Evidential Software Risk Assessment Model on Ordered Frame of Discernment

Xingyuan Chen\textsuperscript{a,b}, Yong Deng\textsuperscript{a,∗∗}

\textsuperscript{a}Institute of Fundamental and Frontier Sciences, University of Electronic Science and Technology of China, Chengdu, China.
\textsuperscript{b}School of Information Engineer, Kunming University, Kunming, China.

Abstract

With the rapid advancement of information technology, software risk assessment plays an increasingly important role in ensuring the stability and security of information systems. The aim of this study is to develop an evidential software risk assessment model using an ordered frame of discernment. A risk criteria assessment was constructed to provide an ordered assessment framework for risk assessment. In the assessment process, a fusion method of expert reliability and expert linguistic information is used to improve the accuracy and reliability of the assessment. In addition, the belief entropy based on ordered set is introduced to calculate the weights of the attributes so as to reflect the degree of contribution of each attribute to the risk accurately. Finally, an software risk assessment model is proposed, which can accurately assess software risk and provide strong support for risk management. The application proves that the use of an ordered framework brings representations closer to the real world. A simple evidence-based structure can reduce the need for parameters. Using belief entropy can effectively measure the uncertainty of risks in an ordered framework.

Keywords: Software Risk, Dempster-Shafer Theory, Ordered Frame of Discernment, Expert Reliability, Belief Entropy

∗Corresponding author: Xingyuan Chen, School of Information Engineer, Kunming University, Kunming, 650214, China. Email address: stargarden.chen@hotmail.com; chenxingyuan@kmu.edu.cn

**Corresponding author: Yong Deng, Institute of Fundamental and Frontier Science, University of Electronic Science and Technology of China, Chengdu, 610054, China. Email address: dengentropy@uestc.edu.cn; prof.deng@hotmail.com
1. Introduction

With the development of artificial intelligence algorithms [1, 2] and big data technology [3], software has been widely used in daily life, business and scientific research. The requirement for improving software stability and reliability becomes increasingly urgent. There are a lot of studies on stability and reliability [4, 5, 6]. In fact, software risk management is an effective way to improve reliability which causes extensive research.

In recent years, new methods and theories are increasingly being applied to risk management. Bayesian Belief Network (BBN) is employed to predict potential risks and identify sources. A method was proposed for applying Bayesian Belief Network (BBN) in software project risk management, using the BBN feedback loop to predict potential risks, identify risk sources, and recommend dynamic resource adjustments [7]. A causal relationship analysis framework based on BBN was proposed [8]. Historical data were used to identify causal relationships between risk factors and project outcomes. A BPMN model for software project risk management was constructed, with a focus on technical risk [9]. BBN effectively handles uncertainty by using probabilities. It can effectively help to analyse and predict risk. However, BBN often relies on historical data. It is challenging when assessing risks that have not occurred before or are not supported by sufficient data. Fuzzy set theory is another effective approach for addressing the uncertainty of risks. A simple and fast applied fuzzy set theory algorithm for calculating aggregation risk in software development was proposed [10]. A hybrid fuzzy machine learning mechanism, combining fuzzy DEMATEL, adaptive neuro-fuzzy inference system, and intuitionistic fuzzy-based TODIM, was proposed for software project risk assessment [11]. All of the above methods are based on fuzzy set theory. Fuzzy set theory use the membership degrees to express the ambiguity and uncertainty of risk information. The membership function usually requires some a priori information or expert judgement. Different experts may have different views, which may lead to some inconsistency in the membership functions used. Besides, in some cases fuzzy set theory may face challenges in dealing with the case of subsets with multiple elements. Entropy is also a useful method for handling unknown risks. It is widely used in many fields, such as politics, economics, sociology, informatics [12, 13]. There are many studies on entropy [14, 15]. Therefore, in risk analysis, entropy weighting method,
as a comprehensive evaluation method, is widely used in various risk assessment and decision making processes [16].

Dempster-Shafer Theory (DST) [17, 18] is considered an effective tool for handling risk information, reasoning and decision-making [19]. It includes the frame of discernment (FoD), basic belief assignment (BBA), and Dempster rule of combination (DRC) for data fusion. There are many studies about BBA [20], which has been used in many fields [21, 22]. Compared to probability theory, DST can update information without prior knowledge. This makes it effective in dealing with risks, including unknown or not supported by enough data [23]. Meanwhile, risk data often involves multiple sources, such as empirical data, expert opinions, market research and data analyses, among others. Multi-source information fusion is a widely researched problem [24, 25]. D numbers [26] and quantum mothed [27, 28] are both utilized for information fusion. DST can integrate evidence from different sources to improve the accuracy and reliability of assessment results. Furthermore, when there is a conflict between different sources, the DST provides fusion rules for dealing with conflicting evidence [29]. In addition, experts are frequently invited to assess risk. A expert may provide a very certain assessment such as \{Low\} or \{High\}. However, multiple values may also be given, such as \{High, Very high\}. This may be due to objective constraints and lack of expert knowledge. DST has an advantage in handling multiple values. An information system security risk assessment method based on the evidence theory confidence function model was proposed, which is able to better handle uncertainty and promote effective risk management through cost-benefit analysis [30]. A DEMATEL method based on multi-expert probabilistic approach using Fuzzy Cognitive Map and evidence theory for integrated risk assessment was proposed in [31]. A hybrid AHP and Dempster-Shafer Theory model for project risk assessment proposed in [32]. An information system security risk assessment method based on the belief function model is able to better handle uncertainty and facilitate effective risk management through cost-benefit analysis [33].

As mentioned above, DST has some special advantages in the risk management process. Nevertheless, DST also has some limitations on risk management. Although DST can better combined the state of the evaluation using the multi-element subset, it lacks the ability to reflect the order of the expert’s semantic information. For example, the assessment of risk is
unlikely to be \{Very low, High, Very high\}. It is counter-intuitive that Very low and Very high occur at the same time. Therefore, more rational evaluation criteria can be expressed as ordered rather than disorganised. It is difficult for traditional methods to deal with this relationship between elements in this case. Additionally, different experts have their own areas of expertise. For example, if Expert A is more specialized in business compared to Expert B, then Expert A should be more reliable than that of Expert B in business risk assessment. Therefore, it is reasonable to consider the reliability of experts in risk assessments. In addition, assessment may be influenced by expert experience and bias, which leads to inaccuracy. At present, the common method is to set subjective weight and objective weight. Some weight methods may involve complex calculation processes, which can increase the cost and difficulty of calculation, especially in the case of large-scale data sets or real-time applications.

