文章编号: 1001-0920(2019)11-2445-07 DOI: 10.13195/j.kzyjc.2019.0240

基于D-AHP和TOPSIS的火电厂控制系统信息安全风险评估

彭道刚[1], 卫 涛[1], 赵慧荣[1†], 姚 峻[2], 王维建[3]

(1. 上海电力大学 自动化工程学院，上海 200090；2. 上海明华电力科技有限公司，上海 200090；3. 上海新华控制技术集团科技有限公司，上海 200241)

摘 要: 火电厂控制系统信息安全风险评估往往存在主观性强和不确定性等问题,而这些问题会对评估结果产生一定影响. 对此,提出一种基于D 数偏好关系改进层次分析法(D-AHP) 和逼近理想解排序法(TOPSIS) 的电厂控制系统信息安全风险评估方法. 根据工业控制系统风险评估的相关行业标准,识别工业控制系统的资产、威胁、脆弱性及现有安全措施,建立评估指标体系和层次结构模型. 针对评估专家经验差异导致的评估信息不确定性,先使用D-AHP 方法求解各指标影响权重,再使用TOPSIS 法求出专家权重,最后得到电厂控制系统信息安全风险值. 实例分析表明了所提出方法的有效性,同时提高了评估结果的正确性.

关键词: 火电厂控制系统；风险评估；D数理论；层次分析法；逼近理想解排序法；信息安全风险值

中图分类号: TP309；TM621 **文献标志码:** A

Cyber security risk assessment of power plant control system based on D-AHP and TOPSIS

PENG Dao-gang[1], *WEI Tao*[1], *ZHAO Hui-rong*[1†], *YAO Jun*[2], *WANG Wei-jian*[3]

(1. College of Automation Engineering，Shanghai University of Electric Power，Shanghai 200090，China；2. Shanghai Minghua Power Science & Technology Co.，Ltd，Shanghai 200090，China；3. Shanghai Xinhua Control Technology Group Co.，Ltd，Shanghai 200241，China)

Abstract: Cyber security risk assessment of control system power plant control systems often has strong subjective and uncertainty problems, and these issues will have a certain impact on the assessment results. To solve this problem, a method of information security risk assessment of power plant control systems based on the D-AHP and the TOPSIS is proposed. According to the relevant industry standards for risk assessment of industrial control systems, assets, threats, vulnerabilities and existing safety measures of industrial control systems are identified, and the assessment index system and a hierarchical structure model are established. Aiming at the uncertainty of assessment information caused by the differencesin expert's experience, the D-AHP is used to solve the impact weights of each index. Then the TOPSIS is used to find the expert weight. Finally, the information security risk value of the control system for power plants is obtained. Example analysis shows the effectiveness of the proposed method and the better accuracy of assessment results.

Keywords: power plant control system；risk assessment；D number theory；AHP；TOPSIS；information security risk value

0 引 言

随着工业4.0、互联网+和工业互联网的不断发展,工业控制系统信息安全问题已引起国内外广泛关注,研究工业控制系统的信息安全是当前国家和社会的重大需求[1]. 2017年新一轮勒索病毒“Petya”使欧洲多个国家的电力系统和通讯系统受到了巨大的影响[2]. 作为国民经济最重要的基础支撑,截止2018年底,全国火电发电装机容量已达到11.45亿千瓦时,亚临界、超临界和超超临界机组已成为主力发电机组,由于电厂全网电气设备与控制信息互联,非法入侵造成的安全隐患非常大,应加强电厂控制系统信息安全的风险评估. 2015年国家能源局颁布了《电力监控系统安全防护评估规范》,因此,非常有必要结合规范及电厂控制系统的特点来研究相应的风险评估方法.

收稿日期: 2019-03-03；**修回日期:** 2019-08-05.

基金项目: 上海市“科技创新行动计划”高新技术领域项目(18511105700, 18511105800).

责任编委: 刘向杰.

[†]通讯作者. E-mail: 766070277@qq.com.

