Sustainable Cities and Society 60 (2020) 102199

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs

Risk assessment of the UPIoT construction in China using combined dynamic weighting method under IFGDM environment

Qiqing Wang[a,b,*], Defu Zhao[a,b], Bo Yang[c], Cunbin Li[a,b]

[a] School of Economics and Management, North China Electric Power University, Beijing, 102206, PR China
[b] Beijing Key Laboratory of New Energy and Low-Carbon Development, Beijing, 102206, PR China
[c] School of Computer and Electronic Information, Guangxi University, Nanning, Guangxi, 530004, PR China

ARTICLE INFO

Keywords:
The ubiquitous power Internet of things (UPIoT)
intuitionistic fuzzy group decision-making
combined dynamic weighting
intuitionistic fuzzy AHP-DEMATEL
risk assessment

ABSTRACT

Large-scale integration of renewable energy systems poses challenges to the ubiquitous power Internet of things (UPIoT) construction in China. This paper aims to study beyond these challenges from a risk assessment perspective, using the combined dynamic weighting evidence fusion (CDWEF) method under the intuitionistic fuzzy group decision-making (IFGDM) environment. The UPIoT construction risk is identified and characterized by a 17-indicator system which is scored by intuitionistic fuzzy relations (IFRs) from experts. The IFRs are corrected by the dynamic expert weight determined from both the intuitionistic fuzzy entropy and conflicts among IFRs. The IF-AHP-DEMATEL method is adopted to determine the combined indicator weight for correcting the risk mass functions, which are obtained from the IFRs with the evidence fusion theory. The proposed risk assessment method is validated in a case study, indicating that the UPIoT construction risk in China is high in communication networks and business innovation.

1. Introduction

A major current focus of the State Grid Corporation of China (SGCC) is how to ensure the security and sustainability of the main grid by establishing the ubiquitous power Internet of things (UPIoT). With large-scale integration of intermittent renewable energy systems (RESs) such as photovoltaic systems (PVs) and wind turbines (WTs), it is undoubted that the uncertainties in RESs can negatively impact the stability of the power system. Fig. 1 shows the dramatic increase in China's RES capacity from 2013 to 2019, where the proportion of PVs and WTs generations in the total RES capacity arrived at 50% in 2019. Moreover, the share of total RES capacity in China has grown to about 39% recently(NEA, 2020). As a result, the high proportion of intermittent RESs such as PVs and WTs poses a threat to the main grid in China (Li et al., 2019).

Another challenge to the UPIoT is depicted in Fig. 2. While the total electricity consumption increased steadily from 2013 to 2019, the annual net profit of State Grid Corporation in China (SGCC) has declined for two constitutive years. The largest state-owned enterprise of China choose to develop new businesses through the construction of UPIoT (Jiang et al., 2019).

Therefore, the main goal of UPIoT construction in China is to deal with the challenges from uncertain RESs penetration and profit shrinkage of SGCC (Ting et al., 2019). The UPIoT can accomplish its mission via the following routes.

- State-of-the-art technologies such as 5 G and IoT are used to collect the data from hundreds of millions of smart meters and sensors distributed in every corner of China's power grid(De Dutta & Prasad, 2019).
- A cloud data center is established to store valuable results from analyzing the obtained power grid operation data.
- Lots of application scenarios are developed to explore the potential value of data sharing, supporting the power grid operation, integrated energy services, and business improvement, etc (Hu et al., 2019).

However, the UPIoT construction is risky under the new challenges from China's power system (Losavio et al., 2018).

1.1. Literature review

Since the UPIoT is technically the extension of IoT that has been widely used in the smart grid (Saleem et al., 2019), there is extensive literature on the UPIoT risks from studying IoT security (Lin et al., 2017). For example, physical-layer security of IoT was studied in

* Corresponding author at: School of Economics and Management, North China Electric Power University, Beijing, 102206, PR China.
E-mail addresses: wqq757@qq.com (Q. Wang), zdf737477@163.com (D. Zhao), 839807994@qq.com (B. Yang), lcb999@263.net (C. Li).

https://doi.org/10.1016/j.scs.2020.102199
Received 25 November 2019; Received in revised form 9 April 2020; Accepted 10 April 2020
Available online 23 May 2020

Nomenclature

Parameters

t	Number of the first-layer risk indicators
m	Number of the second-layer risk indicators
m_s	Number of the second-layer indicators belong to -th first-layer indicator
n	Risk levels
P	Number of experts
σ	Controller parameter for consistency repair
λ_i	The centrality of i -th indicator
α	Combining coefficient for the expert weight
l_i	Defense cost to deal with i -th risk level
γ_{ij}^{kl}	Belief interval-based evidence distance
κ_{ij}^{kl}	Conflict coefficient between m_{ij}^{k} and m_{ij}^{l}
η	Discount weight for evidence fusion
γ	Risk preference coefficient of the expert group

Variables

F_{si}	The i -th second-layer indicator of F_s
F_s	The s -th first-layer indicator
D_k	The k -th expert
V_j	The j -th risk level
A^k	Importance comparison matrix for first-layer indicators
B^k	Interaction comparison matrix for first-layer indicators
C^k	Risk membership matrix for second-layer indicators
ξ_A^{ik}	Expert weights from A^k
ξ_B^{ik}	Expert weights from B^k
ξ_C^{ik}	Expert weights from C^k
e_{ij}^{k}	Intuitionistic fuzzy entropy
E_i^k	Intuitionistic fuzzy entropy on i -th indicator
ew_i^k	Expert weight from entropy
cf_{ij}^{kl}	Conflict between different judgment information
sw_i^k	The expert weight from the conflict information
$\overline{w}_i$	The value weight for i -th indicator
$\widetilde{H}$	Comprehensive influence matrix
cw_i	Combined weight for first-layer indicators
G_s	The intuitionistic fuzzy risk of indicator F_s
$\overline{M}$	A mass function vector for indicator F_s
$\widetilde{m}_s$	Corrected risk mass function for indicator F_s
S_F	The risk value of indicator F
$\widetilde{M}$	Discounted mass function matrix for first-layer indicator risks
Δd_F	Measurement on the effect of weights to the first-layer indicator

Indices

s	Index of first-layer indicators number
i	Index of second-layer indicators number
j	Index of risk levels number
k	Index of experts numb

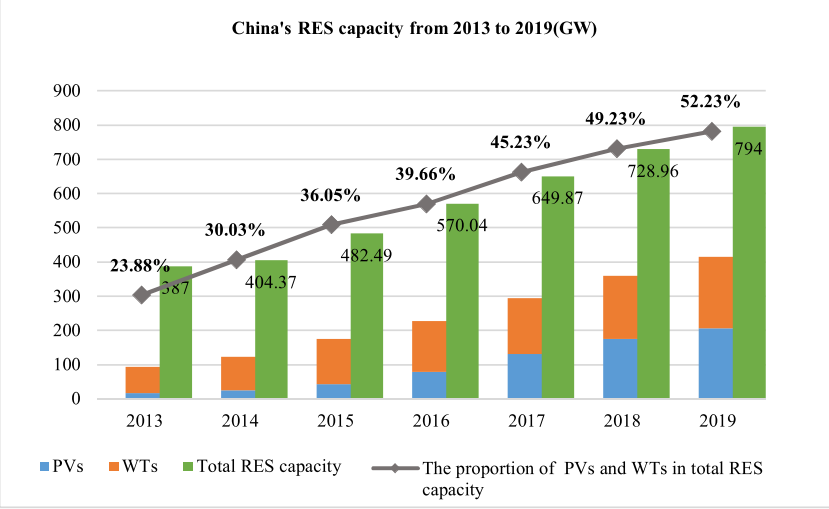

Fig. 1. Renewable energy power generation of China from 2013 to 2019. Related data comes from the Center for Renewable Energy Development of China (http://www.cnrec.org.cn/).

(Mukherjee, 2015); (Bhoyar et al., 2019) discussed the communication challenges of IoT while meeting energy consumption, throughput, latency, and security criteria; and the security requirements of IoT application protocols was presented in (Nastase, 2017). Apart from the risk of IoT architectures, (Stergiou et al., 2018) studied the privacy issues in the context of the big data era.

Microgrids (MGs) and smart grids (SGs) are established with the deep integration of the RES and IoT technology, providing another view for the UPIoT risk analysis. (Khalili et al., 2019b) investigated optimal scheduling of the microgrids by considering the stochastic nature of RES generations, while (Bahramara & Golpira, 2018) took the uncertain behavior of electric vehicles into account. Impacts on modern power systems may also come from man-made behaviors, the UPIoT superimposed on an IoT based SG would contains millions of nodes that are likely to be attached by hacks (Kimani et al., 2019). Furthermore, the UPIoT can be threatened by state-of-the-art technologies such as the 5 G network (De Dutta & Prasad, 2019), blockchain (Tariq et al., 2019), and artificial intelligence (Hossain et al., 2019).

As aforementioned, the UPIoT construction risk has been demonstrated from its endogenous structure and exogenous factors, but the UPIoT focuses more on the holistic perception and ubiquitous connection of energy. These ambitious goals can also add weight to the UPIoT construction risk (Jiang et al., 2019). For instance, cyber security and privacy issues on the Energy Internet (EI) was investigated in (Sani et al., 2019), (Shakerighadi et al., 2018) reviewed the challenges that an IoT based modern energy system must deal with, such as energy

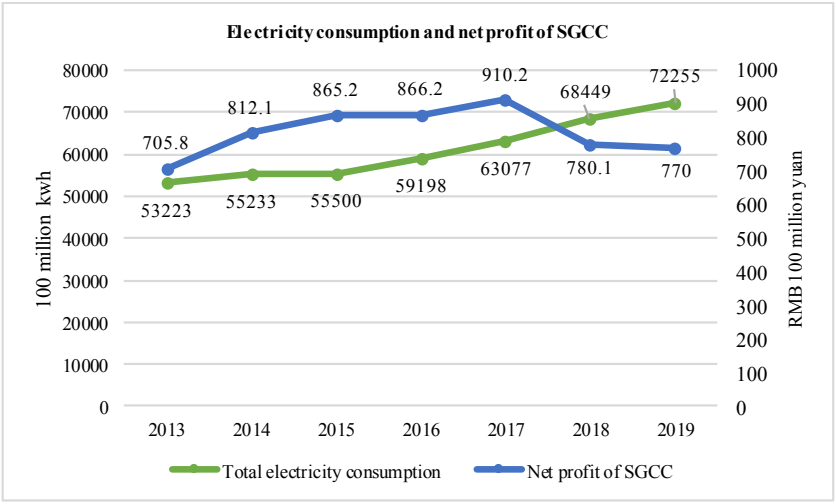

Fig. 2. Total power generation and net profit of SGCC from 2013 to 2019. Related data comes from the SGCC (http://www.sgcc.com.cn/).

supply, big data processing, standards, etc. As for energy consumption in the UPIoT, (Li et al., 2018) optimized the dispatch strategy of virtual power plant under cyber-attacks, while (Jafari et al., 2020) analyzed the impact of demand response program when determining optimal capacity and type of the generation resources for microgrids (MGs).

For the UPIoT construction risk management methods, optimization and evaluation models are most commonly used. (Samper et al., 2019) optimized the distribution system with high penetrations of solar photovoltaic via a heuristic algorithm using modified risk-adjusted cost ratios, while (Khalili et al., 2019a) investigated optimal reliable and resilient construction of microgrids by the fuzzy satisfying approach and Pareto optimality methods. Evaluation models often study the planning risks through combining multiple mathematical models. For example, (Luis & Jose, 2019) analyzed the risk of renewable energy construction projects based on the Monte Carlo approach and Probabilistic Fuzzy Sets with AHP, (Wu & Zhou, 2019) evaluated the urban rooftop distributed PVs with hesitant fuzzy linguistic term sets and DEMATEL, an integrated method of Mahalanobis-Taguchi Gram-Schmidt and TOPSIS was applied to regional energy security assessment (Yuan & Luo, 2019). The optimization method features accurate but needs adequate data from the existing system, whereas the evaluation method based on experts' knowledge can analyze the system risk without obtaining any objective data.

However, although risk issues on IoT, SGs, and MGs that related to the UPIoT were well studied over the past few years, little attention has been paid to the comprehensive risk assessment of the UPIoT construction.

