计算机科学
COMPUTER SCIENCE

基于改进模糊综合评价法的电力监控系统网络可靠性分析

邴英澳, 王文婷, 孙圣泽, 刘鑫, 聂其贵, 刘京

引用本文

邴英澳, 王文婷, 孙圣泽, 刘鑫, 聂其贵, 刘京基于改进模糊综合评价法的电力监控系统网络可靠性分析[J]. 计算机科学, 2023, 50(6A): 220400293-7.

BING Ying'ao, WANG Wenting, SUN Shengze, LIU Xin, NIE Qigui, LIU Jing. Network Reliability Analysis of Power Monitoring System Based on Improved Fuzzy ComprehensiveEvaluation Method [J]. Computer Science, 2023, 50(6A): 220400293-7.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220400293

基于改进模糊综合评价法的电力监控系统网络可靠性分析

邴英澳[1] 王文婷[2] 孙圣泽[1] 刘 鑫[2] 聂其贵[2] 刘 京[2]
1 东北电力大学计算机学院 吉林 132012
2 国网山东省电力公司电力科学研究院 济南 250013
(18865382590@163.com)

摘 要 网络攻击层出不穷,电力行业风险管控的重要性日益凸显。然而,复杂新式的网络攻击手段、生产设备存在遗漏的系统漏洞、物理-信息网络融合的复杂性,无疑对电力监控系统的风险管控提出了新的挑战。针对如何全面准确合理地判断多因素综合影响下的电力监控系统网络的可靠性,建立一个健全的可靠性评估体系,提出了一种基于模糊评价的电力监控系统可靠性评估模型。文中从电力监控系统设备节点存在的漏洞入手,综合分析系统内的风险与系统所处的环境风险,使电力监控系统在运行过程中进行安全定级从而进行安全决策。该方法首先采用网络安全定级标准,结合工业系统漏洞库建立评估指标体系,从网络通信可靠性、业务可靠性、系统可靠性3个方面确定可靠性评估指标;然后采用改进灰狼优化算法优化调整层次分析权重,结合模糊综合评价方法对电力监控系统进行可靠性分析,根据评估结果进行针对性加强维护,在评估过程中使用更精确的量化指标,以达到细粒度级的风险评估;最后,针对电力搭建了一套半虚拟系统环境,综合分析评价电力监控系统的风险等级和可靠性验证该可靠性评估方法的有效性。

关键词:电力监控系统;灰狼优化算法;模糊综合评价;层次分析法;网络可靠性评价模型
中图法分类号 TP393

Network Reliability Analysis of Power Monitoring System Based on Improved Fuzzy Comprehensive Evaluation Method

BING Ying'ao[1],WANG Wenting[2],SUN Shengze[1],LIU Xin[2],NIE Qigui[2] and LIU Jing[2]
1 School of Computer Science,Northeast Electric Power University,Jilin 132012,China
2 State Grid Shandong Electric Power Research Institute,Jinan 250013,China

Abstract Network attacks emerge one after another,and the importance of risk management and control in the power industry is increasing day by day. However,complex and new network attack methods,missing system loopholes in production equipment,and the complexity of the integration of physical and information networks will undoubtedly bring forward the risk management and control of power monitoring systems. Aiming at how to comprehensively,accurately and reasonably judge the network reliability of the power monitoring system under the comprehensive influence of multiple factors,a sound reliability evaluation system is established,and a reliability evaluation model of the power monitoring system based on fuzzy evaluation is proposed. This paper starts with the loopholes existing in the equipment nodes of the power monitoring system,and comprehensively analyzes the risks in the system and the environmental risks outside the system,so that the power monitoring system can be safely graded during the operation process to make security decisions. This method adopts network security classification. The standard is combined with the industrial system vulnerability database to establish an evaluation index system,and the reliability evaluation index is determined from the three aspects of network communication reliability,business reliability,and system reliability. The reliability analysis of the power monitoring and monitoring system is carried out,targeted maintenance is carried out according to the evaluation results,and more accurate quantitative indicators are used to achieve fine-grained risk assessment in the evaluation process. Finally,a set of semi-virtual system environment synthesis is built for power. The risk level and reliability of the power monitoring system are analyzed and evaluated to verify the validity of the reliability evaluation method.

