渐深入，考虑信息完整性攻击的风险评估研究也逐步展开。在信息系统的分析中，信息完整性攻击引入的仍是 0-1 变量，即节点或路径是否攻击成功。但当风险传递到物理系统时，其在物理系统引入的干扰不再是 0-1 变量，而是一个连续变量。该变化不会对电力系统物理损失量的形式造成影响，其对应的物理量损失仍是电力系统物理量偏离，但物理量偏离的来源则可能是由于错误数据导致的调度决策错误，引发的供需不平衡[63]和系统动态失稳[64] [65]。同时连续变量所对应的系统状态比 0-1 变量更多，电力系统物理损失量的分析可能会变得更加复杂。

4. 结语

本文对面向网络攻击的电力 CPS 风险量化评估研究进行了综述。在传统信息系统和电力系统风险评估的基础上，电力 CPS 风险量化评估需是在概率计算中进一步风险从信息系统向电力系统的传播。目前考虑的主要攻击形式是面向信息可用性的攻击，随着对数据安全的重视程度不断提高，面向信息完整性攻击的风险评估也逐步展开。

网络攻击相对于元件自然失效具有更强的随机性，且可供参考的历史数据有限，难以从历史数据中统计出攻击成功率，因此目前的网络攻击成功率计算中需要较强的人工经验干预，对很多条件进行了预设和简化，可能存在计算精度不高的问题。由于可供分析的历史数据有限，电力 CPS 风险的准确评估依

赖于高精度模拟真实系统的仿真平台建设，通过仿真模拟精细刻画电力 CPS 运行状态，基于充分的研究数据，结合人工智能方法强大的数据挖掘能力，更加科学准确地统计分析网络攻击成功概率，并提取风险传播特征。

基金项目

国电南京自动化股份有限公司科技项目(SA23 技靶场)；四川省自然科学基金面上项目(2024NSFSC0493)。

参考文献

[1] Yu, X. and Xue, Y. (2016) Smart Grids: A Cyber-Physical Systems Perspective. *Proceedings of the IEEE*, **104**, 1058-1070. https://doi.org/10.1109/jproc.2015.2503119

[2] 张涛, 费稼轩, 王琦, 等. 电力信息物理系统跨域攻击协同防御架构及机制研究[J]. 电子学报, 2024, 52(4): 1205-1218.

[3] 王琦, 李梦雅, 汤奕, 等. 电力信息物理系统网络攻击与防御研究综述(一)建模与评估[J]. 电力系统自动化, 2019, 43(9): 9-21.

[4] 甘德强, 胡江溢, 韩祯祥. 2003 年国际若干停电事故思考[J]. 电力系统自动化, 2004, 28(3): 1-4, 9.

[5] 胡江, 孙国臣, 张加军, 等. 由“震网”病毒事件浅议核电站信息安全现状及监管[J]. 核科学与工程, 2015, 35(1): 181-185, 192.

[6] 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.

[7] 黄鑫, 陈德成, 孙军, 等. 网络攻击下电力系统信息安全研究综述[J]. 电测与仪表, 2017, 54(23): 68-74.

[8] 房岭峰, 黄丽, 赵琪, 等. 从委内瑞拉大停电看特大型城市电网安全问题[J]. 电力与能源, 2019, 40(6): 674-677.

[9] National Institute for Standards and Technology (NIST) (2010) Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References: NISTIR 7628.

[10] Rawat, D.B. and Bajracharya, C. (2015). Cyber Security for Smart Grid Systems: Status, Challenges and Perspectives. *SoutheastCon* 2015, Fort Lauderdale, 9-12 April 2015, 1-6. https://doi.org/10.1109/secon.2015.7132891

[11] 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, 1763.

