DOI:10.20033/j.1003-7241.(2025)10-0143-05

基于可视化技术的电力用户信息安全预警系统构建

曲 艺[1],徐 强[2],谢 青[2],周晓旭[1]
(1.国家电网有限公司客户服务中心,天津 300300;2.北京中电普华信息技术有限公司,北京 100031)

摘 要:在信息技术迅速发展的同时,许多技术的进展中存在未被有效解决的安全漏洞,甚至还存在一些尚未识别的安全隐患。为提升电力系统安全,对智能电网中的可视化技术进行研究,提出智能电网可视化系统的设计总体思路与原则。通过对电网中的主要功能进行分析,并构建用户信息安全预警系统。根据系统安全风险的预测值,实现对用户信息安全风险的预测功能。最后通过神经网络的风险动态评估算法,对用户信息进行持续的安全风险评估。结果显示,方法在风险预测中精确度达到了 0.9,且与实际值误差基本保持在 0.01 左右,证明了信息安全预警系统在可视化智能电网中,可以对信息系统的安全风险价值的整体水平进行预测,并作出了客观的定量分析,从而实现了对信息系统安全风险的有效的管理和控制。

关键词:智能电网;可视化技术;用户信息安全;预警系统;风险预测
中图分类号:TP393.08 **文献标志码**:A **文章编号**:1003-7241(2025)10-0143-05

Construction of information security early warning system for power users based on visualization technology

QU Yi[1], XU Qiang[2], XIE Qing[2], ZHOU Xiaoxu[1]
(1. State Grid Customer Service Centre, Tianjin 300300, China;
2. Beijing China Power Information Technology Co., Ltd., Beijing 100031, China)

Abstract: A long with the rapid development of information technology, there are many unresolved security vulnerabilities and even some unidentified security risks in the progress of technology. In order to improve the security of the power system, this paper firstly researches the visualization technology in the smart grid, and puts forward the general ideas and principles of the design of the smart grid visualization system. Then by analyzing the main functions in the power grid and constructing the user information security early warning system. According to the predicted value of system security risk, the prediction function of user information security risk is realized. Finally, through the risk dynamic assessment algorithm of neural network, continuous security risk assessment of user information is carried out. The results show that the accuracy of this paper's method in risk prediction reaches 0.9, and the error with the actual value basically stays around 0.01. It is proven that the information security warning system can predict the overall level of security risk value of information systems in a visualized smart grid, and make objective quantitative analysis, thereby achieving effective management and control of information system security risks.
Keywords: smart grid; visualization technology; user information security; early warning system; risk prediction

0 引言

随着科技的进步,信息技术已经被广泛应用于电力系统的各个方面,使得二者之间的联系变得更加紧密,从而为未来的智能电网提供了强大的支撑。随着信息技术向电力系统基础设施和应用领域的深入渗透,信息网络与电力系统紧密相连,并将在未来的智能电网中发挥关键作用。智能电网所固有的自动化、开放性和信息共享性,促使电网企业在部门间互动和市场交易中追求优化实时电网运行管理的目标[1-2]。然而,正是因为智能电网具备上述特性,也为其带来了信息安全方面的威胁。在信息技术迅速发展的同时,许多技术的发展中存在未被有效解决的安全漏洞,甚至还存在一些尚未识别的安全隐患。

目前,还没有完全了解信息网与电力网之间的联系及其产生的效果。由于它们之间的紧密联结,导致了一些严重的安全隐患。例如,恶意的攻击很容易导致大规模的断电[3-4]。通过研究之间的相互依赖发现,电力网更加倚重于信息网。随着技术的进步,智慧型电网的建设和应用变得越来越重要[5]。它不仅可以有效地控制和管理电源和负载,而且还可以有效地保护数据的完整性,避免数据的泄漏和丢失。为了确保智慧型电网的可靠运营,必须加强对信息安全的监管,确保其稳定可靠地运转[6]。

