Research Article

Combination of D-AHP and Grey Theory for the Assessment of the Information Security Risks of Smart Grids

Hua Dong ¹, Jun Zhao ², Xiaoyu Yang ¹ and Kun Yang¹

¹School of Economics and Management, North China Electric Power University, Beijing 102206, China

²School of Humanities and Social Sciences, North China Electric Power University, Beijing 102206, China

Correspondence should be addressed to Jun Zhao; zhaoj@ncepu.edu.cn

Received 8 March 2020; Revised 20 July 2020; Accepted 20 August 2020; Published 24 October 2020

Academic Editor: Guido Ala

Copyright © 2020 Hua Dong et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As a modern power infrastructure, smart grids have great advantages over traditional power grids, but their effective operation is largely restricted by information security. Hence, a smart grid information security risk assessment (ISRA) method is proposed. This method combines D numbers to improve the classical analytic hierarchy process (D-AHP) independent of experts' subjective qualitative assessment and then integrated with grey theory which does not require complete and unambiguous information. First, we establish a smart grid ISRA system according to the characteristics and development reality of smart grid technology. The proposed system includes 5 first-level indexes as an intelligent terminal, a wireless communication channel, password security, application code and embedded system, and corresponding 13 secondary indexes. Second, a D-AHP method aimed at the uncertainty of human subjective judgment and fuzziness of language assessment is used to obtain the weight of each index. The D-AHP method is then combined with the grey assessment matrix solved by grey theory, to obtain the comprehensive assessment value and corresponding risk grade. With a smart grid demonstration project in Suzhou, China, as an example, an empirical study is carried out using expert scoring. The comprehensive assessment risk value is 3.8199, and the corresponding risk level is moderate. The results of this work could serve as a reference for the information security protection of smart grids.

1. Introduction

Smart grids are regarded not only as advanced grids but also as an advanced modern power infrastructure, which occupies an important strategic position in national transmission and distribution systems [1]. The National Institute of Standards and Technology (NIST) describes a smart grid as the integration of the traditional grid in the last century and the development of information and communication technology in this century [2]. As smart grids are complex systems, they are prone to attacks [3]. Therefore, smart grid information security is particularly important. The reduction of information security risks to an acceptable level directly affects the stable and efficient operation of smart grids.

Thus far, scholars have mainly studied information security risks in various fields and have used different methods to evaluate them. In [4], a hierarchical model of threat

identification and vulnerability identification is built for information security risk. However, because the analytic hierarchy process (AHP) relies on expert scoring, subjective uncertainty easily leads to the judgment matrix not satisfying the consistency test. The research in [5, 6] contends that although grey theory can compensate for missing parameters and extract valuable information, it does not consider the uncertainty of the assessment values of parameters in the assessment process. In [7, 8], the AHP is combined with fuzzy theory to estimate information security risk objectively. Fuzzy theory improves the accuracy of information security risk assessment (ISRA) to a certain extent. In [9], the ordered weighted averaging operator is used to assign subjectively strong and small values to a weak position, and group decision theory is introduced to improve the accuracy and objectivity of the risk assessment. In [10, 11], the Bayesian network assessment model is improved by establishing and analyzing the relationship between elements; this

approach shows great advantages in dealing with uncertain information. The AHP method is often combined with the technique for order preference by similarity to ideal solution (TOPSIS). In [12], the AHP-TOPSIS method extended with Pythagorean fuzzy sets is proposed and applied to information security risk analysis. However, this method relies too much on expert experience and fails to consider the influence between risk parameters. In [13], enterprise architecture management (EAM) is conducive to information system security risk management (ISSRM) and thereby establishes the EAM-ISSRM model. However, only the framework system is formed, and the risk is not calculated.

Hence, the current work proposes a method to improve the information security risk of smart grids by combining D-AHP and grey theory. D-AHP retains the clear hierarchical logic and simple calculation of the AHP algorithm, but the AHP algorithm cannot form subjective data with nonreal number uncertainty into a paired complementary judgment matrix due to differences in expert experiences. Therefore, the preference relationship of D numbers is introduced to improve the AHP algorithm. The proposed method can deal with the assessment of uncertain (degree of preference) and incomplete (experts who do not give assessment opinions) information in multiattribute group decision making, thereby replacing the paired complementary judgment matrix that must exist in real numbers. This method has been effectively applied to the field of enterprise management and engineering [14, 15]. In addition, the method itself is constantly being improved and strengthened [16]. AHP methods are often used in conjunction with multiple methods [17–20].

Although D-AHP can restore objective facts, it still relies entirely on expert scoring. The subjective component still occupies a large proportion. Hence, quantitatively reflecting on the influence of subjective factors on results remains difficult. The whitening weight function in grey theory added to the D-AHP method can transform a qualitative problem into a quantified one. In other words, the whitening weight function in grey theory can be determined according to the actual background to quantitatively describe the degree of belongingness to a certain grey class (the degree of preference for different values within the value range of the grey class).

Therefore, this study aims to further improve the accuracy of smart grid ISRA by combining the D-AHP method with grey theory. The risk assessment value obtained with this combined model is intuitive and could serve as a scientific reference for avoiding the information security risk of smart grids.

This paper is organized as follows: Section 2 constructs the smart grid information security risk index system, Section 3 presents the model that combines D-AHP and grey theory, Section 4 reports a case study, and Section 5 concludes the paper.

2. Construction of Smart Grid Information Security Risk Index System

2.1. Smart Grid Concept. Smart grids are aimed at fully satisfying user demand for power and optimizing resource

allocation. They also help ensure the security, reliability, and economy of power supply while satisfying environmental protection constraints. Moreover, they are useful in ensuring power quality and adapting to the development of the power market. In sum, smart grids are used to realize reliable, economic, clean, and interactive power supply and value-added services for users. Each country maintain its own definition of smart grids, as presented in Table 1.

2.2. Challenges of Smart Grids. Changing from traditional power base to smart grid will bring great social and technical benefits [3]. It also changes from the single energy flow of traditional power grid to the bidirectional energy flow and information flow of smart grid (Figure 1). Unlike traditional power grids, smart grids can maximize energy demand distribution, improve efficiency, minimize losses, and make large-scale renewable energy (such as solar and wind energy deployments) a reality [2]. Enhanced multi-energy transmission management and the intervention of intelligent management improve system recovery capabilities [24, 25].

New areas of development often coexist with challenges. Smart grids are highly dependent on information and communication technology and are interconnected with the Internet. Hence, network security and privacy issues are inevitable. Each network layer and technology used may become possible targets, and thus, smart grids have a huge attack surface. For example, threats can use the network to access smart appliances through smart meters to steal user data.