1.2. Novelty and contributions

The present study comprehensively evaluates the UPIoT construction risk from four dimensions: basic support, business, cyber security, and management, which has not been performed by other literature so far. Novelty and contributions of this paper are briefly presented below:

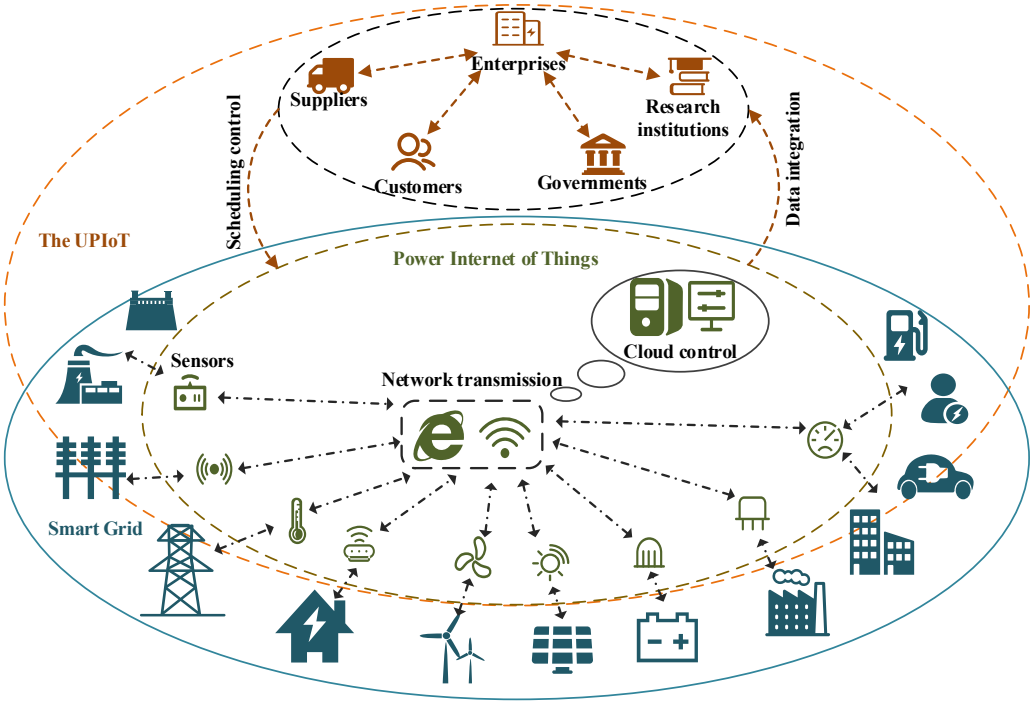

Fig. 3. The relationship among the UPIoT, PIoT, and SG.

- A two-layer risk indicator system is established to cover all risk factors that may impact the UPIoT, including four indicators in the first layer and 17 in the second.
- The UPIoT construction risk is evaluated via the IFGDM-CDWEF method that considers both the interaction between risk factors and the domain knowledge of decision-makers.
- The research results indicate that the UPIoT construction risk is high in communication network and conventional business innovation, providing a risk management perspective for further establishing the sustainable energy ecosystem in China.

1.3. Paper organization

This paper is organized as follows: Section 1 is the introduction related to the research issue as aforementioned, followed by Section 2 identifies detailed risk factors from the UPIoT construction. Section 3 focuses on the risk assessment model used in the case study, and the results are shown in Section 4. The study is concluded in Section 5.

2. Overview and risk identification of the UPIoT construction

In this subsection, the basic concept of UPIoT construction in China is introduced, and the UPIoT construction risk is identified and decomposed to form a hierarchical indicator system.

2.1. The concept of UPIoT

The UPIoT is an intelligent and ubiquitous network that connects all things and people related to the existing power system via IoT technologies (Hu et al., 2019b). A large number of entities like power generation companies, power grid companies, power suppliers, and power users are connected by the UPIoT, thus the flow of information, energy, and business underlying in the entities can be accelerated to provide high-quality and innovative services (Jiang et al., 2019).

Fig. 3 shows relationships between the Power Internet of Things (PIoT), the UPIoT, and the SG. Both the UPIoT and SG are supported by the PIoT, while the former can communicate with entities outside the SG. Specifically, the PIoT is integrated into the SG to support its power generation, transmission, and distribution by monitoring and uploading operational data. Based on that, the resources of external enterprises, suppliers, and users are involved to form a larger power network called the UPIoT, which gets more advanced capabilities than the PIoT.

Due to the functional similarity with IoT, the crucial point of UPIoT construction in China can be divided into four layers corresponding to the hierarchical structure of IoT (Jiang et al., 2019).

- The perception layer: The construction work of this layer focuses on the infrastructure for data collecting, such as smart meters, intelligent substations, RFID tags, etc.
- The network layer: The communication networks and advanced communication technologies play an important role in the construction of this layer.
- The platform layer: Massive data is uploaded to this layer through the perception layer and the network layer, thus a unified data center needs to be established for mining the potential value of the data.
- The application layer: This layer concentrates more on the service than the technology, and opens a window leading to more promising applications such as energy services, customer services, and lean enterprise management.

Hence, the UPIoT is a ubiquitous network focusing on data sharing and prospective businesses.

2.2. Risk identification of the UPIoT construction

2.2.1. Basic support risk (F1)

The basic support risk means that the IoT technology or facilities do not fully support and coordinate the SG so that the components of UPIoT fails to achieve the expectative construction goals.

(1) Sensor device coverage (F11): The UPIoT must get enough sensor devices such as smart meters and smart substations to collect massive operational data of SGs (Kumar et al., 2019).

(2) Communication network support (F12): The speed and bandwidth of the communication network must meet the needs of UPIoT to transmit massive data (Kuzlu et al., 2014).

(3) Heterogeneous data fusion (F13): It is critical to fuse and share the heterogeneous data generated by various data sources during the SG operation (Pacevicius, Roverso, Salvo Rossi, & Paltrinieri, 2018).

(4) Unified cloud platform (F14): Building an uniformed and automatic cloud-based platform that enables to process data produced by dispersed equipment is essential for the UPIoT (Wilcox et al., 2019).

(5) Emerging technology applications (F15): The application of emerging technologies such as blockchain, 5 G and artificial intelligence poses threats to the UPIoT (Akpakwu et al., 2018).

2.2.2. Business risk (F2)

With the development of the renewable industry including electric vehicles and charging piles, the business risk is mainly caused by the traditional power grid services that cannot meet the new emerging demand of customers.

(1) End-user services (F21): The UPIoT needs to satisfy end-users with flexible and convenient services such as electronic payment, automatic meter reading (Ellabban and Abu-Rub, 2016).

(2) Corporate asset management (F22): A large number of corporate assets in the power system needs to be managed online, including not only the official materials for daily use but also plenty of power grid devices widely distributed in cities and suburbs (Kure & Islam, 2019).

(3) Power grid operation management (F23): The UPIoT is responsible to assess and forecast the health status of the power grid based on the widely collected data from weather, equipment, and even people, etc (Wu et al., 2018).

(4) Conventional business innovation (F24): Traditional power grid business needs to be promoted through the UPIoT construction, becoming more convenient and interconnected (Skvortsova et al., 2019).

(5) Energy industrial ecosystem building (F25): The goal of UPIoT is to establish an energy industrial ecosystem with coordinating external entities such as universities, governments, and research institutes. The ecosystem can enhance the ability of the power grid to consume more renewable energy and provide more innovative services (Jiang et al., 2019).

2.2.3. Cyber security risk(F3)

It is important to prevent the UPIoT from cyber security threats due to its ubiquitous distributed IoT infrastructures (Ferrag et al., 2018). Risk factors are identified from the hierarchical structure of the UPIoT as follows (Ande et al., 2019).

(1) Perception layer security (F31): The sensors in the perception layer of the UPIoT are susceptible to natural disasters or man-made sabotage because they are usually exposed to the air (Khattak et al., 2019).

(2) Network layer security (F32): IoT devices in the UPIoT are vulnerable to cyberattacks (Habibi Gharakheili et al., 2019), especially the wireless sensor network for power grid operational data transmission (Kimani et al., 2019).

(3) Platform layer security (F33): The information of power users is managed by the platform layer of the UPIoT, data leakage and privacy problems may occur when the platform interface is intruded by

hackers (Girma, 2018).

(4) Application layer security (F34): As the platform data is available for many entities via software or web services, there may be potential threats of data stealing and database attacks (Radoglou Grammatikis et al., 2019).

2.2.4. Management risk (F4)

Constructing the UPIoT is an innovative revolution that requires all the organizations and individuals to make changes and maintain the same goal. However, human-involved projects often get managerial uncertainties.

(1) Obstacles from customers (F41): Due to the unawareness of project prospects, the UPIoT construction process may be blocked by power users (Sovacool et al., 2019).

(2) Obstacles from employees (F42): Decision-makers should persuade employees to participate in the UPIoT construction and deal with the possible boycotts from old employees who are unwilling to make changes (Rafferty & Jimmieson, 2017).

(3) Organizational guarantee (F43): Adequate supports from the responsible organization is required when constructing the UPIoT (Ibadov, 2017).

Consequently, a hierarchical indicator system is established with the above risk factors, the two-layer system shown in Fig. 4 can specifically outline the UPIoT construction risk from multiple perspectives.

3. Risk assessment model for the UPIoT construction

An IFGDM-CDWEF method is proposed to evaluate the UPIoT construction risk based on the indicator system shown in Fig. 4. For lack of factual data in the early stage of UPIoT construction, the risk indicators are scored by experts using intuitionistic fuzzy relations (IFRs) under the IFGDM environment. The subjectivity of IFRs is minimized with the combined dynamic weighting (CDW) method, which is composed of the combined indicator weight and dynamic expert weight, the former is determined by IF-AHP-DEMATEL method, while the latter is obtained from the underlying uncertainty and conflict of the IFRs. According to the evidence fusion (EF) theory, the UPIoT construction risk is integrated without conflict. Fig. 5 shows the framework of UPIoT construction risk assessment based on the IFGDM-CDWIF method, including totally five phases listed below.

- Phase 1: Selecting several experts who are professional in the UPIoT and asking them to score the risk indicator system with IFRs;
- Phase 2: The diversification in the domain knowledge of experts is considered for determining the dynamic expert weight, which is obtained from the intuitionistic fuzzy entropy and conflict information in the IFRs;
- Phase 3: Determining the combined weight of first-layer indicators by an IF-AHP-DEMATEL method;
- Phase 4: Using the combined dynamic weights (CDWs) came from the Phase 2 and 3, the IFRs on second-layer indicators are integrated via the evidence fusion method to obtain risk mass functions of the first-layer indicators;
- Phase 5: Evaluating and analyzing the construction risk of UPIoT with weighted aggregating the risk mass functions.

The step-by-step illustration for the risk assessment model is displayed in the following subsections.

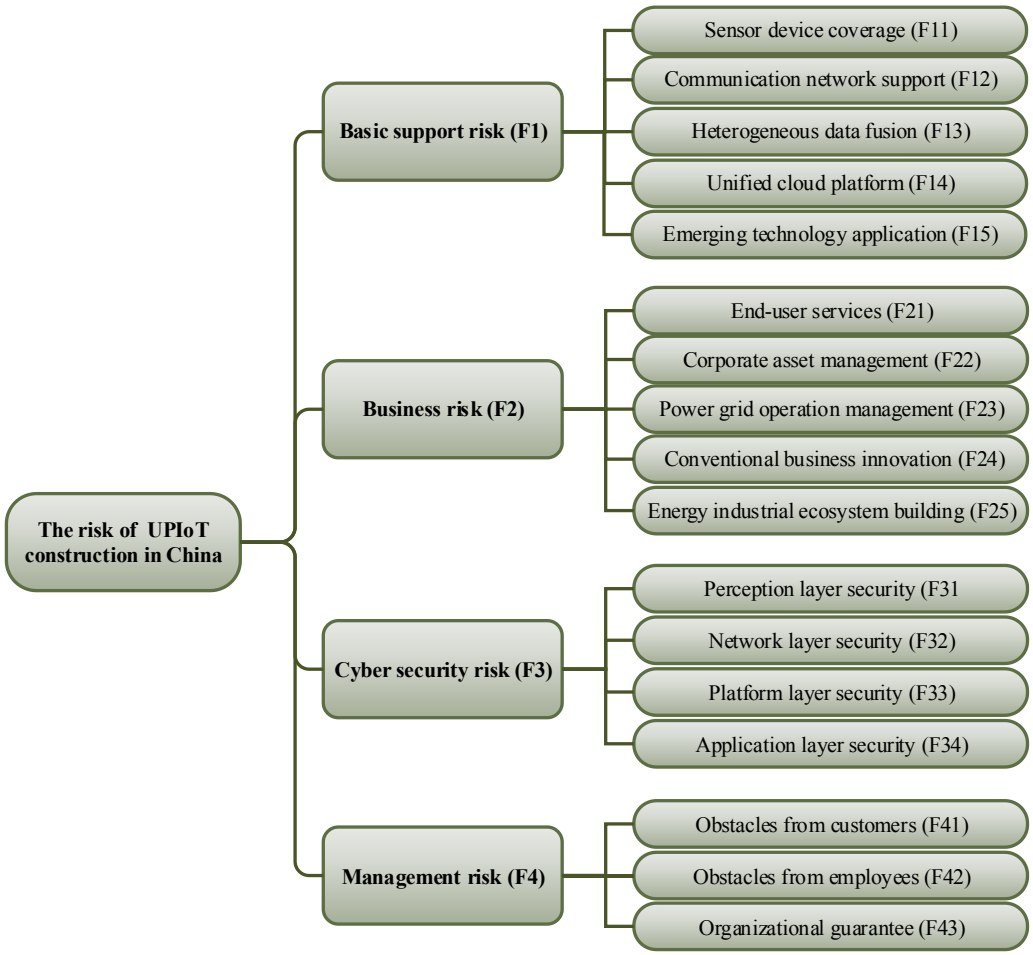

Fig. 4. The two-layer indicator system reflecting the UPIoT construction risk.

