DOI:10.20033/j.1003-7241.(2025)06-0051-05

基于边缘计算的电力网络安全威胁等级评估研究

陈 雪，林奕夫

（国网福建省电力有限公司经济技术研究院，福建 福州 350013）

摘 要：为准确对电力网络安全威胁等级进行评估，研究基于边缘计算的电力网络安全威胁等级评估方法。首先利用电网数据采集单元实时采集数据，由边缘计算处理与分析单元处理与分析采集数据，并将其存储至边缘云存储单元中；然后利用中心云调用存储数据，建立电网安全威胁等级评估体系；最后利用改进最小叉熵法计算各指标权重，结合模糊综合评判法获取电网安全威胁等级评估结果。实验结果表明，该方法可有效采集电网有效数据，实现电网安全威胁等级评估，构建指标体系的对比强度较高、冲突性较小，指标构建效果较优。

关键词：边缘计算；电力网络；安全威胁；等级评估；最小叉熵法；模糊综合评判

中图分类号：TP393.08　　文献标识码：A　　文章编号：1003-7241(2025)06-0051-05

Research on Security Threat Level Assessment of Power Network based on Edge Computing

CHEN Xue, LIN Yi-fu

(State Grid Fujian Electric Power Co., Ltd., Economic and Technological Research Institute, Fuzhou 350013, China)

Abstract: In order to accurately evaluate the power network security threat level, an edge computing-based power network security threat level evaluation method is studied. First, it uses the power grid data acquisition unit to collect data in real time, and then uses the edge computing processing and analysis unit to process and analyze the collected data, and stores it in the edge cloud storage unit, then uses the central cloud to call the stored data to establish a power grid security threat level assessment system. Finally, the weight of each index is calculated by the improved minimum cross entropy method, and the evaluation result of power grid security threat level is obtained by combining with the fuzzy comprehensive evaluation method. The experimental results show that the method can effectively collect the effective data of the power grid and realize the assessment of the security threat level of the power grid. The index system constructed by this method has high contrast intensity and less conflict, that is, the index construction effect is better.

Keywords: edge calculation; power network; security threat; grade evaluation; minimum cross entropy method; fuzzy comprehensive evaluation

0 引言

电力通信网络是保证电网设备安全运行的基础，其主要负责传输电力控制及调度等指令[1]。电网的安全将直接影响指令的传输效果，即对电网的安全运行造成较大影响。为保证电网安全运行，应对其实现实时监测，即建立科学的安全威胁等级评估体系，通过对数据及时分析，科学评估电网的运行状态，来保证电网运行的稳定和安全[2]。近年来，我国众多学者开展此项研究，得到一定研究成果。如何永贵等人通过融合改进层次分析法与熵值法获取电力物联网安全风险评估指标的权重，结合云模型完成电力物联网安全风险评估，该方法可有效评估电力物联网安全风险，为电力物联网建设提供参考依据[3]。高翔等人通过灰色关联分析法求解电网评估指标权重，通过支持向量机构造评估模型完成电网安全态势评估，该方法可有效评估电网安全态势，具备较优的应用价值[4]。这两种均无法实时采集电网数据，导致评估指标体系构建的全面性较差、精度较低，影响评估效果。边缘计算具备较低的网络通信成本，且具有数据采集速度快、安全性高等优势，在各行各业均有广泛应用[5]。为此，基于边缘计算研究电网安全威胁等级评估方法，希望可实现对电网的科学评估，为促进电网安全提供参考。

1 电网安全威胁等级评估方法

1.1 安全威胁等级评估架构

依据边缘计算具有较强的数据采集与分析处理能力，研究电网安全威胁等级评估方法，该方法的技术架构如图 1 所示。在电网中接入边缘接口及相关设备用于感知电网的实时状态，实现电网结构间的数据通信；利用原