Keywords Power monitoring system,Gray wolf optimization algorithm,Fuzzy comprehensive evaluation,Analytic hierarchy process,Network reliability evaluation model

1 引言

电力行业一直是国民经济生产运作的不可或缺的一部分,电力设备的正常可持续运行是系统安全的最低保障,多样性、实时性是目前电力系统业务的发展方向,但也导致海量多源数据的产生[1]。对风险的及时把控需求也更加迫切,网络攻

基金项目:国网山东省电力公司科技项目(520626220029)
This work was supported by the State Grid Shandong Electric Power Company Technology Project(520626220029).
通信作者:王文婷(13853115319@163.com)

击的不断发生导致网络中不可避免地存在漏洞[2]，而这些漏洞的存在不可避免地为电网造成不确定性的损失，因此开展风险评估具有重大意义[3]。如何描述电力系统运行时产生的各种不确定性的风险，对此国内外的研究者进行了全面深度的研究[4]。可靠性分析的研究主要是对存在的网络风险进行识别，通过对电力监控系统的健壮性进行分析评估，实时做到风险控制管理与评估[5]。本文针对电力监控系统存在的安全风险，重点采用基于攻击图的方式并结合层次分析与模糊评价的方式分析电力监控系统的风险水平。目前，电力系统风险评估的精准率较低，评估时长较长[6]。可靠性模型是完成电力监控系统网络安全评估的有效方法[7]，有效的安全风险评估可以指导配置安全保护资源并补齐短板[8]。通过网络安全风险的评估形式实现网络可靠性评估，利用漏洞扫描工具来发现网络的脆弱信息[9]，但可靠性计算时间复杂度较高[10]。在评估形式上大致分为两种，分别是定性评估和定量评估。定性评估的评估操作相比定量评估更加方便，但缺点是其无法客观地分析安全攻击可能引发的损失。定量安全评估技术和方法能客观描述被测系统的风险等级，特别是对量化方法的研究是当前工业控制系统信息安全评估的主要研究方向。

文献[11]通过概率神经网络的方式对风力发电场景的风险性进行评估，该方法对风力发电机组的状态进行了合理的评估，为运维人员提供了可靠的参考。文献[12]给出了资产的计算方式，同时也对威胁和脆弱性等因子进行了量化。Yang 等提出了一种基于主机重要度的网络主机节点风险评估方法[13]，该方法能够全面地评估网络环境中的主机节点风险，得到更加合理的风险。该方法对于电力监控系统网络风险的适应性还需进一步优化。

本文根据电力监控系统的网络结构，结合构成电力监控系统设备的主要业务功能和业务通信传输的路径，建立相应的可靠性评估指标，运用层次分析法构建层次分析结构模型，结合评估指标体系及专家评价，运用模糊综合评价方式，最终建立起一种针对电力监控系统网络可靠性的评估体系。基于电力监控系统的网络结构，通过该评价体系能够实现对电力监控系统可靠性的综合评估，反映出电力监控系统的可靠程度，为网络安全管理员提供客观的参考和指引。

2 电力监控系统可靠性评估框架

电力监控系统可靠性分析评估模型中，各评估因素对应的权重对最终的可靠性评估起着决定性的作用。指标赋权的方法主要分为客观加权和主观加权两类。主观赋权的缺点是过于依赖经验判断，缺乏一定的客观性，而客观赋权缺乏历史经验支撑，同样也具有局限性[14]。本文模型采用改进的层次分析法求解权重。层次分析法对处理多因素综合影响的评价事物具有客观性，通过层次分析法确定权重，再由状态攻击图与模糊评价法确定可靠性，综合指标权重，将主观与客观相结合，使得电力监控系统可靠性评估结果更加合理全面。

2.1 层次分析法

2.1.1 层次结构模型

层次结构模型的最高层表示决策目标，中间层表示决策因素，底层指解决方案。本文使用层次分析法构建两层的分层结构，获取各决策因素的权重作为可靠性分析框架的参数，为后续评估提供权重分析数据。两层高层为目标层，底层为因素层。底层结构作为各决策因素的权重划分。

2.1.2 构造判断矩阵

确定层次结构后，本文通过指标两两比较来选择最终方案，目的是分析出底层因素对上层影响的权重问题[15]。通过比例标度表来评估判断，给出各因素的两两相互对比结果，构成判断矩阵。表 1 列出了重要性等级判定对比。判断矩阵如式(1)所示：