To solve the mentioned problem, a risk assessment model based on ordered frameworks is proposed. An ordered framework for risk assessment criteria is established. Expert reliability and linguistic information are fused. Calculate attribute weights using belief entropy based on ordered sets. The main contributions of this paper are as follows: In terms of expressing risk, we use an ordered framework that makes the expression closer to the real world. In terms of the risk analysis, we use a simple evidence-based structure that reduces the need for parameters. Meanwhile, we used the belief entropy can effectively measure the uncertainty of risk in the ordered framework.

This paper is structured as follows. In Section 2, review basic definitions and operations. In Section 3, a software risk assessment model based on ordered frames of discernment is introduced. In Section 4, DST was employed for both the reliability of experts and the linguistic information from expert risk assessments. And the proposed belief entropy based on ordered sets was used to calculate the weights of the attributes. A software risk assessment model was presented in 5. Concluded in Section 6.

2. Preliminaries

Some of the basic concepts and operations of DST, Deng entropy and belief functions on ordered discriminant frameworks are introduced in this section.
2.1. Dempster-Shafer theory

Dempster-Shafer theory (DST), also called the D-S evidence theory [17, 18], is an extension of Bayesian theory. Some basic concepts are presented as follows.

Let \( X \) be a set of \( n \) exclusive and exhaustive elements, called the framework of discernment (FOD), defined as follows [18],

\[
X = \{ \theta_1, \theta_2, ..., \theta_n \}
\]

(1)

The power set of \( X \) is denoted as \( 2^X \), defined as follows,

\[
2^X = \{ \emptyset, \{ \theta_1 \}, \{ \theta_2 \}, ..., \{ \theta_n \}, \{ \theta_1, \theta_2 \}, ..., \{ \theta_1, ..., \theta_n \} \}
\]

(2)

where \( \emptyset \) is an empty set.

For FOD \( X \), a mass function \( m \) is a mapping from \( 2^X \) to \([0, 1]\), defined by,

\[
m : 2^X \rightarrow [0, 1]
\]

(3)

constrained conditions as follows,

\[
\begin{align*}
\sum_{A \in 2^X} m(A) &= 1 \\
m(\emptyset) &= 0
\end{align*}
\]

(4)

A mass function can be also called as a basic probability assignment (BPA) or basic belief assignment (BBA). If \( m(A) > 0 \), \( A \) is called focal element. \( m(A) \) represents the belief value of supporting proposition \( A \).

For a proposition \( A \subseteq X \), the belief function \( Bel : 2^X \rightarrow [0, 1] \) is defined as,

\[
Bel(A) = \sum_{B \subseteq A} m(B)
\]

(5)

The plausibility function \( Pl : 2^X \rightarrow [0, 1] \) is defined as,

\[
Pl(A) = 1 - Bel(\bar{A}) = \sum_{B \cap A \neq \emptyset} m(B)
\]

(6)

Apparently, \( \forall A \subseteq X, Bel(A) \leq m(A) \leq Pl(A) \), where \( Bel(A) \) is the lower limit and \( Pl(A) \) is the upper limit of proposition \( A \). \([Bel(A), Pl(A)]\) represents the belief interval of \( A \).
Given two BBAs indicated by $m_1$ and $m_2$, Dempster’s rule of combination, denote by $m_1 \oplus m_2$, is mathematically defined as [18],

$$m(A) = \begin{cases} \frac{1}{1-k} \sum_{B \cap C = A} m_1(B)m_2(C), & A \neq \emptyset \\ 0, & A = \emptyset \end{cases}$$  \hspace{1cm} (7)$$

where $A, B, C \in 2^X$, $k$ is a normalization factor,

$$k = \sum_{B \cap C = \emptyset} m_1(B)m_2(C)$$ \hspace{1cm} (8)$$

Conflict coefficient is $k$, which indicates the conflict degree between two BBAs. When $k = 0$ means $m_1$ is consistent with $m_2$, and when $k = 1$ means $m_1$ totally contradicts $m_2$, that is the two evidences strongly support different hypotheses, and these hypotheses are incompatible.

2.2. Deng entropy

Deng entropy [34], is a measure of uncertainty that has found use in various areas [35, 36]. It has been further developed to handle information volume. The formula for Deng entropy can be expressed as:

$$E_d(m) = - \sum_{A \subseteq X} m(A) \log \frac{m(A)}{2^{|A|} - 1}$$ \hspace{1cm} (9)$$

where $m$ is a BPA defined on the FOD, and $A$ is a focal element of $m$, $|A|$ is the cardinality of $A$. Eq.(9) can be rewritten as follows:

$$E_d(m) = - \sum_{A \subseteq X} \log (2^{|A|} - 1) - \sum_{A \subseteq X} m(A) \log m(A)$$ \hspace{1cm} (10)$$

where $\sum_{A \subseteq X} \log (2^{|A|} - 1)$ and $- \sum_{A \subseteq X} m(A) \log m(A)$ are measurements of nonspecificity and discord, respectively. As a result, Deng entropy is a composite measurement of nonspecificity and discord, which means that it is a tool for measuring total uncertainty.

if and only if $m(A) = \frac{2^{|A|} - 1}{\sum_{A \subseteq X} (2^{|A|} - 1)}$, Deng entropy reaches its maximum value. The maximum Deng entropy is as follows:

$$E_d(m) = \log \sum_{A \subseteq X} (2^{|A|} - 1)$$ \hspace{1cm} (11)$$
2.3. Belief functions on ordered frames of discernment

The ordered power set, denoted as $oPS^X$, is a subset of the power set that consists of the empty set and all the disjunctions of consecutive elements of $X$.