目前,针对工业控制系统常用的评估方法主要有定量评估、定性评估和综合评估[3]. 由于风险评估的特殊性,无法通过具体的现场数据参数得到评价结果,需要参考专家评价,而在数据处理过程中如何减少主观性因素是研究的重点. 许多国内外研究者已经根据模糊层次分析法、DS证据理论、攻击树[4]、神经网络[5]等多种研究方法构建了信息安全风险评估模型,并推动了评估方法的研究进展. 陈卓等[6]提出了基于区间数和理想解的信息安全风险评估方法,有效降低了专家主观性的影响,但在确定指标权重时采用了主观性较强的层次分析法. 林云威等[7]提出了结合DS证据理论和层次分析法来降低主观因素的影响,但存在各安全威胁之间必须无相互影响这一局限性. 钟银超等[8]使用模糊层次分析法(F-AHP)对信息系统进行风险评估,较为客观地反映了系统内部层次结构关系,通过综合评估,在一定程度上提高了评估精度. 但该方法在构建专家评估矩阵时,并未考虑专家经验的差异性对评估结果产生的影响.

基于以上问题,根据发电厂控制系统信息安全的防护要求和风险评估内容的特点,本文利用D数优化层次分析法(D-AHP)建立电厂控制系统信息安全风险评估层次体系,使求得的指标权重更加科学合理,降低专家主观性对评估结果的影响. 结合逼近理想解排序法(TOPSIS)计算专家所给意见的准确度并求得专家评价权重,最后通过计算得到某电厂控制系统信息安全风险值.

1 电厂工业控制系统安全分析

1.1 电厂工业控制系统风险评估目标

发电厂常用的控制系统主要包括分散控制系统(DCS)[9]、可编程控制系统(PLC)以及现场总线系统(FCS). 目前,我国火力发电机组主要采用艾默生、ABB、西门子、国电智深以及北京和利时等公司的DCS. 而发电厂控制系统普遍采用专用的软硬件、操作系统和通信协议,且存在于封闭的网络之中,往往疏于防范,存在着诸多安全隐患[10]. 因此,电厂应建立多技术层面的防护体系,做到物理、网络、终端、数据的多角度、全方位保护. 电厂控制系统安全防护评估规范是通过对资产、威胁、脆弱性评估及赋值,最终得到电厂控制系统的风险综合值. 通过实施风险评估可以发现电厂控制系统存在的安全风险,提出电厂控制系统安全整改建议并实施安全整改,确保电厂控制系统的生命周期安全性.

1.2 构建风险评估指标体系

以国能安全[2015]36号文件作为参考根据,并结合电厂控制系统的实际情况选取评估指标,建立风险评估指标体系[11]. 为了突出重点,对评估指标进行简化. 请专家对资产的保密性、完整性和可用性,环境因素带来的威胁和人为因素造成的威胁,技术脆弱性和管理脆弱性,以及已有的预防性安全措施和保护性安全措施这9个方面进行评估和赋值. 电厂信息安全风险评估体系如表1所示.

表 1 电厂信息安全风险评估体系

一级指标	二级指标	描述
资产(U_1)	保密性(U_{11})	数据所达到的未提供或未泄露给非授权的个人、过程或者其他实体的程度
	完整性(U_{12})	保证信息及信息系统不会被非授权更改或破坏的特性
	可用性(U_{13})	数据或资源的特性,被授权实体按要求能访问和使用的数据或资源
威胁(U_2)	环境因素(U_{21})	自然界不可抗因素和其他物理因素
	人为因素(U_{22})	分为恶意和非恶意两种
脆弱(U_3)	技术脆弱性(U_{31})	包含物理层、网络层、系统层、应用层等各个层面的安全问题
	管理脆弱性(U_{32})	分为技术管理脆弱性和组织管理脆弱性,前者与具体技术活动相关,后者与管理环境相关
已有安全措施(U_4)	预防性安全措施(U_{41})	预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性
	保护性安全措施(U_{42})	保护性安全措施可以减少因安全事件发生后对组织或系统造成的影响

2 控制系统信息安全风险评估算法

2.1 D数理论

D数理论是DS证据理论的扩展,是Deng[12]在DS证据理论基础上提出的不确定性推理理论. 它克服了DS证据理论在表达不确定信息方面的不足,其中基本概率分配(BPA)不需要满足完整性约束,能够处理信息不完整的情况. 与DS证据理论相比,D数理论具有更大的应用范围,可以更好地描述和处理不确定信息. D数理论自从被提出后,由于其独特的优势,目前已应用于不同的领域并取得了很好的效果. 因

此,本文将D数理论用于电厂控制系统风险评估研究.

