A Subjective Safety and Cost Based Decision Model for Assessing Safety Requirements Specifications[1]

J. Wang* *BEng MSc PhD CEng*

***J. B. Yang**◊* *BEng MSc PhD*

* *School of Engineering, Liverpool John Moores University, Liverpool, L3 3AF, UK*

◊*Manchester School of Management, UMIST, Manchester, M60 1QD, UK*

Key words: Fuzzy sets, evidential reasoning, safety-based decision making, safety requirements specifications, safety synthesis, subjective safety assessment.

SUMMARY

This paper presents a subjective safety and cost based modelling approach for evaluating safety requirements specifications in the study of safety-critical software. In the approach fuzzy set modelling and evidential reasoning are combined to assess both the safety associated with and the cost incurred in each option of safety requirements specifications. Both safety and cost estimates are combined to obtain the preference degree associated with each option of safety requirements specifications for selecting the best one. An example is presented to demonstrate the proposed approach for safety based decision making in safety requirements analysis of safety critical software development.

1. Introduction

It has been recognized in recent years that similar to safety analysis of engineering systems software safety analysis should also be integrated into the initial stages of the product development, more specifically into the early stages of the safety-critical software development, so that safety-related concerns can be addressed early to avoid the costs and delays due to major re-work of designs at the later stages. Safety analysis in the development of safety-critical software includes several stages, such as analysis of safety requirements; safety analysis of architectural and detail designs; and safety analysis of code. Safety analysis of architectural and detail designs and safety analysis of code have been extensively studied using various safety analysis approaches [4][5][6][7]. In the above, the

[1] Manuscript submitted to International Journal of Reliability, Quality and Safety Engineering.

analysis of safety requirements plays the most vital role since any faults introduced in this phase may corrupt the subsequent phases [1][11]. The analysis includes safety requirements analysis and safety analysis of the safety requirements specifications where the former produces the safety requirements specifications and the latter aims to reduce risks to a reasonable and acceptable level and provides evidence to support certification [11]. The importance of safety analysis of safety requirements specifications has been well recognised by software safety researchers. Both qualitative and quantitative safety assessment techniques have been used to deal with this issue. It has been recognised that in many circumstances it is difficult to employ traditional safety assessment techniques with confidence mainly due to the fact that software fails differently from hardware and there is a lack of safety data. Therefore, more flexible safety assessment techniques are required to assess the safety associated with safety requirements specifications effectively and efficiently. A novel subjective approach has been developed to deal with safety analysis of safety requirements specifications in a rational way [11]. Using that approach, safety requirement specifications can be analysed on a subjective basis.

In the safety-critical software development process, there may be several options of safety requirements specifications, each of which corresponds to certain levels of safety and cost. To select the most desirable option, it is required to model the cost incurred in each option and also to synthesise the cost and safety associated with each option to select the best one. This paper presents a framework that can be used to synthesise both the cost and safety aspects for each option of safety requirements specifications. The approach may be used to select a particular option of safety requirements specifications in situations where the level of uncertainty for safety based decision-making is high.

2. Subjective Safety Analysis

The modelling approach for subjective safety analysis, presented in this paper, partitions the analysis into smaller phases. Each phase corresponds to a domain of analysis in which requirements analysis and safety analysis are conducted in parallel [1]. The results generated using the approach are encoded in an information model, that is, the Safety Specification Hierarchy (SSH), which records the safety requirements specifications obtained during each phase with respect to an accident, hazard, safety constraint (a condition that negates a hazard) and safety strategy (a scheme to maintain a safety constraint), and their logical relationships.

In the analysis of safety requirements specifications, in many cases, it may be difficult or even impossible to apply traditional safety assessment methods such as fault tree analysis to deal with safety issues due to the nature of software failure. Therefore, analysts may have to describe a failure event in terms of vague and imprecise descriptors like "*reasonably low*" or "*low"* [11]. This kind of judgment is fuzzy in nature and may be more naturally treated using fuzzy set theory. The subjective safety assessment framework for safety requirements specifications presented in this paper combines safety modelling of safety requirements specifications at the bottom level using fuzzy set theory and safety synthesis in a hierarchical process using the evidential reasoning approach [12][13]. The reason why the evidential reasoning approach is used to deal with hierarchical evaluation is that it does not suffer from data loss in subjective information aggregation, which has been experienced by many safety researchers/engineers in traditional subjective safety analysis. The detailed description of the evidential reasoning approach can be founded in [12][13]. It will be briefly described in the context of its application to safety analysis of requirements specifications in the software domain later in this paper. The subjective safety assessment model is shown in Fig. 1 where an ellipse represents the safety evaluation of the named specification and an arrow gives the propagation direction of safety analysis from one level to another. The safety evaluations associated with safety rules at level 5 determine the safety evaluations associated with the safety strategies at level 4 which further determine the safety evaluations associated with the corresponding safety constraints. Furthermore, the safety evaluations associated with the safety constraints at level 3 determine the safety evaluations on hazard modelling that in turn determine safety evaluations on accident modelling (level 1) which finally determine the safety evaluation associated with the safety requirements specifications [11].