A disjunction of consecutive elements from endpoint elements is denoted by:

$$\{\omega_i, \omega_j\}_o = \{\omega_i, \omega_{i+1}, ..., \omega_{j-1}, \omega_j\}, \text{ with } 1 \leq i \leq j \leq n$$  \hspace{1cm} (12)

The ordered power set can be defined as:

$$oPS^X = \{\emptyset, \{\omega_i, \omega_j\}_o \}_{i,j=1,\ldots,n}$$  \hspace{1cm} (13)

The number of elements of $2^X$ is $2^n$, but it is smaller for $oPS^X$. The number of elements of $oPS^X$, with: $X = \{\omega_1, \ldots, \omega_n\}$ is:

$$1 + \frac{n(n+1)}{2}$$  \hspace{1cm} (14)

For all $A \in oPS^X$, the belief function is given by:

$$Bel(A) = \sum_{B \subseteq A, B \neq \emptyset} m(B)$$  \hspace{1cm} (15)

The plausibility function is defined for all $A \in oPS^X$ as follows:

$$Pl(A) = \sum_{B \in oPS^X, B \cap A \neq \emptyset} m(B)$$  \hspace{1cm} (16)

Let two elements $Y_i$ and $Y_j \in oPS^X$, $Y_i = \{\omega_{i_1}, \omega_{i_n}\}_o$ and $Y_j = \{\omega_{j_1}, \omega_{j_n}\}_o$, the union of these two ordered element defined as follows,

$$Y_i \bigcup_o Y_j = \{\min(\omega_{i_1}, \omega_{j_1}), \max(\omega_{i_n}, \omega_{j_n})\}$$  \hspace{1cm} (17)

Let two mass function defined on the ordered power set $oPS^X$, for all $A \in oPS^X$ the disjunctive combination is given by:

$$m_oDis(A) = \sum_{Y_i \cup Y_j = A} m_i(Y_i)m_j(Y_j)$$  \hspace{1cm} (18)

The disjunction combination of $s$ mass functions on the ordered power set $oPS^X$, is given for all $A \in oPS^X$ by

$$m_oDis(A) = \sum_{Y_1 \cup \ldots \cup Y_s = A} \prod_{j=1}^{s} m_j(Y_i)$$  \hspace{1cm} (19)
**Example 1** Suppose $\Theta = \{-2, -1, 0, 1, 2\}$, two BPAs as follows,

\[ m_1 : m_1(\{-1, 0\}) = 0.6, m_1(\{0, 1\}) = 0.4 \]

\[ m_2 : m_2(\{-1\}) = 0.4, m_2(\{0, 1\}) = 0.25, m_2(\theta) = 0.35 \]

According to the Eq. (17) and Eq. (18),

\[ m(\{-1, 0\}) = m_1(\{-1, 0\}) * m_2(\{-1\}) = 0.6 * 0.4 = 0.24 \]

\[ m(\{0, 1\}) = m_1(\{0, 1\}) * m_2(\{0, 1\}) = 0.4 * 0.25 = 0.1 \]

\[ m(\{-1, 0, 1\}) = m_1(\{-1, 0\}) * m_2(\{0, 1\}) + m_1(\{0, 1\}) * m_2(\{-1\}) = 0.6 * 0.25 + 0.4 * 0.4 = 0.31 \]

\[ m(\theta) = m_2(\theta) * m_1(\{-1, 0\}) + m_2(\theta) * m_1(\{0, 1\}) = 0.35 * 0.6 + 0.35 * 0.4 = 0.35 \]

**Example 2** Suppose $\Theta = \{-2, -1, 0, 1, 2\}$, two BPAs as follows,

\[ m_1 : m_1(\{-1\}) = 0.7, m_1(\theta) = 0.3 \]

\[ m_2 : m_2(\{0\}) = 0.65, m_2(\{-2, -1, 0\}) = 0.35 \]

According to the Eq. (17) and Eq. (18),

\[ m(\{-2, -1, 0\}) = m_1(\{-1\}) * m_2(\{-2, -1, 0\}) = 0.7 * 0.35 = 0.245 \]

\[ m(\theta) = m_1(\theta) * m_2(\{0\}) + m_1(\theta) * m_2(\{-2, -1, 0\}) = 0.3 * 0.65 + 0.3 * 0.35 = 0.3 \]

2.4. Pignistic Probability Transform (PPT)

Pignistic probability transform can evenly assign belief of multi-element sets to singletons, thereby converting evidence into a probability distribution [38].

Consider $m$ as a basic probability assignment on a frame of discernment $\Theta$. The pignistic transformation function, denoted as $\Theta \rightarrow [0, 1]$, is established as follows:

\[
\text{BetP}_m(\theta_i) = \sum_{A \subseteq \Theta, \theta_i \in A} \frac{m(A)}{|A|}.
\]

(20)
2.5. Discounting Coefficient

Discounting coefficient can be interpreted as reliability coefficients (\(a\)) that can incorporate the reliability of the information source in data fusion \([18]\). To handle conflict between information sources, a discounting rule has been introduced in the DST given as follows:

\[
m(\theta) = \alpha \times m(\theta) + (1 - \alpha),
\]

\[
m(A) = \alpha \times m(A), \forall A \subset \theta \text{and} A \neq \emptyset.
\]

2.6. Ordered Weighted Averaging

Ordered Weighted Averaging (OWA), proposed by Yager \([39]\), is a method of aggregating multiple criteria or attributes into a single score or ranking. The OWA operator is a mapping \(f : \mathbb{R}^n \to \mathbb{R}\) that has an associated \(n\)-dimensional weight vector \(w = (w_1, ..., w_n)^T\), which satisfies \(\sum_{i=1}^{n} w_i = 1\) and \(w_i \geq 0\). For an \(n\)-dimensional vector \(a\) OWA operator is:

\[
OWA(x_1, x_2, ..., x_n) = \sum_{i=1}^{n} w_i x_i.
\]

where \(x_i\) is the \(i\)th largest element in \(a\).

The property of the OWA operators are as follow:

1. When \(w = (1, 0, ..., 0)^T\), \(f(a_1, ..., a_n) = Max[a_i]\), which is the most optimistic case in decision making.

2. When \(w = (1/n, 1/n, ..., 1/n)^T\), \(f(a_1, ..., a_n) = \frac{1}{n} \sum a_i\), which dose not consider the information of elements order.