2.3. Information Security Risk Index of Smart Grid. On the basis of previous research [24, 26–29], we evaluate the concept of smart grids; select 5 first-level indexes and 13 second-level indexes of a smart terminal, wireless communication channel, password security, application code, and embedded system; and establish the information security risk indexes of smart grids (Table 2).

3. Basic Theory

3.1. D Numbers Theory. D numbers theory [30] is an improvement of D-S evidence theory [31] as it breaks through the deficiency of D-S evidence theory in expressing certain types of information. D numbers theory is based on the advantage of D-S evidence theory in dealing with uncertain information. It is no longer subject to the two conditions of a recognition framework; that is, it must be a mutually exclusive, holistic, and detailed set; and the sum of all propositions is equal to 1 (Figure 2).

In Figure 2, the lines in the graph represent the recognition framework (referred to as domain in D numbers), and the maximum length of a straight line is expressed as 1. The length of the lines occupied by A , B , and C denotes the weight of the elements in the set. This uncertainty information representation method is defined as follows.

Definition 1 (see [31]). Let Ω be a finite nonempty set with mapping D formulated by

TABLE 1: Definition of smart grids.

No.	Country	Department	Time
(1) [2]	CHN	National development and reform commission, national energy administration ¹	2015
(2) [21]	US	National institute of standards and technology (NIST) ²	2013
(3) [21]	EUR	European commission ³	2011
(4) [22]	EUR	European smart grid task force ⁴	2011
(5) [23]	US	US Department of energy <i>Grid2030</i> ⁵	2003
...			

¹By integrating new technologies of renewable energy, new material, new equipment, and advanced sensors; information technology; control technology; and energy storage, smart grids comprise a new-generation electric power system based upon the traditional power system. Smart grids have distinctive features, including highly interactive, informationized, and automatized properties, which help to ensure the safe, reliable, economic, and efficient operation of the power grid. ²The NIST defines a smart grid as the integration of the last century power grid with the current century development in information and communication technologies. ³A smart grid is an upgraded electricity network to which two-way digital communication between suppliers and consumers, intelligent metering, and monitoring systems have been added. ⁴Smart grids are electricity networks that can efficiently integrate the behavior and actions of all users connected to them, so as to effectively provide sustainable economic and safe electricity. ⁵US Department of Energy *Grid 2030*: A smart grid is a fully automated power transmission network that can monitor and control each user and network node, thus ensuring the bidirectional flow of information and energy between all nodes in the transmission and distribution processes from power plants to end users.

FIGURE 1: Comparison between smart grid and traditional grid. (a) Traditional power grid; (b) smart power grid.

$$D : \Omega \longrightarrow [0, 1], \quad (1)$$

with

$$\sum_{B \subseteq \Omega} D(B) \leq 1 \text{ and } D(\emptyset) = 0, \quad (2)$$

where $\emptyset$ is an empty set and B is a subset of Ω . The elements in Ω need not be mutually exclusive; if $\sum_{B \subseteq \Omega} D(B) = 1$, then the information in Ω is considered complete; if $\sum_{B \subseteq \Omega} D(B) \neq 1$, then the information in Ω is considered missing.

TABLE 2: Information security risk indexes of smart grids.

Target level	Primary index	Secondary index	Description
Information security risk of smart grid	Smart terminal [24]	Intelligent terminal for self-security	Configuration of software and hardware, terminal access control, and terminal information security storage
		Intelligent terminal for access security	Terminal identity authentication
		Intelligent terminal data for transmission security	Data encryption transmission
	Wireless communication channel [26]	Wireless communication protocol as self-security mechanism	Contactless interception
		Enhanced security attributes of communication channels	Security enhancement attributes (e.g., private, encrypted, and trusted)
	Password security [27]	Password strength assessment	Effectiveness of guessing or violent cracking
		Password usage mechanism assessment	Cryptographic algorithm, protection mechanism, etc.
	Application code [28]	Key distribution assessment	Not accessed by others, regularly updated, etc.
		Application code design	Single responsibility principle, Liskov substitution principle, etc.
	Embedded system [29]	Application code development	Sustainability, streamlining, timely bug correction, etc.
		Application code test	Controllability, visibility, simplicity, etc.
		Software layer	Memory chip, software code, etc.
		Hardware layer	Reliability, speed, processing power, etc.

FIGURE 2: Difference between evidence theory and D numbers. (a) Identifying the relationship between frames and elements in a set in evidence theory; (b) the relationship between the D numbers field and the elements in a set.

If the discrete set is $\Omega = \{b_1, b_2, \dots, b_i, \dots, b_n\}$, where $b_i \in R$ and $b_i \neq b_j$, and if $i \neq j$, then a special form of D numbers is expressed by

$$\begin{aligned}
 D(\{b_1\}) &= v_1, \\
 D(\{b_2\}) &= v_2, \\
 &\dots \\
 D(\{b_i\}) &= v_i, \\
 &\dots \\
 D(\{b_n\}) &= v_n,
 \end{aligned} \tag{3}$$

or $D = \{(b_1, v_1), (b_2, v_2), \dots, (b_i, v_i), \dots, (b_n, v_n)\}$, $v_i > 0$ and $\sum_{i=1}^n v_i \leq 1$.

Definition 2 (see [31]). If $D = \{(b_1, v_1), (b_2, v_2), \dots, (b_i, v_i), \dots, (b_n, v_n)\}$, then the integration of D is defined as

$$I(D) = \sum_{i=1}^n b_i v_i, \tag{4}$$

where $b_i \in R$, $v_i > 0$, and $\sum_{i=1}^n v_i \leq 1$.

Example 1. Assume 10 experts scoring the two schemes. Of the 10 experts, 7 think that the probability of scheme 1 is

better than that of scheme 2 at 0.75, and 3 experts think that the probability of scheme 1 is better than that of scheme 2 at 0.8. The D numbers are expressed as $D = \{(b_1 = 0.75, v_1 = 0.7), (b_2 = 0.8, v_2 = 0.3)\}$.

$$I(D) = \sum_{i=1}^n b_i v_i = b_1 v_1 + b_2 v_2 = 0.75 \times 0.7 + 0.8 \times 0.3 = 0.765. \quad (5)$$

3.2. D Numbers Preference Relation. Fuzzy preference relation is a commonly used method to compare and assign assessment samples. The decision matrix constructed can reflect the preference degree of assessment experts for specific schemes.