$$\boldsymbol{a}_{ij}=\frac{1}{\boldsymbol{a}_{ji}} \tag{1}$$

表 1 比例标度表

Table 1 Proportional scales

因素 i 相比因素 j	量化值
同等重要	1
稍微重要	2
较强重要	5
强烈重要	7
极端重要	9
两相邻判断的中间值	2,4,6,8

2.1.3 层次单排序及其一致性检验

构造判断矩阵之后，进行层次单排序，判断矩阵的特征值用 λ 表示，λ_{max} 表示最大特征值，将其特征向量 $\boldsymbol{W}$ 进行归一化处理。$\boldsymbol{W}$ 的元素是对可靠性评估目标的因素的相对重要性的排序结果，且 $\boldsymbol{W}$ 中各元素累加和为 1，即 $\sum_{i=1}^{n}w_i=1$，w_i 表示下层的第 i 个因素对上层某个因素的影响程度的权重，这种确定权向量的方法称为特征根法。此外，根据矩阵的定理可知，n 阶一致矩阵的唯一非零特征根为 n；n 阶互反阵 $M(a_{ij}>0, a_{ij}=1/a_{ij}, a_{ii}=1)$ 最大特征根 $\lambda_{max}\geqslant n$，当且仅当 $\lambda=n$ 时，$\boldsymbol{M}$ 为一致矩阵。因此用 $\lambda_{max}-n$ 的数值大小去衡量矩阵 $\boldsymbol{M}$ 的不一致程度，λ_{max} 比 n 大得越多表明 $\boldsymbol{M}$ 的不一致性越严重，所造成的判断误差也越大。

针对层次单排序结果。进行一致性检验，一致性指标用 CI 表示，CI 的计算式如式(2)所示，CI 计算结果越小，表示一致性越大。一致性指标定义为：

$$CI=\frac{\lambda_{max}-n}{n-1} \tag{2}$$

一致性指标 CI 为 0，则层次单排序结果具有完全一致性；若接近 0，表示层次单排序结果具有可接受的一致性；结果越大，越不一致。

为了对 CI 的结果进行评估，采用随机一致性指标 RI 进行判断。

$$RI=\frac{CI_1+CI_2+\cdots+CI_n}{n} \tag{3}$$

根据 RI 指标计算公式，通过重复多次实验，对每次实验都随机产生判断矩阵，计算其 CI 值，然后取算术平方根，即 RI 值，不同阶数的 RI 值与矩阵阶数的对应关系，如表 2 所列。

表 2 对应的矩阵阶数

Table 2 Corresponding matrix order

矩阵的阶数	RI
1	0.00
2	0.00
3	0.58
4	0.90
5	1.12
6	1.24
7	1.32
8	1.41

通过检验系数 CR 检验矩阵的一致性，避免随机原因造成的误差，得出检验系数，公式如下：

$$CR=\frac{CI}{RI} \tag{4}$$

$CR<0.1$，表示矩阵通过一致性检验，否则未通过。

2.1.4 层次总排序及其一致性检验

将所有因素对目标层的权重排序，从最高层向下依次进行，并进行层次一致性检验。

2.2 模糊综合评价法

采用模糊综合评价法将电力监控系统的可靠性评估过程中存在的一些边界不清、不易定量的因素定量化，进行综合评价。多层次、多因素是电力监控系统的主要特征，影响因素往往是众多而复杂的，多维度分析电力监控系统的可靠性相较于单一角度的评价更加合理，因此对电力监控系统的各项指标加以汇总整合，从整体上反映被评估对象的整体情况[16]。

通过 2.1 节确定各个决策因素的权重，构建隶属度矩阵（模糊关系矩阵），然后计算隶属度向量，从而得到综合评价结果，客观地反映出电力监控系统的可靠性程度。

2.3 属性攻击图

根据不同的搜索方向，将攻击图构建算法分为正向和反向攻击图生成算法两种类型。

正向攻击图生成算法是从攻击者的角度考虑的。可以看出，攻击者对目标的攻击过程实际上是对网络中易受攻击的主机进行前向搜索攻击的过程，网络状态的结果必须包括先前的网络状态，这样才能生成最终链路。

攻击图的正向生成算法不需要确定攻击的目标，从开始节点搜索系统内可到达的所有攻击路径；攻击图的反向生成算法，从目标节点向后搜索可以到达目标的所有攻击路径，在此过程中，过滤无关路径，反向攻击图的生成算法适合目标明确的情况。因此使用该算法进行攻击图生成，图 1 为攻击图生成框架图。

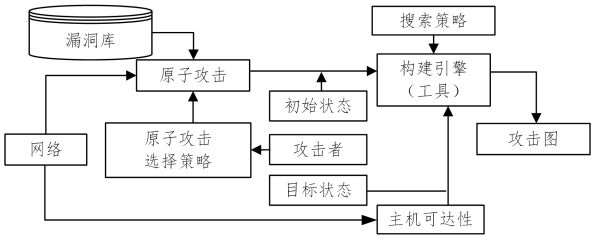

图 1 攻击图生成框架

Fig. 1 Attack graph generation framework

2.4 灰狼优化算法

灰狼优化算法（GWO）采用 α，β，δ，ω 4 种类型的狼模拟领导层。通过灰狼狩猎的 3 个步骤，即寻找目标、包围目标和攻击目标。GWO 算法将最适解作为 α，第二和第三个最佳解决方案分别被命名为 β 和 δ，剩下的候选解被假定为 ω。