定义1　设Ω为一个有限的非空集合,D数是一个映射,定义为D: $\Omega \to [0,1]$,满足条件$\sum\limits_{B\subseteq\Omega} D(B) \leqslant 1$,且$D(\varnothing)=0$. 其中: $\varnothing$为空集,B为Ω的子集. 如果$\sum\limits_{B\subseteq\Omega} D(B)=1$,则说明由D数所表示的信息是完整的;反之,信息是不完整的[13].

定义2　令$D=\{(b_1,v_1),(b_2,v_2),\cdots,(b_i,v_i),\cdots,(b_n,v_n)\}$为一个D数,则D数的融合为

$$I(D)=\sum_{i=1}^{n} b_i v_i, \tag{1}$$

可将D数的集成称为I值.

定义3　设存在评估样本U集,基于$U\times U$以模糊集的方式存在,其模糊偏好关系为

$$\mu_R: U\times U \to [0,1]. \tag{2}$$

以矩阵的形式表示为$R=[r_{ij}]_{n\times n}$,即

$$R=\begin{array}{c|cccc} & U_1 & U_2 & \cdots & U_n \\ \hline U_1 & r_{11} & r_{12} & \cdots & r_{1n} \\ U_2 & r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ U_n & r_{n1} & r_{n2} & \cdots & r_{nn} \end{array}.$$

其中r_{ij}表示专家U_i相较于专家U_j的偏好程度. r_{ij}的赋值及对应含义如下:

$$r_{ij}=\begin{cases} 0,\ U_j\text{比}U_i\text{绝对重要}; \\ \in(0,0.5),\ U_j\text{比}U_i\text{重要一些}; \\ 0.5,\ U_j\text{与}U_i\text{同等重要}; \\ \in(0.5,1),\ U_i\text{比}U_j\text{重要一些}; \\ 1,\ U_i\text{比}U_j\text{绝对重要}. \end{cases}$$

定义4　D数偏好关系R_D是指标U的集合,以D数矩阵的方式存在,有

$$\mu_R: U\times U\to D. \tag{3}$$

以矩阵的形式表示为$R_D=[D_{ij}]_{n\times n}$,即

$$R_D=\begin{array}{c|cccc} & U_1 & U_2 & \cdots & U_n \\ \hline U_1 & D_{11} & D_{12} & \cdots & D_{1n} \\ U_2 & D_{21} & D_{22} & \cdots & D_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ U_n & D_{n1} & D_{n2} & \cdots & D_{nn} \end{array}.$$

其中

$$D_{ij}=\{(b_1^{ij},v_1^{ij}),(b_2^{ij},v_2^{ij}),\cdots,(b_m^{ij},v_m^{ij})\},$$
$$D_{ji}=\{(1-b_1^{ij},v_1^{ij}),(1-b_2^{ij},v_2^{ij}),\cdots,(1-b_m^{ij},v_m^{ij})\},\ \forall i,j\in\{1,2,\cdots,n\};$$
$$b_k^{ij}\in[0,1],\ \forall k\in\{1,2,\cdots,m\};$$
$$D_{ii}=\{(0.5,1.0)\},\ \forall i\in\{1,2,\cdots,n\};$$

b_k^{ij}表示第k位专家认为第i个方案相对于第j个方案的重要程度; v_k^{ij}表示该专家对该重要程度的支持度.

2.2　D-AHP方法

层次分析法(AHP)将与决策目标有关的元素按照层级关系分解成顶层目标、中间层准则以及底层方案的层级结构,是一种定量与定性相结合的综合性分析方法[14]. 但典型的层次分析法不适用于处理存在不确定信息的主观评价. 因此,本文通过采用改进的D-AHP方法来更好地处理不确定环境下的风险评估问题. 火电厂控制系统信息安全风险评估层次结构模型如图1所示.

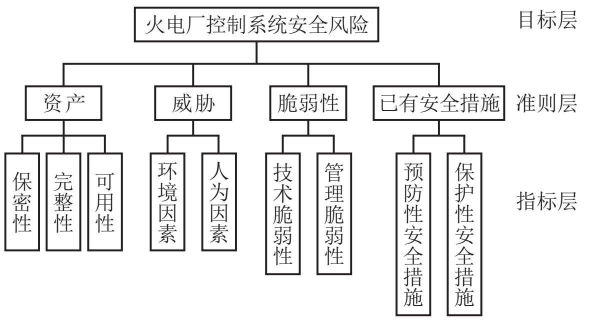

图1　火电厂控制系统信息安全风险评估层次结构模型

计算指标权重的D-AHP方法描述如下.