*基金项目：国家电网公司总部科技项目（SGFJJY00SJJS2200014）

收稿日期：2023-12-15

有的电网数据采集单元，实时采集电网数据，通过数据边缘处理单元去除数据内的噪声，利用数据边缘分析单元分析数据间的关系[6]，并将其转入存储单元之中；依据智能分析后的电网数据，提取电网安全评估指标，利用改进最小叉熵法计算各指标权重，结合模糊综合评判法，获取电网安全威胁等级评估结果；评估结果发布及预警单元可实时呈现电网安全评估结果，并在威胁等级较高时进行预警，工作人员可根据预警结果，制定维修策略，确保电网安全。边缘计算中需利用隔离技术，保证电网安全威胁等级评估过程的稳定性，该技术负责隔离边缘云内电网数据采集、处理与智能分析过程，令三个过程互不干扰，实现隔离处理，各单元的访问需要不同权限。边缘计算中还需要利用安全技术，保证电网数据不会泄露，应用该技术可防止因攻击入侵导致电网数据泄露。

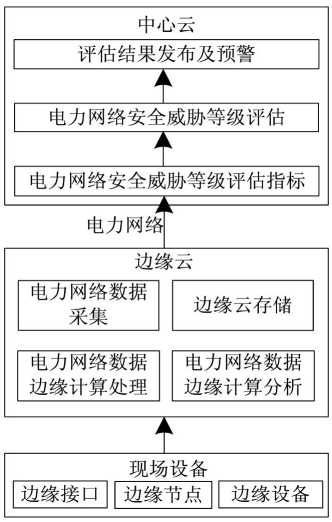


图1　电网安全威胁等级评估技术架构

1.2　电网数据采集与处理

利用电网数据采集智能网关实时采集有效电网数据，电网数据采集与处理分析过程如图2所示。按照电网安全防护规定，在电网各区域间安装横向隔离网闸，确保各电网区域间彼此不影响，通过电网数据采集智能网关实时采集有效电网数据，通过电网数据智能转发网关，将采集的有效电网数据转发至边缘云存储单元内，电网数据处理与智能分析单元，通过调用边缘云存储单元内采集的原始电网数据流，对其进行处理与分析，再将经过边缘计算处理与分析后的电网数据流，传输至边缘云存储单元内。经过边缘计算处理与分析后的电网数据，通过消息队列遥测传输(message queuing telemetry transport，MQTT)监听程序对其展开传输和收集，利用下载程序将该电网数据，下载至中心云内，由中心云展开电网安全威胁等级评估指标构建、评估与发布及预警。电网数据采集与处理过程中使用104协议，确保电网数据采集的稳定性；在智能网关内设置断点续传功能，确保电网数据断点续传情况下，电网数据依旧能够实时传输。通过优先级划分电网实时数据，防止电网数据较多，造成高优先级电网实时数据发送不及时问题出现。