Definition 3 (see [32]). Suppose that set A consists of n assessment indexes. Set $A = \{A_1, A_2, \dots, A_n\}$. Its fuzzy preference relation is as follows:

$$\mu_R: A \times A \longrightarrow [0, 1]. \quad (6)$$

If the cardinality of index A is small, then the fuzzy preference relationship can be expressed by matrix $R = [r_{ij}]_{n \times n}$ that is,

$$R = \begin{matrix} & \begin{matrix} A_1 & A_2 & \dots & A_n \end{matrix} \\ \begin{matrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{matrix} & \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \dots & r_{nn} \end{bmatrix} \end{matrix}, \quad (7)$$

where

- (a) $r_{ij} \geq 0$;
- (b) $r_{ij} + r_{ji} = 1, \forall i, j \in \{1, 2, \dots, n\}$;
- (c) $r_{ii} = 0.5, \forall i \in \{1, 2, \dots, n\}$.

r_{ij} represents the degree of preference of experts for index A_i relative to index A_j .

$$r_{ij} = \mu_R(A_i, A_j) = \begin{cases} 0 & A_j \text{ is completely superior to } A_i, \\ \in (0, 0.5) & \text{the degree of } A_j \text{ is better than } A_i, \\ 0.5 & A_i \text{ is as important as } A_j, \\ \in (0.5, 1) & \text{the degree of } A_i \text{ is better than } A_j, \\ 1 & A_i \text{ is completely superior to } A_j. \end{cases} \quad (8)$$

However, the fuzzy preference relationship is not able to construct a reasonable preference matrix due to the incomplete or uncertain assessment information of experts. The D preference relation proposed by [30] is an extension of fuzzy preference relation based on D numbers theory; it can solve the restriction of the use conditions of fuzzy preference

relation and expand its application to the field of uncertain information. The corresponding matrix is called D numbers preference matrix or simply the D matrix.

Definition 4 (see [31]). Let set $A = \{A_1, A_2, \dots, A_n\}$ of assessment indexes exist, and let the preference relation of D number exist in the form of a matrix expressed as

$$R_D: A \times A \longrightarrow D, \quad (9)$$

$$R_D = \begin{matrix} & \begin{matrix} A_1 & A_2 & \dots & A_n \end{matrix} \\ \begin{matrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{matrix} & \begin{bmatrix} D_{11} & D_{12} & \dots & D_{1n} \\ D_{21} & D_{22} & \dots & D_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ D_{n1} & D_{n2} & \dots & D_{nn} \end{bmatrix} \end{matrix}, \quad (10)$$

where

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

Take Example 1 as an example; it can be expressed as follows according to (10):

$$R_D = \begin{bmatrix} \{(0.5, 1.0)\} & \{(0.75, 0.7), (0.8, 0.3)\} \\ \{(0.25, 0.7), (0.2, 0.3)\} & \{(0.5, 1.0)\} \end{bmatrix}. \quad (11)$$

3.3. Determination of Whitening Weight Function and Construction of Grey Assessment Matrix

3.3.1. Constructing the Assessment Matrix. According to the established assessment index system of information security risk in smart grids, the expert scoring method is used to organize n experts to refer to the assessment grade vector V to score each assessment index. $V = (v_1, v_2, \dots, v_t)$, and t is the number of risk levels; $d_{ij}^{(k)}$ is the assessment value of the k th expert for the j th second-level index of the i th first-level index. The sample matrix D is as follows:

$$D = \begin{bmatrix} d_{11}^{(1)} & d_{12}^{(1)} & \dots & d_{ij}^{(1)} & \dots & d_{mm_i}^{(1)} \\ d_{11}^{(2)} & d_{12}^{(2)} & \dots & d_{ij}^{(2)} & \dots & d_{mm_i}^{(2)} \\ \vdots & \vdots & & \vdots & & \vdots \\ d_{11}^{(k)} & d_{12}^{(k)} & \dots & d_{ij}^{(k)} & \dots & d_{mm_i}^{(k)} \\ \vdots & \vdots & & \vdots & & \vdots \\ d_{11}^{(n)} & d_{12}^{(n)} & \dots & d_{ij}^{(n)} & \dots & d_{mm_i}^{(n)} \end{bmatrix}, \quad (12)$$

$$i = (1, 2, \dots, m; j = 1, 2, \dots, m; k = 1, 2, \dots, n).$$

3.3.2. Determining the Whitening Weight Function. Whitening weight functions have three types that are used to construct the grey assessment matrix in grey statistics. The details are shown in Table 3.

3.3.3. Constructing the Grey Assessment Matrix. Assume E grey classes according to the described problem. Let us determine the whitening weight function f_e . For the second-level assessment index, the grey assessment coefficient of the grey class of the e ($e=1, 2, \dots, E$) assessment is $I_{ij}^{(e)} = \sum_{k=1}^n f_e(d_{ij}^k)$, the total assessment coefficient of the assessment grey is $I_{ij} = \sum_{e=1}^E I_{ij}^{(e)}$, and the grey assessment weight vector of each assessment grey class is $\lambda_{ij}^{(e)} = I_{ij}^{(e)} / I_{ij}$. In this way, the grey assessment weight matrix Λ of each secondary assessment index can be obtained.

$$\Lambda = \begin{bmatrix} \Lambda_1 \\ \vdots \\ \Lambda_i \\ \vdots \\ \Lambda_n \end{bmatrix} = \begin{bmatrix} \lambda_{11}^{(1)} & \dots & \lambda_{11}^{(e)} & \dots & \lambda_{11}^{(E)} \\ \vdots & & \vdots & & \vdots \\ \lambda_{ij}^{(1)} & \dots & \lambda_{ij}^{(e)} & \dots & \lambda_{ij}^{(E)} \\ \vdots & & \vdots & & \vdots \\ \lambda_{nm_i}^{(1)} & \dots & \lambda_{nm_i}^{(e)} & \dots & \lambda_{nm_i}^{(E)} \end{bmatrix}, \quad (13)$$

where $i=1, 2, \dots, m$; $e=1, 2, \dots, E$.

4. Weight Calculation Model Based on D-AHP and Grey Theory

D numbers theory has been widely used in practical multiattribute group decision making because it can effectively describe and process uncertain information and integrate various expert assessment information into group assessment. Aiming toward the grey characteristics of smart grid ISRA with unclear connotation and extension and the assessment language with uncertain language and minimal data, we propose a weight calculation method that combines D-AHP and grey theory. The specific steps are as follows.

Step 1. Organize 10 review experts as an example. According to the smart grid ISRA indexes shown in Table 2, compare the importance and support of each index in terms of the D numbers preference relationship, and establish the D numbers preference matrix R_D .

