专题：工业互联网平台及安全

# 模糊综合评判法在电力企业网络信息安全评估中的应用

刘道远[1]，孙科达[2]，周君良[3]，范海东[3,4]

（1. 淮浙煤电有限责任公司，安徽 淮南 232000；
2. 浙江省能源集团有限公司，浙江 杭州 317000；
3. 浙江浙能技术研究院有限公司，浙江 杭州 317000；
4. 浙江浙能工业信息工程重点企业研究院，浙江 杭州 317000）

**摘　要**：现今电力企业已经实现了信息化的经营生产，网络信息安全评估工作的重要性日益显著。采用二级模糊综合评判法对一种基于 PDRR 模型的电力企业网络信息安全系统进行安全等级评估，并采用 Delphi 法对评估过程中电力影响企业网络安全的各项因素的权重系数进行确定，通过对评估结果的客观分析，找出电力企业网络信息安全系统中存在的突出问题，做出相应的安全加固。验证结果表明，优化后的网络信息安全模型更为坚固，实用性和可操作性都显著提升，有效提高了电力企业的网络信息安全等级，可以作为其他电力企业网络信息安全建设的有利参照。

**关键词**：电力企业；网络信息安全模型；安全等级评估；综合模糊评判法；二级模糊综合评判

**中图分类号**：TP309.2

**文献标识码**：A

**doi:** 10.11959/j.issn.1000−0801.2020065

# Application of fuzzy comprehensive evaluation method in network information security assessment of electric power enterprises

LIU Daoyuan[1], SUN Keda[2], ZHOU Junliang[3], FAN Haidong[3,4]

1. Huaizhe Coal & Power Co., Ltd., Huainan 232000, China
2. Zhejiang Energy Group Co., Ltd., Hangzhou 317000, China
3. Zhejiang Zheneng Technology Research Institute Co., Ltd., Hangzhou 317000, China
4. Zhejiang Zheneng Industrial Information Engineering Key Enterprise Research Institute, Hangzhou 317000, China

**Abstract:** Nowadays, electric power enterprises have realized the operation and production of information technology, and the importance of network information security evaluation is more and more obvious. Two-level fuzzy comprehensive evaluation method was used to evaluate the security level of network information security system of power enterprises based on PRDD model, and Delphi method was used to determine the weight coefficients of various factors of network security of power enterprises in the evaluation process. Through objective analysis of the evaluation results, the network credit of power enterprises was found out. The prominent problems existing in the informa-

收稿日期：2020−01−12；修回日期：2020−03−12

基金项目：浙江省重点研发计划基金资助项目（No.2019C01011）

**Foundation Item:** Zhejiang Province Key Research and Development Program (No.2019C01011)

tion security system should be solved and the corresponding security reinforcement scheme should be formulated. The validation results show that the optimized network information security model is more robust, practicability and operability are significantly improved, which effectively improve the network information security level of power enterprises, and can be used as a favorable reference for the construction of network information security of other power enterprises.

**Key words:** electric power enterprise, network information security model, security grade evaluation, comprehensive fuzzy evaluation method, secondary fuzzy comprehensive evaluation

## 1　引言

在全球信息技术飞速发展的背景下，我国企业信息化发展的进度逐渐加快，而电力行业又是较早步入信息化建设的行业之一。随着电力企业信息化建设水平的不断提高，营销 MIS 系统、网络通信监管系统等信息化平台涌现，但是电力企业在网络信息安全建设方面却存在诸多缺陷，这一点导致对先进信息技术依赖较强的电力企业在实际的运营管理过程中将面临严重的网络信息安全威胁[1-2]。电力企业只有进行强有力的网络信息安全评估才能对现行的网络信息安全模型进行有效的优化改造，以此提高电力企业网络信息安全管理水平和网络信息的安全等级，进一步完善自身的信息化安全建设[3-5]。