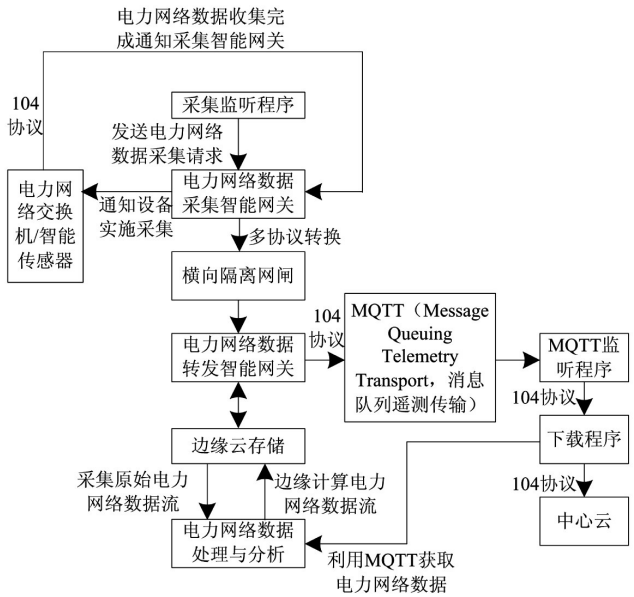


图2　电网数据采集与处理分析过程

1.3　安全威胁等级评估指标的提取

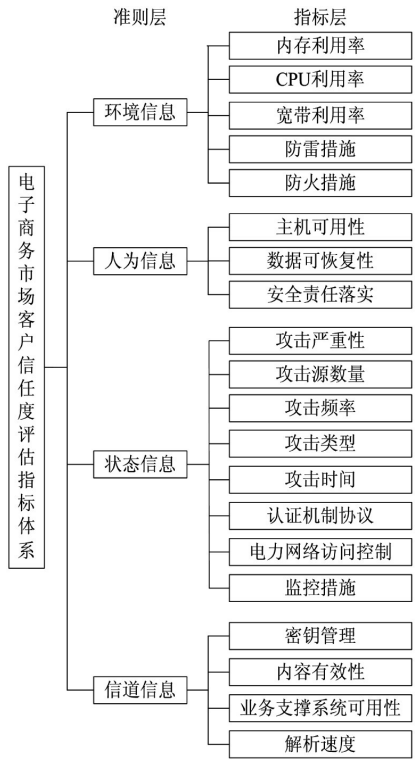


图3　电网安全威胁等级评估指标体系

依据经过边缘计算处理与分析后的电网数据，建立电网安全威胁等级评估指标体系，评估指标体系构建结果如图3所示。电网安全威胁主要包含环境信息、人为信息、状态信息与信道信息等四个方面的信息，环境信息内

的主要指标为带宽利用率，该指标用于衡量电网承受攻击过程中的威胁程度；人为信息主要用于描绘主机状态与人员管理情况；状态信息包含电网受到攻击时不同状态；信道信息用于描绘电网传输数据时的情况。

1.4 基于模糊综合评判法的电网安全威胁等级评估

利用二级模糊综合评判法，针对电网安全威胁等级评估指标体系，完成电网安全评估。令电网安全评估指标的因素集为 U，按照电网安全评估指标属性，综合评估某一类准则层因素集[7]，再对评估结果展开类元素的高层次综合评估。令 $U=\{U_1,U_2,\cdots,U_N\}$，使其符合 $U=\bigcup_{i=1}^{N}U_i$，其中，电网安全威胁等级准则层评估指标数量是 N，编号是 i。在 $i\neq j$ 情况下，$U_i\cap U_j=\varnothing$；其中，第 i、j 个电网安全威胁等级准则层评估指标是 U_i、U_j；空集是 $\varnothing$；对 $\forall i\in\{1,2,\cdots,N\}$ 存在 $U_i\neq\varnothing$。令 $U_i=\{u_{i1},u_{i2},\cdots,u_{i3}\}$ 是 U 的因素子集，第 i 个准则层因素子集内存在的指标层因素(电力安全评估指标)数量是 k_i。

电网安全威胁等级评估的评语集是 $V_i=\{v_{i1},v_{i2},\cdots,v_{in}\}$；评语集数量是 n；U_i 内各因素(电力安全评估指标)对于 V_i 的权重系数是 $W_i=\{w_{i1},w_{i2},\cdots,w_{ik_i}\}$，代表电网安全威胁等级评估时，某指标的相对重要程度；U_i 的 k_i 个因素(电力安全评估指标)对 V_i 的模糊评估矩阵是 R_i，选取一个一级模型对 U_i 展开模糊综合评估，公式如下：

$$B_i=W_iR_i=(b_{i1},b_{i2},\cdots,b_{in}) \tag{1}$$

式中，第 i 个电网安全威胁等级准则层评估指标的评估结果是 B_i。

U 的二级模糊评估矩阵如下：

$$\boldsymbol{R}=\begin{pmatrix}B_1\\B_2\\\vdots\\B_M\end{pmatrix}=\begin{pmatrix}W_1R_1\\W_2R_2\\\vdots\\W_MR_M\end{pmatrix} \tag{2}$$