芦杉在分析影响网络信息安全主要因素的基础上,提出了基于 FAHP 的网络信息安全风险评估模型,并构建了评估指标体系,通过完成指标量化,指标权重确定,关联度计算等,为网络信息安全水平提供理论依据[7]。龙曼丽设计一种基于攻防博弈模型的网络信息安全防护系统,依据 CY8C24533 型号处理器,提高系统数据交换与数据处理

*基金项目:国家电网有限公司项目(SGKFYY00CHJS2310007)
收稿日期:2024-05-21

速度,通过外围底板增强系统的稳定性,并对网络信息安全评估。同时,设定权限管理机制,定义网络攻防博弈的一般策略形式为一个三元组,计算某一个网络区域内被攻击的路径与防御者应选取的防御策略,以此完成基于攻防博弈模型的网络信息安全防护[8]。王梦晓等提出大规模通信网络涉密信息安全动态预警算法,首先采用模糊聚类法处理网络涉密信息,得到相应的特征流量。其次根据样本估计理论确定出具有异常状态的特征流量区域,最后采取妥协率法构建决策者模型,通过对异常特征流量的风险要素排序,完成大规模通信网络涉密信息安全的动态预警[9]。贾若男等通过构建理论模型和收集实际数据验证模型,来对社交网络用户个人信息安全隐私保护行为的影响因素进行探究。并通过问卷调查获取数据,运用结构方程方法对模型的适用性进行检验[10]。胡周达等基于网状关联分析技术研究了一种新的电力监控网络信息安全智能预警方法,采集处理态势数据,在深入理解电力监控网络信息安全态势后,呈现感知结果,根据态势感知结果进行数据融合。深入挖掘网状关联规则,追踪电力网络安全信号,确定安全预警范围,建立关联矩阵,计算信号权重,分析指数变化,根据指数变化定位故障区域,实现安全预警[11]。崔日云等设计基于关键信息基础设施安全保护要求的风险管控流程,从风险识别与分析,技术安全保护,管理安全保护,预警处置等角度,提出关键信息基础设施的信息安全风险管控方法,并给出风险报告示例[12]。张宁选用贝叶斯网络技术作为信息安全预警模型的基础,通过聚类算法对攻击网络信息样本进行计算,对攻击网络信息样本进行分类,实现攻击网络信息样本的自适应分类。根据贝叶斯网络模型结构,建立网络输入输出误差函数,实现对贝叶斯网络模型参数的调整,从而实现对网络信息安全的预警[13]。吴哲翔介绍了智能电网信息安全交互特点,通过对智能电网信息安全交互隐患的分析,讨论模型构建关键技术,并结合量子通信及 IPv6 网络结构优化对用户安全系统进行探索[14]。

本文首先基于可视化技术,对智能电网的主要功能与操作进行分析。并构建了一种用户信息安全预警系统,实现针对未知攻击的在线检测。以电网的实时运行状态信息为数据基础,然后通过构建模糊风险评估模型,计算出在某一时段的风险态势变化曲线,并筛选出信息安全指标类型。最后在实践分析中,通过风险预测、信息安全挖掘、系统多样性检测来验证本文方法的有效性,证明了信息安全预警系统在可视化智能电网中,可以对信息系统的安全风险价值的整体水平进行预测,并作出了客观的定量分析,使得风险度的评估结果更为可靠。

1 智能电网结构

通过先进的计算机技术,可视化系统将给用户带来一个完全模拟的虚拟世界。在这个模拟世界里,不仅可以轻松地进行各种操控,还可以查看配电网络及其他电力系统的总体情况,比如温度、负载的变动,甚至是一些突发的故障报警[15-16]。调度人员可根据配电设备的温度等运行信息,评估对配电网络线路运行的潜在影响,为调节和优化配电网络运行提供数据支持。可视化智能电网架构如图 1 所示。建立的可视化智能电网拥有五大模块:动态监测、环保监督、自主操作、维护管理以及资产全寿命周期管理,综合性功能使得信息的传输变得更加便捷、高效。在辅助控制系统中,客户端显示了来自各子系统收集的数据。且工作人员通过控制该辅助系统设备接口,而后台可以根据接收到的数据定制相应的响应方案,以做出最后的判断。除此之外,为了获取更高效的操作,电网系统可以自动连接不同的子系统,并对各种监测数据和事件信息进行综合评估。通过评估结果决定变电站的日常运行决策。包括自动控制可控设备或子系统维护方面的智能水平。