Step 2. Convert the D numbers preference matrix R_D into a crisp matrix R_C according to formula (4).

Step 3. Construct a probability matrix R_P on the crisp matrix R_C to represent the preference probability of the pairwise comparison index.

The elements in the matrix are recorded as c_{ij} , and the elements in the matrix R_P are represented as $p_{ij} = \Pr(A_i > A_j)$, $\forall i, j \in \{1, 2, \dots, n\}$:

- (i) $c_{ij} + c_{ji} = 1$: if $c_{ij} > 0.5$, then $\Pr(A_i > A_j) = 1$; if $c_{ij} \leq 0.5$, then $\Pr(A_i > A_j) = 0$;
- (ii) $c_{ij} + c_{ji} < 1$: if $c_{ij} \geq 0.5$, then $\Pr(A_i > A_j) = 1$ and $\Pr(A_j > A_i) = 0$; if $c_{ji} \geq 0.5$, then $c_{ji} \geq 0.5$ and $\Pr(A_i > A_j) = 0$;

- (iii) $c_{ij} + c_{ji} < 1$, $c_{ij} < 0.5$, and $c_{ji} < 0.5$; the unallocated preference is $c_{up} = 1 - (c_{ij} + c_{ji})$.

The probability that one index is better than the other is

$$\Pr(A_i > A_j) = 1 - \frac{(0.5 - c_{ij})}{c_{up}}, \quad (14)$$

$$\Pr(A_j > A_i) = 1 - \frac{(0.5 - c_{ji})}{c_{up}}.$$

Step 4. Calculate the sum of each row in the R_P matrix, adjust the order of the row and column in R_P according to the order of the sum of each row, and obtain the triangulation matrix R_P^T . Calculate whether the consistency ratio $I.D. = \sum_{i=1}^n R_P^T(i, j)$, $j < i/n(n-1)/2$ is within the acceptable range.

Step 5. The real number matrix R_C is triangulated according to the triangulation matrix R_P^T , and the real number matrix R_C^T is obtained.

If the elements in R_C^T meet the requirements of $R_C^T(i, j) + R_C^T(j, i) < 1$ (incomplete information), then R_C^T should be standardized further to obtain the normalized matrix R_C^T . The calculation formula is as follows:

$$R_C^T(i, j) = R_C^T(i, j) + \frac{1 - [R_C^T(i, j) + R_C^T(j, i)]}{2}. \quad (15)$$

Step 6. Calculate the weight of each index according to the R_C^T (or R_C^T) matrix. λ refers to the credibility of the information invited by experts and is related to the cognition degree of experts in the field of problem assessment. The larger the value of λ is, the higher the credibility of the expert is. The specific value is as follows [33]:

$$\lambda = \begin{cases} [\underline{\lambda}] & \text{High information credibility,} \\ n & \text{Medium information credibility,} \\ \frac{n^2}{2} & \text{Low information credibility.} \end{cases} \quad (16)$$

Step 7. Determine the risk assessment grade vector V , invite experts to grade the second-level indexes, and construct the sample assessment matrix.

Step 8. Define the whitening weight function according to the assessment level, and calculate the total grey statistics of all secondary indexes and the weight vector of the grey assessment matrix.

Step 9. Calculate the comprehensive assessment vector H , $H = W$ (weight vector obtained by D-AHP) $\times$ (grey assessment matrix obtained by grey statistics method), and the risk assessment value of smart grid information security $\text{Risk} = H \times V^T$.

TABLE 3: Classification of whitening weight functions.

Classification	Grey number $\otimes$	Definition
Upper limit measure	$\otimes \in [d_1, +\infty]$	$f_1(d_{ij}^{(k)}) = \begin{cases} d_{ij}^{(k)}/d_1 & d_{ij}^{(k)} \in [0, d_1] \\ 1 & d_{ij}^{(k)} \in [d_1, +\infty) \\ 0 & d_{ij}^{(k)} \in (-\infty, 0) \end{cases}$
Moderate measure	$\otimes \in [0, d_1, 2d_1]$	$f_2(d_{ij}^{(k)}) = \begin{cases} d_{ij}^{(k)}/d_1 & d_{ij}^{(k)} \in [0, d_1] \\ 2 - (d_{ij}^{(k)}/d_1) & d_{ij}^{(k)} \in [d_1, 2d_1] \\ 0 & d_{ij}^{(k)} \notin (0, 2d_1] \end{cases}$
Lower limit measure	$\otimes \in [0, d_1, d_2]$	$f_3(d_{ij}^{(k)}) = \begin{cases} 1 & d_{ij}^{(k)} \in [0, d_1] \\ d_2 - d_{ij}^{(k)}/d_2 - d_1 & d_{ij}^{(k)} \in [d_1, d_2] \\ 0 & d_{ij}^{(k)} \notin (0, d_2) \end{cases}$

According to the first scoring in Table 2, the expert establishes the D matrix represented by D numbers. Complete and incomplete information need to be subjected to the first five steps. The weight vector W of the D-AHP method is obtained in Step 6. The expert scores for the second time, performs Steps 7 and 8, and obtains the grey assessment matrix Λ of the grey method. Step 9 is the fusion of the two methods to obtain the final smart grid ISRA value Risk. The overall flow chart of D-AHP and the grey method is shown in Figure 3.

5. Case Study

5.1. Building the Index System. To verify the scientific nature of this method in practice, we constructed an ISRA index system for smart power grids (Figure 4) according to the data in Table 2. We evaluate the information security risk of a smart grid in Suzhou, which is located in eastern China and the Pearl River Delta region (Figure 5). The system comprises the following: intelligent terminal, wireless communication channel, password security, application code, and embedded system with five first-level indexes. The intelligent terminal has its own security, access security, data transmission security, etc. The system is embedded with 13

second-level indexes. A total of 10 experts with relatively high credibility in scoring are invited.

5.2. Example Analysis. Take the first-level index as an example. The weights of the intelligent terminal, wireless communication channel, password security, application code, and embedded system relative to the smart grid information security risk are calculated. Note that the indexes are all negative.