式中，电网安全威胁等级指标层评估指标数量是 M。

依据 $\boldsymbol{W}$ 与 $\boldsymbol{R}$ 获取 U 的评估结果，即电网安全威胁等级评估结果 $\boldsymbol{B}=\boldsymbol{WR}=(b_1,b_2,\cdots,b_M)$，按照最大隶属度判决法，将最大隶属度对应的指标等级，当成电网安全威胁等级最终评估结果。电网安全威胁等级取值区间如表 1 所示。

表 1 电网安全威胁等级取值区间

威胁等级	数值
高	(60,100]
中	(30,60]
低	[0,30]

利用改进最小叉熵法确定各电网安全评估指标的权重 W，通过熵权法求解电网安全评估指标的客观权重 $w_h=(w_{h,1},w_{h,2},\cdots,w_{h,M})$，第 l 个指标的客观权重如下：

$$w_{h,l}=\frac{1+\dfrac{\sum_{i=1}^{N}\left(z_{il}\Big/\sum_{i=1}^{N}z_{il}\right)\ln\left(z_{il}\Big/\sum_{i=1}^{N}z_{il}\right)}{\ln N}}{\sum_{l=1}^{M}\left[1+\dfrac{\sum_{i=1}^{N}\left(z_{il}\Big/\sum_{i=1}^{N}z_{il}\right)\ln\left(z_{il}\Big/\sum_{i=1}^{N}z_{il}\right)}{\ln N}\right]} \tag{3}$$

式中，第 i 个准则层内第 l 个电网安全评估指标的决策结果是 z_{il}。

通过效用函数代表各主观权重确定决策者的分析结果，电网安全评估指标主观权重确定步骤如下：

步骤 1：生成一个代表因专家 c 对电网安全评估指标主观认知不同，出现差异的效用函数矩阵 $\boldsymbol{Y}_c$，令 $\boldsymbol{Y}_c=(y_c(z_{il}))$，$c=1,2,\cdots,C$，$\boldsymbol{Y}_c$ 内的效用函数是 y_c；专家数量是 C。

步骤 2：按照 $\boldsymbol{Y}_c$，通过熵权法获取各专家对电网安全评估指标主观权重判断矩阵 $\boldsymbol{X}=(x_{cl})$，计算公式如下：

$$x_{cl}=\frac{1+\dfrac{\sum_{i=1}^{N}\left(y_c(z_{il})\Big/\sum_{i=1}^{N}y_c(z_{il})\right)\ln\left(y_c(z_{il})\Big/\sum_{i=1}^{N}y_c(z_{il})\right)}{\ln N}}{\sum_{l=1}^{M}\left[1+\dfrac{\sum_{i=1}^{N}\left(y_c(z_{il})\Big/\sum_{i=1}^{N}y_c(z_{il})\right)\ln\left(y_c(z_{il})\Big/\sum_{i=1}^{N}y_c(z_{il})\right)}{\ln N}\right]} \tag{4}$$

步骤 3：以 $\boldsymbol{X}$ 为基础，通过熵权法获取决策专家权重向量 $\boldsymbol{\omega}$，避免最小叉熵法内的决策专家权重模糊性，影响主观权重确定结果。决策专家 c 的权重向量为：

$$\varpi_c=\frac{1+\dfrac{\sum_{l=1}^{M}\left(x_{cl}\Big/\sum_{c=1}^{C}x_{cl}\right)\ln\left(x_{cl}\Big/\sum_{c=1}^{C}x_{cl}\right)}{\ln M}}{\sum_{c=1}^{C}\left[1+\dfrac{\sum_{i=1}^{N}\left(x_{cl}\Big/\sum_{c=1}^{C}x_{cl}\right)\ln\left(x_{cl}\Big/\sum_{c=1}^{C}x_{cl}\right)}{\ln M}\right]} \tag{5}$$