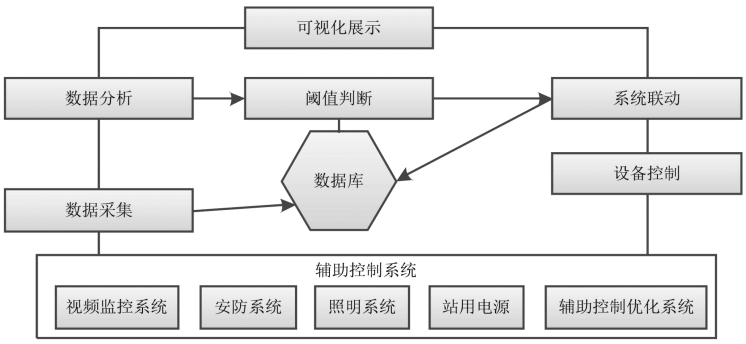

图 1 可视化智能电网架构

2 构建用户信息安全预警系统

2.1 系统构建

由于其卓越的可靠性、安全性和环保性能,我国已将智能电网确定为关键的战略发展目标。应用可视化技术,实现了智能电网设备与用户之间的实时双向的信息交流形式。并且调度员可以根据图形的变化及时发现电网问题与安全态势的变化。但由于用户与电网系统之间的频繁认证与信息采集等行为的发生,会导致新的安全隐患发

生[17-18]。用户信息安全预警系统如图 2 所示，本文开发了一个用户信息安全预警系统。该系统可以收集和传输有关的遥感、遥信信号和通信流量信息，并利用规律性的入侵检测技术来快速准确地发现可疑的威胁。此外，还可以利用异常的入侵检测技术，快速地将潜藏的威胁转化为可控的信息，从而有效地防止可疑的威胁。根据收集到的攻击信息以及可能存在的异常情况，风险评估模块会评估事故的可能性以及事故的危险性。随后，系统会根据这些信息，结合相应的防御策略，经过多维度的优化，以确定出最有效的应急措施。最终，系统会向用户传达相关的操作命令，以便有效地管理配电网。

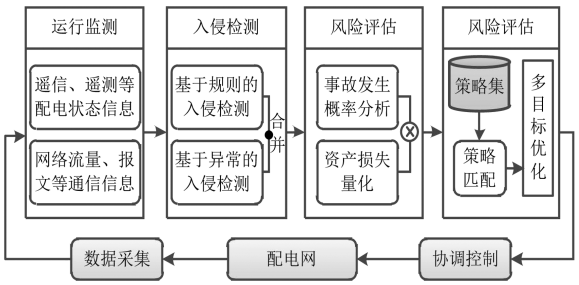

图 2　用户信息安全预警系统

智能电网中，智能电表记录用户的实时用电数据，并周期性地上报配电系统。而且，智能电表通过单跳链路与一个配电系统单元相连。因此，网络结构可以表示为 $S=\{v_1,v_2,\cdots,v_n\}$，S 表示一个地区内的所有智能电表的集合，$S_i(i=1,2,\cdots,k)$ 表示为 S 的所有非空子集，则满足的条件为

$$\bigcup_{i=1}^{i=k} S_i = S \text{ and } \bigcap_{i=1}^{i=k} S_i = \varnothing \tag{1}$$

式中，$i=1,2,\cdots,k$，所有在子集 S_i 中的智能电表直接向某个固定的配电单元传输数据。

2.2　用户风险感知预测

通过对电网信息系统的实时工况信息的收集和分析，可以更好地预测出可能存在的安全风险[19]。因此，在开展风险预测之前，必须确保电网信息系统的运行状态处于良好的状态，以便提供有效的数据支撑。