本文在确定权重系数的过程中采用的是 Delphi 法，并采用模糊综合评判法对电力企业 PDRR 网络安全模型进行安全评估，通过对安全评估结果的客观性分析，发现电力企业 PDRR 网络安全模型在通信协议安全、网络安全、业务应用系统安全、安全监测等方面存有一定的安全漏洞。结合电力企业网络信息系统的实际情况，提出加固电力企业网络信息系统安全的优化模型，并进行了总结和展望。

## 2　电力企业 PDRR 网络安全模型

典型的网络安全模型主要分为 PDR（protection，detectioon，response）网络安全模型、PPDR（policy，protection，detection，response）网络安全模型以及 PDRR（protection，detection，reaction，recovery）网络安全模型 3 类。这些网络安全模型的防护机制和方法都存在不同，各自的优劣势也有所差异。其中 PDRR 网络安全模型将安全防护作为基础，能够通过检测及时发现网络信息系统中存在的安全漏洞并改正，侧重于自动故障恢复功能[6]。

### 2.1　PDRR 网络安全模型的构成

电力企业的网络安全模型主要在 PDRR 模型的基础上根据动态闭环管理念进行构建，分别从安全防护、安全监测、响应与恢复这 3 个功能模块来为电力企业的网络信息安全提供有力的保障[7-8]。电力企业网络安全模型如图 1 所示。

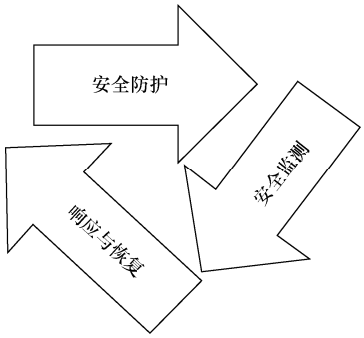



图 1　电力企业网络安全模型

#### 2.1.1　安全防护功能模块

在电力企业网络安全模型中，安全防护功能模块主要包括以下内容。

（1）通信协议的安全

电力企业的网络信息系统需要通过多种通信协议才能实现各主机间的信息传递，例如 TCP/IP、FTP 等。但是这些协议的通信过程在网络层和传输层中

都存在一定的安全隐患，需要在原有协议的基础上添加相应的安全协议来保证网络信息的安全[9]。

（2）网络系统安全

在电力企业网络安全模块的网络系统安全防护中，主要通过保护网络安全、操作系统安全、业务系统安全和数据库安全这 4 个方面来保证整个网络系统的信息安全。

（3）信道数据安全

电力企业网络安全模块通过架设电力光缆组建和接入网络的方法来保证信道数据的安全，并采用必要的加密手段来避免信道数据受到人为攻击或自然灾害带来的安全威胁[10]。

#### 2.1.2 安全监测功能模块

电力企业的网络信息系统复杂程度较高，无法对系统中存在的所有安全威胁进行详细的考虑，而安全监测功能模块则作为一种积极防御手段来弥补上述不足。在电力企业网络安全模型中常见的安全监测技术包括安全漏洞扫描技术、IDS 技术和安全审计技术[11]。电力企业的安全监测结合对系统异常记录的分析，采取针对性的手段来保证网络信息安全。

#### 2.1.3 响应与恢复功能模块

电力企业网络信息系统中所发生的安全事故存在明显的不可预见性，有必要利用有效的响应和恢复功能对突发的信息安全事故进行妥善的处理解决。

### 2.2 PDRR 网络安全模型的特点及缺陷

电力企业 PDRR 网络安全模型的特点主要体现在以下 3 个方面。

（1）技术性

该网络安全模型通过网络安全产品和相关安全防护技术的有机结合，在不断的更新和完善中保证网络信息的安全。

（2）动态性

该网络安全模型通过 3 个功能模块的不断循环执行来确保电力企业网络信息的安全。

（3）实用性

该网络安全模型结构清晰明了，简洁的执行过程能够实现对安全事故的快速定位，响应和恢复速度较快[12]。

PDRR 网络安全模型的缺陷主要体现在以下 3 个方面：

- 欠缺完善的安全运维保障机制；
- 网络安全模型的结果过于简单；
- 安全防护多为静态手段，比较单一。

## 3 电力企业网络信息安全评估

### 3.1 模糊综合评判法

模糊综合评判法是基于模糊线性变换原理，结合被评价事物的相关影响因素进行评价的一种科学评估方法。模糊综合评判法可以分为一级模糊综合评判法和多级模糊综合评判法[13]。本文对电力企业网络信息安全评估中应用的是多级模糊综合评判法中的二级模糊综合评判法，其评判的步骤如图 2 所示。