Step 1: 组织评估专家成对比较各指标并构建D数偏好矩阵R_D;

Step 2: 利用D数融合公式将D数偏好矩阵R_D转化为实数矩阵R_C;

Step 3: 构建基于确定数矩阵R_C的概率矩阵R_P,计算成对比较指标间的偏好概率;

Step 4: 计算R_P矩阵中每行的和并按大小进行排序,然后根据矩阵排序得到三角化矩阵R_P^{T};

Step 5: 根据三角化矩阵R_P^{T}对实数矩阵R_C三角化,得到三角化的实数矩阵R_C^{T};

Step 6: 根据矩阵计算各指标的相对权重.

在计算权重时,由下式计算不一致系数:

$$\mathrm{I.D.}=\frac{\sum\limits_{i=1}^{n} R_P^{\mathrm{T}}(i,j)}{n(n-1)/2},\ j<i, \tag{4}$$

其中n表示成对比较的指标个数.

2.3　TOPSIS方法

TOPSIS称为逼近理想解排序法,是多目标决策问题中一种常用的方法,又称为优劣解距离法[15]. 首先定义决策问题中的理想化目标,即正理想解和负理

想解;然后,通过计算评估样本与正负理想解的相对接近度,作为各个评估样本的优劣程度的标准;最后找到那个距正理想解的距离最近、而距负理想解的距离最远的方案. 该方法的计算步骤如下.

Step 1: 建立初始评判矩阵 M_A. 设评估专家组

$$h=\{h_1,h_2,\cdots,h_n\},$$

评估对象指标集

$$U=\{U_1,U_2,\cdots,U_n\}.$$

构建初始评判矩阵 $M_A=[a_{ij}]_{n\times m}$,即

$$M_A=\begin{bmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{im} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nm} \end{bmatrix}.$$

Step 2: 规范化处理评判矩阵. 区分极大性指标和极小性指标,由以下两式对上述两种评估指标进行规范化处理:

对于极大性指标,有

$$b_{ij}=\frac{a_{ij}-\min(a_{ij})}{\max(a_{ij})-\min(a_{ij})}; \tag{5}$$

对于极小性指标,有

$$b_{ij}=\frac{\max(a_{ij})-a_{ij}}{\max(a_{ij})-\min(a_{ij})}. \tag{6}$$

由 b_{ij} 构成规范化评判矩阵 $M_B=[b_{ij}]_{n\times m}$.

Step 3: 构建加权规范阵. 评估指标权重与规范化判断矩阵 M_B 对应相乘, $M_C=[c_{ij}]_{n\times m}$,其中 $c_{ij}=w_jb_{ij}$.

Step 4: 确定正负理想解. 由下式计算各评估样本指标的理想解:

$$S_j^+=\max_{1\leqslant i\leqslant n}\{c_{ij}\},\ j=1,2,\cdots,m; \tag{7}$$

$$S_j^-=\min_{1\leqslant i\leqslant n}\{c_{ij}\},\ j=1,2,\cdots,m. \tag{8}$$

其中: S_j^+ 表示正理想解, S_j^- 表示负理想解.

Step 5: 由下式计算每个评估样本与正负理想解之间的欧氏距离:

$$D_i^+=\sqrt{\sum_{j=1}^{m}(c_{ij}-S_j^+)^2}, \tag{9}$$

$$D_i^-=\sqrt{\sum_{j=1}^{m}(c_{ij}-S_j^-)^2}, \tag{10}$$

其中 D_i^+ 和 D_i^- 分别表示评估样本与正负理想解之间的欧氏距离.

Step 6: 由下式得出贴进度大小:

$$D_i=\frac{D_i^-}{D_i^++D_i^-}, \tag{11}$$

根据贴进度大小对各样本进行相对优劣排序,然后进行归一化处理便可求得各专家权重. 贴近度 D_i 反映了各样本对象靠近正理想解、远离负理想解的程度.