通过配备状态信息收录机，可以对电力线路的各种参量进行实时监测，以便及时发现可能出现的危害，并且有效地防止可能出现的安全隐患。利用信号运行的频谱用作安全风险的定义，即

$$Z(f)=\begin{cases}2S(f), & f>0\\ S(f), & f=S(f)[1+H(f)]=0\\ 0, & f<0\end{cases} \tag{2}$$

式中，函数 $H(f)$ 代表一个电力系统设备最大振动范围。这个函数的取值随着设备的性能和能耗而变化，它的参数也会随着设备的性能而改变。通过使用自适应匹配技术，能够将收到的运行状态信息进一步分析，从而生成一个风险函数 $H(f)$，这个函数的参数设置在设备的最大振动范围内，则在 1、0 和−1 之间。可以据此得出相应的网络信息系统运行状态以及风险函数 $K(t)$，计算公式为

$$K(t)=\frac{w\times e^{\varphi}}{Z(f)} \tag{3}$$

式中，电力线路的采样数据的输入结构为 w，并且还可以获得与之匹配的随机频率 ϑ。

假设电网信息系统的运行状态可以通过分类来获取，而这些数据集 T 中包含 m 组交互式概率矩阵，参数的值 $\boldsymbol{T}_m$ 可能随着特定条件 A_n 的改变而发生变化。因此，为了实现数据的标准化，可以采用公式(4)来进行处理，即

$$\boldsymbol{l}'_{mn}=\frac{100\times(\max(l_n)-l_{mn})\boldsymbol{T}_m}{\max(l_n)-\min(l_n)}\times k(t) \tag{4}$$

式中，$\max(l_n)$ 和 $\min(l_n)$ 分别表示数据的聚类特征的最高或者最低水平，通过 $\boldsymbol{M}$ 代表交互式适应度函数，为

$$\boldsymbol{M}=\frac{\max(l_n)q}{\min(l_n)\chi^2}\times l'_{mn} \tag{5}$$

式中，偏移量 q 和聚类因子 χ 被用来描述数据的聚类分析。通过采用系统稳定性预测指标，可以准确地衡量数据传输的稳定性，其中包括风险指标 w_{ss}，计算公式为

$$w_{ss}=\frac{\int_0^t \left| M\times W_{\text{total}}\right| \mathrm{d}t}{W_b} \tag{6}$$

式中，可以计算出电网系统的运行时长 t，以及稳定性指数 W_b 和总输出指数 W_{total}。

通过采取多种指标，如风险预测指数、指数权重等，可以准确地预测电力公司的信息系统的安全性，并且可以有效地防范可能发生的威胁。本研究通过深入探究 3 个主要领域，即系统网络攻击、用户行为以及系统硬件设施故障，以期达到预测的目的。使用这个方法，能够得出一个关于系统安全的总体公式，为

$$R=\frac{V_{ij}\times A\times T_s}{T_f}V \tag{7}$$

式中，能够准确地估算出各种因素对于信息资产 A、网络攻击 T_s、用户行为 T_f 和硬件设备的潜在危害 V。这些因素共同决定了整个系统进行有效的安全风险评估的指标。

2.3　信息安全风险评估

为了实现动态风险评估，需要收集大量有用的网络数据，以确保其准确性和可靠性。并利用神经网络算法对安全风险进行持续评估，以便后续可以在不同的时期计算出动态变化趋势。本文提出了一种新的模型，它能够有效地评估威胁场景下的风险。该模型通过将输入指标划分为 12 个部分，并使用 $I_1\sim I_{12}$ 来表示每个部分的具体内容，如表 1 所示。这些指标分别代表攻击成功概率 P、影响程度 E 和不可控性 T。