3. When \(w = (0, 0, ..., 1)^T\), \(f(a_1, ..., a_n) = Min[a_i]\), which is the most cautious case in decision making.

\[
\sum_{i=1}^{n} \left( \frac{n - i}{n - 1} - \frac{1}{n} h^{n-i} \right) = 0.
\]

Calculate the weights vector \(t\) based on the h

\[
t_i = \frac{h^{n-i}}{\sum_{j=1}^{n} h^{n-j}}.
\]
3. Software Risk Assessment Model Based On Ordered Frames of Discernment

3.1. Motivation

Risk analysis usually involves assessing the likelihood of a risk event occurring and its loss if it does occur. This is a fundamental component of risk management, commonly known as Probability and Impact Analysis (PIA). In reference [40], the software risk can be defined in this context as follows:

\[
Risk = \text{Prob}(P) \times \text{Loss}(L).
\] (25)

Assuming a risk assessment for a software development project, let’s consider a specific risk. If we use probability analysis with \( P(\{\text{High}\}) = 0.7 \) and \( L(\{\text{Medium}\}) = 0.4 \), for this risk, the risk value from PIA is 0.28. And if we use DST, \( P(\{\text{High}\}) \) and \( L(\{\text{Medium}\}) \) such evaluations are allowed. Furthermore, \( P(\{\text{Medium, High}\}) = 0.7 \) and \( L(\{\text{High, Very High}\}) = 0.4 \) are still allowed. The DST is able to express more information of the likelihood and level of loss. Meanwhile, when there are more than one expert performing the assessment, the information can be well fused without loss by using DRC. Furthermore, DST can provide a unified framework for integrating risk data from multiple sources, such as empirical data, expert opinion, market research and data analytic. That is why we use DST to handle risk.

However, these are some problem in DST. In previous method [41], experts can use a single assessment criterion, such as medium, high. Alternatively, experts might use an ambiguity assessment criterion, such as between medium and high when the situation is uncertain. Furthermore, when faced with more uncertainty, they could use between medium and very high. However, in any case, it would be illogical and contradictory to assess low and very high at the same time. But low and very high at the same time are allowed in the unordered frame. Therefore, the ordered assessment framework is more appropriate to the realities of the situation. Therefore, in order to make a more rational risk assessment, we propose a software risk assessment model based on ordered frames of discernment.

3.2. Software Risk Assessment Framework

This paper presents a software risk assessment model based on ordered frames of discernment. The model includes the following steps, as illustrated in Fig. 1:
Figure 1: Evidential Software Risk Assessment Model

**Step 1.** Risk factor identification.

Identifying potential project-related risks is crucial during the initial stage of risk assessment, as it forms the foundation for subsequent work. This crucial task can be accomplished through various methods, such as brainstorming, risk registers, reviewing historical data from similar projects, and expert assessments etc. Since risk factors change with the environment and different software projects may have unique risk. Therefore, the selection of risk identification methodologies should be adjusted according to the specific situation.

**Step 2.** Risk factor representation.

**Step 2.1.** Establishing assessment criteria.

The establish evaluation criteria as illustrated in Table 1. The criteria are not fixed, and can be adjusted according to the actual situation.

It is worth noting that this assessment criteria represents an ordered framework. That means the assignment such as “Low”, “Low-Medium” or “Low-Medium-High” are reasonable, while “Low-High” or “Low-Medium- Very high” that do not follow a sequence do not make sense.
Table 1: Evaluation Linguistic Set

<table>
<thead>
<tr>
<th>Level</th>
<th>Linguistic</th>
<th>Integral</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_{-2}</td>
<td>Very low</td>
<td>1</td>
</tr>
<tr>
<td>S_{-1}</td>
<td>Low</td>
<td>2</td>
</tr>
<tr>
<td>S_0</td>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>S_1</td>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>S_2</td>
<td>Very high</td>
<td>5</td>
</tr>
</tbody>
</table>

within the ordered framework of assessment criteria.

**Step 2.2.** Translate the assessment of the experts into BPA.

To assess the probability and severity of risks using the evaluation criteria in Table 1, N experts are invited. For instance, \{s_{-1}(0.6)\} denotes that the probability of “low” is 60%, while \{s_1, s_2(0.8)\} suggests that there is an 80% likelihood of being indecisive between “high” and “very high”. Then the assessment results must then be translated into BPAs. \{s_{-1}(0.6)\} can be represented as \(m(\{s_{-1}\}) = 0.6\), and \{s_1, s_2(0.8)\} can be represented as \(m(\{s_1, s_2\}) = 0.8\).

**Step 3.** Integration experts evaluation.

For each risk, the assessment values given by all experts are fused using the DRC. For example, three experts assessed the probability and severity of project management \(PM\) risks and then converted them to \(bpm\) with the following values.

The possibility of \(PM\):

\[
m_1 : m_1(\{s_1\}) = 0.78, \quad m_2 : m_2(\{s_1, s_2\}) = 0.88, \quad m_3 : m_3(\{s_0, s_1\}) = 0.6918.
\]

According to Eq. (7), we obtain the possibility of \(PM\):

\[
m(\{s_1\}) = 0.9136, m(\{s_0, s_1\}) = 0.0182, m(\{s_1, s_2\}) = 0.06, m(\{S\}) = 0.0082.
\]
The serious of PM:

\[
m_1 : m_1(\{s_0, s_1\}) = 0.78,
\]
\[
m_2 : m_2(\{s_{-1}, s_0, s_1\}) = 0.88,
\]
\[
m_3 : m_3(\{s_0, s_1\}) = 0.6918.
\]

According to Eq. (7), we obtain the serious of PM:

\[
m(\{s_0, s_1\}) = 0.9318, m(\{s_{-1}, s_0, s_1\}) = 0.06, m(\{S\}) = 0.0082.
\]

**Step 4.** Risk information integration.

For each risk, we use the DRC to combine probability and severity into one using Eq. (7). Then, use the PPT to assign beliefs from the multiple-factor set to individual factors, employing Eq. (20).

**Step 5.** Ranking of risks.

Based on the integral in the last column of Table 1, calculate the value at risk. For example, for PM, the fused value is \(m(s_{-1}) = 0.0002, m(s_0) = 0.0131, m(s_1) = 0.9864, m(s_2) = 0.0003\), then according to the scores, the risk value is \(0.0002 \times 2 + 0.0131 \times 3 + 0.9864 \times 4 + 0.0003 \times 5 = 3.9868\).