3 实例分析

3.1 计算评估指标权重

本文以某火电厂300 MW机组作为评估对象,其控制系统为MaxDNA分散控制系统. 电厂控制系统信息安全风险评估方法流程如图2所示. 通过对电厂进行调研并加以分析,建立简化的电厂信息安全风险评估指标体系,然后通过问卷调查收集行业专家评估数据,构建评估指标的D数偏好矩阵.

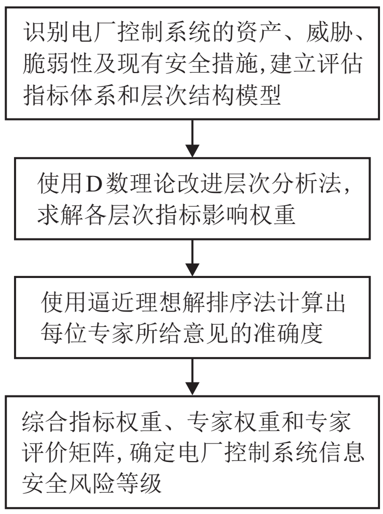

图 2 电厂控制系统信息安全风险评估方法流程

以资产、威胁、脆弱性、已有的安全措施这4个一级指标为例,计算各指标相对于火电厂控制系统信息安全风险的权重.

1) 为确定各一级指标关于信息安全风险的相对重要性,建立基于D数偏好关系的D数偏好矩阵 R_D,即

$$R_D=\begin{array}{c} \\ U_1 \\ U_2 \\ U_3 \\ U_4 \end{array}\begin{array}{c} \begin{array}{cccc} U_1 & U_2 & U_3 & U_4 \end{array} \\ \begin{bmatrix} \{(0.50,1.00)\} & \{(0.10,1.00)\} & \{(0.75,1.00)\} & \{(0.60,0.70),(0.70,0.30)\} \\ \{(0.90,1.00)\} & \{(0.50,1.00)\} & \{(0.75,1.00)\} & \{(0.60,1.00)\} \\ \{(0.25,1.00)\} & \{(0.25,1.00)\} & \{(0.50,1.00)\} & \{(0.80,1.00)\} \\ \{(0.40,0.70),(0.30,0.30)\} & \{(0.40,1.00)\} & \{(0.20,1.00)\} & \{(0.50,1.00)\} \end{bmatrix} \end{array}.$$

2) 利用D数融合公式将D数偏好矩阵R_D转化为实数矩阵R_C,即

$$R_C = I(R_D) = \begin{array}{c} \\ U_1 \\ U_2 \\ U_3 \\ U_4 \end{array}\begin{array}{c} \begin{array}{cccc} U_1 & U_2 & U_3 & U_4 \end{array} \\ \begin{bmatrix} 0.50 & 0.10 & 0.75 & 0.63 \\ 0.90 & 0.50 & 0.75 & 0.60 \\ 0.25 & 0.25 & 0.50 & 0.80 \\ 0.37 & 0.40 & 0.20 & 0.50 \end{bmatrix} \end{array}.$$

3) 构建基于R_C的概率矩阵R_P,通过三角化方法将概率矩阵R_P转化为R_P^{T},有

$$R_P^{\mathrm{T}} = \begin{array}{c} \\ U_2 \\ U_1 \\ U_3 \\ U_4 \end{array}\begin{array}{c} \begin{array}{cccc} U_2 & U_1 & U_3 & U_4 \end{array} \\ \begin{bmatrix} 0.00 & 1.00 & 1.00 & 0.90 \\ 0.00 & 0.00 & 1.00 & 1.00 \\ 0.00 & 0.00 & 0.00 & 1.00 \\ 0.00 & 0.10 & 0.00 & 0.00 \end{bmatrix} \end{array}.$$

对准则层的4个一级指标进行排序,得到的结果是:$U_2 \succ U_1 \succ U_3 \succ U_4$. 此结果表明,对火电厂控制信息安全风险重要程度由高到低依次是:威胁U_2、资产U_1、脆弱性U_3和已有安全措施U_4.

由式(4)计算得到的R_D不一致系数$\mathrm{I.D.} = 0.02$,该值在容许范围之内.