灰狼围捕猎物的行为定义为：

$$D=|\boldsymbol{C}\cdot X_P(t)-X(t)| \tag{5}$$

$$X(t+1)=X_P(t)-\boldsymbol{A}\cdot D \tag{6}$$

式(5)表示灰狼与目标的距离，式(6)表示灰狼位置变换规则。其中，t 表示迭代数，向量 $\boldsymbol{A}$ 和向量 $\boldsymbol{C}$ 是系数，X_P 为目标位置，X 为灰狼位置。$\boldsymbol{A}$ 和 $\boldsymbol{C}$ 的表达式如下：

$$\boldsymbol{A}=2a\cdot r_1-a \tag{7}$$

$$\boldsymbol{C}=2\cdot r_2 \tag{8}$$

a 为收敛因子，其值随迭代次数的增加线性减小，r_1 和 r_2 为随机数，其值取[0,1]。

当灰狼发现目标所处位置，β 和 δ 在 α 的带领下指导狼群向目标包围。包围的数据模型如式(9)所示：

$$\begin{aligned}D_\alpha&=|\boldsymbol{C}_1\cdot X_\alpha-X|\\D_\beta&=|\boldsymbol{C}_2\cdot X_\beta-X|\\D_\delta&=|\boldsymbol{C}_3\cdot X_\delta-X|\end{aligned} \tag{9}$$

其中，D_α，D_β，D_δ 分别表示 α，β 和 δ 与其他个体间的距离。

X_α，X_β 和 X_δ 分别代表 α，β 和 δ 的当前位置；$\boldsymbol{C}_1$，$\boldsymbol{C}_2$，$\boldsymbol{C}_3$ 是随机向量，X 是当前灰狼的位置。

$$\begin{aligned}X_1&=X_\alpha-A_1\cdot(D_\alpha)\\X_2&=X_\beta-A_1\cdot(D_\beta)\\X_3&=X_\delta-A_1\cdot(D_\delta)\end{aligned} \tag{10}$$

$$X(t+1)=\frac{X_1+X_2+X_3}{3} \tag{11}$$

式(10)表示灰狼 ω 个体向 α，β 和 δ 位置更新的距离，最终的位置由式(11)表示。

3 可靠性分析框架

3.1 指标集与评价集的建立

可靠性指标是衡量系统可靠性的基础，是可靠性理论应用于系统分析的结果[17]。电力监控系统网络风险评价指标体系结合目前的网络安全等级保护三级基本要求，综合考虑到等级保护中要求的安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全建设管理 5 个方面的安全考核，综合分析增加业务的安全考核，汇总凝练为从通信风险、业务风险、系统风险 3 个方面考虑，建立电力监控系统网络风险评价指标体系。如图 2 所示。

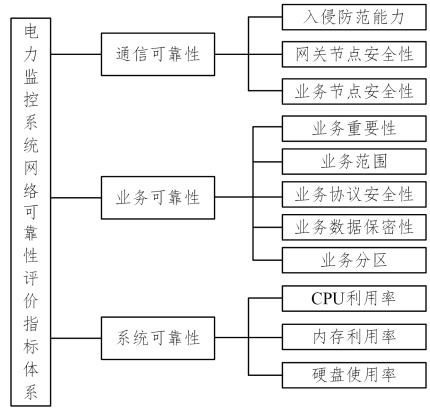

图 2 电力监控系统网络风险评价指标体系

Fig. 2 Network risk evaluation index system of power monitoring system

指标集的建立分为 3 个大指标，11 细化指标，其中，$T=\{T_1,T_2,T_3\}=$｛通信风险，业务风险，系统风险｝。

细化指标包含，$T_1=\{T_{11},T_{12},T_{13}\}=$｛入侵防范能力，网关节点安全性，感知节点安全性｝；$T_2=\{T_{21},T_{22},T_{23},T_{24},T_{25}\}=$｛业务重要性，业务范围，业务协议安全性，业务数据保密性，业务分区｝；$T_3=\{T_{31},T_{32},T_{33}\}=$｛CPU 利用率，内存利用率，硬盘使用率｝。

评价集的建立分为 5 个评价指标，分别是健康、正常、注意、异常、严重，如表 3 所列。

表 3 评价指标

Table 3 Evaluation indicators

等级	解释	分值
健康 V_1	低风险	小于等于 0.1
正常 V_2	较低风险	0.1～0.3
注意 V_3	中等风险	0.3～0.6
异常 V_4	较高风险	0.6～0.8
严重 V_5	高风险	大于于等于 0.8