In subjective safety analysis, there are three basic parameters (i.e. failure likelihood, consequence severity and failure consequence probability) which are usually used to assess the safety associated with an event on a subjective basis [2][9][10]. The subjective safety associated with a safety rule can also be modelled in terms of these three parameters. In this case, the failure likelihood defines the probability that the safety rule is violated, the consequence severity describes the magnitude of possible consequences and the failure consequence probability defines the likelihood that failure effects will occur given the violation of the safety rule [11]. The logical relationships between the safety specifications can be reflected by failure consequence probabilities associated with safety rules. Since great uncertainty is involved in assessing the three parameters associated with a safety rule, subjective linguistic variables are appropriate. To estimate the failure likelihood, for example, one may often use such variables as "*highly frequent",* "*frequent*", "*reasonably frequent*",

"*average*", "*reasonably low*", "*low*" and "*very low*", to estimate the consequence severity, one may often use such variables as "*catastrophic*", "*critical*", "*marginal*" and "*negligible*", and to estimate the failure consequence probability, one may often use such variables as "*definite*", "*highly likely*", "*reasonably likely*", "*likely*", "*reasonably unlikely*", "*unlikely*" and "*highly unlikely*". The typical linguistic variables for describing these three parameters may be defined in terms of membership degrees belonging to the seven categories (shown in Tables 1, 2 and 3) [11]. Membership degrees associated with the three basic parameters of a safety rule can be assigned by safety analysts, with reference to Tables 1, 2 and 3, to reflect their judgments [11].

Suppose $L_{i,j,k,l}$ represents the fuzzy set of the failure likelihood of occurrence associated with $Rule_{i,j,k,l}$ (i.e. the likelihood that $Rule_{i,j,k,l}$ is violated), $C_{i,j,k,l}$ represents the fuzzy set of the consequence severity, and $E_{i,j,k,l}$ represents the failure consequence probability. The subjective safety description $S_{i,j,k,l}$ associated with $Rule_{i,j,k,l}$ can be defined as follows [2][9][10]:

$$S_{i,j,k,l} = C_{i,j,k,l} \circ E_{i,j,k,l} \times L_{i,j,k,l}$$

where the symbol "$\circ$" represents the composition operation and "$\times$" the Cartesian product operation in fuzzy set theory.

The relationship between the membership functions associated with $S_{i,j,k,l}$, $C_{i,j,k,l}$, $E_{i,j,k,l}$ and $L_{i,j,k,l}$ is described as follows:

$$\mu_{S_{i,j,k,l}} = \mu_{C_{i,j,k,l}} \circ \mu_{E_{i,j,k,l}} \times \mu_{L_{i,j,k,l}}$$

2.1 Fuzzy Safety Identification

Safety can be expressed by degrees to which it belongs to such linguistic variables as "*poor*", "*fair*", "*average*" and "*good*" that are referred to as *safety expressions*. To evaluate $S_{i,j,k,l}$ in terms of those safety expressions, it is necessary to characterise them using membership degrees with respect to the same categories used, in order to project the obtained subjective safety description onto the safety expressions. The four safety expressions are defined as shown in Table 4 [11].