4) 根据指标排序将矩阵R_C表示为R_C^{T},有

$$R_C^{\mathrm{T}} = \begin{array}{c} \\ U_2 \\ U_1 \\ U_3 \\ U_4 \end{array}\begin{array}{c} \begin{array}{cccc} U_2 & U_1 & U_3 & U_4 \end{array} \\ \begin{bmatrix} 0.50 & 0.90 & 0.75 & 0.60 \\ 0.10 & 0.50 & 0.75 & 0.63 \\ 0.25 & 0.25 & 0.50 & 0.80 \\ 0.40 & 0.37 & 0.20 & 0.50 \end{bmatrix} \end{array}.$$

根据该矩阵解方程组

$$\begin{cases} \lambda(\omega_{U_2} - \omega_{U_1}) = 0.90 - 0.50, \\ \lambda(\omega_{U_1} - \omega_{U_3}) = 0.75 - 0.50, \\ \lambda(\omega_{U_3} - \omega_{U_4}) = 0.80 - 0.50, \\ \omega_{U_1} + \omega_{U_2} + \omega_{U_3} + \omega_{U_4} = 1, \end{cases}$$

$$\lambda > 0,\ \omega_{U_i} \geqslant 0,\ \forall i \in \{1, 2, 3, 4\}.$$

其中:ω_{U_i}表示电厂控制系统信息安全风险评估体系中第i个一级指标的权重;λ表示信息的可信程度,其取值与参评专家的可信度有关. 因为参评专家经验丰富且可信度较高,所以$\lambda = 2$. 由此可得准则层各一级指标的权重:$U_1 = 0.300, U_2 = 0.500, U_3 = 0.175, U_4 = 0.025$. 由此可以看出,影响电厂控制系统信息安全最大的是电厂面临的各类威胁.

表2　评估指标权重

目标层	一级指标	权重	二级指标	权重	综合权重
电厂控制系统信息安全风险	U_1	0.300	U_{11}	0.395 5	0.118 7
			U_{12}	0.241 1	0.072 3
			U_{13}	0.363 4	0.109 0
	U_2	0.500	U_{21}	0.600 0	0.300 0
			U_{22}	0.400 0	0.200 0
	U_3	0.175	U_{31}	0.385 3	0.067 4
			U_{32}	0.614 7	0.107 6
	U_4	0.025	U_{41}	0.695 4	0.017 4
			U_{42}	0.304 6	0.007 6

同理,可求得各二级指标相对于电厂控制系统信息安全风险评估准则层一级指标的权重,以及相对于目标层的综合权重. 计算结果如表2所示.

各二级指标综合权重向量为

$$W = [0.118\,7, 0.072\,3, 0.109\,0, 0.300\,0, 0.200\,0, 0.067\,4, 0.107\,6, 0.017\,4, 0.007\,6].$$

3.2　TOPSIS法综合评判

结合上文确定的评估指标体系,组织4位评估专家对9项指标按照1～10分的评估标准进行赋值. 对评估指标体系进行分析:确定极大性指标有2个,包括预防性安全措施(U_{41})和保护性安全措施(U_{42}),其评估赋值越大越好;极小性指标有7个,包括保密性(U_{11})、完整性(U_{12})、可用性(U_{13})、环境因素(U_{21})、人为因素(U_{22})、技术脆弱性(U_{31})和管理脆弱性(U_{32}),其评估赋值越小越好. 4位专家分别用h_1、h_2、h_3、h_4表示,专家评判矩阵如表3所示.

表3　专家评判矩阵

专家	因素								
	U_{11}	U_{12}	U_{13}	U_{21}	U_{22}	U_{31}	U_{32}	U_{41}	U_{42}
h_1	3	5	3	4	7	4	5	6	7
h_2	4	3	5	5	6	4	5	6	6
h_3	4	4	4	3	5	3	5	7	7
h_4	3	4	3	4	6	6	4	5	6

1) 由式(5)和(6),对初始评判矩阵M_A极大值和极小值指标进行规范化处理,得到规范化评判矩阵M_B. 然后利用D数改进层次分析法,求得各二级指标权重向量.

2) 对评判矩阵进行加权处理,构建的加权评判矩阵如表4所示.