Step 1. The indexes are compared in pairs, and the D numbers preference matrix R_D is established on the basis of the D numbers preference relation to represent the importance and support of each index.

$$\lambda = \begin{cases} \lceil \frac{\lambda}{2} \rceil & \text{High information credibility,} \\ n & \text{Medium information credibility,} \\ \frac{n^2}{2} & \text{Low information credibility.} \end{cases} \quad (17)$$

Step 2. According to formula (4), D numbers preference matrix R_D is transformed into a crisp matrix R_C .

$$R_D = \begin{matrix} & B_1 & B_2 & B_3 & B_4 & B_5 \\ \begin{matrix} B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \end{matrix} & \begin{bmatrix} \{(0.5, 1.0)\} & \{(0.1, 1.0)\} & \{(0.3, 0.7), (0.4, 0.3)\} & \{(0.75, 1.0)\} & \{(0.8, 1.0)\} \\ \{(0.9, 1.0)\} & \{(0.5, 1.0)\} & \{(0.2, 0.9)\} & \{(0.9, 1.0)\} & \{(0.7, 1.0)\} \\ \{(0.7, 0.7), (0.6, 0.3)\} & \{(0.8, 0.9)\} & \{(0.5, 1.0)\} & \{(0.55, 0.8)\} & \{(0.65, 1.0)\} \\ \{(0.25, 1.0)\} & \{(0.1, 1.0)\} & \{(0.45, 0.8)\} & \{(0.5, 1.0)\} & \{(0.8, 1.0)\} \\ \{(0.2, 1.0)\} & \{(0.3, 1.0)\} & \{(0.35, 1.0)\} & \{(0.2, 1.0)\} & \{(0.5, 1.0)\} \end{bmatrix} \end{matrix} \quad (18)$$

FIGURE 3: Overall flow chart of D-AHP and grey method.

FIGURE 4: Information security risk index system for smart grids.

FIGURE 5: Geographical location of smart grid project in Suzhou.

Step 3. Construct probability matrix R_p on the basis of R_C .

$$R_C = \begin{matrix} & B_1 & B_2 & B_3 & B_4 & B_5 \\ \begin{matrix} B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \end{matrix} & \begin{bmatrix} 0.5 & 0.1 & 0.33 & 0.75 & 0.8 \\ 0.9 & 0.5 & 0.18 & 0.9 & 0.7 \\ 0.67 & 0.72 & 0.5 & 0.44 & 0.65 \\ 0.25 & 0.1 & 0.36 & 0.5 & 0.8 \\ 0.2 & 0.3 & 0.35 & 0.2 & 0.5 \end{bmatrix} \end{matrix} \quad (19)$$

Step 4. Calculate the sum of each row in the R_p matrix, adjust the order of the row and column in R_p according to the order of the sum of each row, and derive the triangulation matrix R_p^T .

$$R_p = \begin{matrix} & B_1 & B_2 & B_3 & B_4 & B_5 \\ \begin{matrix} B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \end{matrix} & \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0.7 & 1 \\ 0 & 0 & 0.3 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (20)$$

Remove alternative B_5 . Then,

$$R_p = \begin{matrix} & B_1 & B_2 & B_3 & B_4 & B_5 & sum \\ \begin{matrix} B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \end{matrix} & \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0.7 & 1 \\ 0 & 0 & 0.3 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (21)$$

Remove alternative B_2 . Then,

$$R_p^T = \begin{matrix} & B_1 & B_2 & B_3 & B_5 & sum \\ \begin{matrix} B_1 \\ B_2 \\ B_4 \\ B_5 \end{matrix} & \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (22)$$

Remove alternative B_1 . Then,

$$R_p^T = \begin{matrix} & B_1 & B_4 & B_5 & sum \\ \begin{matrix} B_1 \\ B_4 \\ B_5 \end{matrix} & \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (23)$$

Remove alternative B_4 . Then,

$$R_p^T = \begin{matrix} & B_1 & B_5 & sum \\ \begin{matrix} B_1 \\ B_5 \end{matrix} & \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \end{matrix} \quad (24)$$

Remove alternative B_5 . Thus, the ranking of alternatives is $B_3 > B_2 > B_1 > B_4 > B_5$, where $>$ only represents the priority of the order and has no mathematical meaning. Derive triangular matrix R_p^T .

$$R_p^T = \begin{matrix} & B_5 & sum \\ \begin{matrix} B_5 \end{matrix} & \begin{bmatrix} 0 & 0 \end{bmatrix} \end{matrix} \quad (25)$$

Calculate the consistency ratio $I.D. = 0.3/5(5-1)/2 = 0.03 < 0.1$, which is considered as an acceptable level, and proceed to the next step.

Step 5. Triangulate real matrix R_C according to triangulation matrix R_p^T , and obtain triangulation real matrix R_C^T .

$$R_p^T = \begin{matrix} & B_3 & B_2 & B_1 & B_4 & B_5 \\ \begin{matrix} B_3 \\ B_2 \\ B_1 \\ B_4 \\ B_5 \end{matrix} & \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0.7 & 1 \\ 0 & 0 & 0.3 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (26)$$

As $(B_3, B_2) + (B_2, B_3)$ and $(B_3, B_4) + (B_4, B_3) < 1$ in the matrix, further specification is needed.

$$R_C^T = \begin{matrix} & B_3 & B_2 & B_1 & B_4 & B_5 \\ \begin{matrix} B_3 \\ B_2 \\ B_1 \\ B_4 \\ B_5 \end{matrix} & \begin{bmatrix} 0.5 & 0.72 & 0.67 & 0.44 & 0.65 \\ 0.18 & 0.5 & 0.9 & 0.9 & 0.7 \\ 0.33 & 0.1 & 0.5 & 0.75 & 0.8 \\ 0.36 & 0.1 & 0.25 & 0.5 & 0.8 \\ 0.35 & 0.3 & 0.2 & 0.2 & 0.5 \end{bmatrix} \end{matrix} \quad (27)$$

Step 6. According to the experience of experts, determine λ , and calculate weight W . Obtain the values of W_i and λ as follows:

$$\begin{cases} \lambda(w_3 - w_2) = 0.77 - 0.5, \\ \lambda(w_2 - w_1) = 0.9 - 0.5, \\ \lambda(w_1 - w_4) = 0.75 - 0.5, \\ \lambda(w_4 - w_5) = 0.8 - 0.5, \\ w_1 + w_2 + w_3 + w_4 + w_5 = 1, \\ \lambda > 0, \\ w_i \geq 0, \quad \forall i \in \{1, 2, 3, 4\}, \end{cases} \quad (28)$$

$$\begin{cases} w_1 = \frac{1}{5} - \frac{0.054}{\lambda}, \\ w_2 = \frac{1}{5} + \frac{0.346}{\lambda}, \\ w_3 = \frac{1}{5} + \frac{0.616}{\lambda}, \\ w_4 = \frac{1}{5} - \frac{0.304}{\lambda}, \\ w_5 = \frac{1}{5} - \frac{0.604}{\lambda}, \\ \lambda \in [3.02, +\infty), \end{cases} \quad (29)$$

$$\begin{cases} w_1 \in [0.182, 0.2), \\ w_2 \in (0.2, 0.315], \\ w_3 \in (0.2, 0.404], \\ w_4 \in [0.099, 0.2), \\ w_5 \in [0, 0.2). \end{cases} \quad (30)$$

As most of the experts are university research scholars who do not have first-hand experience in professional smart grid research and given that their ability to learn and understand is higher than that of ordinary experts, taking $\lambda = 5$ information with a moderate level of credibility is appropriate. The obtained W is $W_1 = 0.1892$, $W_2 = 0.2692$, $W_3 = 0.3232$, $W_4 = 0.1392$, $W_5 = 0.0792$. The floating matrix (Figure 6) is obtained.