[12] Deng, S., Zhang, J., Wu, D., He, Y., Xie, X. and Wu, X. (2023) A Quantitative Risk Assessment Model for Distribution Cyber-Physical System under Cyberattack. *IEEE Transactions on Industrial Informatics*, **19**, 2899-2908. https://doi.org/10.1109/tii.2022.3169456

[13] Lachkov, P., Tawalbeh, L. and Bhatt, S. (2022) Vulnerability Assessment for Applications Security through Penetration Simulation and Testing. *Journal of Web Engineering*, **21**, 2187-2208. https://doi.org/10.13052/jwe1540-9589.2178

[14] Kumar, D., *et al*. (2019) All Things Considered: An Analysis of IoT Devices on Home Networks. *Proceedings of the* 28*th USENIX Conference on Security Symposium*, 14-16 August 2019, Santa Clara, 1169-1185.

[15] 李艳, 黄光球, 张斌. 基于攻击事件的动态网络风险评估框架[J]. 计算机工程与科学, 2016, 38(9): 1803-1811.

[16] 钱胜, 王琦, 颜云松, 等. 计及网络攻击影响的安全稳定控制系统风险评估方法[J]. 电力工程技术, 2022, 41(3): 14-21.

[17] 王元卓, 林闯, 程学旗, 等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报, 2010, 33(9): 1748-1762.

[18] Mell, P., Scarfone, K. and Romanosky, S. (2006) Common Vulnerability Scoring System. *IEEE Security and Privacy Magazine*, **4**, 85-89. https://doi.org/10.1109/msp.2006.145

[19] Poolsappasit, N., Dewri, R. and Ray, I. (2012) Dynamic Security Risk Management Using Bayesian Attack Graphs. *IEEE Transactions on Dependable and Secure Computing*, **9**, 61-74. https://doi.org/10.1109/tdsc.2011.34

[20] Abraham, S. and Nair, S. (2015) A Predictive Framework for Cyber Security Analytics Using Attack Graphs. *International journal of Computer Networks & Communications*, **7**, 1-17. https://doi.org/10.5121/ijcnc.2015.7101

[21] 张宇航, 倪明, 孙永辉, 等. 针对网络攻击的配电网信息物理系统风险量化评估[J]. 电力系统自动化, 2019, 43(21): 12-22, 33.

[22] Hou, D., Sun, Y., Jin, H., Du, X., He, Y. and Zhou, W. (2022). Risk Assessment Method of Distribution CPS Based on Entropy Weight Fuzzy Analytic Hierarchy Process. 2022 *Power System and Green Energy Conference* (*PSGEC*), Shanghai, 25-27 August 2022, 620-625. https://doi.org/10.1109/psgec54663.2022.9881081

[23] 周亮, 李俊娥, 陆天波, 等. 信息系统漏洞风险定量评估模型研究[J]. 通信学报, 2009, 30(2): 71-76.

[24] 谷卫星, 王婷婷, 张鹏, 等. 基于组合赋权和 TOPSIS 的配电网 CPS 系统脆弱性评估[J]. 华北电力大学学报(自然科学版), 2023, 50(1): 56-66, 131.

[25] 何永贵, 刘江. 基于组合赋权-云模型的电力物联网安全风险评估[J]. 电网技术, 2020, 44(11): 4302-4309.

[26] 严康, 陆艺丹, 覃芳璐, 等. 配电网用户侧异构电力物联设备网络风险量化评估[J]. 电力系统保护与控制, 2023, 51(11): 64-76.

[27] 林云威, 陈冬青, 彭勇, 等. 基于 D-S 证据理论的电厂工业控制系统信息安全风险评估[J]. 华东理工大学学报(自然科学版), 2014, 40(4): 500-505.

[28] 彭道刚, 卫涛, 赵慧荣, 等. 基于 D-AHP 和 TOPSIS 的火电厂控制系统信息安全风险评估[J]. 控制与决策, 2019, 34(11): 2445-2451.