步骤 4：建立以综合主观权重 $\boldsymbol{\omega}_h$ 和 $\boldsymbol{\omega}_c$ 距离 D 最近的最小叉熵模型，获取电网安全评估指标的综合主观权重 $\boldsymbol{\omega}_h=(\boldsymbol{\omega}_{h,1},\boldsymbol{\omega}_{h,2},\cdots,\boldsymbol{\omega}_{h,M})$，公式如下：

$$\begin{cases}\min D=\sum_{c=1}^{C}\lambda\varpi_cD_c(\omega_h,\omega_c)\\ s.t.\sum_{l=1}^{M}\omega_{h,l}=1\quad\omega_{h,l}\geq0\end{cases} \tag{6}$$

式中，可调节因子是 λ；ω_h 与 ω_c 间的距离是 $D_c(\omega_h,\omega_c)$。

第 l 个电网安全评估指标主观权重如下：

$$\omega_{h,l}=e^{\lambda\varpi_c\sum_{c=1}^{C}\ln x_{cl}}\Big/\sum_{l=1}^{M}e^{\sum_{c=1}^{C}\lambda\varpi_c\ln x_{cl}} \tag{7}$$

依据分配系数 θ，融合电网安全评估指标的客观与主

观权重，第 l 个电网安全评估指标的综合权重如下：

$$w_l = \frac{\omega_{h,l}^{\theta_l} w_{h,l}^{1-\theta_l}}{\sum_{l=1}^{M} \omega_{h,l}^{\theta_l} w_{h,l}^{1-\theta_l}} \tag{8}$$

式中，第 l 个电网安全评估指标权重分配系数是 θ_l。

2 实验结果与分析

以某市级电业局的电网为研究对象，该电网内共包含 10 个 IP 网络主机，利用本文方法评估该电网安全威胁等级，验证本文方法威胁等级评估的可行性。

为该电网内共设置 11 次攻击，攻击类型分别是 DoS 与 DDoS，利用本文方法实时采集该电网数据，部分电网状态信息数据采集结果如表 2 所示。根据表 2 可知，实时采集到的攻击次数为 11 次，攻击类型分别是 DoS 与 DDoS，与实际情况相符，说明本文方法可精准实时采集电网数据，为后续构建电网安全评估指标体系提供较好的服务。

表 2 部分电网状态信息数据采集结果

攻击时间点	源地址	目的地址	攻击严重性	攻击类型
8:28:33	200.192.9.0	183.27.2.118	2 692	DoS
10:22:07	25.212.16.159	183.27.2.112	2 633	DDoS
10:22:07	25.212.16.159	183.27.2.116	2 283	DDoS
10:22:07	25.212.16.159	183.27.2.118	2 881	DDoS
11:05:17	196.227.163.115	183.27.2.122	5 699	DoS
11:05:17	196.227.163.115	183.27.2.100	25 996	DoS
15:42:21	140.96.35.0	183.27.2.102	2 839	DDoS
15:42:21	140.96.35.0	183.27.2.106	3 999	DDoS
15:42:21	140.96.35.0	183.27.2.108	7 998	DDoS
15:42:21	140.96.35.0	183.27.2.109	2 941	DDoS
15:42:21	140.96.35.0	183.27.2.123	39 598	DDoS

利用本文方法计算各电网安全评估指标的权重与威胁等级，计算结果如表 3 所示。根据表 3 可知，结合表 1 的威胁等级取值区间得知，该电网中环境信息与人为信息的威胁等级均为低威胁；状态信息中仅有攻击时间、电网访问控制与监控措施的威胁等级评估结果为低，其余指标的等级评估结果均为中、高威胁，按照最大隶属度原则，状态信息的评估等级为高威胁；信道信息内仅有解析速度的评估等级为低威胁，其余两个指标的评估结果均为中威胁，按照最大隶属度原则，信道信息的评估结果为中威胁；综合分析可知，该电网安全等级评估结果为高威胁，需及时发出预警。工作人员需先重点针对高威胁等级的指标，即攻击频率与攻击类型，制定相应的改进方案，再针对中威胁等级的指标，制定相应改进方案，提升电网安全，避免出现信息泄露风险。