According to 17–(30), calculate the weight of each secondary index relative to the primary index, and obtain the final comprehensive weight W (Table 4).

Obtain the comprehensive weight $W = (0.0406, 0.0617, 0.0869, 0.1299, 0.1393, 0.1074, 0.1300, 0.0858, 0.0480, 0.0571, 0.0341, 0.0410, 0.0382)$, and draw the broken line statistical chart of comprehensive weight (Figure 7).

Step 7. Determine the risk assessment level vector V , invite experts to give a second score, and obtain the grey assessment matrix. According to the secondary assessment index, five experts are invited to score. The higher the score is, the higher the information security risk value of the smart grid is. 5, 4, 3, 2, and 1, respectively, represent very high, high, moderate, low, and extremely low. The scoring results are shown in Table 5.

Take the secondary indexes C_{11} , C_{12} , and C_{13} under the primary assessment index B_1 (intelligent terminal) as an example to form the sample assessment matrix D_1 .

$$D_1 = \begin{bmatrix} 4 & 3.5 & 5 \\ 4 & 4 & 4.5 \\ 3 & 3 & 5 \\ 3.5 & 4 & 4 \\ 4.5 & 3.5 & 4 \end{bmatrix}. \quad (31)$$

According to the assessment level, the five whitening weight functions are defined as $f_1(x)$, $f_2(x)$, $f_3(x)$, $f_4(x)$, and $f_5(x)$. The function expression is as follows:

$$f_1(x) = \begin{cases} \frac{x}{5}, & x \in [0, 5], \\ 1, & x \in [5, +\infty), \\ 0, & x \in (-\infty, 0), \end{cases}$$

$$f_2(x) = \begin{cases} \frac{x}{4}, & x \in [0, 4], \\ \frac{(8-x)}{4}, & x \in [4, 8], \\ 0, & x \notin [0, 8], \end{cases}$$

FIGURE 6: Floating matrix diagram of first-level index weight.

TABLE 4: Summary of index weights and comprehensive weights at all levels.

Target level	Primary index	Weight	Secondary index	Weight	Comprehensive weight
Smart grid information security risk (A)	B_1	0.1892	C_{11}	0.2144	0.0406
			C_{12}	0.3261	0.0617
			C_{13}	0.4594	0.0869
	B_2	0.2692	C_{21}	0.4825	0.1299
			C_{22}	0.5175	0.1393
			C_{31}	0.3322	0.1074
	B_3	0.3232	C_{32}	0.4022	0.1300
			C_{33}	0.2656	0.0858
			C_{41}	0.3450	0.0480
	B_4	0.1392	C_{42}	0.4100	0.0571
			C_{43}	0.2450	0.0341
			C_{51}	0.5175	0.0410
	B_5	0.0792	C_{52}	0.4825	0.0382

FIGURE 7: Broken line statistical chart of comprehensive weight.

TABLE 5: Experts' second scoring.

	C_{11}	C_{12}	C_{13}	C_{21}	C_{22}	C_{31}	C_{32}	C_{33}	C_{41}	C_{42}	C_{43}	C_{51}	C_{52}
Expert1	4	3.5	5	4	3	5	2.5	4	1.5	3	3.5	2	1.5
Expert2	4	4	4.5	4.5	3	5	4	5	4	3.5	4	3	2
Expert3	3	3	5	3.5	3.5	4.5	3	2.5	2.5	3	4.5	3.5	3
Expert4	3.5	4	4	4	3	5	5	3	3	4	2.5	3	2.5
Expert5	4.5	3.5	4	4	3.5	4.5	3.5	4	3	3	3	2.5	3

$$\begin{aligned}
f_3(x) &= \begin{cases} \frac{x}{3}, & x \in [0, 3], \\ \frac{(6-x)}{3}, & x \in [3, 6], \\ 0, & x \notin [0, 6], \end{cases} \\
f_4(x) &= \begin{cases} \frac{x}{2}, & x \in [0, 2], \\ \frac{(4-x)}{2}, & x \in [2, 4], \\ 0, & x \notin [0, 4], \end{cases} \\
f_5(x) &= \begin{cases} 1, & x \in [0, 1], \\ 2-x, & x \in [1, 2], \\ 0, & x \notin [0, 2]. \end{cases}
\end{aligned} \quad (32)$$

Obtain the total assessment coefficient and grey assessment weight vector (Table 6), and the calculation process is shown in the supplementary material.

Step 9. Calculate the comprehensive assessment vector H , $H = W$ (weight vector obtained by D-AHP) $\times \Lambda$ (grey assessment matrix obtained by grey statistical method), and the smart grid ISRA value $\text{Risk} = H \times V^T$. $H = W \times \Lambda = (0.2956, 0.3281, 0.2803, 0.0928, 0.0032)$. $W = (0.0406, 0.0617, 0.0869, 0.1299, 0.1393, 0.1074, 0.1300, 0.0858, 0.0480, 0.0571, 0.0341, 0.0410, 0.0382)$.

$$\Lambda = \begin{bmatrix} 0.2988 & 0.3539 & 0.2883 & 0.0590 & 0.0000 \\ 0.2748 & 0.3435 & 0.3053 & 0.0763 & 0.0000 \\ 0.3956 & 0.3846 & 0.2198 & 0.0000 & 0.0000 \\ 0.3243 & 0.3851 & 0.2703 & 0.0203 & 0.0000 \\ 0.2308 & 0.2885 & 0.3365 & 0.1442 & 0.0000 \\ 0.4444 & 0.3704 & 0.1852 & 0.0000 & 0.0000 \\ 0.2820 & 0.3133 & 0.2878 & 0.1175 & 0.0000 \\ 0.2942 & 0.3280 & 0.2783 & 0.0994 & 0.0000 \\ 0.2105 & 0.2632 & 0.3008 & 0.1880 & 0.0376 \\ 0.2413 & 0.3016 & 0.3291 & 0.1280 & 0.0000 \\ 0.2650 & 0.3312 & 0.2902 & 0.1136 & 0.0000 \\ 0.2054 & 0.2567 & 0.3178 & 0.2200 & 0.0000 \\ 0.1791 & 0.2239 & 0.2985 & 0.2612 & 0.0373 \end{bmatrix}. \quad (33)$$

Thus, the final $\text{Risk} = H \times V^T = 3.8199$.