通过使用层次分析法，可以计算出各个指标的权重。这些权重可以通过建立矩阵 B 来进行计算。计算公式为

表 1 信息安全风险指标

代码	风险指标	代码	风险指标
I_1	威胁动机	I_7	完整性影响
I_2	攻击能力	I_8	可用性影响
I_3	攻击复杂度	I_9	关联影响度
I_4	漏洞利用率	I_{10}	隐蔽性检测能力
I_5	资产吸引力	I_{11}	多样性检测能力
I_6	机密性影响	I_{12}	突防抵御能力

$$\boldsymbol{B}=\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix} \tag{8}$$

式中，b_{ij} 可以根据上一层指标 $\boldsymbol{B}_i$ 的结果来计算下一层指标 $\boldsymbol{B}_{i+1}$ 的相对重要性。并计算的特征向量 $\boldsymbol{M}$，为

$$\boldsymbol{M}=(m_1,m_2,\cdots,m_n) \tag{9}$$

式中，$m_i=\sqrt[n]{b_{i1}b_{t2}\cdots b_{in}}$ 指标相对权重集是通过对特征向量 M 进行处理得到的，即

$$W=(w_1,w_2,\cdots,w_n) \tag{10}$$

式中，$w_i=m_i/\sum_{i=1}^{n}m_i$，计算矩阵最大特征根 $\lambda_{\max}$，得

$$\lambda_{\max}=\sum_{i=0}^{n}\frac{(BW)_i}{nw_i} \tag{11}$$

对判断矩阵进行一致性检验，即

$$C=\frac{\lambda_{\max}-n}{n-1} \tag{12}$$

通过加权平均法，可以计算出安全风险度 R。这种方法将隶属度作为权重系数 b_i，并将评语集 V 分成不同的等级 $H_V=\{h_1,h_2,\cdots,h_n\}$。随着等级 v_i 的提升，风险度 h_i 也会相应提高，最终可以得出

$$R=\frac{\sum_{i=1}^{n}h_i\times b_i}{\sum_{i=1}^{n}b_i} \tag{13}$$

信息安全的风险值是对各层权重值进行排序后，选出顶层的权重乘积之和，为

$$W'=WW_g \tag{14}$$

每个信息安全事件的风险值可通过式计算实现，为

$$W_j'=\sum_{j=1}^{j}W_jW_{gj} \tag{15}$$

式中，W_j 与 W_{gj} 分别代表为准则层的数目和权值。

利用各信息事件的风险值来确定影响较大的安全事件，并采取必要措施加以控制。

3 用户信息安全预警系统实践分析

3.1 风险预测

为了测试用户信息安全预警系统是否实现了设计目标，在电网信息系统环境中，设计并进行测试实验，以验证系统的效果和性能。为了准确评估两个电网的安全风险，需要将它们放置于完全一致的环境条件下，并采取直流配置，其中 220 V 的电源，2 %的总谐波畸变，3.5 kBaud 的电网信号传输速度，以及 0 到 90 dB 的带宽。经过一系列的试验，发现两种模型的风险预测能力有显著的差异。通过数据分析和实证检查，来衡量这两种模型的精度。图 3 为实验结果。随着科技的发展，新一代的智慧电力用户信息安全预警系统可以有效地减少传统安全风险预测模式所带来的巨大偏差，其精度误差可以保持在 0.01 左右，这个数据显著优于以往的方法。经过本次研究得出结论：采用本文的模型，不仅可以大大改善预测精度，还能有效地减少系统的安全隐患，从而极大地增强了整个系统的安全性和稳健性。此外，还采取了可视化技术，搭建了一个智慧的电力网络，以便及早发现、识别并处理各种危机，并且及早采取应急措施。通过考虑到相关财富的重要性，建立起一套完善的风险管理体系，以预测和防范各类安全事故，从而确保企业的信息安全。