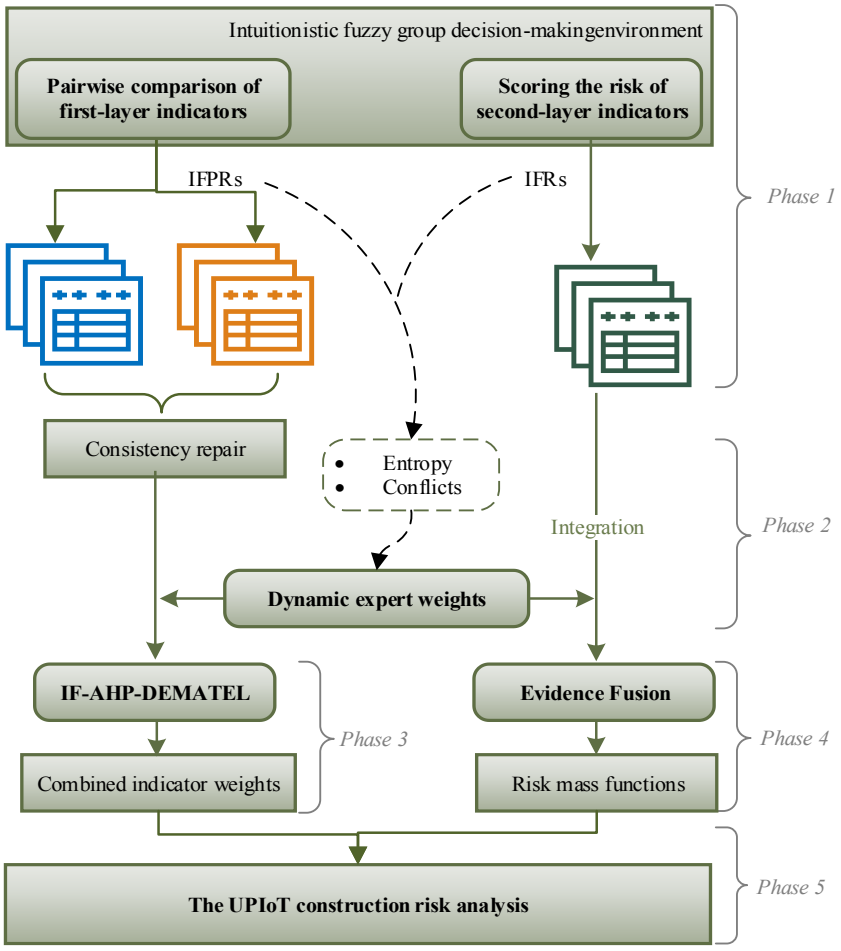

Fig. 5. Risk assessment framework of the UPIoT construction.

3.1. Phase 1: Problem definition and data collection

According to the indicator system of UPIoT construction risk built in Fig. 4, let $\{F_{s1}, F_{s2}, ..., F_{sm_s}\}$ be the second-layer indicator set and $F_s(s = 1, 2, ..., t)$ be the first-layer indicator set, where m_s refers to the number of second-layer indicators that belong to the corresponding first-layer indicator F_s, and $m = \sum_{i=1}^{t} m_i$ represents the number of second-layer indicators.

Since no historical data is available, the raw data used in the risk assessment model is scored by experts in the domain of UPIoT. Intuitionistic fuzzy numbers (IFNs) capable of reflecting the hesitation of decision makes are used for scoring the risk indicators of UPIoT construction (Atanassov, 1999). P experts under the IFGDM environment are asked to give three intuitionistic fuzzy relations (IFRs) on the risk indicator system. Specifically, each expert $D_k(k = 1, 2, ..., P)$ pairwise compares first-layer indicators and gives two intuitionistic fuzzy preference relations (IFPRs) based on their importance relative to the UPIoT construction risk and their interactions, respectively (Xu, 2007). Assuming that each second-layer risk indicator gets n risk levels (each level denoted as $V_j(j = 1, 2, ..., n)$), its membership degree to the risk levels is scored by the expert via the intuitionistic fuzzy judgment matrix (IFJM). All the IFRs including IFPRs and IFJM are listed below.

- $A^k = (a_{ij}^k)_{t\times t}(i, j = 1, 2, ..., t, k = 1, 2, ..., P)$ is an IFPR scored for first-layer indicator value weights determination, where $a_{ij}^k = \langle \mu_{ij}^k, \upsilon_{ij}^k, \pi_{ij}^k \rangle$represents the relative importance of indicator$F_i$andF_j;
- $B^k = (b_{ij}^k)_{t\times t}(i, j = 1, 2, ..., t, k = 1, 2, ..., P)$ is also an IFPR scored for first-layer indicators comprehensive weights determination, where $b_{ij}^k = \langle \mu_{ij}^k, \upsilon_{ij}^k, \pi_{ij}^k \rangle$ represents the influence degree between indicator F_i and F_j;
- $C^k = (c_{ij}^k)_{m\times n}(i = 1, 2, ..., m, j = 1, 2, ..., n, k = 1, 2, ..., P)$ is an intuitionistic fuzzy judgment matrix (IFJM) scored for second-layer indicator risk assessment, where $c_{ij}^k = \langle \mu_{ij}^k, \upsilon_{ij}^k, \pi_{ij}^k \rangle$ represents the risk membership of $i - th$ second-layer indicator with respect to risk level $V_j(j = 1, 2, ..., n)$.

The element in the IFRs given by expert D_k can be generally represented by $\langle \mu_{ij}^k, \upsilon_{ij}^k, \pi_{ij}^k \rangle$, where μ_{ij}^k, υ_{ij}^k represents the membership degree and non-membership degree of i -th indicator relative to j -th indicator, respectively. Since $\pi_{ij}^k = 1 - \mu_{ij}^k - \upsilon_{ij}^k$ represents the hesitation of the expert, the element is often simply denoted as $\langle \mu_{ij}^k, \upsilon_{ij}^k \rangle$. Additionally, experts can score each indicator according to the reference scale shown in Table 1.

3.2. Phase 2: Determining the dynamic weight of experts

Due to differences in knowledge background, cognitive ability, and work experience, the scoring information given by experts needs to be corrected for maximizing the accuracy of group decision-making activity (Du et al., 2018). Therefore, in this study, a method for determining dynamic expert weights is proposed to correct the IFRs on the UPIoT construction risk. The method calculates the expert weight by fully considering the intuitionistic fuzzy entropy (IFE) and the potential conflicts compared with other experts' judgments. Take the IFJM C^k as an example, the following demonstrates how to calculate the dynamic weight $\xi_C^{ik}(i = 1, 2, ..., m, k = 1, 2, ..., P)$ of expert D_k relative to the $i - th$ indicator. Similarly, ξ_A^{ik}, ξ_B^{ik} can be calculated based on A^k and B^k

Table 1
Reference scale for scoring indicators.

Preference description	Reference value
Indicator i is much more important than j	(0.9,0.1,0.0)
Indicator i is even more important than j	(0.8,0.1,0.1)
Indicator i is more important than j	(0.7,0.2,0.1)
Indicator i is a bit more important than j	(0.6,0.3,0.1)
Indicator i and j are equally important	(0.5,0.5,0.1)

Note: IFNs in the table are for reference only, experts can score indicators with more values beyond the table.

in the same way.

3.2.1. IFE based expert weights

The intuitionistic fuzzy entropy (IFE) reflects how much a decision-maker knows about the problem. For example, expert D_k who is not sure about the membership of i -th indicator to the risk level $V_j(j = 1, 2, ...,n)$ tends to get a fairly high IFE . The IFE e_{ij}^k can be measured by eq. (1) defined in (Chen & Li, 2010).

$$e_{ij}^k = \frac{1 - |\mu_{ij}^k - \upsilon_{ij}^k| + \pi_{ij}^k}{1 + \mu_{ij}^k - \upsilon_{ij}^k + \pi_{ij}^k} \tag{1}$$

Therefore, the IFE of expert D_k on the i -th indicator can be obtained via eq. (2).

$$E_i^k = \frac{1}{n}\sum_{j=1}^{n} e_{ij}^k \tag{2}$$

Where E_i^k indicates the IFE expert D_k relative to the i -th indicator. Then the corresponding IFE based weight of expert D_k can be calculated by eq. (3).

$$ew_i^k = (1 - E_i^k)/(P - \sum_{k=1}^{P} E_i^k) \tag{3}$$

Where $ew_i^k(i = 1, 2, ...,m)$ represents the expert weight that based on the IFJM C^k, indicating how well the expert D_k understands the i -th risk indicator of UPIoT construction.

3.2.2. Weight correction from conflicts

In the group decision-making environment, the judgment that contradicts with others is unreliable, thus the expert D_k gives a more controversial IFR should be assigned with a smaller weight. The method proposed in (Wang et al., 2019) that can measure the conflict between two experts is adopted to correct the weight of experts.

Firstly, according to the evidence theory, each element in C^k is converted into a mass function via eq. (4):

$$\begin{cases} m_i^k(\varnothing) = 0,\ m_i^k(V_j) = \dfrac{\mu_i^k(V_j)}{\sum_{j=1}^{n}[1 - \upsilon_i^k(V_j)]} \\ m_i^k(\Theta) = 1 - \sum_{j=1}^{n} m_i^k(V_j) \end{cases} \tag{4}$$

Where $\Theta = \{V_j|j = 1, 2, ...,n\}$ is the recognition framework, thus $m_{ij}^k(\theta)$ and $m_{ij}^l(\theta)$ can represent the evidence give by expert D_k and D_l $(k \neq l)$ on the hypothesis $\theta(\theta \in 2^{\Theta})$, respectively. Then the conflict between corresponding elements in C^k and C^l is denoted as cf_{ij}^{kl}, which can be calculated by eq. (5).

$$cf_{ij}^{kl} = \begin{cases} 0,\ \forall\ \theta \in 2^{\Theta},\ m_{ij}^k(\theta) = m_{ij}^l(\theta) \\ 1,\ (\cup A_k) \cap (\cup B_k) = \varnothing \\ where(m_{ij}^k(A_k) > 0) and (m_{ij}^k(B_l) > 0) \\ \sqrt{\dfrac{\kappa_{ij}^{kl} + \gamma_{ij}^{kl}}{2}},\ (\cup(\arg\max(BetP_{m_{ij}^k}(\theta))))\cap \\ (\cup\ (\arg\max(BetP_{m_{ij}^k}(\theta)))) = \varnothing \\ \dfrac{\kappa_{ij}^{kl} + \gamma_{ij}^{kl}}{2},\ else \end{cases} \tag{5}$$

Where $\arg\max(BetP_{m_{ij}^k}(\theta))$ represents the maximum support hypothesis on the recognition framework Θ, γ_{ij}^{kl} is the belief interval-based evidence distance defined in (Han et al., 2018), and κ_{ij}^{kl} is the conflict coefficient between m_{ij}^k and m_{ij}^l that can be obtained in (Dempster, 2008).

The weight of expert D_k depends on the supports from other experts, it can be calculated via eq. (6).

$$sw_i^k = \frac{\sum_{l=1,l\neq k}^{P}(1 - cf_i^{kl})}{\sum_{k=1}^{P}\sum_{l=1,l\neq k}^{P}(1 - cf_i^{kl})} \tag{6}$$

Where sw_i^k represents the expert weight from the conflict information, $1 - cf_i^{kl}$ indicates the extent to which expert D_k is supported by other experts, and cf_i^{kl} is obtained by eq. (7).

$$cf_i^{kl} = \frac{1}{n}\sum_{j=1}^{n} cf_{ij}^{kl} \tag{7}$$

Finally, the dynamic weight of expert D_k calculated from C^k is denoted as $\xi_C^{ik} = (ew_i^k + sw_i^k)/2$, which is the combination of the IFE based weight ew_i^k and the conflict based weight sw_i^k.