表4 加权评判矩阵

专家	因素								
	U_{11}	U_{12}	U_{13}	U_{21}	U_{22}	U_{31}	U_{32}	U_{41}	U_{42}
h_1	0.118 7	0.000 0	0.150 0	0.150 0	0.000 0	0.044 7	0.000 0	0.008 7	0.007 6
h_2	0.000 0	0.072 3	0.000 0	0.000 0	0.100 0	0.044 7	0.000 0	0.008 7	0.000 0
h_3	0.000 0	0.072 3	0.545 0	0.300 0	0.200 0	0.067 4	0.000 0	0.017 4	0.007 6
h_4	0.118 7	0.072 3	0.109 0	0.150 0	0.100 0	0.000 0	0.107 6	0.000 0	0.000 0

3) 取各项指标的最大值和最小值作为正负理想解,由式(9)～(11)求得各评估对象与理想解的欧氏距离及贴进度,并进行排序,如表5所示.

表5 评价矩阵与正负理想解的综合距离

专家	D_i^+	D_i^-	贴近度
1	0.240 8	0.225 0	0.483 0
2	0.378 1	0.131 6	0.258 2
3	0.464 5	0.378 3	0.448 9
4	0.193 4	0.274 4	0.586 6

4) 将贴进度归一化处理后可以计算出专家意见的权重向量为

$$W_h = [0.271\,9, 0.145\,3, 0.252\,7, 0.330\,1].$$

5) 最后,综合专家权重W_h、各二级指标权重W和专家评价矩阵,通过公式$\mathrm{Risk} = W_h \times M_A \times W^{\mathrm{T}}$确定某电厂控制系统信息安全风险等级,得出风险值为4.447 6,且风险等级介于$[4, 5]$之间.

3.3 评估结果分析

本文采用D-AHP和TOPSIS方法经计算得到了某电厂控制系统信息安全风险值,其风险值大小处于中等水平,因此,需要采取相应系统防护措施以减低或控制风险等级,使得安全风险达到一个可以接受的水平. 该火电厂面临最大风险是威胁,其中包括拒绝服务攻击、恶意软件、设备与软件被破坏等. 发电厂信息安全防护需要从管理和技术两个方面综合考虑. 通过本次评估发现,该电厂生产大区缺少安全防护措施,工业控制系统自身存在漏洞,防护措施薄弱,操作系统和应用程序软件存在漏洞、威胁多途径侵入并且缺失安全策略和安全管理. 存在的这些安全漏洞使电厂控制系统难以防范病毒的入侵,并且容易遭受拒绝服务、数据窃取、通信篡改和恶意操作. 因此,有必要对电厂出现的这些风险进行整改并根据电厂实际需求进行安全防护,例如对电厂布置审计、边界防火墙、入侵检测系统、工控主机卫士和统一管理平台等.

4 结 论

本文针对发电厂控制系统信息安全风险评估中存在主观性强和不确定性的问题,提出了基于D-AHP和TOPSIS的风险评估方法. 首先通过D-AHP法得到指标权重,然后利用决策方法TOPSIS计算出评估专家的权重,最后计算出某电厂的风险等级. 该方法有效解决了风险评估过度依赖专家经验和存在不确定性等问题,而且提高了评估结果的准确性.

另外,本文为了突出方法的重点,在构建电厂控制系统信息安全评估指标时进行了简化,难免存在指标不健全的情况. 因此,完善电厂控制系统信息安全评估指标体系以及分析指标间的关联性是下一步需要研究的内容.

参考文献(References)

[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] 李田, 苏盛, 杨洪明, 等. 电力信息物理系统的攻击行为与安全防护[J]. 电力系统自动化, 2017, 41(22): 162-167.
(Li T, Su S, Yang H M, et al. Attacks and cyber security defense in cyber-physical power system[J]. Automation of Electric Power Systems, 2017, 41(22): 162-167.)

[3] 陶耀东, 李宁, 曾广圣. 工业控制系统安全综述[J]. 计算机工程与应用, 2016, 52(13): 8-18.
(Tao Y D, Li N, Zeng G S. Review of industrial control systems security[J]. Computer Engineering and

Applications, 2016, 52(13): 8-18.)

[4] 任秋洁, 潘刚, 白永强. 基于FAHP和攻击树的信息系统安全风险评估[J]. 电子技术应用, 2018, 44(8): 119-123.
(Ren Q J, Pan G, Bai Y Q. Security risk assessment of information system based on FAHP andattack tree[J]. Application of Electronic Technique, 2018, 44(8): 119-123.)

[5] 赵冬梅, 刘金星, 马建峰, 等. 基于改进小波神经网络的信息安全风险评估[J]. 计算机科学, 2010, 37(2): 90-93.
(Zhao D M, Liu J X, Ma J F, et al. Risk assessment of information security based on improved wavelet neural network[J]. Computer Science, 2010, 37(2): 90-93.)