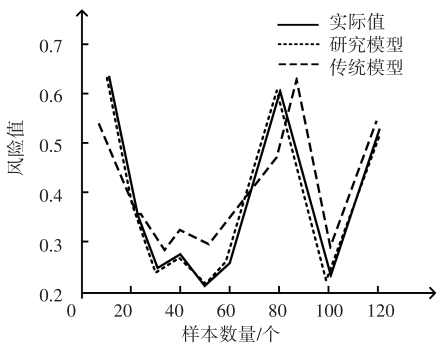

图 3 预测准确率比较

为了能够了解该模型在信息安全风险管理中预测的效果，将决策树模型和 SVM 模型分别对相同数据建模，并进行 6 折交叉检验，最终得出平均精确度、召回率和 F_1 值如表 2 所示。从三种方法的预测结果对比来看，本文方法有更高的精确度，在召回率上和其他算法相差无几。根据三种方法的对比结果显示，基于可视化技术的智能电网在信息安全风险管理的预测中，召回率与 F_1 值分别达到 0.85 与 0.84，确保了安全预警系统的正确性和时效性。同时，精确度达到了 0.9，提高了用户信息安全风险预测能力。说明了在智能电网中，通过引入基础的用户信息安全预警系统，不仅可以准确地评估电网的故障状态，而且还可以实时监控和评估各种潜在的危害因素，从而更好地保护和改善电力系统的稳定性和可靠性。

表 2 交叉检验结果

预测模型	精确度	召回率	F 值
决策树模型	0.73	0.82	0.8
SVM 模型	0.82	0.81	0.82
可视化模型	0.9	0.85	0.84

3.2 信息安全挖掘

通过模拟，可以发现该方法可以有效地检测和评估无

线异构多数据传感蜂窝网络系统的安全危险性。本文将样本量调整至 1 200,并调整网络信息的采集频率至 2.4 ms,以此来评估该技术的可靠性。经过这一过程,获取的信息挖掘结果见图 4。经过深入研究发现,当使用 80 个不同类型的无线异构多传感蜂窝网络时,其相互之间会有 0.32 的相似程度。利用这一特征,制定出一个用于衡量网络系统中潜在风险的模型,以便准确地判断出哪些是重大、哪些是潜在危害、哪些是脆弱性,从而提高了经营风险检测的效率。

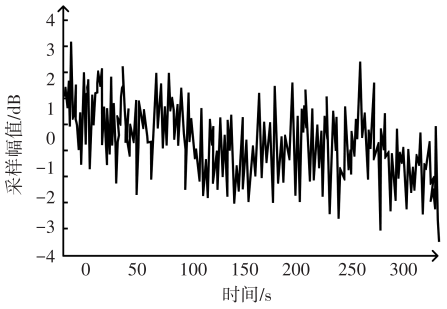

图 4 信息挖掘结果

3.3 多样性检测

经过系统性的研究,可以确信采用本文提出的评估方法可以有效地检测出用户隐私信息安全的风险。为了更好地反映实际情况,采取了二次模糊化的措施,以减少主观因素对评估结果的不利影响。因此本文对传统电网系统与可视化智能电网系统进行编码检测,通过设定不同的迭代次数后,观测 2 种系统风险检测误差与运行时间的对应关系。表 3 为编码检测结果,当节点数增加时,2 种系统的误差值与运行时间也随之变化。当编码节点达到 35 时,传统电网系统检测误差值达到了 0.154 3,而可视化智能电网系统误差值为 0.143 7,运行时间仅需 0.88 s。说明在用户信息多样性检测中,本文方法可以将误差值缩减至最小,且系统运行效率保持最高。并针对在满足复杂网络环境下的应用需求,对风险效益进行深入分析,以提升评估的准确性。此外,还建立一个风险要素的模型,来更好地评估用户隐私信息安全的风险,并将其作为未来研究的重点。

表 3 编码检测结果

节点数	传统电网系统	可视化智能电网系统	
	误差	运行时间/s	误差
5	0.045 5	0.05	0.036 9
10	0.069 8	0.28	0.063 3
15	0.072 2	0.45	0.068 9
20	0.070 9	0.52	0.053 3
25	0.066 9	0.63	0.042 6
30	0.118 9	0.98	0.105 5
35	0.154 3	0.90	0.143 7