3.2 改进灰狼优化算法优化层次分析法权重

电力监控系统网络可靠度评估主要采用层次分析法确定权重，通过改进的灰狼优化算法优化权重，最终给出各评价因素的权重，再通过模糊评价法构造评判矩阵，给出电力监控系统可靠性分析结果。

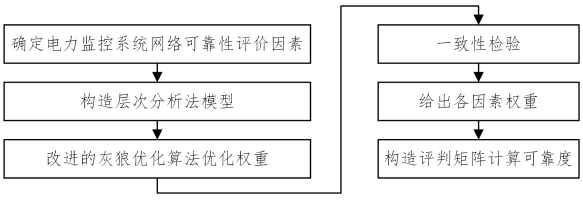

图 3 层次分析法优化权重模型

Fig. 3 AHP optimization weight model

构建灰狼优化算法模型，采用布谷鸟搜索算法优化灰狼模型，构建层次分析法适应度函数，由式(1)可得出各可行解的判断矩阵，将式(2)、式(4)作为约束条件，也作为优化算法的判断结束条件，通过算法寻找最优的特征值与特征向量，构造各指标判断矩阵。

风险判断得分如表 4 所列。

表 4 风险指标判断矩阵

Table 4 Risk indicator judgment matrix

风险	通信风险	业务风险	系统风险
通信风险	1	1/9	1
业务风险	9	1	5
系统风险	1	1/5	1

$CI=0.0194$，$CR=0.0216$，$CR<0.1$ 通过一致性检验。

通信风险指标判断得分如表 5 所列。

表 5 通信风险指标判断矩阵

Table 5 Judgment matrix of communication risk indicators

T_1	T_{11}	T_{12}	T_{13}
T_{11}	1	3	3
T_{12}	1/3	1	1
T_{13}	1/3	1	1

$CI=2.2\times10^{-16}$，$CR=2.4\times10^{-16}$，$CR<0.1$ 通过一致性检验。

业务风险指标判断得分如表 6 所列。

表 6 业务风险指标判断矩阵

Table 6 Business risk indicator judgment matrix

T_2	T_{21}	T_{22}	T_{23}	T_{24}	T_{25}
T_{21}	1	9	5	5	9
T_{22}	1/9	1	1/7	1/7	1
T_{23}	1/5	7	1	3	7
T_{24}	1/5	7	1/3	1	7
T_{25}	1/9	1	1/7	1/7	1