3.3. Phase 3: Determining the comprehensive weight of first-layer indicators

Using the preference information on a hierarchical system, the Analytic Hierarchy Process (AHP) (Saaty, 2001) has deep expertise in analyzing the importance of different indicators relative to the target,

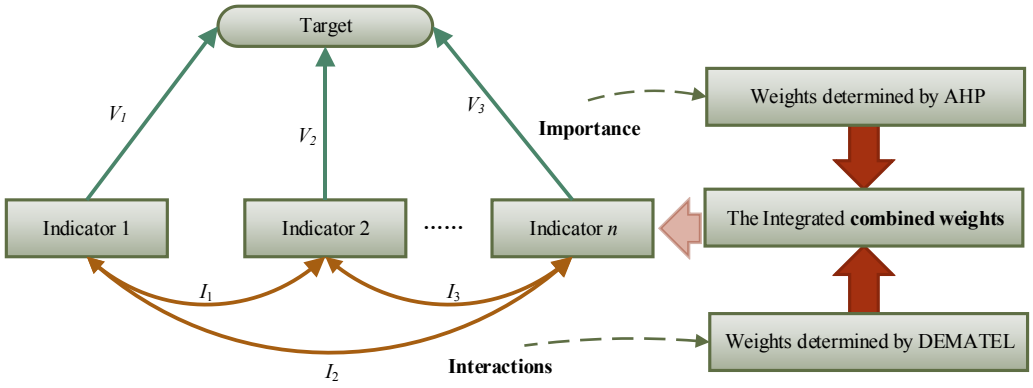

Fig. 6. The determination framework for the combined indicator weight.

while the decision-making trial and evaluation laboratory (DEMATEL) focuses on the interaction between indicators (Fontela & Gabus, 1976). Fig. 6 illustrates the complementary advantages of AHP and DEMATEL in determining indicator weights. Therefore, an intuitionistic fuzzy group decision making (IFGDM) based AHP-DEMATEL method is proposed in this study to determine the combined weight of first-layer indicators. The specifics of the method are demonstrated as follows.

3.3.1. Preprocessing the IFPRs

In order to avoid misleading solutions, it is important to study the consistency of preference relations expressed by decision-makers (Herrera-Viedma et al., 2004), thus the consistency of IFPRs A^k and B^k given by expert $D_k(k = 1, 2, ...,P)$ needs to be checked before they are used to determine the comprehensive weight of UPIoT construction risk indicators.

The IFPR should be corrected when its consistency is unacceptable, but the traditional correction method is time-consuming because it requires the iterative participation of experts. An automatic algorithm defined in (Xu & Liao, 2014) for repairing the inconsistent IFPR is used here to preprocess A^k and B^k.

For each IFPR A^k, its perfect consistent intuitionistic fuzzy preference matrix $\overline{A}^k = (\overline{a}_{ij}^k)$ is produced by eqs. (8)(9).

$$\overline{\mu}_{ij}^k = \begin{cases} \mu_{ij}^k, \ i = jORi + 1 = j \\ \dfrac{\sqrt[j-i-1]{\prod_{q=i+1}^{j-1} \mu_{iq}^k \mu_{qj}^k}}{\sqrt[j-i-1]{\prod_{q=i+1}^{j-1} a\mu_{iq}^k \mu_{qj}^k} + \sqrt[j-i-1]{\prod_{q=i+1}^{j-1} (1-\mu_{iq}^k)(1-\mu_{qj}^k)}}, \ i+1<j \\ \overline{\mu}_{ji}^k, \ i > j \end{cases} \tag{8}$$

$$\overline{\nu}_{ij}^k = \begin{cases} \nu_{ij}^k, \ i = jORi + 1 = j \\ \dfrac{\sqrt[j-i-1]{\prod_{q=i+1}^{j-1} \mu_{iq}^k \mu_{qj}^k}}{\sqrt[j-i-1]{\prod_{q=i+1}^{j-1} \mu_{iq}^k \mu_{qj}^k} + \sqrt[j-i-1]{\prod_{q=i+1}^{j-1} (1-\mu_{iq}^k)(1-\mu_{qj}^k)}}, \ i+1<j \\ \overline{\nu}_{ji}^k, \ i > j \end{cases} \tag{9}$$

Where $\overline{a}_{ij}^k = \langle \overline{\mu}_{ij}^k, \overline{\nu}_{ij}^k \rangle$, $i, j = 1, 2, ...,t$. Then the consistency of A^k is measured by eq. (10).

$$d(\overline{A}^k, A^k) = \frac{1}{2(n-1)(n-2)} \sum_{i=1}^{t} \sum_{j=1}^{t} (|\overline{\mu}_{ij}^k - \mu_{ij}^k| + |\overline{\nu}_{ij}^k - \nu_{ij}^k| + |\overline{\pi}_{ij}^k - \pi_{ij}^k|) \tag{10}$$

Where $d(\overline{A}^k, A^k)$ represents the distance between $\overline{A}^k$ and A^k, and A^k is acceptable when $d(\overline{A}^k, A^k) \le 0.1$. However, if $d(\overline{A}^k, A^k) > 0.1$, then A^k is merged with $\overline{A}^k$ to form a new IFPR A_1^k according to eq. (11).

$$\begin{cases} \widetilde{\mu}_{ij}^k = \dfrac{(\mu_{ij}^k)^{1-\sigma}(\overline{\mu}_{ij}^k)^{\sigma}}{(\mu_{ij}^k)^{1-\sigma}(\overline{\mu}_{ij}^k)^{\sigma} + (1-\mu_{ij}^k)^{1-\sigma}(1-\overline{\mu}_{ij}^k)^{\sigma}} \\ \widetilde{\nu}_{ij}^k = \dfrac{(\nu_{ij}^k)^{1-\sigma}(\overline{\nu}_{ij}^k)^{\sigma}}{(\nu_{ij}^k)^{1-\sigma}(\overline{\nu}_{ij}^k)^{\sigma} + (1-\nu_{ij}^k)^{1-\sigma}(1-\overline{\nu}_{ij}^k)^{\sigma}} \end{cases} \tag{11}$$

Where $\sigma \in [0, 1]$ is a controlling parameter, it can be noted that when $\sigma = 0$, $A_1^k = A^k$, and when $\sigma = 1$, $A_1^k = \overline{A}^k$. Correspondingly, a new $d(\overline{A}^k, A_1^k)$ is obtained. If $d(\overline{A}^k, A_1^k) \le 0.1$, A_1^k is accepted, otherwise A_1^k needs to be merged with $\overline{A}^k$ iteratively to produce a new IFPR via eq. (11) until the IFPR is acceptable. Finally, the repaired IFPR A^k is denoted as $\widetilde{A}^k = (\widetilde{a}_{ij}^k)_{t\times t}$.

Hence, two acceptable IFPRs $\widetilde{A}^k$ and $\widetilde{B}^k$ of each expert D_k are obtained with the consistency repairing algorithm.

3.3.2. Determining the value weights

The importance of the first-layer indicators can be expressed by the value weights that are calculated from all the IFPRs $\widetilde{A}^k(k = 1, 2, ...,P)$ using the intuitionistic fuzzy AHP (IF-AHP) method. Firstly, each IFPR $\widetilde{A}^k$ is converted to a vector with t dimensions via eq. (12).

$$w_i^k = \left\langle \frac{\sum_{j=1}^{t} \widetilde{\mu}_{ij}^k}{\sum_{i=1}^{t}\sum_{j=1}^{t}(1-\widetilde{\nu}_{ij}^k)}, 1 - \frac{\sum_{j=1}^{t}(1-\widetilde{\nu}_{ij}^k)}{\sum_{i=1}^{t}\sum_{j=1}^{t}\widetilde{\mu}_{ij}^k} \right\rangle \tag{12}$$

where w_i^k represents the weight of i -th indicator, thus the weight vector of each expert D_k can be denoted as $w^k = [w_1^k, w_2^k, ...w_t^k]^T$.

According to the Phase 2, the expert weight $\xi_A^{ik}(i = 1, 2, ...,t, k = 1, 2, ...,P)$ can be obtained from IFPR A^k. Then the Intuitionistic Fuzzy Weighted Average (IFWA) operator defined in (Xu, 2006) is applied to integrate the vector w^k by eq. (13).

$$w = \begin{bmatrix} IFWA_{\xi_A^1}(w_1^k) \\ IFWA_{\xi_A^2}(w_2^k) \\ \vdots \\ IFWA_{\xi_A^k}(w_t^k) \end{bmatrix} = \begin{bmatrix} \left\langle 1 - \prod_{k=1}^{P}(1-\mu_{w_1^k})^{\xi_A^{1k}}, \prod_{k=1}^{P}(\nu_{w_1^k})^{\xi_A^{1k}} \right\rangle \\ \left\langle 1 - \prod_{k=1}^{P}(1-\mu_{w_2^k})^{\xi_A^{1k}}, \prod_{k=1}^{P}(\nu_{w_2^k})^{\xi_A^{1k}} \right\rangle \\ \vdots \\ \left\langle 1 - \prod_{k=1}^{P}(1-\mu_{w_t^k})^{\xi_A^{1k}}, \prod_{k=1}^{P}(\nu_{w_t^k})^{\xi_A^{1k}} \right\rangle \end{bmatrix} \tag{13}$$

Where the $\langle \mu_{w_i^k}, \nu_{w_i^k} \rangle$ represents the IFN in w_i^k, w represents the integrated weight vector for the first-layer indicators, thus the real number value weights can be calculated via eq. (14).

$$\overline{w}_i = \frac{H_{score}(w_i)}{\sum_{i=1}^{t} H_{score}(w_i)} \tag{14}$$

Where $\overline{w}_i$ is the value weight of the $i-th$ indicator, $H_{score} = (1-v)/(2-u-v)$ is the scoring function for an IFN (Atanassov, 1999).

3.3.3. Comprehensive weight determination considering interactions

The IFPRs $\widetilde{B}^k(k = 1, 2, ...,P)$ are used to determine final weights of the first-layer indicators following the basic ideas of the DEMATEL. Firstly, with the expert weight ξ_B^{ik} obtained from the Phase 2, P IFPRs are aggregated via eq. (15).

$$h_{ij} = \langle \mu_{ij}, \nu_{ij} \rangle = \left\langle 1 - \prod_{k=1}^{P}(1-\widetilde{\mu}_{ij}^k)^{\xi_B^{ik}}, \prod_{k=1}^{P}(\widetilde{\nu}_{ij}^k)^{\xi_B^{ik}} \right\rangle \tag{15}$$

Where $\langle \widetilde{\mu}_{ij}^k, \widetilde{\nu}_{ij}^k \rangle$ is the element of $\widetilde{B}^k$, $H = (h_{ij})_{t\times t}$ is the integrated IFPR. Then considering the risk appetite of experts, the defuzzification is performed on H via eq. (16) (Xie et al., 2014).

$$\overline{h}_{ij} = w_{.j}[\mu_{ij} - \nu_{ij} + (2\gamma - 1)\pi_{ij}], i, j = 1, 2, ...,t \tag{16}$$

Where $w_{.j}$ is the value weight of the $j-th$ indicator, γ is the risk preference coefficient, and $\gamma > 0.5$ indicates that most of the experts are risk lovers, and vice versa. Then the real matrix $\overline{H} = (\overline{h}_{ij})_{t\times t}$ is normalized to form $\widetilde{H} = (\widetilde{h}_{ij})_{t\times t}$ via eq. (17).

$$\widetilde{h}_{ij} = \frac{\overline{h}_{ij}}{\max(\max\limits_{1\le i\le n}\sum_{j=1}^{n}\overline{h}_{ij}, \max\limits_{1\le j\le n}\sum_{i=1}^{n}\overline{h}_{ij})} \tag{17}$$

Finally, a comprehensive influence matrix $U = (u_{ij})_{t\times t}$ of the indicators can be calculated by (18)

$$U = \widetilde{H}(I - \widetilde{H})^{-1} \tag{18}$$

Where I is a unit matrix and $(I - \widetilde{H})^{-1}$ is the inverse matrix of $(I - \widetilde{H})$. Therefore, the comprehensive weight cw_i of the the $i-th$ indicator is obtained via eq. (19).

$$cw_i = \frac{\lambda_i}{\sum_{i=1}^{t}\lambda_i} \tag{19}$$

Where λ_i standards for the centrality in DEMATEL, the comprehensive weight vector can be represented by $cw = [cw_1, cw_2, ..., cw_t]$.

3.4. Phase 4: Aggregating the risk of second-layer indicators

Each first-layer indicator $F_s(s = 1, 2, ..., t)$ is decomposed into m_s second-layer indicators, so the IFJM $C^k = (c_{ij}^k)_{m\times n}(i = 1, 2, ..., m, j = 1, 2, ..., n, k = 1, 2, ..., P)$ contains several sub-matrixes, i.e. $C^k = [C_1^k, C_2^k, ..., C_t^k]^T$. The IFJM $C_s^k = (c_{ij}^k)_{m_s\times n}$ represents the second-layer indicator risks judged by expert D_k, then an integrated IFJM $G_s = (g_{ij})_{m_s\times n}$ representing the risk of indicator F_s is obtained by eq. (20).

$$g_{ij} = \langle \mu_{ij}, \nu_{ij} \rangle = \left\langle 1 - \prod_{k=1}^{P}\left(1 - \mu_{c_{ij}^k}\right)^{\xi_{C_s}^{ik}}, \prod_{k=1}^{P}\left(\nu_{c_{ij}^k}\right)^{\xi_{C_s}^{ik}} \right\rangle \tag{20}$$

Where $\langle \mu_{c_{ij}^k}, \nu_{c_{ij}^k} \rangle$ is the element of C_s^k, $\xi_{C_s}^{ik}$ is the expert weight calculated from the IFPR C_s^k. Then based on evidence theory, a mass function $\overline{m}_s$ on the first-layer indicator F_s can be obtained by eq. (21).

$$\begin{aligned}\overline{m}_s &= m_1^s(V) \oplus m_2^s(V) \oplus \cdots \oplus m_{m_s}^s(V) \\ &= \frac{\sum_{V_1\cap V_2\cap\cdots\cap V_n = V} m_1^s(V_1) m_2^s(V_2)\cdots m_{m_s}^s(V_j)}{1-\eta}\end{aligned} \tag{21}$$

Where $m_i^s(V_j)(i = 1, 2, ..., m_s, j = 1, 2, ..., n)$ is the mass function converted from the $i-th$ row of G_s via eq. (4),η represents the discount weight calculated by eq. (22).

$$\eta = \sum_{V_1\cap V_2\cap\cdots\cap V_n = \varnothing} m_1(V_1) m_2(V_2)\cdots m_{m_s}(V_n) \tag{22}$$

Therefore, a risk vector of first-layer indicators is obtained, denoted as $\overline{M} = [\overline{m}_1, \overline{m}_2, ..., \overline{m}_t]$.