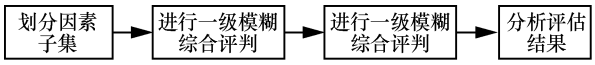



图 2 二级综合模糊评判法的评判步骤

### 3.2 电力企业网络信息安全评估

#### 3.2.1 确定因素集

依据电力企业 PDRR 网络安全模型可以发现，对电力企业网络信息安全造成影响的因素众多，必须从整体上对全部影响因素进行综合分析，以此保证安全评估决策的正确性[14]。在对电力企业网络信息安全进行评估的过程中，结合图 1 所示的网络安全模型，可以对影响电力企业网络信息安全的诸因素进行确定，表示为如下因素集：$U=\{U_1,U_2,U_3,U_4,U_5,U_6,U_7,U_8,U_9\}$，这些因素分别表示物理环境、网络环境、信道数据、通信协议、人员组织、法律规制、管理体制、教育培训、运维过程。对这 9 个主因素的一级子因素集进行确定，如下所示：

- $U_1=\{u_{11},u_{12},u_{13}\}=$ {设备安全，机房环境安全建设，存储介质管理}；
- $U_2=\{u_{21},u_{22},u_{23},u_{24}\}=$ {网络安全，操作系统安全，业务系统安全，数据库安全}；
- $U_3=\{u_{31},u_{32},u_{33}\}=$ {抗攻击性能，线缆保护，数据加密技术}；
- $U_4=\{u_{41},u_{42},u_{43},u_{44}\}=$ {网络层协议，数据链路层协议，传输层协议，高层协议}；
- $U_5=\{u_{51},u_{52},u_{53},u_{54}\}=$ {责任落实，人事管理，机构设置，部门合作}；
- $U_6=\{u_{61},u_{62},u_{63}\}=$ {法律规范执行程度，制度制定的完整程度，制度执行程度}；
- $U_7=\{u_{71},u_{72},u_{73},u_{74}\}=$ {管理方案制定，管理方案执行，管理方案验收，问题处理}；
- $U_8=\{u_{81},u_{82},u_{83},u_{84}\}=$ {培训规划，岗前培训，安全培训教育，考核验收}；
- $U_9=\{u_{91},u_{92},u_{93},u_{94},u_{95},u_{96},u_{97}\}=$ {安全评估，策略制定，安全监测，响应与恢复，安全加固，安全通报，运维执行}。

3.2.2　确定权重系数

在本文对电力企业网络信息的安全评估中，确定权重系数采用的是 Delphi 法，详细步骤如下。

**步骤 1**　确定因素 $u_i$ 的重要性序列数值。在此步骤中采用的是专家经验法确定重要性序列值[15]。重要性序列值集表示为 $e(e_i\in\{i=1,2,\cdots,m\})$，将最不重要因素对应的 $e_i$ 值确定为 1；将最重要因素对应的 $e_i$ 值确定为 $m$。根据 $k$ 位专家给定的重要性序列值得出 $e_i$ 值表，见表 1。

**表 1　$k$ 位专家对各因素的重要性序列值**

| 因素序号 | $e_i$ 值 |
|---|---|
| $u_1$ | $e_1(k)$ |
| $u_2$ | $e_2(k)$ |
| $u_3$ | $e_3(k)$ |
| … | … |
| $u_m$ | $e_m(k)$ |