Once all the risk values have been calculated, the risks can be ranked.

### 3.3. Application

A software company is working on a large complex project with multiple modules and subsystems. Different development teams develop relevant modules and subsystems. The project relies on a variety of external libraries, services and technologies. At the same time, the project involves a number of stakeholders, each with different needs and expectations. Therefore, the project is facing many challenges, such as technical complexity, changing requirements, teamwork, environmental changes, and so on. Risks have increased due to the complexity and uncertainty of the project. The project invited three experts to do a risk assessment. In this complex software development environment, there are important advantages to using DST. Therefore, our proposed method is used.

**Step 1.** Risk factor identification. Based on the actual situation of the project, in this paper, we focus on five specific categories of risks, which include: Requirement Risk (RE), Project...
Management Risk (PM), Technology Risk (TC), Team & People Risk (TP), and Business Risks (BN). The detailed information of risks is in the Table 2.

Table 2: The areas of risk

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement (RE)</td>
<td>Requirement analysis, requirements definition and re-</td>
</tr>
<tr>
<td></td>
<td>quirement changes</td>
</tr>
<tr>
<td>Project Management (PM)</td>
<td>Risk is unlikely to occur</td>
</tr>
<tr>
<td>Technology (TC)</td>
<td>Risk may or may not occur</td>
</tr>
<tr>
<td>Team &amp; People (TE)</td>
<td>Risk is highly likely to occur</td>
</tr>
<tr>
<td>Business (BN)</td>
<td>Risk is almost inevitable</td>
</tr>
</tbody>
</table>

**Step 2.** Risk factor representation. In this paper, three experts were invited to evaluate both the likelihood and severity of risk using the criteria presented in Table 1. The assessment results are presented in Table 3.

**Step 3 - Step 4.** The calculation results contained in each step are presented in the Table 4, Table 5 and Table 6.

**Step 5.** Ranking of risks. According to integral calculate the value of the risk. $RE = 4.4989, PM = 3.9868, TC = 2.9540, TP = 2.3881, BN = 3.3478$. The risk factors can be sorted. $RE > PM > BN > TC > TP$.

3.4. Discussion

It can be seen that, on the one hand, the proposed model is practical. Ordered frames of discernment is realistic in assessing risk. It is more accurate to represent the state of uncertainty and ambiguity in the assessment. On the other hand, the model is flexible. It can deal with more complex problems and more complex indicators. Firstly, the evaluation scale can be flexibly adjusted by modifying the evaluation linguistic set. Secondly, no matter how many experts there are, the expert evaluation can be fused by using DRC. So, it is a general model that can solve universal risk analysis.
**Table 3: Experts assignment**

<table>
<thead>
<tr>
<th>Risks</th>
<th>Experts</th>
<th>P</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE</td>
<td>(m_1(.))</td>
<td>({s_1, s_2(0.8)})</td>
<td>({s_1, s_2(0.8)})</td>
</tr>
<tr>
<td></td>
<td>(m_2(.))</td>
<td>({s_1(0.8)})</td>
<td>({s_1, s_2(0.8)})</td>
</tr>
<tr>
<td></td>
<td>(m_3(.))</td>
<td>({s_0, s_1, s_2(0.8)})</td>
<td>({s_2(0.8)})</td>
</tr>
<tr>
<td>PM</td>
<td>(m_1(.))</td>
<td>({s_1(0.78)})</td>
<td>({s_0, s_1(0.78)})</td>
</tr>
<tr>
<td></td>
<td>(m_2(.))</td>
<td>({s_1, s_2(0.88)})</td>
<td>({s_1, s_0, s_1(0.88)})</td>
</tr>
<tr>
<td></td>
<td>(m_3(.))</td>
<td>({s_0, s_1(0.6918)})</td>
<td>({s_0, s_1(0.6918)})</td>
</tr>
<tr>
<td>TC</td>
<td>(m_1(.))</td>
<td>({s_1(0.1414)})</td>
<td>({s_1, s_0, s_1(0.1414)})</td>
</tr>
<tr>
<td></td>
<td>(m_2(.))</td>
<td>({s_0(0.3257)})</td>
<td>({s_0, s_1, s_2(0.3257)})</td>
</tr>
<tr>
<td></td>
<td>(m_3(.))</td>
<td>({s_0(0.75)})</td>
<td>({s_1, s_0(0.75)})</td>
</tr>
<tr>
<td>TP</td>
<td>(m_1(.))</td>
<td>({s_1(0.7)})</td>
<td>({s_0(0.7)})</td>
</tr>
<tr>
<td></td>
<td>(m_2(.))</td>
<td>({s_2s_1(0.4247)})</td>
<td>({s_0s_1(0.4247)})</td>
</tr>
<tr>
<td></td>
<td>(m_3(.))</td>
<td>({s_1s_0(0.2577)})</td>
<td>({s_1(0.2577)})</td>
</tr>
<tr>
<td>BN</td>
<td>(m_1(.))</td>
<td>({s_0, s_1(0.187)})</td>
<td>({s_1, s_2(0.187)})</td>
</tr>
<tr>
<td></td>
<td>(m_2(.))</td>
<td>({s_0(0.6)})</td>
<td>({s_0, s_1, s_2(0.6)})</td>
</tr>
<tr>
<td></td>
<td>(m_3(.))</td>
<td>({s_1s_0(0.0584)})</td>
<td>({s_2(0.0584)})</td>
</tr>
</tbody>
</table>

**Table 4: Integration expert evaluation (Probability)**

<table>
<thead>
<tr>
<th>Risks</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE</td>
<td>(m(.))</td>
</tr>
<tr>
<td>PM</td>
<td>(m(.))</td>
</tr>
<tr>
<td>TC</td>
<td>(m(.))</td>
</tr>
<tr>
<td>TP</td>
<td>(m(.))</td>
</tr>
<tr>
<td>BN</td>
<td>(m(.))</td>
</tr>
</tbody>
</table>