3.5. Phase 5: Weighted aggregating the UPIoT construction risk

Before upward aggregating UPIoT construction risks, $\overline{M} = [\overline{m}_1, \overline{m}_2, ..., \overline{m}_t]$ needs to be corrected by the comprehensive weight cw_i of the first-layer indicators. The mass function $\overline{m}_s$ can be weighted by eq. (23).

$$\begin{cases}\widetilde{m}^s(\varnothing) = 0, \ \widetilde{m}^s(V_j) = \varepsilon_s \bullet \overline{m}_s(V_j) \\ \widetilde{m}^s(\Theta) = 1 - \varepsilon_s + \varepsilon_s \bullet \overline{m}_s(\Theta)\end{cases} \tag{23}$$

Where $\varepsilon_s = cw_s/\max(cw)$, $\widetilde{m}_s$ is the corrected mass function for the first-layer indicator $F_s(s = 1, 2, ..., t)$. Then repeating the information fusion process via eq. (21),t mass functions are merged into a single function denoted as m^r, which is defined on the risk level set $V = \{V_1, V_2, ..., V_n\}$. Each element $m(V_j)$ indicates the possibility of evaluating the UPIoT construction risk as V_j level.

4. Case study

In this section, with the application of IFGDM-CDWEF method proposed in Section 3, the UPIoT construction risk in China is evaluated thoroughly and comprehensively from multiple aspects, the risk assessment results are also demonstrated and discussed.

4.1. Data collection and preparation

As aforementioned, the IFGDM-CDWEF method is based on the preference information provided by experts. Therefore, 10 experts in the UPIoT domain are asked to score the UPIoT construction risk based on their domain knowledge and work experience. Table 2 lists the detailed information of the experts. Each expert D_k receives a questionnaire that includes the description of risk levels, scoring rules, and indicators identified in Section 2, the expert uses the IFNs to score the indicator risk and then returns the feedback.

Consequently, A^k, B^k, C^k are extracted from the returned questionnaire, where A^k and B^k are 4×4 dimensional IFPRs on the first-layer indicators, and C^k is 17×5 dimensional IFJM on the second-layer indicators, all the data collected from experts is available in the Appendix A. Other parameter values used in the case study are listed in Table 3, and notably, the variable symbols used in this section share the same meaning defined in Section 3 as well as the nomenclature.

Therefore, based on the collected data and set parameters, the UPIoT construction risk can be evaluated following the procedure of IFGDM-CDWEF method.

4.2. Results

The UPIoT construction risk of China is evaluated via Matlab programming that realizes the IFGDM-CDWEF method, the Matlab project can be accessed in the Appendix A. This subsection demonstrates the UPIoT construction risk assessment results based on the proposed method.

4.2.1. Dynamic expert weights

According to the dynamic expert weight determination method proposed in Section 3.2, the IFRs A^k, B^k and C^k scored by experts are used to determine their weights on first-layer indicators.

The initial IFE based expert weight ew_i^k is determined by eqs. (1), (2), and (3), then the IFRs are converted into mass functions via eq. (4). After that, according to eq. (5), the mass functions are used to measure the conflicts between different experts, thus the conflict information based expert weight sw_i^k can be calculated by eqs. (6) and (7). Finally, the expert weights ξ_A^{ik}, ξ_B^{ik} and ξ_C^{ik} are obtained by averaging ew_i^k and sw_i^k. The weight matrixes of experts are available in the Appendix A,ξ_A^{ik} and ξ_B^{ik} are both 4×10 dimensional matrixes, while ξ_C^{ik} is a 17×10 dimensional matrix.

Fig. 7 shows the expert weight distribution of $\xi_A^{ik}(k = 1, 2, ..., 10, i = 1, 2, ..., 4)$, it can be seen that different experts

Table 2
Basic information of interviewed experts.

Expert ID	Professional title	Professional field	Working years	Working department
1	Director	Power system operation and IoT	24	Science and Technology Department of SGCC
2	Assistant	Power system operation	9	Science and Technology Department of SGCC
3	Manager	State Grid innovation and entrepreneurship	11	E-commerce company of SGCC
4	Assistant	The Internet and informatization	6	E-commerce company of SGCC
5	Business manager	Sales and grid business innovation	12	E-commerce company of SGCC
6	Secretary	Innovation and development policy	5	E-commerce company of SGCC
7	Professor	Energy Internet and Electricity Market	25	North China Electric Power University
8	Professor	Emerging grid technology application and risk management	27	North China Electric Power University
9	Professor	Information economy research in power grid	22	North China Electric Power University
10	Ph. D	Power system big data analysis	5	North China Electric Power University

Table 3
The parameter values for the UPIoT construction risk assessment.

Parameter	Value	Description
t	4	Number of first-layer indicators
m	17	Number of second-layer indicators
$m_s(1, 2, ..., t)$	[5,5,4,3]	Number of subordinate indicators of the first-layer indicator F_s
n	5	Number of risk levels
$V_j(j = 1, 2, ..., n)$	{'Very high',' High', 'General',' Low',' Very low'}	Risk level scales
γ	0.7	Risk-biased experts accounted for 70%
σ	0.8	Controlling parameter for consistency repairing
α	{0,0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1}	Combination coefficient for the expert weight

get different weights, but the weight is dynamic because one expert can be weighted with various values according to different indicators. For example, expert D_2 gets the lowest weight on the indicator F_3, indicating that the expert may be less familiar with F_3 than other indicators. Therefore, the proposed expert weight determining method can well discriminate the domain knowledge of experts, this capability is crucial for correcting the IFRs used in the subsequent risk assessment phases.

4.2.2. Combined first-layer indicator weights

The comprehensive weight of first-layer risk indicators can be determined by the IF-AHP-DEMATEL method proposed in Section 3.3. First of all, the consistency of IFPRs A^k, B^k is checked and automatically repaired by eqs. (8)~(11), obtaining the consistent matirx $\widetilde{A}^k$ and $\widetilde{B}^k$. Then using eqs. (12)(13)(14), the value weight $\overline{w}$ of indicators can be determined from $\widetilde{A}^k$, where $\overline{w} = [0.2676,0.2808,0.2373,0.2143]$. The value weight indicates that the importance of first-layer indicators relative to the UPIoT construction risk can be ranked as $F_2 \succ F_1 \succ F_3 \succ F_4$.

Afterwards, $\widetilde{B}^k$ is processed with eqs. (15)~(19) to produce the influence relation matrix U, where

$$U = \begin{bmatrix} 0.3062 & 0.8008 & 0.5831 & 0.4267 \\ 0.3478 & 0.3593 & 0.3798 & 0.3530 \\ 0.3557 & 0.6538 & 0.2794 & 0.4022 \\ 0.5390 & 0.7790 & 0.5157 & 0.3050 \end{bmatrix} \tag{24}$$

Finally, the comprehensive weight of first-layer indicators can be obtained, denoted as $cw = [0.2481, 0.2730, 0.2335, 0.2454]$. Compared with $\overline{w}$, the weight of indicators F_1, F_2, and F_3 decreases, while the weight of indicator F_4 increases and exceeds the weight of F_3. Therefore, the first-layer indicator weight can be ranked as $F_2 \succ F_1 \succ F_4 \succ F_3$, the management risk indicator is emphasized with the integration of DEMATEL.

Moreover, the comprehensive influence matrix $U = (u_{ij})_{4\times4}$ can be transformed into an upper triangular matrix $U' = (u_{ij})_{4\times4}$, where $u'_{ij} = u_{ij} - u_{ji}(i < j)$ and $u'_{ij} = 0(i = j)$. $u'_{ij} > 0$ represents the impact of indicator F_i on F_j, while $u'_{ij} < 0$ represents the opposite. Therefore, the interaction of first-layer indicators is shown in Fig. 8.

$$U' = \begin{array}{c} \\ F_1 \\ F_2 \\ F_3 \\ F_4 \end{array} \begin{array}{c} \begin{array}{cccc} F_1 & F_2 & F_3 & F_4 \end{array} \\ \begin{bmatrix} 0 & 0.4530 & 0.2274 & -0.1123 \\ - & 0 & -0.2739 & -0.4261 \\ - & - & 0 & -0.1135 \\ - & - & - & 0 \end{bmatrix} \end{array} \tag{25}$$

It can be observed that the business risk (F_2) is prone to be largely affected by other indicators, thus its weight decreases slightly in cw, on contrary, the weight of the management risk (F_4) increases dramatically due to its wide impact on all other three indicators. Since the Fig. 8 is a fully-connected directed diagram, one risk indicator can become a high-influence risk source by affecting another through different paths. For example, the basic support risk (F_1) is more important than the cyber security risk(F_3) because it gets two influence paths to the indicator F_2 while the later gets only one path. Therefore, although it is crucial to construct the UPIoT businesses such as comprehensive energy service and energy data service, the impact of related risk factors including basic support, cybersecurity, and management cannot be neglected.

4.2.3. Second-layer indicator risk comparison

In this section, the IFJM $C^k(k = 1, 2, ..., 10)$ is processed with the determined expert weights and first-layer indicator weights for the UPIoT construction risk assessment. Firstly, all the IFJMs given by experts are integrated with the expert weight $\xi_C^{ik}(i = 1, 2, ..., 17)$ via eq. (20), thus a comprehensive IFJM G that consists of four sub-matrixes $G_s(s = 1, 2, 3, 4)$ is obtained, each of them represents the risk of second-layer indicators that belong to the corresponding first-layer indicator F_s. Then the sub-matrixes are converted into risk mass functions $\overline{m}_i^s(i = 1, 2, ..., m_s)$.

Fig. 9 shows the risk integration results of all second-layer indicators. According to the Maximum Membership Principle (MMP) (Boltyanski & Poznyak, 2012), the indicator risk can be judged as level $V_j(j = 1, 2, ..., 5)$ when $\overline{m}_i^s(V_j)$ is the largest membership degree among others. Therefore, the block with the darkest color in Fig. 9 represents the risk level of the corresponding second-layer indicator. It can be observed that most second-layer indicators are at *'High'* risk level, other indicators like F_{14}, F_{24}, F_{25}, F_{34} are at *"Very high"* risk level, while F_{15} and F_{21} are at *'General'* risk level.

However, there are two blocks with very similar colors on the same horizontal line of Fig. 9, thus the risk level of the risk indicator corresponding to the line is difficult to determine. For instance, the mass function of indicator F_{32} is

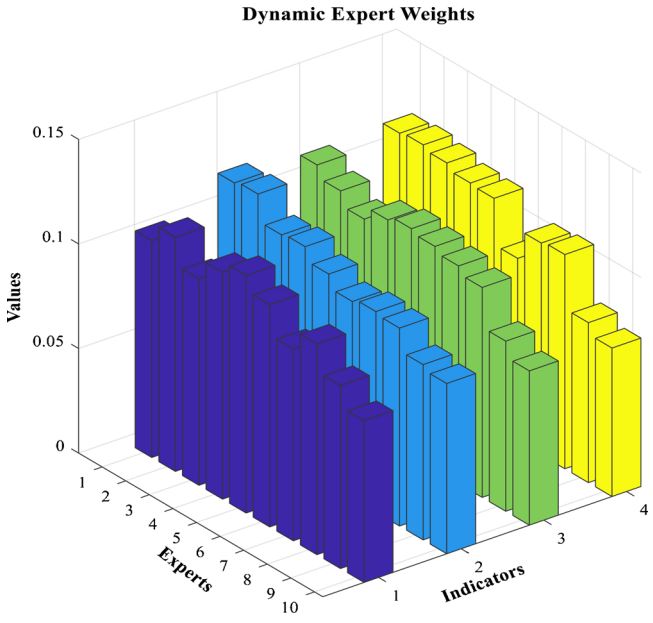

Fig. 7. Dynamic expert weight distribution on first-layer indicators. The expert weights under different indicators are described by bar groups with different colors.