**步骤 2**　编制优先得分表。根据上述 $e_i$ 值进行以下计算：当 $\frac{e_j(k)}{e_i(k)}>1$ 时，$A_{ij}(k)=1$；当 $\frac{e_j(k)}{e_i(k)}<1$ 时，$A_{ij}(k)=0$。

假设共有 $b$ 位专家进行评估，则得到如下数值：

$$A_{ij}=\sum_{k=1}^{b}A_{ij}(k),i,j=1,2,3,\cdots,m \tag{1}$$

由此能成功编制出优先得分表，见表 2。

**表 2　优先得分**

| 因素序号 | $u_1$ | $u_2$ | … | $u_m$ |
|---|---|---|---|---|
| $u_1$ | $A_{11}$ | $A_{12}$ | … | $A_{1m}$ |
| $u_2$ | $A_{21}$ | $A_{22}$ | | $A_{2m}$ |
| … | … | … | … | … |
| $u_m$ | $A_{m1}$ | $A_{m2}$ | | $A_{mm}$ |

**步骤 3**　计算 $A_i$ 值。通过对优先得分表中的数值进行累加，令 $A_{\max}=\max\{A_1,A_2,\cdots,A_m\}$、$A_{\min}=\min\{A_1,A_2,\cdots,A_m\}$，得出 $A_{\max}$ 对应的因素最重要，$A_{\min}$ 对应的因素最不重要。

**步骤 4**　计算极差值和权重系数值。令 $a_{\max}=1$、$a_{\min}=0.1$，则能得出极差 $d$ 为：

$$d=\frac{A_{\max}-A_{\min}}{a_{\max}-a_{\min}} \tag{2}$$

得出权重系数值如下：

$$a_i=1-\frac{A_{\max}-A_i}{d}(i=1,2,3,\cdots,m) \tag{3}$$

**步骤 5**　根据上述步骤得出的 $a_i$，得出权重系数的模糊集：

$$A_i=(a_1,a_2,a_3,\cdots,a_m) \tag{4}$$

以上是电力企业网络信息安全评估中确定权重系数的步骤。本文中邀请的专家有 8 位，分别对上述的子因素进行评价。将上述确定的 9 个主因素集及其子因素集代入其中，首先对 $U_1$ 的子因素权重系数进行确定，则能得出电力企业网络信息安全子因素的 $e_i$ 值表和优先得分表[6]，见表 3 和表 4。

表 3 $U_{1i}$子因素的 $e_i$值

| 因素号 | 因素（$U_{1i}$） | 专家 1 的 $e_i$ 值 | 专家 2 的 $e_i$ 值 | 专家 3 的 $e_i$ 值 | 专家 4 的 $e_i$ 值 | 专家 5 的 $e_i$ 值 | 专家 6 的 $e_i$ 值 | 专家 7 的 $e_i$ 值 | 专家 8 的 $e_i$ 值 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 设备安全 | 2 | 4 | 5 | 3 | 3 | 3 | 5 | 4 |
| 2 | 机房环境安全建设 | 3 | 3 | 4 | 1 | 2 | 2 | 3 | 5 |
| 3 | 存储介质管理 | 1 | 1 | 2 | 4 | 1 | 1 | 2 | 2 |

表 4 $U_{1i}$子因素的优先得分

| 因素序号 | $u_{11}$ | $u_{12}$ | $u_{13}$ | $A_i$ | $a_i$ |
|---|---|---|---|---|---|
| $u_{11}$ | — | 6 | 7 | 13 | 1.000 |
| $u_{12}$ | 2 | — | 7 | 9 | 0.673 |
| $u_{13}$ | 1 | 1 | — | 2 | 0.100 |