**Table 5: Integration expert evaluation (Severity)**

<table>
<thead>
<tr>
<th>Risks</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE</td>
<td>(m(.))</td>
</tr>
<tr>
<td>PM</td>
<td>(m(.))</td>
</tr>
<tr>
<td>TC</td>
<td>(m(.))</td>
</tr>
<tr>
<td>TP</td>
<td>(m(.))</td>
</tr>
<tr>
<td>BN</td>
<td>(m(.))</td>
</tr>
</tbody>
</table>
Table 6: Risk information integration

<table>
<thead>
<tr>
<th>Risks</th>
<th>$S_{-2}$</th>
<th>$S_{-1}$</th>
<th>$S_0$</th>
<th>$S_1$</th>
<th>$S_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE</td>
<td>0</td>
<td>0</td>
<td>0.0003</td>
<td>0.4998</td>
<td>0.4998</td>
</tr>
<tr>
<td>PM</td>
<td>0</td>
<td>0.0002</td>
<td>0.0131</td>
<td>0.9864</td>
<td>0.0003</td>
</tr>
<tr>
<td>TC</td>
<td>0.0047</td>
<td>0.0653</td>
<td>0.9106</td>
<td>0.0109</td>
<td>0.0086</td>
</tr>
<tr>
<td>TP</td>
<td>0.0293</td>
<td>0.6029</td>
<td>0.3286</td>
<td>0.0287</td>
<td>0.0104</td>
</tr>
<tr>
<td>BN</td>
<td>0.0219</td>
<td>0.0254</td>
<td>0.6664</td>
<td>0.1560</td>
<td>0.1304</td>
</tr>
</tbody>
</table>

4. Belief Information Measure based Software Risk Assessment model

4.1. Motivation

In practical applications, there are many uncertainty-oriented reliability studies [42]. This paper focuses on the reliability of expert. The reliability of experts is not static but varies depending on the field. For example, if Expert 1 is more specialised in business than Expert 2, then Expert 1 should be more reliable than Expert 2. Therefore, it is more reasonable that the reliability of the experts should be taken into account in the assessment. However, if there are three experts, you need to give three reliability. And if there are ten, give ten reliability. This method is rather complexity. Besides, in [41], the semantic information of the evaluation is given, and also values like 80% are given by the experts. In reality, experts are more likely to give the semantic information. Therefore, a novel approach is proposed which requires few parameters and incorporates semantic information for risk assessment and expert reliability information.

4.2. BPA Based on Expert Reliability

The model includes the following steps, as illustrated in Fig. 2:

**Step 1.** Ranking of experts in different fields.

Due to the varying expertise and experiences of the experts in different professional fields, rankings can be provided for experts in different fields.

**Step 2.** Give Orness measure, either in ascending or descending order, but choose only one.

**Step 3.** Calculating the reliability of experts.

The reliability of experts can be calculated through the sorting of expert domains and the Orness measure. For example, if experts are ranked as Expert 1 < Expert 2 < Expert 3 and
Orness measure is 0.54. Then, according to Eq.(24), we can get $w_1 = 0.6162$, $w_2 = 0.2676$, $w_3 = 0.1162$. So $Expert_1w = 0.1162$, $Expert_2w = 0.2676$, $Expert_3w = 0.6162$.

Subsequently, utilize Eq. (26) to determine the reliability values of the experts.

$$W(i)_{re} = \frac{Expert(i)w}{Expert_{max}}$$ (26)

**Step 4.** Give the value of the expert’s combined assessment and convert it to bpa.

$$bpa = w \ast W_{re}$$ (27)

4.2.1. Application

In this paper, we give a ranking of experts in five areas. In RE, Expert 1 = Expert 2 = Expert 3. In PM, Expert 3 < Expert 1 < Expert 2. Other parts can be seen in Table 7. At the same time, we use the Orness measure in descending order. In RE, the Orness value is 0.5, which means that the expert level is close. The Orness value of 0.75 in TC and 0.82 in BN means that the level of difference between experts is greater in BN than in TC. By use Eq.(23) and Eq.(24), we can get the values of columns 2-4, $w_1$, $w_2$ and $w_3$ in Table 8. Subsequently, following Step 3, obtain
Expert Reliability, and based on the provided combined assessments, utilize Step 4 to derive BPA.

Table 7: Expert sorting and Orness

<table>
<thead>
<tr>
<th>Risks</th>
<th>Expert sorting</th>
<th>Orness</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE</td>
<td>Expert 1 = Expert 2 = Expert 3</td>
<td>0.5</td>
</tr>
<tr>
<td>PM</td>
<td>Expert 3 &lt; Expert 1 &lt; Expert 2</td>
<td>0.54</td>
</tr>
<tr>
<td>TC</td>
<td>Expert 1 &lt; Expert 2 &lt; Expert 3</td>
<td>0.75</td>
</tr>
<tr>
<td>TP</td>
<td>Expert 3 &lt; Expert 2 &lt; Expert 1</td>
<td>0.66</td>
</tr>
<tr>
<td>BN</td>
<td>Expert 3 &lt; Expert 1 &lt; Expert 2</td>
<td>0.82</td>
</tr>
</tbody>
</table>

Table 8: OWA Weights, Orness, Expert Reliability and BPA

<table>
<thead>
<tr>
<th>Risks</th>
<th>OWA Weights</th>
<th>Expert Reliability</th>
<th>combined assessment</th>
<th>BPA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$w_1$</td>
<td>$w_2$</td>
<td>$w_3$</td>
<td>$E_1$</td>
</tr>
<tr>
<td>RE</td>
<td>0.3300</td>
<td>0.3300</td>
<td>0.3300</td>
<td>1</td>
</tr>
<tr>
<td>PM</td>
<td>0.3741</td>
<td>0.3317</td>
<td>0.2941</td>
<td>0.8867</td>
</tr>
<tr>
<td>TC</td>
<td>0.6162</td>
<td>0.2676</td>
<td>0.1162</td>
<td>0.1886</td>
</tr>
<tr>
<td>TP</td>
<td>0.5063</td>
<td>0.3072</td>
<td>0.1864</td>
<td>1</td>
</tr>
<tr>
<td>BN</td>
<td>0.7092</td>
<td>0.2216</td>
<td>0.0690</td>
<td>0.3125</td>
</tr>
</tbody>
</table>

4.3. Risk Information Fusion Based on Belief Entropy

Shannon entropy plays an important role in information theory and it is an important tool for measuring information uncertainty. However, Shannon entropy has limitations in the framework of DST, so entropy in the framework of DST is an open issue. Deng entropy presents a good solution idea for uncertainty measurement in the framework of DST. However, uncertainty measurement in the framework of ordered identification is still a problem worth studying. Therefore, an entropy of the ordered frame of discernment is proposed in this paper.