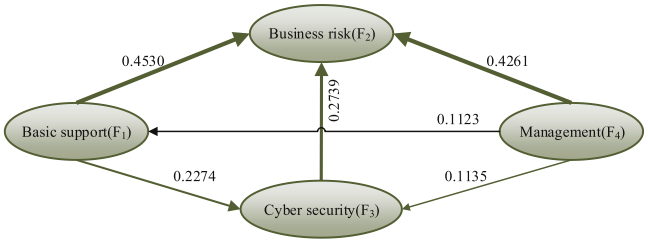

Fig. 8. The influence relation between first-layer indicators. Numbers in the directed graph represent the influence weight of upstream nodes.

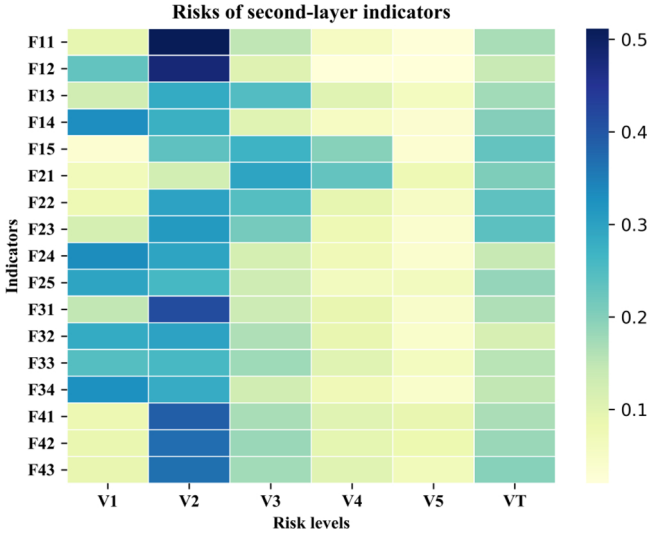

Fig. 9. The heat map for second-layer indicator risks. VT on the x-axis represents an unknown and uncertain risk level).

$$\overline{m}_2^3 = [0.2868\ 0.2995\ 0.1649\ 0.0909\ 0.0406\ 0.1173] \tag{26}$$

Where $\overline{m}_2^3(V_1) = 0.2868$ is very close to $\overline{m}_2^3(V_2) = 0.2995$, but according to the MMP, the risk level of F_{32} is considered as V_2. This may be unfair because the strong membership degree $\overline{m}_2^3(V_1)$ is disregarded, thus the MMP can be too simple and rough to judge the risk level of the indicator which gets two very close or even the same membership degrees in its risk mass function.

In order to accurately compare risk values among different indicators, an equation to calculate the comprehensive risk value of each second-layer indicator is proposed on the basis of risk management theory. Assuming that the defense cost for the risk with different levels is $l_i (i = 1, 2, \ldots, 5)$, then l_i increases as the indicator risk level goes up. The risk value of second-layer indicators can be calculated according to eq. (27).

$$S_F = (1 - m(\theta)) \sum_{i=1}^{n} l_i \bullet m_F(V_i) \tag{27}$$

Where S_F was the risk of indicator F, θ was the identification framework and $m_F(V_i)$ represents the mass function of indicator F, and $V_i \subset 2^{\theta}$. This method converts the risk mass function into a real number and takes into account all the information contained in the membership.

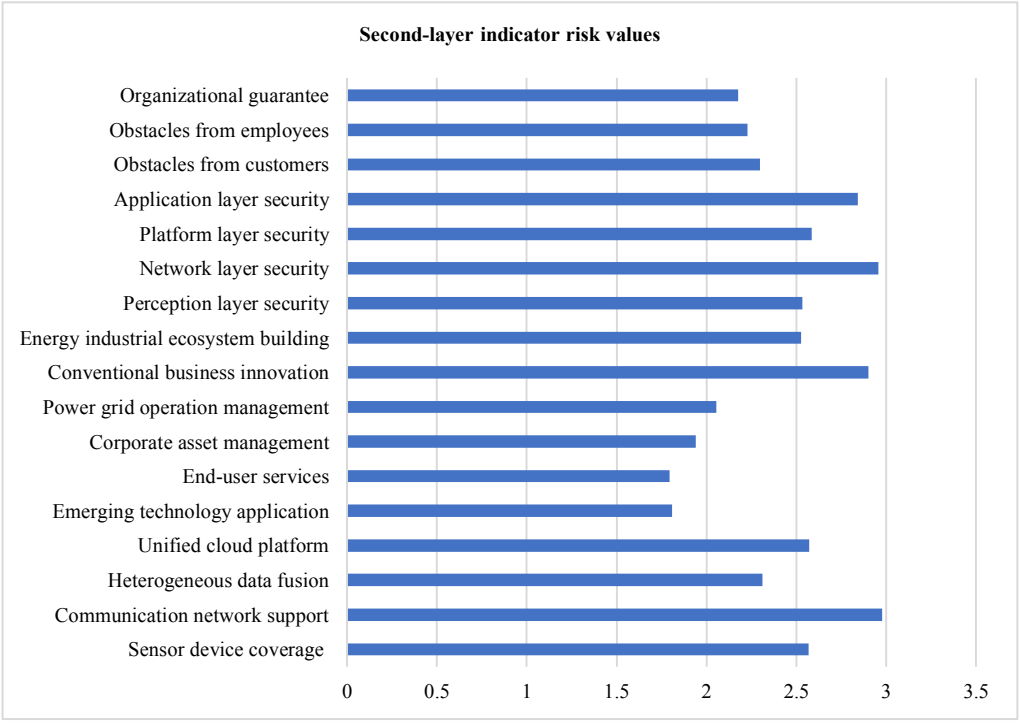

Fig. 10. Comprehensive risk values of second-layer indicators.

Therefore, let l_i change linearly from 5 to 1, then $l = (5, 4, 3, 2, 1)$, Fig. 10 shows the risk values of all second-layer indicators obtained from $\overline{M}$.

Each bar in the Fig. 10 represents the corresponding second-layer indicator risk value calculated by eq. (27). It can be seen that communication network support risk (F12) is the highest, followed by network layer security risk (F32), conventional business innovation risk (F24), and application layer security risk (F34). Therefore, much attention should be paid to the communication network construction as well as its security issue. High innovation risk to the conventional business indicates that it is hard for power grid companies to improve their existing businesses because they have been profiting from electricity sales for decades. The risk of application layer security is also at a high level, indicating that the deployment of external applications on the UPIoT may be harmful to the data inside the power grid.

The lowest risk indicators are end-user services (F21) and emerging technology application (F15). Notably, since the second-layer indicators can be grouped by different first-layer indicators, the second-layer indicator risk values often get polarized distribution in the same group. For example, the difference between the risk values of indicators F24 and F21 is fairly large, while both of them belong to the business risk indicator that gets the highest weight cw_2. This phenomenon indicates that it is hard to compare the risk of first-layer indicators purely according to the second-layer indicator risk values, and there may be conflicts between the risk mass functions of second-layer indicators, thus a risk integration method such as evidence fusion that considers the conflict information is needed.

4.2.4. The UPIoT construction risk integration

The mass functions of second-layer indicator risks can be integrated by eq. (21) to obtain the mass function $\overline{m}_s(s = 1, 2, ...,4)$ of first-layer indicators, where

$$\overline{M} = \begin{array}{c} \\ F_1 \\ F_2 \\ F_3 \\ F_4 \end{array} \begin{array}{c} V1 \quad V2 \quad V3 \quad V4 \quad V5 \quad \Theta \\ \begin{bmatrix} 0.0678 & 0.8383 & 0.0797 & 0.0107 & 0.0031 & 0.0003 \\ 0.1545 & 0.5179 & 0.2533 & 0.0567 & 0.0164 & 0.0011 \\ 0.3004 & 0.5707 & 0.0896 & 0.0297 & 0.0092 & 0.0005 \\ 0.0498 & 0.6762 & 0.1554 & 0.0636 & 0.0467 & 0.0083 \end{bmatrix} \end{array} \tag{28}$$

According to eq. (23), the mass functions representing first-layer indicator risk are discounted with the indicator weight cw.

$$\widetilde{M} = \begin{array}{c} \\ F_1 \\ F_2 \\ F_3 \\ F_4 \end{array} \begin{array}{c} V1 \quad V2 \quad V3 \quad V4 \quad V5 \quad \Theta \\ \begin{bmatrix} 0.0617 & 0.7620 & 0.0725 & 0.0098 & 0.0028 & 0.0914 \\ 0.1545 & 0.5179 & 0.2533 & 0.0567 & 0.0164 & 0.0011 \\ 0.2569 & 0.4881 & 0.0766 & 0.0254 & 0.0078 & 0.1451 \\ 0.0447 & 0.6080 & 0.1397 & 0.0571 & 0.0420 & 0.1084 \end{bmatrix} \end{array} \tag{29}$$

Where $\widetilde{M}$ is the discounted mass function matrix for the risk of first-layer indicators. Compared with eq. (28), except for the mass function of indicator F_2 with the highest indicator weight, the mass function values of other indicators decreases. The maximal membership of $\widetilde{m}_3$ is smaller than that of $\widetilde{m}_2$ in eq. (29), but the opposite is true in the eq. (28). These observations indicate that the first-layer indicator weight can discriminatively discount the risk mass functions, some of them are largely discounted, some of them are lightly discounted, but the risk mass function of the indicator that gets the largest indicator weight stay unchanged.

Then using the evidence fusion process shown in eq. (21) again, $\widetilde{M}$ is integrated to form a mass function m^r that represents the comprehensive UPIoT construction risk, where

$$m^r = [0.0223\ 0.9505\ 0.0259\ 0.0011\ 0.0002] \tag{30}$$

Hence, the overall risk to China's UPIoT construction is at a 'High' level, indicating that lots of risk factors may threat the construction process of UPIoT.

4.2.5. Sensitivity analysis on the combined dynamic weights

IFGDM-CDWEF method is a risk assessment model with combined dynamic weights (CDWs) including the combined indicator weight and the dynamic expert weight. In this subsection, sensitivity analysis is performed, and four scenarios listed below are designed for exploring the effect on the first-layer indicator risks.

- Scenario 1: The first-layer indicator risk is integrated without considering the expert weight or the indicator weight.
- Scenario 2: The first-layer indicator risk is integrated with the corresponding indicator weight, but the expert weight is not considered.
- Scenario 3: Contrary to the scenario 3, the first-layer indicator risk is integrated with the expert weight, but the indicator weight is not used.
- Scenario 4: The first-layer indicator risk is integrated with both the expert weight and the indicator weight.

All the four scenarios are simulated based on the data declared in Section 4.1, and the condition of disregarding expert weights in a scenario is equivalent to setting all expert weights to 1 / P, where P is the number of experts. In Section 3.2, the expert weight is combined by averaging the sum of ew_i^k and ew_i^k, but in the simulation scenarios, the weight is obtained by eq. (31).

$$\xi^{ik} = \alpha \bullet ew_i^k + (1 - \alpha) \bullet sw_i^k \tag{31}$$

Where the combination coefficient $\alpha = \{0,0.1,0.2,...,1\}$ is set to test the effect on the results with respect to different parts of the expert weight. The simulation results of each scenario are shown below.

Table 4 lists the first-layer indicator risks obtained from scenario 1 and scenario 2, the results from the two scenarios are similar to eqs. (28) and (29), respectively. However, since eqs. (28) and (29) are obtained considering the expert weight that is not included in scenarios 1 and 2, the discounting effect of first-layer indicator weights exists whether the expert weight is considered or not.

These two scenarios provide the baseline for scenario 3 and scenario 4 that are simulated with the expert weight. In Section 4.2.3, it has been found that the MMP can be unconvincing when judging the risk level of an indicator with two very close membership degrees on different risk levels. Therefore, a distinction value Δd_F is defined in eq. (32) to measure the effect of CDWs on the first-layer indicator risk assessment.

$$\Delta d_F = \max(m_F) - \sec\max(m_F) \tag{32}$$

where $\max(m_F)$ represents the maximum membership an indicator risk mass function m_F, and $\sec\max(m_F)$ represents the second largest one. Hence the larger the index Δd_F, the easier it is to distinguish the risk level of the indicator, and vice versa. For example, in the scenario 1 in Table 4,$\Delta d_{F_2} = 0.3658 > \Delta d_{F_3} = 0.0013$, indicating that the risk level of F_2 are more distinguishable than F_3.

Fig. 11 shows the distinction values simulated from scenarios 1 and 3, both of them do not consider the influence of first-layer indicator weights, but scenario 3 is simulated with varying expert weights. In subgraphs a) and b), the distinction values obtained from scenario 3 are

Table 4
Simulated results of scenarios 1 and 2.