5.3. Result Analysis. According to the broken line statistical chart of comprehensive weights obtained by D-AHP, we can

TABLE 6: Total grey assessment coefficient and grey assessment weight vector.

Assessment index	Total grey assessment coefficient	Grey assessment weight vector
C_{11}	12.7167	(0.2988, 0.3539, 0.2883, 0.0590, 0.0000)
C_{12}	13.1000	(0.2748, 0.3435, 0.3053, 0.0763, 0.0000)
C_{13}	11.3750	(0.3956, 0.3846, 0.2198, 0.0000, 0.0000)
C_{21}	12.3333	(0.3243, 0.3851, 0.2703, 0.0203, 0.0000)
C_{22}	13.8667	(0.2308, 0.2885, 0.3365, 0.1442, 0.0000)
C_{31}	10.8000	(0.4444, 0.3704, 0.1852, 0.0000, 0.0000)
C_{32}	12.7667	(0.2820, 0.3133, 0.2878, 0.1175, 0.0000)
C_{33}	12.5750	(0.2942, 0.3280, 0.2783, 0.0994, 0.0000)
C_{41}	13.3000	(0.2105, 0.2632, 0.3008, 0.1880, 0.0376)
C_{42}	13.6750	(0.2413, 0.3016, 0.3291, 0.1280, 0.0000)
C_{43}	13.2083	(0.2650, 0.3312, 0.2902, 0.1136, 0.0000)
C_{51}	13.6333	(0.2054, 0.2567, 0.3178, 0.2200, 0.0000)
C_{52}	13.4000	(0.1791, 0.2239, 0.2985, 0.2612, 0.0373)

intuitively conclude that C_{13} – C_{33} has a high weight value and a centralized distribution range. Hence, the risk value of this index is high under the information risk of the Suzhou smart grid in China. The indexes in this range are mostly related to wireless channels and passwords. This result shows that the Internet brings convenience but also increases the threat of information leakage and dangerous invasion. Network link channels and network security have become the fourth battlefield, following the battlefields in sea, land, and air. However, the risk values of the intelligent terminal, application code, and embedded system are relatively low. Therefore, the hardware and software equipment is mature relative to the password and wireless channels in the research and development process. Moreover, the risk value is relatively low.

The fusion of grey theory makes full use of limited information resources in the process of assessment and effectively avoids the phenomenon of information loss. From the five values of the grey assessment weight vector, we observe that the probability of the C_{13} – C_{33} index interval falling to 5 and 4 is significantly higher than that for the other indexes (except C_{22}). This outcome is basically consistent with the result of D-AHP and proves the scientificity of the D-AHP method.

Step 9 combines the D-AHP method with grey theory and obtains the comprehensive assessment vector $H = (0.2956, 0.3281, 0.2803, 0.0928, 0.0032)$. By multiplying the comprehensive assessment vector H and $V = (1, 2, 3, 4, 5)^T$, the final ISRA value of the Suzhou smart grid in China is obtained; that

is, $\text{Risk} = H \times V^T = 3.8199$. $3 < 3.8199 < 4$ indicates that the risk value is moderately high. Close attention should be paid to the three primary and secondary indexes of intelligent terminal (B_1), wireless communication channel (B_2), and password security (B_3).

6. Conclusions

The Internet has gradually penetrated the field of smart grids, but it has also brought new challenges to the information security of smart grids. To obtain the threat factors of information security in the field of smart grids, we established a smart grid ISRA system. The Suzhou smart grid project in China was taken as an example. Using grey theory and D-AHP, we conclude that a wireless communication channel B_2 and password security B_3 are important risk factors leading to the security of smart grid information. The authentication mechanism, password security, and other factors are important indicators that affect the information security of smart grids. In guaranteeing smart grid information security so as to achieve safe and reliable smart grids, the following measures should be implemented:

- (i) Improve smart grid users' awareness about information security protection. Smart grid users are more diverse than the users of traditional power grids. Irregular smart grid use might lead to the leakage of users' personal information and threaten the smart devices in power systems.
- (ii) Strengthen the information security protection measures of smart grid users. The smart grid not only transmits electricity prices but also serves as a channel for buying and selling electricity. Hacker attacks on smart grids have greater economic benefits than those done on traditional grids. Forward-looking security encryption measures should be taken.
- (iii) Improve the safety supervision mechanism of smart grid information by relevant departments. Regulatory authorities should also consider working with the state grid, the government, and other collaborators to formulate strategies and further form a standard set of guidelines.

In this work, the D-AHP method, which does not rely on the subjective experience of experts, is combined with the grey method, which does not rely on complete information, to avoid the disadvantages of other methods that cannot express uncertain and insufficient information. The combination of the two methods not only retains their advantages but also verifies the results based on practical examples. The combination of the D-AHP method and grey theory method can be effectively used to evaluate the information security risk level of smart grids and improve the accuracy of dealing with problems. In the future, we can study the fusion of D-AHP and other methods and the consistency ratio I.D. problem in D-AHP.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

Hua Dong was responsible for conceptualization, methodology, software, formal analysis, investigation, resources, data curation, writing—original draft preparation, and visualization. Hua Dong, Jun Zhao, and Kun Yang performed validation. Jun Zhao and Xiaoyu Yang performed reviewed and edited the article. Jun Zhao and Kun Yang supervised the study. Jun Zhao was responsible for project administration and funding acquisition. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

The authors wish to express their gratitude for the support of Jun Zhao and Kun Yang. This research was funded by the Energy Foundation, grant number G-1509-23762.