表 3 评估指标权重与威胁等级

准则层	权重	指标层	权重	威胁等级
环境信息	0.15	内存利用率 A_{11}	0.17	18
		CPU 利用率 A_{12}	0.19	22
		宽带利用率 A_{13}	0.35	5
		防雷措施 A_{14}	0.13	4
		防火措施 A_{15}	0.16	13
人为信息	0.22	主机可用性 A_{21}	0.42	28
		数据可恢复性 A_{22}	0.34	15
		安全责任落实 A_{23}	0.24	7
状态信息	0.35	攻击严重性 A_{31}	0.14	44
		攻击源数量 A_{32}	0.13	51
		攻击频率 A_{33}	0.16	82
		攻击类型 A_{34}	0.17	76
		攻击时间 A_{35}	0.08	7
		认证机制协议 A_{36}	0.09	55
		电网访问控制 A_{37}	0.12	11
		监控措施 A_{38}	0.11	16
信道信息	0.28	密钥管理 A_{41}	0.31	59
		内容有效性 A_{42}	0.29	42
		业务支撑系统可用性 A_{43}	0.13	33
		解析速度 A_{44}	0.27	27

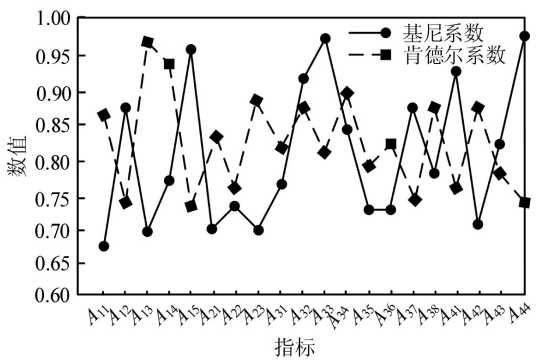


图 4 基尼系数与肯德尔系数分析结果

利用基尼系数与肯德尔系数分析本文方法电网安全评估指标体系构建效果，前者代表评估指标间的对比强度，其取值区间是[0，1]。当评估指标的基尼系数是 1 时，说明该指标与其余指标完全不同；当基尼系数是 0 时，说明该指标与其余指标非常接近，即该值越高，评估指标的对比强度越佳，评估指标体系构建效果越佳。后者代表评估指标间的冲突性，其取值区间是[0，1]，当评估指标的肯德尔系数是 1 时，说明该指标和其余指标存在较高的相关性，肯德尔系数是 0 时，说明该指标和其余指标彼此无关，该值越高，评估指标的冲突性越小。基尼系数与肯德尔系数的最低值均须超过 0.6，才可确保指标体系构建效果较优。本文方法构建安全评估体系的基尼系数与肯德尔系数分析结果如图 4 所示。根据图 4 可知，本文选取的各指标基尼系数与肯德尔系数均明显高于 0.65，说明各指标的对比强度较高，冲突性较小。实验证明本文方法具备较优的电网安全评估指标体系构建效果。

3 结束语

电网业务形式逐渐丰富，网络自身的运行方式会受到影响，导致其安全受到威胁，为此研究基于边缘计算的电网安全威胁等级评估。本文方法可有效评估电网安全威胁等级，及时了解电网中存在的不足，并加以改进，提升电网安全性，确保电网能够安全完成相应任务。

参考文献：

[1] 李刚，黄沛烁，陈怡潇，等.考虑威胁传播特性的电力CPS安全态势评估方法[J].电力建设，2019，40(5)：29-37.

[2] 李雨泽，张中信.基于排队模型的网络安全风险损失评估方法[J].计算机仿真，2021，38(4)：258-262.

[3] 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.

[4] 高翔，陈贵凤，赵宏雷.基于数据挖掘的电力信息系统网络安全态势评估[J].电测与仪表，2019，56(19)：102-106.

[5] 官丽，焦阳，张彩霞，等.电力监控系统无线接入安全风险的模糊评估方法研究[J].能源与环保，2021，43(6)：163-167.