再根据上述的极差值计算式，得出 $U_1$ 极差 $d \approx 12.222$，每个子因素的权重系数 $a_1 = 1 - \frac{13 - A_1}{12.222}$，由此得出 $U_1$ 中各子因素的权重系数为 $A_1 = (1.000, 0.673, 0.100)$；同理得出全部 9 个主因素的权重系数，再通过归一化处理，得出如下权重系数：

$$A_1 = (0.564, 0.380, 0.056)$$
$$A_2 = (0.373, 0.045, 0.127, 0.455)$$
$$A_3 = (0.476, 0.476, 0.048)$$
$$A_4 = (0.357, 0.330, 0.036, 0.277)$$
$$A_5 = (0.228, 0228, 0.495, 0.050)$$
$$A_6 = (0.061, 0.333, 0.606)$$
$$A_7 = (0.036, 0.250, 0.357, 0.357)$$
$$A_8 = (0.208, 0.042, 0.333, 0.417)$$
$$A_9 = (0.143, 0.092, 0.177, 0.024, 0.024, 0.194, 0.126) \quad (5)$$

之后再采用同样的方法对主因素的权重系数进行确定，并进行归一化处理，得出：

$$A = (0.038, 0.192, 0.067, 0.078, 0.122, 0.019, 0.177, 0.129, 0.177) \quad (6)$$

### 3.2.3 利用模糊综合评判法进行安全评估

本文采用二级模糊综合评判法对电力企业的网络信息安全进行评估，首先对模糊综合评判表进行构建，表 5 为 $U_1$ 主因素集的模糊综合评判表。

同理得出电力企业其他主因素的模糊综合评判表。

（1）进行一级模糊综合评判，得出评判矩阵如下：

$$R_1 = \begin{bmatrix} 0 & 0.375 & 0.250 & 0.375 & 0 \\ 0.125 & 0.375 & 0.375 & 0.125 & 0 \\ 0.125 & 0.375 & 0.250 & 0.125 & 0.125 \end{bmatrix} \quad (7)$$

则 $U_1$ 中子因素对应的权重系数为：$A_1 = (0.564, 0.380, 0.056)$，由此所选择的评判模型 $M = (\bullet, +)$ 的计算结果为 $B_1 = A_1 * R_1 = (0.055, 0.376, 0.298, 0.267, 0.007)$，*表示广义模糊合成运算，同理得出其他主因素的一级模糊综合评判结果为：

$$B_2 = (0.074, 0.417, 0.261, 0.229, 0.022)$$
$$B_3 = (0.179, 0.191, 0.263, 0.310, 0.060)$$
$$B_4 = (0.085, 0.332, 0.456, 0.129, 0)$$
$$B_5 = (0.159, 0.308, 0.399, 0.246, 0.062)$$
$$B_6 = (0.084, 0.443, 0.402, 0.057, 0.008)$$
$$B_7 = (0.120, 0.218, 0.038, 0237, 0.045)$$

表 5 $U_1$主因素集的模糊综合评判表

| 1 级因素集 | 1 级权重系数 | 2 级因素集 | 2 级权重系数 | 模糊综合评判矩阵 | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | $v_1$ | $v_2$ | $v_2$ | $v_4$ | $v_5$ |
| $U_1$ | 0.038 | $u_{11}$ | 0564 | 0 | 0.375 | 0.250 | 0.375 | 0 |
| | | $u_{12}$ | 0.380 | 0.125 | 0.375 | 0.375 | 0.125 | 0 |
| | | $u_{13}$ | 0.056 | 0.125 | 0.375 | 0.250 | 0.125 | 0.125 |

$$B_8 = (0.120, 0.281, 0.396, 0.151, 0.052)$$

$$B_9 = (0.138, 0.343, 0.245, 0.114, 0.037) \quad (8)$$

（2）根据上述得出的一级模糊综合评判结果，进行二级模糊综合评判，因确定的权重系数为 $A = (0.038, 0.192, 0.067, 0.078, 0.122, 0.019, 0.177, 0.129, 0.177)$，所以得出二级模糊评判结果为：

$$B = A * R = (0.116, 0.315, 0.333, 0.197, 0.038) \quad (9)$$

（3）分析模糊综合评判结果。通过二级模糊综合评判得出的电力企业网络信息安全评估结果为 $B = (0.116, 0.315, 0.333, 0.197, 0.038)$。之后依据模糊分布法的评语集 $\{v_1, v_2, v_3, v_4, v_5\} = \{$很好，好，一般，差，很差$\}$，对电力企业网络信息安全进行评估，相对应的比例分别为：11.6%、31.5%、33.3%、19.7%、3.8%。由此可见，电力企业网络信息的安全等级一般。