		V1	V2	V3	V4	V5	Θ
Scenario 1	F1	0.0666	0.8396	0.0796	0.0107	0.0031	0.0004
	F2	0.1536	0.5194	0.2528	0.0566	0.0164	0.0011
	F3	0.4280	0.4267	0.0807	0.0422	0.0164	0.0060
	F4	0.0574	0.6109	0.1932	0.0700	0.0521	0.0165
Scenario 2	F1	0.0611	0.7698	0.0730	0.0099	0.0028	0.0834
	F2	0.1536	0.5194	0.2528	0.0566	0.0164	0.0011
	F3	0.3668	0.3657	0.0692	0.0361	0.0141	0.1481
	F4	0.0519	0.5524	0.1747	0.0633	0.0471	0.1106

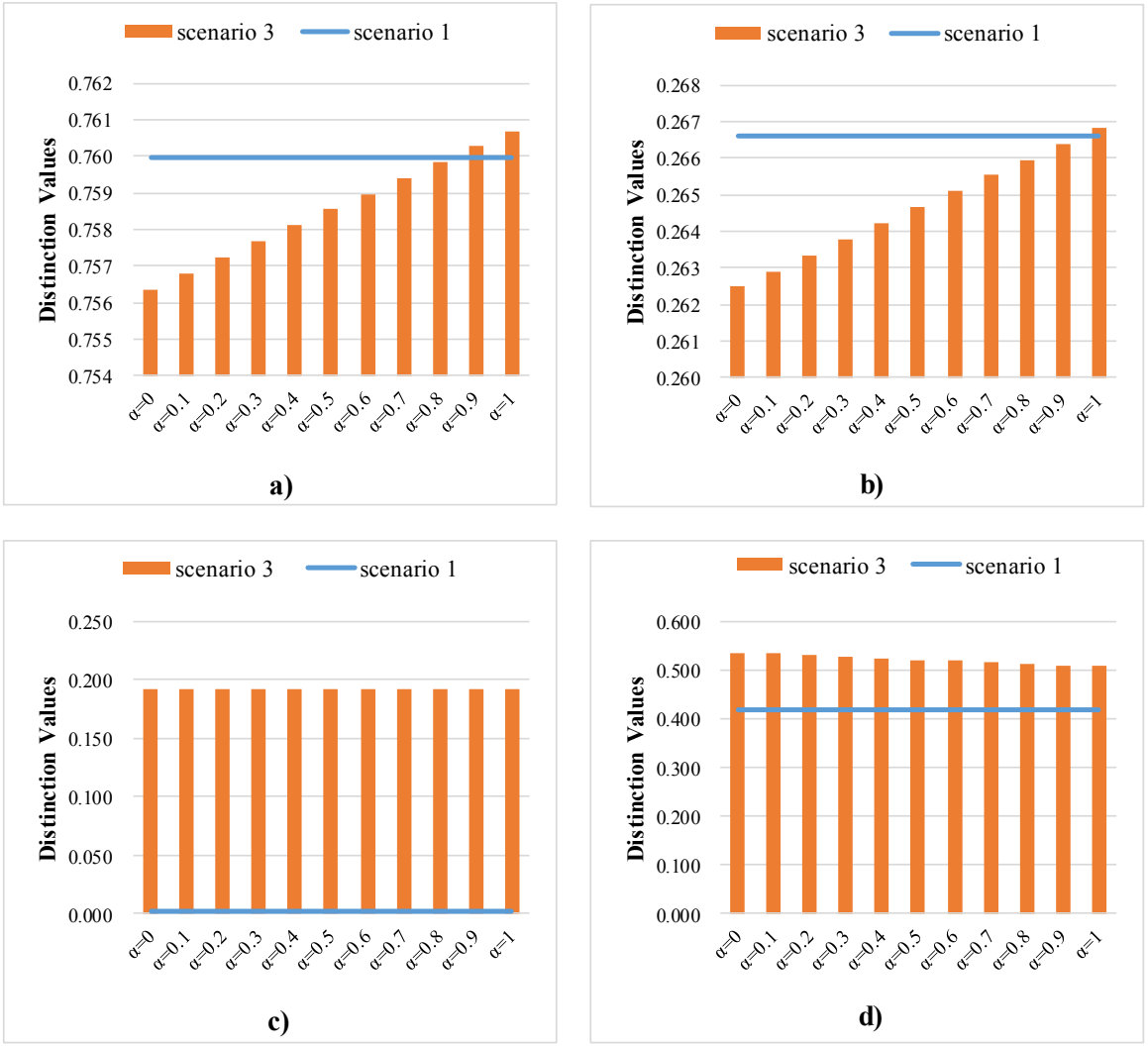

Fig. 11. Simulation results of scenario 1 and scenario 3: a) indicator F_1, b) indicator F_2, c) indicator F_3, d) indicator F_4. (Note: The distinction values are calculated by eq. (31)).

sensitive to the variation of parameter α and increase steadily, while the corresponding values in the subgraphs c) and d) are more insensitive. Compared with scenario 1, Δd_{F_1} and Δd_{F_2} of scenario 3 are relatively small at the beginning, but exceeds those of scenario 1 eventually as the parameter α increase. However, Δd_{F_3} and Δd_{F_4} of scenario 3 are larger than scenario 1 regardless of the parameter value α. Notably, in the subgraph c), it is difficult to determine the risk level of indicator F_3 according to scenario 1 because its Δd_{F_3} is close to zero, but the dilemma is well solved in scenario 3 due to its relatively large distinction values distributed on the parameter α.

Fig. 12 shows the simulation results of scenario 4 and scenario 2, both of them consider the influence of first-layer indicator weights, but the scenario 2 is simulated without the expert weight. It can be seen that the subgraphs b), c) and d) in Fig. 12 are similar to the Fig. 11, but the highest distinction values in the subgraphs a), c) and d) are a little lower than those shown in the Fig. 11 due to the participation of first-layer indicator weights. Nevertheless, contrary to the scenario 3 in the subgraph a) in Fig. 11, the distinction values of scenario 4 decrease as the parameter α increases. Since the only difference between scenarios 3 and 4 is that the latter considers the first-layer indicator weights, the discounting effect of the weight on different membership degrees of a risk mass function can lead to a downward trend in the distinction values.

4.3. Discussion of the results

According to Fig. 7, each expert can be weighted from the IFE and conflict information capable of measuring the uncertainty caused by differential domain knowledge and working experience, thus the weight changes dynamically with different experts and indicators. Fig. 8 indicates that risk factors do not affect the UPIoT construction independently, the interactions between indicators can change their weight in the system. Therefore, with the discounting effect from CDWs, the risk mass function of UPIoT construction becomes more comprehensive and representative, suggesting that the UPIoT construction risk of China is at a relatively high level, especially the basic support risk shown in the eq. (29). Fig. 9 intuitively shows the risk mass functions of second-layer indicators, but Fig. 10 provides a more clear and quantitative comparison of the second-layer indicator risk, indicating that the communication network support risk, the conventional business innovation risk, and the network layer security are three the most threatening factors underlying the UPIoT construction risk. Consequently, when constructing the UPIoT, SGCC should concentrate more on the IoT structure including the network layer and application layer, especially the infrastructure and security of communication networks. Moreover, since SGCC is a conventional state-owned company, the risk from its internal resistance to innovative new businesses cannot be ignored.

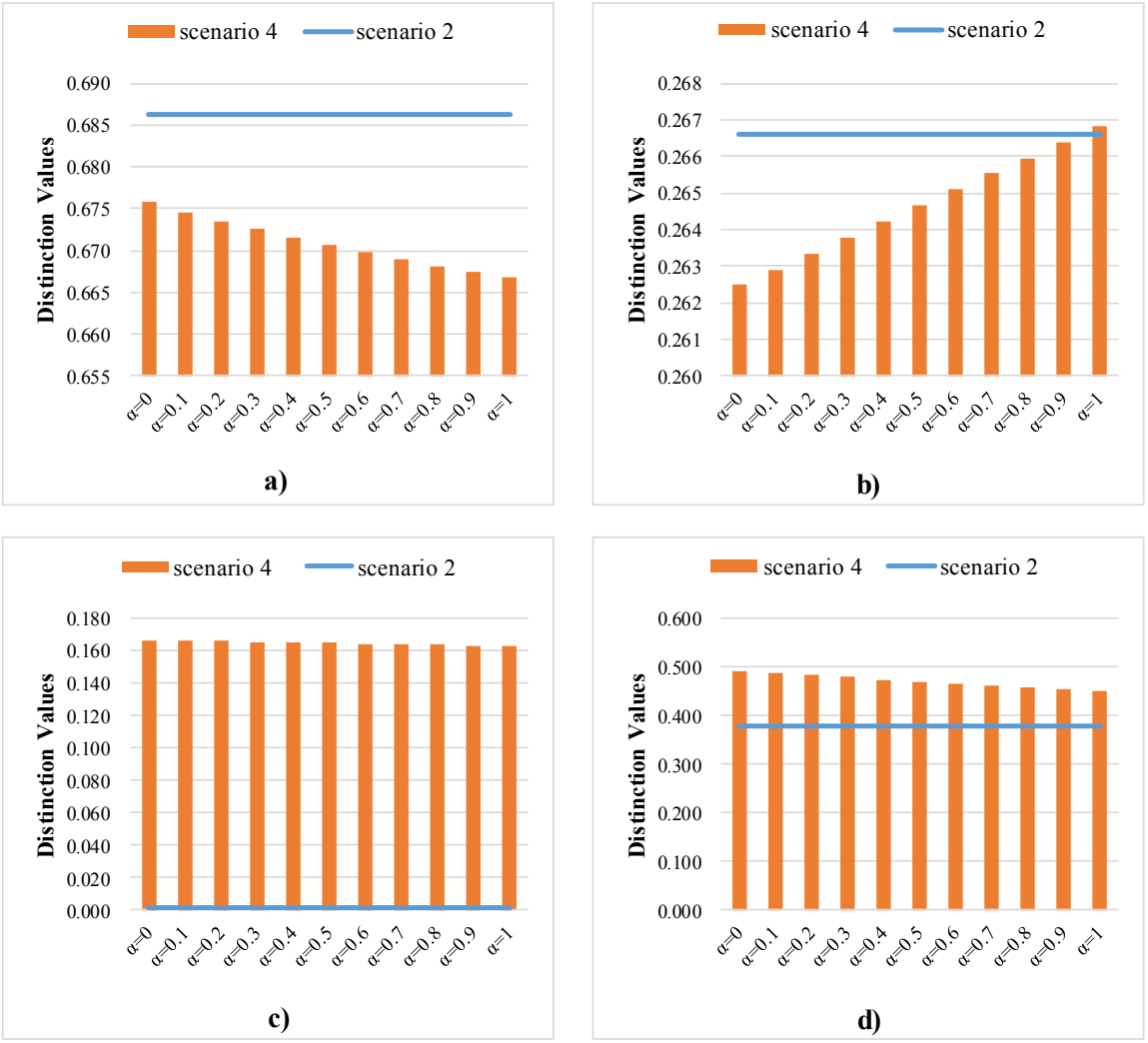

Fig. 12. Simulation results of scenario 2 and scenario 4: a) indicator F_1, b) indicator F_2, c) indicator F_3, d) indicator F_4.

In terms of the sensitivity analysis, Figs. 11 and 12 display the effects of changing CDWs. When the expert weights are not considered in scenarios 1 and 2, two membership degrees in the risk mass function of an indicator may be too close to distinguish which risk level the indicator belongs to. Nevertheless, in scenarios 3 and 4, this embarrassment can be greatly improved by including the expert weight capable of weighting different IFRs in the risk integration process, even though the risk mass functions of some indicators fluctuate slightly with the increase of the combination coefficient α. Hence, the IFGDM-CDWEF method is able to deal with the conflict information from multiple experts, obtaining a fairly stable and comprehensive indicator risk value.

However, although the proposed method has potential in comprehensive risk assessment areas that lack objective data, it is inevitable that there are some limitations need to be improved in the future. For example, this study dedicates to find out the risk factors that pose the greatest threat to the UPIoT construction, but lacks the mechanism analysis on how each risk factor affects the UPIoT. The method for determining the weight and risk in this paper is chosen based on the problem characteristics, thus further details need to be discussed when dealing with other problems beyond the scope of UPIoT.

5. Conclusions

In this paper, the risk of UPIoT construction in China is studied with a comprehensive risk assessment framework based on the IFGDM-CDWEF method. A hierarchical indicator system with two-layer risk factors affecting the UPIoT construction is identified from four aspects: basic support, business, cyber security, and management. Under the IFGDM environment, the combined indicator weight determined via the IF-AHP-DEMATEL method can effectively discount the risk mass functions of first-layer indicators. Moreover, the dynamic expert weight obtained from the entropy and conflict information of IFRs is able to discriminate and correct the multi-source scoring data. Therefore, both the IFRs and risk mass functions of indicators can be well corrected by the CDWs. Based on the sensitivity analysis, although the changing CDWs result in a slight fluctuation of the risk mass function, the dynamic expert weight is able to resolve the vagueness of indicator risk levels by correcting the IFRs. Moreover, the risk comparison method that considers the risk defense cost is more thoughtful and practical than the pure application of MMP. According to the evidence fusion theory, the UPIoT construction risk is comprehensively integrated considering conflicts. The results indicate that China's UPIoT construction risk is generally at a high level, especially in the construction of strong communication networks and innovative businesses, providing a risk preventing perspective for establishing the sustainable ecosystem in China.