[6] 常瑞莉.一种基于BP神经网络的移动通信网络故障检测方法[J].自动化技术与应用，2023，42(6)：123-126.

[7] 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.

作者简介：陈雪(1982—)，女，硕士，高级工程师，研究方向：配电技术。

(上接第41页)

为在第一时间控制配电变压器潜在故障风险，减少电网人力物力损失，将故障风险控制延时作为评估指标，探究三种系统在时效性方面的优劣。设置共完成400次控制任务，对比每50次实验的控制耗时均值，结果如图9所示。

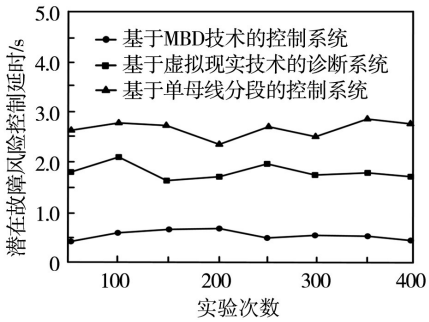


图9 潜在故障风险控制延时对比

从图9中可以看出，随着实验数量持续增多，基于MBD技术的控制系统在进行故障风险控制时始终具备较小的系统延迟，获得计算任务后能以最快速度分析控制变量，数据连接效率高，实用性更好。

4 结束语

潜在故障风险控制是建设智能电网的核心技术之一，在一定程度上改进了配网变压器检修的不足，是一种先进的电网防风险机制。为提升变压器运行可靠性与经济性，设计了基于MBD技术的配电变压器潜在故障风险控制系统，及时查明配网变压器潜在故障因素，设置对应系统软件实现高精度故障风险控制目标，为电网稳定运行提供可靠参考。

参考文献：

[1] 柳轶彬，梁得亮，王宇珩，等.混合式配电变压器的动态模型与内环控制系统[J].电工技术学报，2021，36(7)：1537-1546.

[2] 陈磊，姜飞，涂春鸣.考虑负荷最大概率分布与故障风险的配电变压器优选方法[J].电网技术，2021，45(3)：1109-1116.

[3] 张华，林茂君，张道农，等.一种基于单母线分段的变压器风冷控制系统设计[J].电力系统保护与控制，2019，47(14)：153-159.

[4] Gao J，Guo Q，Li L，et al.Research on operation status and fault deduction system design of transformer in large sports venues[J].Energy Reports，2022，8(4)：539-546.

[5] 张乐，雷沛，谭红，等.基于CATIA CAA二次开发的MBD数模信息对称技术研究与应用[J].现代制造工程，2022(6)：49-55，62.

[6] 周智行，石立宝.考虑风电不确定性及系统调频作用的电网连锁故障风险评估[J].中国电机工程学报，2021，41(10)：3305-3316，3657.

[7] 刘一民，郑少明，董鹏，等.基于PSCAD的光伏电站交流侧故障暂态特性分析[J].自动化技术与应用，2023，42(10)：180-184.

[8] 薛俞，李月乔，刘文霞，等.柔性互联配电系统连锁故障风险评估[J].电力系统自动化，2021，45(8)：112-119.

[9] 张红，石峰豪，陈苏坤.基于免疫算法的暖通空调系统传感器故障诊断研究[J].机械制造与自动化，2022，51(2)：214-217.

[10] 刘雨濛，顾雪平，王涛.计及传播路径的电力系统连锁故障多阶段阻断控制[J].电力自动化设备，2021，41(12)：151-157.

[11] 任庭昊，包义钊.基于离散傅立叶变换的配电网小电流接地线路故障选线[J].自动化技术与应用，2023，42(4)：67-70.

[12] 宫成，王卫，赵正奎，等.基于改进锁频器频率偏差检测的光伏逆变器快速频率响应控制[J].电工电能新技术，2021，40(9)：10-17.

作者简介：黄丹(1984—)，女，硕士，高级工程师，研究方向：电力营销技术。