$CI=0.117$，$CR=0.094$，$CR<0.1$ 通过一致性检验。

系统风险判断得分如表 7 所列。

表 7 系统风险判断矩阵

Table 7 System risk judgment matrix

T_3	T_{31}	T_{32}	T_{33}
T_{31}	1	3	3
T_{32}	1/3	1	1
T_{33}	1/3	1	1

$CI=2.2\times10^{-16}$，$CR=2.4\times10^{-16}$，$CR<0.1$ 通过一致性检验。

通信风险指标权重结果如表 8 所列。

表 8 通信风险指标权重

Table 8 Weights of communication risk indicators

T_1	T_{11}	T_{12}	T_{13}
W_1	0.6	0.2	0.2

业务风险指标权重结果如表 9 所列。

表 9 业务风险指标权重

Table 9 Weights of business risk indicators

T_2	T_{21}	T_{22}	T_{23}	T_{24}	T_{25}
W_2	0.5261	0.0371	0.2315	0.1683	0.0371

系统风险指标权重结果如表 10 所列。

表 10 系统风险指标权重

Table 10 Weights of system risk indicators

T_3	T_{31}	T_{32}	T_{33}
W_3	0.6	0.2	0.2

因素层指标权重结果如表 11 所列。

表 11 因素层指标权重

Table 11 Indicator weights of factor layer

T	T_1	T_2	T_3
W	0.1062	0.7651	0.1288

通过改进灰狼优化算法进行优化权重，收敛结果如图 4 所示。

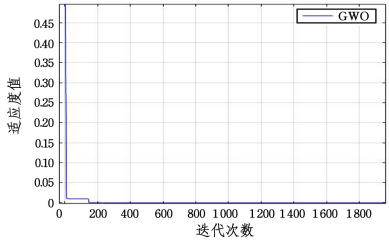

图 4 改进灰狼优化算法收敛结果

Fig. 4 Convergence results of improved grey wolf optimization algorithm

权重优化结果如图 5 所示。

$W_1=\{0.6,0.2,0.2\}$

$W_2=\{0.5261,0.0371,0.2315,0.1683,0.0371\}$

$W_3=\{0.6,0.2,0.2\}$

$W=\{0.1062,0.7651,0.1288\}$

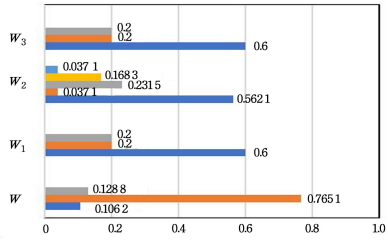

图 5 权重结果示意图

Fig. 5 Schematic diagram of weight results

3.3 建立模糊评价模型

(1)设立因子集合 T

主要因子集合 $T=\{T_1,T_2,T_3\}=\{$通信风险，业务风险，系统风险$\}$；

次要因子集合 $T_1=\{T_{11},T_{12},T_{13}\}=\{$入侵防范能力，网关节点安全性，感知节点安全性$\}$；

$T_2=\{T_{21},T_{22},T_{23},T_{24},T_{25}\}=\{$业务重要性，业务范围，业务协议安全性，业务数据保密性，业务分区$\}$；

$T_3=\{T_{31},T_{32},T_{33}\}=\{$CPU 利用率，内存利用率，硬盘使用率$\}$。

(2)构筑有关风险评价集合 Z

$Z=\{Z_1,Z_2,Z_3,Z_4,Z_5\}=\{$健康，正常，注意，异常，严重$\}$，不同指标归一化结果。

(3)确定模糊关系矩阵 $\boldsymbol{R}$

模糊关系矩阵由每个元素的评价结果构成，因素集 T 中第 i 个因素对风险评价集合 Z 的隶属度为 r_{i1}，则第 i 个因素评价的结果为 $R_i=(r_{i1},r_{i2},r_{i3},r_{i4},r_{i5})$，$T$ 中所有 11 个因素的评价结果构成模糊关系矩阵 $\boldsymbol{R}$。本文中隶属度结果通过从事电力系统安全的专家评审，取专家评审的平均值作为最终隶属度结果。

(4)建立综合评价模型

确定模糊关系矩阵 $\boldsymbol{R}$ 和各因素的权重值 W 后，则综合评价结果 B 可表示为 $B=W\cdot\boldsymbol{R}$，其中，综合评价合成算法取加权平均型。

4 实验仿真与分析

4.1 实验仿真环境介绍

火电厂仿真场景模拟火电厂中的锅炉、汽轮机和发电机相关工艺，采用模型展示火力发电机发电，经升压站输入到高压电网的过程。仿真场景采用虚拟机仿真火电厂中的辅控系统、SIS 系统、生产 MIS 系统及工程师运维工作站，使用多套 PLC 设备模拟压力、温度等数据采集和发电机控制过程。场景业务拓扑如图 6 所示。

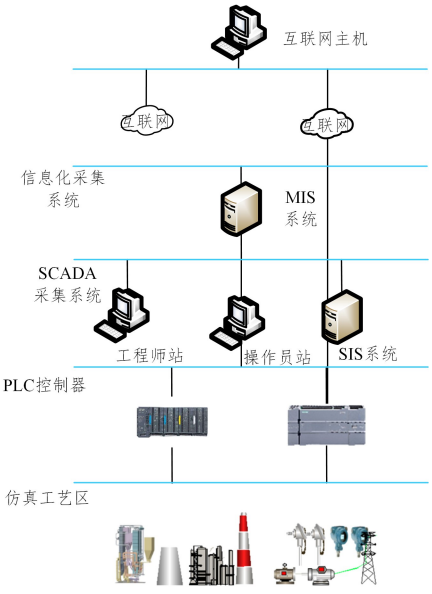

图 6 火力发电仿真场景拓扑

Fig. 6 Topology of thermal power generation simulation scenario

仿真场景由辅控系统、SIS 系统、生产 MIS 系统、工程师站、PLC 设备、传感器和火力发电模型组成。系统数据传输流程如下：辅控系统实时监控发电机运行情况，使用 PLC 设备实现传感器数据采集和发电机控制功能。工程师站用于配置 PLC 设备参数。辅控系统将实时数据转发 SIS 系统。SIS 系统部署接口服务器，具有生产控制大区数据与管理信息大区数据传输的功能。发电机和升压站实时数据经 SIS 系统传输至生产 MIS 系统。表 12、表 13 列出了火力发电场景 ip 地址与存在的漏洞点隐患。

表 12 火力发电场景 IP 地址

Table 12 IP addresses of thermal power generation scenarios

系统	上联 IP	下联 IP
MIS 系统	192.168.3.11	192.168.4.101
SIS 系统	192.168.4.114	192.168.5.102
工程师站	192.168.5.112	192.168.100.100
操作员站	192.168.5.113	192.168.100.101
PLC(左)	192.168.100.201	
PLC(右)	192.168.100.202	