## 4　电力企业网络信息安全系统的缺陷及安全加固

### 4.1　电力企业网络信息安全系统的缺陷

通过模糊综合评判法对电力企业网络信息安全进行评估，发现电力企业网络信息安全系统主要存在以下 4 个方面的缺陷。

（1）通信协议安全方面

通信协议安全方面存在的缺陷体现在电力企业网络信息系统中的 VLSN 划分及维护困难，一旦出现设备故障就会造成相关信息的丢失，并且会导致网络中断，严重影响运营；部分协议在安全方面有所不足，为不法分子的恶意攻击行为创造了机会；公网网站的访问缺少限制[17]；内网中核心交换机的负载不均衡，无法实现信息资源的合理配置[18]。

（2）业务系统安全方面

业务系统安全方面存在的缺陷体现在不同部门业务系统之间能够进行相互间的访问，极有可能发生数据篡改的情况，不利于系统的稳定运行。

（3）网络安全方面

电力企业网络信息系统中的安全设备主要是防火墙，但是只能单纯地实施静态防御，无法对系统中出现的动态攻击和实时异常行为进行及时的响应[19]。

（4）安全监测方面

在安全监测方面，电力企业网络安全模型存在的缺陷体现在响应和恢复的时间较长，缺少能够对全部网络设备进行实时监测且能快速响应及恢复的机制，直接影响了电力企业网络信息系统的故障恢复效率。

### 4.2　电力企业网络信息安全系统的加固改善

为了保证电力企业的网络安全模型能够完全适合企业网络信息系统的安全运行，对其原有的 PDRR 网络安全模型进行改善，得出如图 3 所示的基于电力企业 PDRR 模型的网络安全模型。

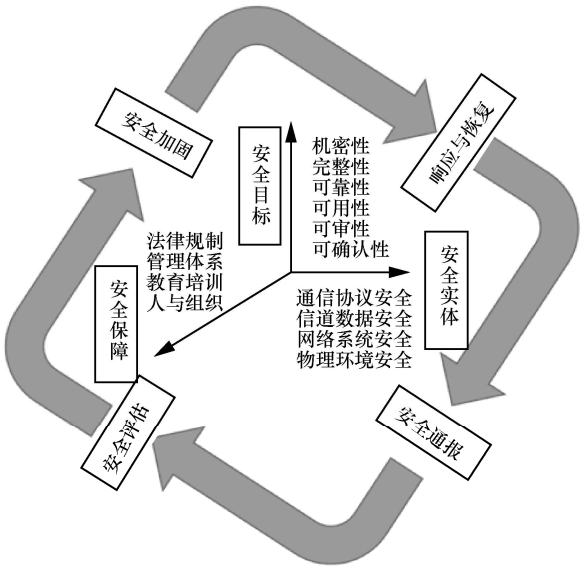



图 3　基于电力企业 PDRR 模型的网络安全模型

- 加固改善后的网络安全模型满足电力企业网络信息安全的六大需求：机密性、完整性、可靠性、可用性、可审性以及可确认性[20]。
- 加固改善后的网络安全模型增添了安全加固、安全通报和必要的评估模块。这些模

块与原有的安全防护、安全监测及响应与恢复模块共同组成更为完善的动态闭环管理保障机制，能够有效适用于电力企业这种网络系统规模较大、复杂程度较高的系统信息安全防护工作。同时，在网络安全模型中加入的安全防护模块，能够通过安全等级评估工作对系统中存在的漏洞进行查找，提高了网络信息的安全强度。

- 加固完善后的网络安全模型考虑了法律规范、物理环境、教育培训、规章制度等对网络安全有影响的因素，并加强了这些因素的保障要求，切实实现了电力企业网络信息系统的闭环动态管理。