Declaration of Competing Interest

The authors declare that there are no conflicts of interest.

Acknowledgements

This study is funded by the National Natural Science Foundation of China (Grant number: 71840004) and the State Grid Nanjing Power Supply Company (Project: Research on collaborative innovation mechanism and construction effect evaluation of innovation and entrepreneurship Park of electric power Internet of things).

Appendix A

Data materials and programming codes for the research paper are available in the website: https://github.com/WangQiqing/UPIoT-construction-risk.git.

References

Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2018). A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges. *IEEE Access, 6*, 3619–3647. https://doi.org/10.1109/ACCESS.2017.2779844.

Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2019). Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*. https://doi.org/10.1016/j.scs.2019.101728 101728.

Atanassov, K. T. (1999). *Intuitionistic Fuzzy Sets*. https://doi.org/10.1007/978-3-7908-1870-3.

Bahramara, S., & Golpira, H. (2018). Robust optimization of micro-grids operation problem in the presence of electric vehicles. *Sustainable Cities and Society, 37*, 388–395. https://doi.org/10.1016/j.scs.2017.11.039.

Bhoyar, P., Sahare, P., Dhok, S. B., & Deshmukh, R. B. (2019). Communication technologies and security challenges for internet of things: A comprehensive review. *AEU - International Journal of Electronics and Communications, 99*, 81–99.

Boltyanski, V. G., & Poznyak, A. S. (2012). *The Robust Maximum Principle*. https://doi.org/10.1007/978-0-8176-8152-4_3.

Chen, T.-Y., & Li, C.-H. (2010). Determining objective weights with intuitionistic fuzzy entropy measures: A comparative analysis. *Information Sciences, 180*, 4207–4222. https://doi.org/10.1016/j.ins.2010.07.009.

De Dutta, S., & Prasad, R. (2019). Security for Smart Grid in 5G and Beyond Networks. *Wireless Personal Communications, 106*, 261–273. https://doi.org/10.1007/s11277-019-06274-5.

Dempster, A. P. (2008). Upper and Lower Probabilities Induced by a Multivalued Mapping. In R. R. Yager, & L. Liu (Eds.). *Classic Works of the Dempster-Shafer Theory of Belief Functions* (pp. 57–72). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-540-44792-4_3.

Du, Y. W., Yang, N., & Ning, J. (2018). IFS/ER-based large-scale multiattribute group decision-making method by considering expert knowledge structure. *Knowledge-Based Systems, 162*, 124–135. https://doi.org/10.1016/j.knosys.2018.07.034.

Ellabban, O., & Abu-Rub, H. (2016). Smart grid customers' acceptance and engagement: An overview. *Renewable and Sustainable Energy Reviews, 65*, 1285–1298. https://doi.org/10.1016/j.rser.2016.06.021.

Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2018). A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustainable Cities and Society, 38*, 806–835. https://doi.org/10.1016/j.scs.2017.12.041.

Fontela, E., & Gabus, A. (1976). *The DEMATEL observer, DEMATEL 1976 Report*Switzerland Geneva: Battelle Geneva Research Center.

Girma, A. (2018). Analysis of Security Vulnerability and Analytics of Internet of Things (IOT) Platform. In S. Latifi (Vol. Ed.), *Information Technology - New Generations. Advances in Intelligent Systems and Computing: 738*. Cham: Springer.

Habibi Gharakheili, H., Sivanathan, A., Hamza, A., & Sivaraman, V. (2019). Network-Level Security for the Internet of Things: Opportunities and Challenges. *Computer (USA), 52*, 58–62.

Han, D., Dezert, J., & Yang, Y. (2018). Belief Interval-Based Distance Measures in the Theory of Belief Functions. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48*, 833–850. https://doi.org/10.1109/TSMC.2016.2628879.

Herrera-Viedma, E., Herrera, F., Chiclana, F., & Luque, M. (2004). Some issues on consistency of fuzzy preference relations. *European Journal of Operational Research, 154*, 98–109. https://doi.org/10.1016/S0377-2217(02)00725-7.

Hossain, E., Khan, I., Un-Noor, F., Sikander, S. S., & Sunny, M. S. H. (2019). Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. *IEEE Access, 7*, 13960–13988. https://doi.org/10.1109/ACCESS.2019.2894819.

Hu, W., Li, H. H., Yao, W. H., & Hu, Y. W. (2019). Energy Optimization for WSN in Ubiquitous Power Internet of Things. *Int. J. Comput. Commun. Control, 14*, 503–517. https://doi.org/10.15837/ijccc.2019.4.3572.

Ibadov, N. (2017). Selection of Construction Project Taking into Account Technological and Organizational Risk. *Acta Phys. Pol. A, 132*, 974–977. https://doi.org/10.12693/APhysPolA.132.974.

Jafari, A., Khalili, T., Ganjehlou, H. G., & Bidram, A. (2020). Optimal integration of renewable energy sources, diesel generators, and demand response program from pollution, financial, and reliability viewpoints: A multi-objective approach. *J. Clean Prod. 247*, 119100. https://doi.org/10.1016/j.jclepro.2019.119100.

Jiang, A., Yuan, H., Li, D., & Tian, J. (2019). Key technologies of ubiquitous power Internet of Things-aided smart grid. *J. Renew. Sustain. Energy, 11*, 062702. https://doi.org/10.1063/1.5121856.

Khalili, T., Hagh, M. T., Zadeh, S. G., & Maleki, S. (2019a). Optimal reliable and resilient construction of dynamic self-adequate multi-microgrids under large-scale events. *IET Renew. Power Gener. 13*, 1750–1760. https://doi.org/10.1049/iet-rpg.2018.6222.

Khalili, T., Nojavan, S., & Zare, K. (2019b). Optimal performance of microgrid in the presence of demand response exchange: A stochastic multi-objective model. *Comput. Electr. Eng. 74*, 429–450. https://doi.org/10.1016/j.compeleceng.2019.01.027.

Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. *Future Generation Computer Systems, 100*, 144–164. https://doi.org/10.1016/j.future.2019.04.038.

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection, 25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001.

Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J. S., & Martin, A. (2019). Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. *IEEE Communications Surveys and Tutorials, 21*, 2886–2927.

Kure, H. I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Phys. Syst., Theory Appl. (UK), 4*, 332–340.

Kuzlu, M., Pipattanasomporn, M., & Rahman, S. (2014). Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks, 67*, 74–88. https://doi.org/10.1016/j.comnet.2014.03.029.

Li, P., Liu, Y., Xin, H., & Jiang, X. (2018). A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant Under Cyber-Attacks. *IEEE Transactions on Industrial Informatics, 14*, 4343–4352. https://doi.org/10.1109/TII.2017.2788868.

Li, Q., Zhang, J., Chen, J., & Lu, X. (2019). Reflection on opportunities for high penetration of renewable energy in China. *Wiley Interdiscip. Rev. Energy Environ. 8*, e344. https://doi.org/10.1002/wene.344.

Lin, J., Yu, W., Zhang, N., & Yang, X. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things, 4*(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200.

Losavio, M., Elmaghraby, A., & Losavio, A. (2018). Ubiquitous Networks, Ubiquitous Sensors: Issues of Security, Reliability and Privacy in the Internet of Things. In N. Boudriga, M. S. Alouini, S. Rekhis, E. Sabir, & S. Pollin (Vol. Eds.), *Ubiquitous Networking. UNet 2018. Lecture Notes in Computer Science: 11277*. Cham: Springer.

Luis, S. G., & Jose, I. M. H. (2019). Monte Carlo approach to fuzzy AHP risk analysis in renewable energy construction projects. *PLoS One, 14*, e0215943. https://doi.org/10.1371/journal.pone.0215943.

Mukherjee, A. (2015). Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. In: *Proceedings of the IEEE, 103*, 1747–1761. https://doi.org/10.1109/JPROC.2015.2466548.

Nastase, L. (2017). Security in the Internet of Things: A Survey on Application Layer Protocols. *2017 21st International Conference on Control Systems and Computer Science (CSCS)* (pp. 659–666). . https://doi.org/10.1109/CSCS.2017.101.

NEA (2020). *National Energy Administration: Online Press Conference in the First Quarter of 2020*. Accessed 6 Apr 2020 http://www.nea.gov.cn/2020-03/06/c_138850234.htm/.

Pacevicius, M., Roverso, D., Salvo Rossi, P., & Paltrinieri, N. (2018). *Smart Grids: Challenges of Processing Heterogeneous Data for Risk Assessment*. Los Angeles, CA, United states: The PSAM Conference.

Radoglou Grammatikis, P. I., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things, 5*, 41–70. https://doi.org/10.1016/j.iot.2018.11.003.

Rafferty, A. E., & Jimmieson, N. L. (2017). Subjective Perceptions of Organizational Change and Employee Resistance to Change: Direct and Mediated Relationships with Employee Well-being. *British Journal of Management, 28*, 248–264. https://doi.org/10.1111/1467-8551.12200.

Saaty, T. L. (2001). Analytic hierarchy process. In S. I. Gass, & C. M. Harris (Eds.). *Encyclopedia of Operations Research and Management Science* (pp. 19–28). New York: Springer. https://doi.org/10.1007/1-4020-0611-X_31.

Saleem, Y., Crespi, N., Rehmani, M. H., & Copeland, R. (2019). Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions. *IEEE Access, 7*, 62962–63003. https://doi.org/10.1109/ACCESS.2019.2913984.

Samper, M. E., Eldali, F. A., & Suryanarayanan, S. (2019). Risk assessment in planning high penetrations of solar photovoltaic installations in distribution systems. *Int. J. Electr. Power Energy Syst. 104*, 724–733. https://doi.org/10.1016/j.ijepes.2018.07.052.

Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems, 93*, 849–859.

Shakerighadi, B., Anvari-Moghaddam, A., Vasquez, J. C., & Guerrero, J. M. (2018). Internet of Things for Modern Energy Systems: State-of-the-Art, Challenges, and Open Issues. *Energies, 11*, 1252. https://doi.org/10.3390/en11051252.

Skvortsova, I., Latyshev, R., & Truntsevsky, Y. (2019). Innovation through improvement in the energy efficiency of business processes. *E3S Web of Conferences*.

Sovacool, B. K., Kivimaa, P., Hielscher, S., & Jenkins, K. (2019). Further reflections on vulnerability and resistance in the United Kingdom's smart meter transition. *Energy Policy, 124*, 411–417. https://doi.org/10.1016/j.enpol.2018.08.038.

Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy efficiency of sustainable Cloud Computing for Big Data IoT. *Sustain. Comput. Inform. Syst. (Netherlands), 19*, 174–184.

Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M., et al. (2019). The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. *Sensors, 19*, 1788. https://doi.org/10.3390/s19081788.

Ting, Y., Feng, D., Yingjie, Z., & Haibo, P. (2019). Explanation and Prospect of Ubiquitous

Electric Power Internet of Things. *AEPS, 43*, 9–20. https://doi.org/10.7500/AEPS20190418015.

Wang, P., Chen, Y., Cai, Z., & Zhang, Y. (2019). Method for Group Decision-making Based on Intuitionistic Judgment Matrix and Evidence Theory. *Fire Control & Command Control, 44*, 60–66. https://doi.org/10.3969/j.issn.1002-0640.2019.03.011.

Wilcox, T., Jin, N., Flach, P., & Thumim, J. (2019). A Big Data platform for smart meter data analytics. *Computers in Industry, 105*, 250–259. https://doi.org/10.1016/j.compind.2018.12.010.

Wu, J., Ota, K., Dong, M., Li, J., & Wang, H. (2018). Big Data Analysis-Based Security Situational Awareness for Smart Grid. *IEEE Trans. Big Data (USA), 4*, 408–417.

Wu, Y., & Zhou, J. (2019). Risk assessment of urban rooftop distributed PV in energy performance contracting (EPC) projects: An extended HFLTS-DEMATEL fuzzy synthetic evaluation analysis. *Sust. Cities Soc. 47*, 101524. https://doi.org/10.1016/j.scs.2019.101524.

Xie, H., Duan, W., & Sun, Y. (2014). Group DEMATEL decision approach based on intuitionistic fuzzy preference. *Computer Engineering and Applications, 50*, 33–38.

Xu, Z. (2007). Intuitionistic preference relations and their application in group decision making. *Inf. Sci. 177*, 2363–2379. https://doi.org/10.1016/j.ins.2006.12.019.

Xu, Z. (2006). Induced uncertain linguistic OWA operators applied to group decision making. *Information Fusion, 7*, 231–238. https://doi.org/10.1016/j.inffus.2004.06.005.

Xu, Z., & Liao, H. (2014). Intuitionistic Fuzzy Analytic Hierarchy Process. *IEEE Transactions on Fuzzy Systems, 22*, 749–761. https://doi.org/10.1109/TFUZZ.2013.2272585.

Yuan, J., & Luo, X. (2019). Regional energy security performance evaluation in China using MTGS and SPA-TOPSIS. *Sci. Total Environ. 696*. https://doi.org/10.1016/j.scitotenv.2019.133817 UNSP 133817.