[29] 杨珂, 王栋, 李达, 等. 虚拟电厂网络安全风险评估指标体系构建及量化计算[J]. 中国电力, 2025, 57(8): 130-137

[30] 詹雄, 郭昊, 何小芸, 等. 国家电网边缘计算信息系统安全风险评估方法研究[J]. 计算机科学, 2019, 46(z2): 428-432.

[31] 吉德志, 秦丞, 颜丽渊. 融合 Autoencoder 方法的电力系统网络安全风险评估技术[J]. 沈阳工业大学学报, 2023, 45(4): 366-370.

[32] 葛海慧, 肖达, 陈天平, 等. 基于动态关联分析的网络安全风险评估方法[J]. 电子与信息学报, 2013, 35(11): 2630-2636.

[33] 刘仁山, 孟祥宏. 攻击图和 HMM 结合的网络安全风险评估方法研究[J]. 信阳师范学院学报(自然科学版), 2015, 28(1): 146-150.

[34] 徐伟, 黄学鹏. 层次化动态网络入侵风险量化评估仿真研究[J]. 计算机仿真, 2018, 35(4): 408-411, 466.

[35] 王赛娥, 刘彩霞, 刘树新, 等. 一种基于攻击树的 4G 网络安全风险评估方法[J]. 计算机工程, 2021, 47(3): 139-146, 154.

[36] 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.

[37] Qin, H., Weng, J.M., Liu, D., *et al*. (2021) Risk Assessment and Defense Resource Allocation of Cyber-Physical Distribution System Under Denial of Service Attack. *CSEE Journal of Power and Energy Systems*.

[38] Zhang, Z., Huang, S., Chen, Y., Li, B. and Mei, S. (2022) Diversified Software Deployment for Long-Term Risk Mitigation in Cyber-Physical Power Systems. *IEEE Transactions on Power Systems*, **37**, 377-387. https://doi.org/10.1109/tpwrs.2021.3086681

[39] 武文博, 康锐, 李梓. 基于攻击图的信息物理系统信息安全风险评估方法[J]. 计算机应用, 2016, 36(1): 203-206.

[40] 李存斌, 张磊, 刘定, 等. 基于复杂网络的能源互联网信息物理融合系统跨空间风险传递研究[J]. 运筹与管理, 2019, 28(4): 139-147.

[41] 胡怡霜, 丁一, 朱忆宁, 等. 基于状态依存矩阵的电力信息物理系统风险传播分析[J]. 电力系统自动化, 2021, 45(15): 1-10.

[42] 陈天平, 许世军, 张串绒, 等. 基于攻击检测的网络安全风险评估方法[J]. 计算机科学, 2010, 37(9): 94-96.

[43] 龙门, 夏靖波, 张子阳, 等. 节点相关的隐马尔可夫模型的网络安全评估[J]. 北京邮电大学学报, 2010, 33(6): 121-124.

[44] 韩丽芳, 胡博文, 杨军, 等. 基于攻击预测的电力 CPS 安全风险评估[J]. 中国电力, 2019, 52(1): 48-56.

[45] 李冬冬, 王雄. 基于多阶段攻击的网络安全风险评估方法[J]. 通信技术, 2007, 40(11): 283-285.

[46] 王永杰, 鲜明, 刘进, 等. 基于攻击图模型的网络安全评估研究[J]. 通信学报, 2007, 28(3): 29-34.

[47] 王金芳, 郭渊博. 基于攻击图的物理信息系统网络安全风险评估[J]. 科学技术与工程, 2023, 23(28): 12175-12181.

[48] 罗新宇, 段斌, 吴俊锋, 等. 基于证据推理的风电场 SCADA 系统安全脆弱性定量评估方法[J]. 电力系统自动化, 2020, 44(11): 25-31.

[49] Lyu, X., Ding, Y. and Yang, S. (2020) Bayesian Network Based C2P Risk Assessment for Cyber-Physical Systems. *IEEE Access*, **8**, 88506-88517. https://doi.org/10.1109/access.2020.2993614

[50] Wu, C.S., Xie, W.Q., Ji, Y.X., *et al*. (2019) Survey on Network System Security Metrics. *Journal on Communications*, **40**, 14-31.