## 5 结束语

在全球信息化技术飞速发展的背景下，网络信息系统中的安全问题越发严峻，构建安全有效、覆盖范围全面的网络信息安全模型是电力企业迫切的需求。本文在电力企业现有网络安全模型的基础上，利用二级模糊综合评判法对电力企业网络信息安全进行评估，发现电力企业现有的网络安全模型的缺陷，在此基础上提出加固后的电力企业网络信息安全模型，使该模型更适用当前电力企业复杂且多变的网络信息环境，实现了对电力企业网络信息安全的有效保护。

## 参考文献：


[1] 周慎学, 范渊, 夏克晁, 等. 台二电厂工控系统信息安全防护体系的建设[J]. 中国电力, 2017, 50(8): 53-57.
ZHOU S X, FAN Y, XIA K C, et al. Construction of information security protection system for industrial control system in Taizhou 2nd power plant[J]. Electric Power, 2017, 50(8): 53-57.

[2] 王波, 王威, 李丰伟. 电网集中监控下海量信息导致的安全风险及应对策略[J]. 中国电力, 2015, 48(12): 27-32.
WANG B, WANG W, LI F W. Research on grid security risk and response strategies on centralized monitoring of massive information[J]. Electric Power, 2015, 48(12): 27-32.

[3] 张瑞敏, 冯建民. 信息安全及其在电力系统中的应用[J]. 中国电力教育, 2012(z2): 458-459.
ZHANG R M, FENG J M. Research on grid security risk and response strategies on centralized monitoring of massive information[J]. China Electric Power Education, 2012(z2): 458-459.

[4] 朱晓燕, 方泉. 美国电力行业信息安全运作机制和策略分析[J]. 中国电力, 2015, 48(5): 81-88.
ZHU X Y, FANG Q. Study on mechanism and strategy of cyber security in U.S. electric power industry[J]. Electric Power, 2015, 48(5): 81-88.

[5] 赵婷, 高昆仑, 郑晓崑, 等. 智能电网物联网技术架构及信息安全防护体系研究[J]. 中国电力, 2012, 45(5): 87-90.
ZHAO T, GAO K L, ZHENG X K, et al. Research on technical framework and cyber security protection system of IoT in smart grid[J]. Electric Power, 2012, 45(5): 87-90.

[6] 何蕾. 基于改进 PDRR 模型的电力企业网络安全模型研究[D]. 北京: 华北电力大学, 2015.
HE L. Research on power enterprise network security model based on improved PDRR model[D]. Beijing: North China Electric Power University, 2015.

[7] 付沙, 宋丹. 基于AHP和模糊综合评判的信息安全风险评估方法[J]. 实验室研究与探索, 2012, 31(6): 207-210.
FU S, SONG D. An information security risk assessment method based on AHP and fuzzy comprehensive evaluation[J]. Research and Exploration in Laboratory, 2012, 31(6): 207-210.

[8] 吴文刚, 张志文, 王庆生. 基于模糊综合评判和 AHP 信息安全风险评估模型[J]. 重庆理工大学学报（自然科学版）, 2017, 31(7): 156-161.
WU W G, ZHANG Z W, WANG Q S. A information security risk assessment model based on AHP and fuzzy comprehensive evaluation[J]. Journal of Chongqing Institute of Technology (Natural Science), 2017, 31(7): 156-161.

[9] 杨肖, 杨力, 杨子纯. 基于模糊层次分析的工业 SCADA 安全风险评估方法研究与应用[J]. 计算机应用与软件, 2017, 34(5): 54-60.
YANG X, YANG L, YANG Z C. Research and application of industrial SCADA security risk assessment method based on fuzzy AHP[J]. Computer Applications and Software, 2017, 34(5): 54-60.

[10] 姚晓勇, 徐略红, 黄华平, 等. 电力企业信息安全防护体系的构建与实现[J]. 自动化技术与应用, 2018, 37(9): 150-155.
YAO X Y, XU L H, HUANG H P, et al. Establishment and implementation of information security protection system in power enterprises[J]. Techniques of Automation and Applications, 2018, 37(9): 150-155.