Supplementary Materials

Supplementary Materials Computational process of total grey assessment coefficient. (*Supplementary Materials*)

References

- [1] C. Clastres, "Smart grids: another step towards competition, energy security and climate change objectives," *Energy Policy*, vol. 39, no. 9, pp. 5399–5408, 2011.
- [2] W. Wang and Z. Lu, "Cyber security in the smart grid: survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.
- [3] R. Leszczyna, "Standards on cyber security assessment of smart grid," *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 70–89, 2018.
- [4] N. Xu and D. M. Zhao, "The research of information security risk assessment method based on AHP," *Advanced Materials Research*, vol. 187, pp. 575–580, 2011.
- [5] H. Luo, Y. Shen, G. Zhang et al., "Information security risk assessment based on two stages decision model with grey synthetic measure," in *Proceedings of the 6th IEEE International Conference on Software Engineering and Service Science*, pp. 795–798, IEEE, Beijing, China, September 2015.
- [6] Q. Yu and Y. Shen, "Research of information security risk prediction based on grey theory and ANP," in *Proceedings of the IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pp. 107–113, IEEE, Xi'an, China, October 2016.
- [7] A. Rodríguez, F. Ortega, and R. Concepción, "A method for the evaluation of risk in IT projects," *Expert Systems with Applications*, vol. 45, pp. 273–285, 2016.
- [8] F. Sha and H. Zhou, "The information security risk assessment based on AHP and fuzzy comprehensive evaluation," in *Proceedings of the IEEE 3rd International Conference on*

- Communication Software and Networks*, pp. 124–128, IEEE, Xi'an, China, May 2011.
- [9] Y. N. Imamverdiev and S. A. Derakshande, "Fuzzy OWA model for information security risk management," *Automatic Control and Computer Sciences*, vol. 45, no. 1, pp. 20–28, 2011.
 - [10] Z. Q. Cai, J. B. Zhao, Y. Li et al., "Information security evaluation of system based on Bayesian network," in *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 315–319, IEEE, Singapore, December 2015.
 - [11] M. F. Ak and M. Gul, "AHP-TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis," *Complex & Intelligent Systems*, vol. 5, no. 2, pp. 113–126, 2019.
 - [12] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, and R. Wieringa, "An integrated conceptual model for information system security risk management supported by enterprise architecture management," *Software & Systems Modeling*, vol. 18, no. 3, pp. 2285–2312, 2019.
 - [13] J. Wang, K. Fan, W. Mo, and D. Xu, "A method for information security risk assessment based on the dynamic bayesian network," in *Proceedings of the International Conference on Networking and Network Applications (NaNA)*, pp. 279–283, IEEE, Hakodate, Japan, July 2016.
 - [14] G. Fan, D. Zhong, F. Yan, and P. Yue, "A hybrid fuzzy evaluation method for curtain grouting efficiency assessment based on an AHP method extended by D numbers," *Expert Systems with Applications*, vol. 44, pp. 289–303, 2016.
 - [15] X. Deng, Y. Hu, Y. Deng, and S. Mahadevan, "Supplier selection using AHP methodology extended by D numbers," *Expert Systems with Applications*, vol. 41, no. 1, pp. 156–167, 2014.
 - [16] X. Zhou, X. Deng, Y. Deng, and S. Mahadevan, "Dependence assessment in human reliability analysis based on D numbers and AHP," *Nuclear Engineering and Design*, vol. 313, pp. 243–252, 2017.
 - [17] B. Wang, J. Song, J. Ren, K. Li, H. Duan, and X. e. Wang, "Selecting sustainable energy conversion technologies for agricultural residues: a fuzzy AHP-VIKOR based prioritization from life cycle perspective," *Resources, Conservation and Recycling*, vol. 142, pp. 78–87, 2019.
 - [18] Y. A. Solangi, Q. Tan, N. H. Mirjat, and S. Ali, "Evaluating the strategies for sustainable energy planning in Pakistan: an integrated SWOT-AHP and Fuzzy-TOPSIS approach," *Journal of Cleaner Production*, vol. 236, Article ID 117655, 2019.
 - [19] I. Konstantinos, T. Georgios, and A. Garyfalos, "A decision support system methodology for selecting wind farm installation locations using AHP and TOPSIS: case study in Eastern Macedonia and Thrace region, Greece," *Energy Policy*, vol. 132, pp. 232–246, 2019.
 - [20] İ. Akgün and H. Erdal, "Solving an ammunition distribution network design problem using multi-objective mathematical modeling, combined AHP-TOPSIS, and GIS," *Computers & Industrial Engineering*, vol. 129, pp. 512–528, 2019.
 - [21] M. A. Ponce-Jara, E. Ruiz, R. Gil, E. Sancristóbal, C. Pérez-Molina, and M. Castro, "Smart Grid: assessment of the past and present in developed and developing countries," *Energy Strategy Reviews*, vol. 18, pp. 38–52, 2017.
 - [22] J. Sun, *A Study on Smart Grid Transient Failure Detection and Current Overload Preventive Control. Doctor's Degree of Engineering*, College of Automation, Chongqing University, Chongqing, China, 2014, in Chinese.
 - [23] S. Angom, C. Tuboi, M. G. U. Ghazi, R. Badola, and S. A. Hussain, "Demographic and genetic structure of a severely fragmented population of the endangered hog deer (*Axis porcinus*) in the Indo-Burma biodiversity hotspot," *PLoS one*, vol. 15, no. 2, Article ID e0210382, 2020.
 - [24] X. Zhang, "Method for controlling terminal device and the smart terminal device thereof," U.S. Patent, 2016.
 - [25] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.
 - [26] S. M. Aldossari and K.-C. Chen, "Machine learning for wireless communication channel modeling: an overview," *Wireless Personal Communications*, vol. 106, no. 1, pp. 41–70, 2019.
 - [27] B. Ur, J. Bees, S. M. Segreti et al., "Do users' perceptions of password security match reality?" in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 6651–6656, Association for Computing Machinery, San Jose, CA, USA, May 2016.
 - [28] D. R. Sahu and D. S. Tomar, "Analysis of web application code vulnerabilities using secure coding standards," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 885–895, 2017.
 - [29] C. Konstantinou and M. Maniatakis, "Hardware-layer intelligence collection for smart grid embedded systems," *Journal of Hardware and Systems Security*, vol. 3, no. 2, pp. 132–146, 2019.
 - [30] Y. Deng, "D numbers: theory and applications," *Journal of Information & Computational Science*, vol. 9, no. 9, pp. 2421–2428, 2012.
 - [31] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," *The Annals of Mathematical Statistics*, vol. 38, no. 2, pp. 325–339, 1967.
 - [32] T. Tanino, "Fuzzy preference orderings in group decision making," *Fuzzy Sets and Systems*, vol. 12, no. 2, pp. 117–131, 1984.
 - [33] X. Deng and Y. Deng, "D-AHP method with different credibility of information," *Soft Computing*, vol. 23, no. 2, pp. 683–691, 2019.