表 13 火力发电场景漏洞点

Table 13 Vulnerability points of thermal power generation scenarios

业务系统	操作系统	漏洞点
MIS 系统	WIN7SP1	.MS17-010 PHPStuday 后门文件上传漏洞
SIS 系统	WIN7SP1	MS17-010 VNC 弱口令
工程师站	WIN7SP1	MS17-010 VNC 弱口令
操作员站	WIN7SP1	MS17-010 VNC 弱口令
PLC(左) PLC(右)	S7-300 S7-1200	1. 锅炉炉内火焰指示灯熄灭 2. 发电机停止运行 3. 篡改 SCADA 上位机上温度和压力数值不变

根据业务拓扑以及通过扫描器发现存在的漏洞点，构造属性攻击图，如图 7 所示，矩形表示使用的攻击属性，椭圆表示节点。将火电场景的各系统依次编号，MIS 系统、SIS 系统、工程师站、操作员站，依次编号为 1，2，3，4，编号 0 表示攻击节点，MS17-010(0,1)表示从节点 0 到节点 1 使用 MS17-010 进行攻击，获取节点 1 的 user 权限。

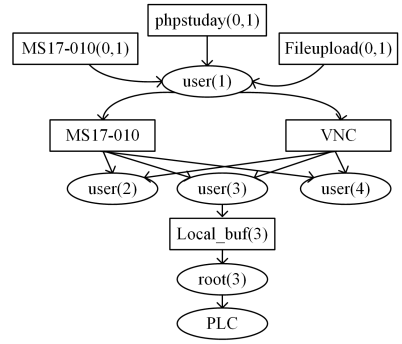

图 7 火力发电场景攻击图

Fig. 7 Attack diagram of thermal power generation scenario

模糊矩阵 $\boldsymbol{R}$ 的确定，表 14 列出了火力发电单因素评分结果。

表 14 火力发电单因素评分结果

Table 14 Single factor scoring results of thermal power generation

	V_1	V_2	V_3	V_4	V_5
T_{11}	0.3	0.3	0.3	0.4	0.2
T_{12}	0.3	0.3	0.3	0.35	0.2
T_{13}	0.2	0.3	0.3	0.25	0.2
T_{21}	0.4	0.4	0.5	0.35	0.2
T_{22}	0.8	0.8	0.85	0.3	0.2
T_{23}	0.3	0.45	0.5	0.3	0.3
T_{24}	0.3	0.4	0.4	0.3	0.3
T_{25}	0.7	0.8	0.85	0.2	0.2
T_{31}	0.2	0.4	0.6	0.3	0.1
T_{32}	0.3	0.4	0.4	0.3	0.1
T_{33}	0.4	0.5	0.5	0.4	0.2

根据评价结果，采用灰色关联分析结合 TOPSIS 方法对评分结果进行综合评价，评价结果如图 8 所示。

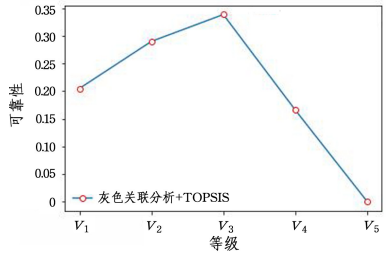

图 8 灰色关联综合评价结果图

Fig. 8 Gray relational comprehensive evaluation results

由前文确定的层次权重结合模糊评价方法对评分结果进行综合评价可得评价结果，评价结果如图 9 所示。

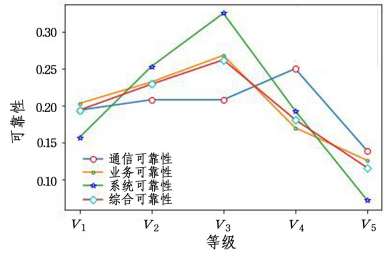

图 9 模糊综合评价结果图

Fig. 9 Fuzzy comprehensive evaluation results

具体评价结果：

通信可靠性{0.194,0.208,0.208,0.25,0.139}

业务可靠性{0.203,0.232,0.268,0.17,0.126}

系统可靠性{0.157,0.253,0.325,0.193,0.072}

可靠性{0.194,0.229,0.262,0.181,0.116}

由上述结果可知，火力发电在可靠性评估结果中，系统在通信可靠性上处于“正常”的可靠状态，但是在系统可靠性以及业务可靠性上处于注意的可靠状态，表明系统在该项评估中存在中等风险，不加处理会导致系统可靠状态继续恶化。因此该方法给出的综合可靠性也是达到“注意”级别，相较于灰色关联分析得出的结果，两者得出的结果均表明该火力发电场景状态处于“注意”状态。但本文提出的方法更加全面合理地解释了电力监控系统的可靠状态，也具体展现了电力监控系统网络空间中需注意的地方，便于网络安全运维人员全面合理地了解电力监控系统的可靠状态。