In DST framework, the entropy of the ordered frame of discernment $E_{od}$ is proposed as
follows,

\[
E_{od}(m) = - \sum_{A \subseteq oPS^X} m(A) \log_2 \frac{m(A)}{n(n+1)}
\]

\[= - \sum_{A \subseteq oPS^X} m(A) \log_2 \frac{2m(A)}{n(n+1)}.
\]

Where \(oPS^X\) is the order power set, \(m\) is a BPA defined on \(oPS^X\), \(A\) is a focal element of \(m\), and \(\frac{n(n+1)}{2}\) is the number of elements in \(oPS^X\) excluding the empty set.

With a transformation, we can obtain:

\[
E_{od}(m) = - \sum_{A \subseteq oPS^X} m(A) \log_2 \frac{m(A)}{n(n+1)}
\]

\[= - \sum_{A \subseteq oPS^X} m(A) \left( \log_2 m(A) - \log_2 \frac{n(n+1)}{2} \right)
\]

\[= - \sum_{A \subseteq oPS^X} m(A) \log_2 m(A) + \sum_{A \subseteq oPS^X} m(A) \log_2 \frac{n(n+1)}{2}.
\]

Similar to the Deng entropy, the proposed entropy can be expressed as two terms. The first term, \(- \sum_{A \subseteq oPS^X} m(A) \log_2 m(A)\), measures discord, while the second term, \(\sum_{A \subseteq oPS^X} m(A) \log_2 \frac{n(n+1)}{2}\), measures non-specificity. In addition, there are some properties of the proposed entropy that need to be discussed.

4.3.1. Performance of Proposed Belief Entropy

1) Probabilistic consistency

When there is only a single element in a BPA or \(n \equiv 1\), the proposed belief entropy is calculated as follows:

\[
E_{od}(m) = - \sum_{A \subseteq oPS^X} m(A) \log_2 \frac{2m(A)}{n(n+1)}
\]

\[= - \sum_{A \subseteq oPS^X} m(A) \log_2 \frac{2m(A)}{1(1+1)}
\]

\[= - \sum_{A \subseteq oPS^X} m(A) \log_2 m(A)
\]

\[E_{od}(m) = E_s(m).
\]

The entropy of the ordered frame of discernment is an extension of Deng entropy and is formally similar to it. However, there is a difference in that the belief of each focal element \(A\) is divided by the number of possible states in \(A\), which is \(n(n+1)\). If BPA degenerates into probability, the belief entropy can degenerate into Shannon entropy.
2) Efficiency of uncertainty measurement in ordered frame of discernment

Since the discernment framework is ordered, the number of beliefs for each focal element is relatively small, which makes the proposed entropy value smaller than the other entropy values. The ordered framework emphasises the relationships and ordering between elements, it is better able to represent the structure and patterns inherent. It therefore provides comprehensive and insightful information in uncertainty measurement.

4.3.2. Application

In order to evaluate the uncertainty of the risk information in the above application, we have performed a calculation with the proposed entropy.

For example, in table 4, the entropy of RE is calculated as:

\[
E_{od}(m) = -0.8 \times \log_2 \frac{0.8}{1} - 0.16 \times \log_2 \frac{0.16}{3} - 0.032 \times \log_2 \frac{0.032}{6} - 0.008 \times \log_2 \frac{0.008}{15} = 1.2628
\]

Since each risk value has two aspects, one is probability and the other is severity, Eq. (28) is used to calculate the assessment values in Table 4 and 5. The results are shown in Table 8, the second column is the probability entropy value and the third column is the severity entropy value. The higher the entropy, the greater the uncertainty. So we need to compare the entropy both of them. Calculated using Eq. (29) and Eq. (30), discounting the one with the higher entropy. Then generate the weights \(W_{en}\).

\[
EW_p(m) = \left| \frac{E_{od}^p(m)}{\max(E_{od}^p(m), E_{od}^s(m))} \right|
\]

\[
EW_s(m) = \left| \frac{E_{od}^s(m)}{\max(E_{od}^p(m), E_{od}^s(m))} \right|
\]

\[
W_{en} = |EW_p(m) - EW_s(m)|
\]

It is worth noting that If \(EW_p > EW_s\), the corresponding weight \(W_{en}\) belongs to P, and the discount applies to P. Conversely, if \(EW_s\) is greater, the weight belongs to S, and the discount applies to s. The last column of Table 9 is the value of risk weight \(W_{en}\). The discounted value is displayed in Table 10 and 11.
Table 9: The Entropy Value of Risk

<table>
<thead>
<tr>
<th>Risks</th>
<th>$E^P_{od} m(.)$</th>
<th>$E^S_{od} m(.)$</th>
<th>$EW_{pm}(.)$</th>
<th>$EW_{sm}(.)$</th>
<th>$W_{en}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE</td>
<td>1.2628</td>
<td>1.1060</td>
<td>1</td>
<td>0.8758</td>
<td>0.1242 (P)</td>
</tr>
<tr>
<td>PM</td>
<td>0.6806</td>
<td>2.0593</td>
<td>0.3305</td>
<td>1</td>
<td>0.6695 (S)</td>
</tr>
<tr>
<td>TC</td>
<td>1.4485</td>
<td>3.4945</td>
<td>0.4145</td>
<td>1</td>
<td>0.5855 (S)</td>
</tr>
<tr>
<td>TP</td>
<td>1.9531</td>
<td>2.2547</td>
<td>0.8662</td>
<td>1</td>
<td>0.1338 (S)</td>
</tr>
<tr>
<td>BN</td>
<td>2.6775</td>
<td>4.3801</td>
<td>0.6113</td>
<td>1</td>
<td>0.3887 (S)</td>
</tr>
</tbody>
</table>

Table 10: Expert evaluation after discount (Probability)