4 结束语

本文通过对可视化智能电网进行研究,构建了用户信息安全预警系统,通过构建风险动态评估模型,对该系统进行实践检测。结论如下:(1) 在用户信息安全检测中,本文构建的系统预测风险值与实际值基本相同,且误差基本保持在 0.01 左右,精确度达到了 0.9。通过科学、合理的方法,可以准确地预测电网信息系统的故障情况,并全面、客观地评估电网的风险。(2) 信息安全挖掘与多样性检测中,信息安全风险评价的关联系数为 0.32。系统运行时间仅需 0.88 s,且编码数达到最高时误差值仅为 0.143 7。提高了智能电网预警的可靠性和及时性,有效保障电网的安全运行。

参考文献

[1] 程杉, 黄悦华, 王凌云, 等. IIP 型智能电网信息工程新工科专业人才培养的探索与实践[J]. 中国电机工程学报, 2021, 41(23): 8250-8258.
[2] 王昕, 周育忠, 石家豪, 等. 基于 WebGIS 的智能电网信息标准化管理系统设计[J]. 自动化技术与应用, 2024, 43(4): 159-163.
[3] 周雄. 智能电网建设中电气工程及其自动化技术的探究[J]. 今日自动化, 2021(12): 2.
[4] 杨云华. 大数据背景下的智能电网信息安全防护[J]. 计算机应用文摘, 2023, 39(12): 216-218.
[5] 严昭. 智能电网云数据储存平台次月留存数据聚类方法[J]. 自动化技术与应用, 2023, 42(5): 176-179.
[6] 李慧. 基于主被动防御结合的智能电网信息安全防护体系研究[J]. 工程技术研究, 2021, 3(10): 157-158.
[7] 芦杉. FAHP 和物元模型在网络信息安全风险评估中的应用[J]. 电子世界, 2021(11): 176-177.
[8] 龙曼丽. 基于攻防博弈模型的网络信息安全防护系统设计[J]. 现代电子技术, 2021, 44(4): 115-118.
[9] 王梦晓, 刘学军, 操凤萍. 通信网络用户涉密信息安全动态预警仿真[J]. 计算机仿真, 2023, 40(5): 422-425.
[10] 贾若男, 王晰巍, 范晓春. 社交网络用户个人信息安全隐私保护行为影响因素研究[J]. 现代情报, 2021, 41(9): 105-114.
[11] 胡周达, 隆运鸿, 许丰, 等. 基于网状关联分析的电力监控网络信息安全智能预警方法[J]. 现代电子技术, 2023, 46(3): 69-74.
[12] 崔日云, 付晓丹. 基于关键信息基础设施安全保护要求的风险管控研究[J]. 铁路计算机应用, 2023, 32(11): 11-14
[13] 张宁, 范海涛. 基于贝叶斯网络的信息安全预警模型[J]. 微型电脑应用, 2022, 38(6): 135-138.
[14] 吴哲翔, 邵航军, 金旭. 智能电网信息安全交互模型及关键技术分析[J]. 电工技术, 2021(15): 127-128.
[15] 王岚岚, 林耳. “电工鲁师傅”配电故障抢修沟通法的应用与实施[J]. 企业管理, 2017(S1): 236-237.
[16] 翁冬凤. 面向智能电网应用的电力大数据三维场景可视化技术研究[J]. 城市建筑空间, 2022, 29(S01): 181-182.
[17] 王宁, 田家英, 董宁, 等. 基于改进 SVM 的智能电网调控系统实时风险评估与预警技术[J]. 沈阳工业大学学报, 2022, 44(1): 7-13.
[18] 夏盛海, 杨攀, 罗宇. 智能电网调控技术支持系统中设备监控大数据分析研究[J]. 现代工业经济和信息化, 2022, 12(7): 114-116.
[19] 曾颖, 武斌, 田宁姗. 基于云模型和改进证据理论的电力监控系统风险评估[J]. 计算机系统应用, 2022, 31(8): 55-63.

作者简介:曲 艺(1986—),男,硕士,高级工程师,研究方向:电力营销,营销信息化,大数据。