结束语 本文提出了一种基于改进模糊层次分析法的电力监控系统网络可靠性分析模型。该模型结合网络等级保护方案明确电力监控系统可靠性因素，通过层次分析法确定各因素对电力监控系统的权重，采用灰狼优化算法并结合优化层次分析方法求取各权重的最优解。最后构建模糊评价矩阵，计算电力监控系统可靠性结果对于评价集的隶属度，给出电力监控系统的可靠性结果，辅助网络安全运维人员运维，通过灰色关联分析结合 TOPSIS 方法进行对比，所提方法能细粒度地、全面客观地反映电力监控系统的可靠性程度，具有实际应用价值。

同时，受所采用的算法模型的限制，文中阐述的可靠性评价方法在构建指标系统及权重时需要依赖专家经验判断，存在明显的局限性。在后续的进一步研究中，建议通过大数据挖掘和分析技术确定初始的指标体及其权重，对其风险进行评价，同时实现对权重参数的动态调整。这样的可靠性评估方法将能够更加准确地体现出电力监控系统的风险水平。

参 考 文 献

[1] ZHAN X, GUO H, HE X Y, et al. Research on security risk assessment method of state grid edge computing information system[J]. Computer Science, 2019, 46(S2): 428-432.

[2] WANG H, ZHANG J, ZHAO Y, et al. A new Bayesian model for network risk assessment[J]. Small and Microcomputer Systems, 2020, 41(9): 1898-1904.

[3] DING M S, SUN W J, CAI X P, et al. Risk assessment and prevention of extreme events in power system[J]. China Electric Power, 2020, 53(1): 32-39, 65.

[4] WANG W H, GUO P, ZHU J, et al. Risk assessment and fault location method of relay protection system based on fault tree and Bayesian network[J]. Journal of Electric Power Science and Technology, 2021, 36(4): 81-90.

[5] YIN J J, ZHAO D M. Power system backup risk assessment method based on full probability risk measurement[J]. Electric Power Automation Equipment, 2020, 40(1): 156-162.

[6] BU Y, GAO C H, LI W F, et al. Risk assessment of power system under the framework of big data[J]. Power Grid and Clean Energy, 2021, 37(1): 77-83.

[7] WEI Y, CUI J B, LIU X T, et al. Reliability analysis method of power system wide area protection communication system based on improved dynamic fault Tree[J]. Power System Protection and Control, 2021, 49(23): 171-177.

[8] ZHU R C, LI X, LIN X N. Security risk analysis method of video private network based on Bayesian network[J]. Information Network Security, 2021, 21(12): 91-101.

[9] ZHOU W, ZHANG H, LI B H. Network risk assessment method based on attack and defense state graph model[J]. Journal of Southeast University(Natural Science Edition), 2016, 46(4): 688-694.

[10] FU J J, WU Z H, SHI Z. Reliability optimization algorithm for power communication network based on improved clustering algorithm[J]. Computing Technology and Automation, 2020, 39(4): 92-95.

[11] LI W T, JIAO Y L, YANG Z L, et al. Risk assessment of centralized control wind farm based on probabilistic neural network[J]. Electrical Measurement and Instrumentation, 2019, 56(17): 76-81, 152.

[12] LI S B, LI J, TANG G, et al. Network security status prediction and risk assessment method of industrial control system based

on HMM [J]. Information Network Security, 2020,20(9): 57-61.

[13] YANG H Y,YUAN H H,ZHANG L. A network host node risk assessment method based on host importance [J/OL]. Journal of Beijing University of Posts and Telecommunications, 2022:1-5.

[14] HE Y G,LIU J. Security Risk Assessment of Power Internet of Things Based on Combination Empowerment-Cloud Model[J]. Power SystemTechnology,2020,44(11):4302-4309.

[15] ZHAO X L,ZHAO B,ZHAO J J,et al. Research on network security measurement method based on attack identification[J]. Information Network Security,2021,21(11):17-27.

[16] WANG Y,LIU Y,SONG W H. Research on the evaluation method of emergency response capability of petrochemical enterprises based on fuzzy comprehensive evaluation method [J]. Journal of Nankai University(Natural Science Edition),2021, 54(6):75-80.

[17] LI H,YANG J F. Design of reliability assessment software for substation automation system based on fault tree analysis method[J]. Automation and Instrumentation,2016(2):138-141.

BING Ying'ao, born in 1999, postgraduate. His main research interests include power system security and network security.

WANG Wenting, born in 1988, postgraduate. Her main research interests include power system security, network security and ICT(information and communications technology).