[51] 孙子文, 张书国. 工业信息物理系统安全风险动态表现分析量化评估模型[J]. 控制与决策, 2021, 36(8): 1939-1946.

[52] 刘鹏, 孙子文. 随机混合系统模拟物理状态的 ICPS 动态风险评估[J/OL]. 控制理论与应用: 1-9. http://kns.cnki.net/kcms/detail/44.1240.tp.20240229.1727.012.html, 2024-07-24.

[53] 高妮, 高岭, 贺毅岳, 等. 基于贝叶斯攻击图的动态安全风险评估模型[J]. 四川大学学报(工程科学版), 2016, 48(1): 111-118.

[54] 曾昆仑, 张尼, 李维皓, 等. 基于贝叶斯攻击图的网络资产安全评估模型[J]. 计算机科学, 2023, 50(12): 349-358.

[55] 方锡康, 周纯杰. 基于细胞自动机的电力 CPS 安全风险预测方法[J]. 信息技术, 2020, 44(10): 7-11, 18.

[56] Hu, B., Zhou, C., Tian, Y., Du, X. and Hu, X. (2023) Attack Intention Oriented Dynamic Risk Propagation of Cyberattacks on Cyber-Physical Power Systems. *IEEE Transactions on Industrial Informatics*, **19**, 2453-2462. https://doi.org/10.1109/tii.2022.3168774

[57] Li, B., Chen, Y., Huang, S., Yao, R., Xia, Y. and Mei, S. (2019) Graphical Evolutionary Game Model of Virus-Based Intrusion to Power System for Long-Term Cyber-Security Risk Evaluation. *IEEE Access*, **7**, 178605-178617. https://doi.org/10.1109/access.2019.2958856

[58] 崔鸣石, 张勇生, 杜娜, 等. 考虑节点异质性和故障函数的电力信息物理系统风险传播模型[J]. 科学技术与工程, 2023, 23(14): 6063-6073.

[59] 曲朝阳, 赵腾月, 张玉, 等. 基于渗流理论的电力 CPS 网络风险传播阈值确定方法[J]. 电力系统自动化, 2020, 44(4): 16-23.

[60] 张晶晶, 吴佳瑜, 齐先军, 等. 基于网络依存关系的 CPPS 连锁故障分析及风险评估[J]. 电力系统保护与控制, 2023, 51(5): 164-171.

[61] Cao, G., Gu, W., Li, P., Sheng, W., Liu, K., Sun, L., *et al*. (2020) Operational Risk Evaluation of Active Distribution Networks Considering Cyber Contingencies. *IEEE Transactions on Industrial Informatics*, **16**, 3849-3861. https://doi.org/10.1109/tii.2019.2939346

[62] Yan, K., Liu, X., Lu, Y. and Qin, F. (2023) A Cyber-Physical Power System Risk Assessment Model against Cyberattacks. *IEEE Systems Journal*, **17**, 2018-2028. https://doi.org/10.1109/jsyst.2022.3215591

[63] 梁皓澜, 刘东奇, 曾祥君, 等. 电力高级量测体系网络攻击致损路径图构建及风险评估[J]. 电力系统自动化, 2024, 48(12): 89-99.

[64] Ten, C., Yamashita, K., Yang, Z., Vasilakos, A.V. and Ginter, A. (2018) Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems. *IEEE Transactions on Smart Grid*, **9**, 4405-4425. https://doi.org/10.1109/tsg.2017.2656068

[65] Zeng, R., Cao, Y., Li, Y., Hu, S., Shao, X., Xie, L., *et al*. (2024) A General Real-Time Cyberattack Risk Assessment Method for Distribution Network Involving the Influence of Feeder Automation System. *IEEE Transactions on Smart Grid*, **15**, 2102-2115. https://doi.org/10.1109/tsg.2023.3302287