[6] 陈卓, 邹华莎, 沈华, 等. 基于区间数和理想解的信息安全风险评估研究[J]. 计算机应用研究, 2017, 34(8): 2469-2472.
(Chen Z, Zou H S, Shen H, et al. Research on information security risk assessment based on interval number and TOPSIS[J]. Application Research of Computers, 2017, 34(8): 2469-2472.)

[7] 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.
(Lin Y W, Chen D Q, Peng Y, et al. Cyber security risk assessment of industrial control system for power plant using DS evidence theory[J]. Journal of East China University of Science and Technology: Natural Sciences, 2014, 40(4): 500-505.)

[8] 钟银超, 谭世海, 杨太国. 基于模糊层次分析法的电力安全风险评估[J]. 重庆电力高等专科学校学报, 2011, 16(5): 53-56.
(Zhong Y C, Tan S H, Yan T G. Risk assessment of power safety based on FAHP[J]. Journal of Chongqing Electric Power College, 2011, 16(5): 53-56.)

[9] 张敏, 张五一, 韩桂芬. 工业控制系统信息安全防护体系研究[J]. 工业控制计算机, 2013, 26(10): 25-27.
(Zhang M, Zhang W Y, Han G F. Industrial control system information system security[J]. Industrial Control Computer, 2013, 26(10): 25-27.)

[10] 魏晓雷, 刘龙涛. 电力行业工业控制系统信息安全风险评估研究[J]. 信息安全研究, 2018, 4(10): 904-913.
(Wei X L, Liu L T. Research on information security risk assessment of power industry control system[J]. Journal of Information Security Research, 2018, 4(10): 904-913.)

[11] 卢慧康, 陈冬青, 彭勇, 等. 工业控制系统信息安全风险评估量化研究[J]. 自动化仪表, 2014, 35(10): 21-25.
(Lu H K, Chen D Q, Peng Y, et al. Quantitative research on risk assessment for information security of industrial control system[J]. Process Automation Instrumentation, 2014, 35(10): 21-25.)

[12] Deng Y. D numbers: Theory and applications[J]. Journal of Information and Computational Science, 2012, 9(9): 2421-2428.

[13] 王宁奎, 魏代俊. 基于D数理论的不确定多属性决策方法[J]. 湖北民族学院学报: 自然科学版, 2016, 34(1): 35-39.
(Wang N K, Wei D J. Uncertain multiattribute decision making method based on D numbers[J]. Journal of Hubei University for Nationalities: Natural Sciences, 2016, 34(1): 35-39.)

[14] 柴继文, 王胜, 梁晖辉, 等. 基于层次分析法的信息安全风险评估要素量化方法[J]. 重庆大学学报: 自然科学版, 2017, 40(4): 44-53.
(Chai J W, Wang S, Liang H H, et al. An AHP-based quantified method of information security risk assessment elements[J]. Journal of Chongqing University: Natural Sciences, 2017, 40(4): 44-53.)

[15] 黄玉洁, 唐作其, 梁静. 基于信息熵与三参数区间的信息安全风险评估[J]. 计算机工程, 2018, 44(12): 178-183.
(Huang Y J, Tang Z Q, Liang J. Information security risk assessment based on information entropy and three-parameter interval[J]. Computer Engineering, 2018, 44(12): 178-183.)

作者简介

彭道刚 (1977–), 男, 教授, 博士, 从事智能发电、能源互联网、工控安全等研究, E-mail: pengdaogang@126.com;

卫涛 (1995–), 男, 硕士生, 从事智能发电信息安全技术的研究, E-mail: weitao_zdh@163.com;

赵慧荣 (1990–), 女, 讲师, 博士, 从事智能发电优化控制、智能发电信息安全技术的研究, E-mail: 766070277@qq.com;

姚峻 (1970–), 男, 高级工程师, 硕士, 从事发电厂过程控制的功能设计、优化调试等研究, E-mail: yaoj@mhdlshanghaipower.com;

王维建 (1974–), 男, 高级工程师, 博士, 从事信号处理、工业控制系统安全等研究, E-mail: wangwj@xinhuagroup.com.

(责任编辑: 李君玲)