<table>
<thead>
<tr>
<th>Risks</th>
<th>m(.)</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE</td>
<td>$s_1(0.0993), s_1s_2(0.0199), s_0s_1s_2(0.0040), s(0.8768)$</td>
<td></td>
</tr>
<tr>
<td>PM</td>
<td>$s_1(0.9136), s_0s_1(0.0182), s_1s_2(0.06), s(0.0082)$</td>
<td></td>
</tr>
<tr>
<td>TC</td>
<td>$s_{-1}(0.0265), s_0(0.8104), s(0.1631)$</td>
<td></td>
</tr>
<tr>
<td>TP</td>
<td>$s_{-1}(0.7328), s_{-2}s_{-1}(0.0932), s_{-1}s_0(0.0452), s(0.1288)$</td>
<td></td>
</tr>
<tr>
<td>BN</td>
<td>$s_0(0.6046), s_{-1}s_0(0.0194), s_0s_1(0.0714), s(0.3046)$</td>
<td></td>
</tr>
</tbody>
</table>

Table 11: Expert evaluation after discount (Severity)

<table>
<thead>
<tr>
<th>Risks</th>
<th>m(.)</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE</td>
<td>$s_2(0.8), s_1s_2(0.192), s(0.008)$</td>
<td></td>
</tr>
<tr>
<td>PM</td>
<td>$s_0s_1(0.6238), s_{-1}s_0s_1(0.0402), s(0.3360)$</td>
<td></td>
</tr>
<tr>
<td>TC</td>
<td>$s_0(0.1449), s_{-1}s_0(0.2942), s_0s_1(0.0068), s_{-1}s_0s_1(0.0138), s_0s_1s_2(0.0415), s(0.4989)$</td>
<td></td>
</tr>
<tr>
<td>TP</td>
<td>$s_0(0.0882), s_1(0.0077), s_{-1}s_0(0.0159), s(0.8882)$</td>
<td></td>
</tr>
<tr>
<td>BN</td>
<td>$s_2(0.0233), s_1s_2(0.0694), s_0s_1s_2(0.1776), s(0.7297)$</td>
<td></td>
</tr>
</tbody>
</table>
Subsequently, compute the data in Table 10 and 11 using the procedures outlined in steps 4 and 5 of Chapter 3. The results are presented in Table 12.

<table>
<thead>
<tr>
<th>Risks</th>
<th>$S_{-2}$</th>
<th>$S_{-1}$</th>
<th>$S_0$</th>
<th>$S_1$</th>
<th>$S_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE</td>
<td>0.0015</td>
<td>0.0015</td>
<td>0.0015</td>
<td>0.1171</td>
<td>0.8782</td>
</tr>
<tr>
<td>PM</td>
<td>0.0006</td>
<td>0.0007</td>
<td>0.0123</td>
<td>0.9758</td>
<td>0.0107</td>
</tr>
<tr>
<td>TC</td>
<td>0.0164</td>
<td>0.0627</td>
<td>0.8824</td>
<td>0.0199</td>
<td>0.0186</td>
</tr>
<tr>
<td>TP</td>
<td>0.0698</td>
<td>0.8145</td>
<td>0.0649</td>
<td>0.0260</td>
<td>0.0249</td>
</tr>
<tr>
<td>BN</td>
<td>0.0473</td>
<td>0.0548</td>
<td>0.6954</td>
<td>0.1174</td>
<td>0.0852</td>
</tr>
</tbody>
</table>

According to integral calculate the value the of the risk. $RE = 4.8687, PM = 3.9954, TC = 2.9621, TP = 2.1216, BN = 3.1388$. The risk factors can be sorted as $RE > PM > BN > TC > TP$. Upon comparing the data before and after the application of entropy, the risk ranking in this article remains unchanged, but the values have shifted. It’s possible that the ranking would have changed if there had been greater uncertainty in the expert assessment values.

4.4. Discussion

In risk management, entropy in an ordered framework is a unique and effective tool for measuring and understanding uncertainty in risky systems. Due to the ordered frame of discernment, the amount of relevant information is more centralised and unnecessary redundant calculations are avoided, so it makes the calculation of the proposed entropy measure more efficient. At the same time, the entropy metric in the ordered framework helps to adapt to complex risk systems because it can better deal with the structure and associative relationships in the system.

5. Overall Framework

This paper presents a software risk assessment model based on expert reliability and ordered frames of discernment. The model includes the following steps, as illustrated in Figure 3:
Figure 3: Overall Framework

Identification of risk factors

Step 1

Risk list

Step 2

Ordered assessment criteria

Step 3

Expert Reliability

Ranking of experts in different fields

Give Orness measure

Calculating the reliability of experts

Give the value of the expert’s combined assessment and convert to BPA

Step 4

Step 5

Integrate Expert Assessments using DST

Step 6

Analyze Risks

Belief Entropy

Calculate entropy

Apply Entropy for Discount

Step 7

Integrate Risk Information using DST

Step 8

Prioritize Risks

Integral Calculation
Step 1. Identification of risk factors.
Step 2. Representation of risk factors and establishment of assessment criteria.
Step 3. Calculating expert reliability.
Step 4. Give the value of the experts combined assessment and convert it to BPA.
Step 5. Integration expert evaluation.
Step 6. Apply the proposed entropy for discounting.
Step 7. Risk information integration.
Step 8. Ranking of risks.

6. Conclusion

For better risk assessment, this study establishes an evidence-based software risk assessment model based on an ordered identification framework. A risk criterion evaluation is constructed to provide an ordered framework for risk assessment. And the fusion method of expert confidence and expert linguistic information is used in the evaluation process. In addition, belief entropy based on ordered sets is introduced to calculate the weights of each attribute.

The specific contributions of the paper are as follows: (1) The use of ordered framework: In risk representation, we adopt an ordered framework, which makes the risk representation closer to the real world. (2) Evidence-based structure: In risk analysis, a simple evidence-based structure is adopted, which effectively reduces the need for parameters and makes the assessment easier and more efficient. (3) Introduction of belief entropy: Belief entropy is used to effectively measure the uncertainty of risk in the ordered framework, providing more comprehensive information for risk assessment.

In the future, our research direction involves considering the inherent connections among risks. By analyzing the connections of nodes and edges in a complex network [43, 44], we aim to uncover potential issues within the system.

Acknowledgments

The work is partially supported by National Natural Science Foundation of China (Grant No. 62373078).
References