[11] 李冰霞. 电力信息网络安全态势评估与预测方法研究[D]. 保定: 华北电力大学, 2014.
LI B X. Research on security situation assessment and prediction method of electric power information network[D]. Baoding: North China Electric Power University, 2014.

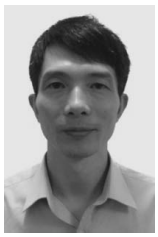
[12] HERVE C, FREDERIC G. Maturity assessment and process improvement for information security management in small and medium enterprises[J]. Journal of Software: Evolution and

Process, 2014, 26(5): 496-503.
[13] 石江红. 基于模糊测度理论的电力通信网风险评估[D]. 保定: 华北电力大学, 2017.
SHI J H. Risk assessment of electric power communication network based on fuzzy measure theory[D]. Baoding: North China Electric Power University, 2017.
[14] 崇小蕾, 庄子旻, 路超, 等. 基于层次模糊综合评价法的信息安全评价[J]. 信息安全与通信保密, 2014(11): 137-139, 143.
CHONG X L, ZHUANG Z M, LU C, et al. Information security analysis based on AHP and fuzzy comprehensive evaluation[J]. Information Security and Communications Privacy, 2014(11): 137-139, 143.
[15] 王姣, 范科峰, 莫玮. 基于模糊集和DS证据理论的信息安全风险评估方法[J]. 计算机应用研究, 2017, 34(11): 3432-3436.
WANG J, FAN K F, MO W. Method for information security risk assessment based on fuzzy set theory and DS evidence theory[J]. Application Research of Computers, 2017, 34(11): 3432-3436.
[16] 苏琦, 王玮, 刘荫, 等. 电力行业的信息安全防护方案研究[J]. 信息网络安全, 2017(11): 84-88.
SU Q, WANG W, LIU Y, et al. Research on the scheme of information security protection in electric power industry[J]. Netinfo Security, 2017(11): 84-88.
[17] 王静, 高昆仑, 张波. 基于网络隔离与安全数据交换的发电集团双网体系研究与设计[J]. 电信科学, 2017, 33(2): 163-172.
WANG J, GAO K L, ZHANG B. Research and design in dual network scheme of power corporation based on network isolation and secure data exchange[J]. Telecommunications Science, 2017, 33(2): 163-172.
[18] 梁智强, 林丹生. 基于电力系统的信息安全风险评估机制研究[J]. 信息网络安全, 2017(4): 86-90.
LIANG Z Q, LIN D S. Information security risk assessment mechanism research based on power system[J]. Netinfo Security, 2017(4): 86-90.
[19] 姜红红, 张涛, 赵新建, 等. 基于大数据的电力信息网络流量异常检测机制[J]. 电信科学, 2017, 33(3): 134-141.
JIANG H H, ZHANG T, ZHAO X J, et al. A big data based flow anomaly detection mechanism of electric power information network[J]. Telecommunications Science, 2017, 33(3): 134-141.
[20] 王凯, 李婉卿, 白雨欣. 基于模糊综合评判法的电力系统安全评估[J]. 数字技术与应用, 2019, 37(1): 65-67.
WANG K, LI W Q, BAI Y X. Power system security assessment based on fuzzy comprehensive evaluation method[J]. Digital Technology and Application, 2019, 37(1): 65-67.

[作者简介]

**刘道远**（1972− ），男，淮浙煤电有限责任公司高级工程师，主要研究方向为能源工程及自动化。

**孙科达**（1980− ），男，浙江省能源集团有限公司高级工程师，主要研究方向为能源信息技术。



**周君良**（1973− ），男，浙江浙能技术研究院有限公司高级工程师，主要研究方向为能源信息技术。

**范海东**（1979− ），男，浙江浙能技术研究院有限公司、浙江浙能工业信息工程重点企业研究院教授级高级工程师，主要研究方向为能源工程及自动化。