Suppose safety expressions "*poor*", "*fair*", "*average*" and "*good*" are described by safety expressions 1, 2, 3 and 4, respectively. The extent to which $S_{i,j,k,l}$ belongs to the *m*th (*m* = 1, 2, 3 or 4) safety expression can be described by $\beta^m_{i,j,k,l}$ (*m* = 1, 2, 3 or 4), which can be calculated as follows [11]:

$$\beta^m_{i,j,k,l} = \frac{\alpha^m_{i,j,k,l}}{\sum_{T=1}^{4} \alpha^T_{i,j,k,l}}$$

where $\alpha^m_{i,j,k,l}$ (m = 1, 2, 3 or 4) represents the reciprocal of the relative distance between $S_{i,j,k,l}$ and the mth safety expression [9]. $\alpha^m_{i,j,k,l}$ can be obtained by:

$$\alpha^m_{i,j,k,l} = \frac{1}{d^m_{i,j,k,l} / d^M_{i,j,k,l}}$$

where $d^m_{i,j,k,l}$ is the Euclidean distance between $S_{i,j,k,l}$ and the mth safety expression, and $d^M_{i,j,k,l}$ is the minimum value for $d^m_{i,j,k,l}$ (m = 1, 2, 3 and 4).

2.2 Fuzzy Set Modelling by Multiple Safety Analysts

If multiple safety analysts are involved in the safety analysis process, their judgments need to be synthesised. A diagram for synthesising the judgments on a safety rule produced by multiple safety analysts is shown in Fig .2. Suppose there are N safety analysts who assign membership degrees for three basic safety parameters associated with a safety rule. Suppose $C_{i,j,k,l,n}$, $E_{i,j,k,l,n}$ and $L_{i,j,k,l,n}$ represent the three basic safety parameters associated with $Rule_{i,j,k,l}$ judged by safety analyst n (n = 1, …, or N), respectively. The subjective safety description $S_{i,j,k,l,n}$ associated with $Rule_{i,j,k,l}$ judged by safety analyst n can be obtained by:

$$S_{i,j,k,l,n} = C_{i,j,k,l,n} \circ E_{i,j,k,l,n} \times L_{i,j,k,l,n}$$

$S_{i,j,k,l,n}$ (n = 1, …, or N) can be mapped onto the defined safety expressions to identify the safety evaluation $S(S_{i,j,k,l,n})$ associated with $Rule_{i,j,k,l}$ judged by safety analyst n. Suppose $\beta^m_{i,j,k,l,n}$ (m = 1, 2, 3 or 4) represents the extent to which $S_{i,j,k,l,n}$ belongs to the mth safety expression. $S(S_{i,j,k,l,n})$ can be expressed in the following form:

$$S(S_{i,j,k,l,n}) = \{(\beta^1_{i,j,k,l,n}, 'poor'), (\beta^2_{i,j,k,l,n}, 'fair'), (\beta^3_{i,j,k,l,n}, 'average'), (\beta^4_{i,j,k,l,n}, 'good')\}$$

It is required to synthesise all $S(S_{i,j,k,l,n})$ (n = 1, …, and N) to obtain the safety evaluation associated with $Rule_{i,j,k,l}$. The evidential reasoning approach can be employed to synthesise all $S(S_{i,j,k,l,n})$ (n = 1, …, and N) and take into account the weight of each safety analyst in such a synthesis process.

2.3 Synthesis of the Judgments on Each Safety Rule Produced by Multiple Safety Analysts

The evidential reasoning approach used in this paper is well suited to handling uncertain and inconsistent safety evaluations [12][13]. It is based on the principle that it will become more likely that a given hypothesis is true if more pieces of evidence support that hypothesis. As stated previously, the problems of information loss in the synthesis process of fuzzy descriptions can be

avoided by employing the evidential reasoning approach. This approach is briefly described as follows to make this paper self-contained.

In Fig. 2, whether the safety evaluation associated with a safety rule belongs to "*poor*", "*fair*", "*average*" or "*good*" judged by a safety analyst can be regarded as a hypothesis. Suppose H represents the set of the four safety expressions. Then, H can be expressed by:

$H = \{H_1 \ H_2 \ H_3 \ H_4\}$

where H_1, H_2, H_3 and H_4 represent "*poor*", "*fair*", "*average*" and "*good*", respectively.

Let $\lambda_{i,j,k,l,n}$ (n = 1, …, or N) be the normalised relative weight of safety analyst n in the safety evaluation process where $0 \le \lambda_{i,j,k,l,n} \le 1$. The weight $\lambda_{i,j,k,l,n}$ (n = 1, …, and N) can be calculated on the basis of the relative weights of safety analysts. In this paper, it is assumed that if all safety analysts judge the safety associated with a safety rule as "*good*", the safety associated with the safety rule is evaluated as "*good*" with a belief degree Ω of over 99.5 percent. The following formula can be used to obtain the value of $\lambda_{i,j,k,l,n}$ (n = 1, …, or N) [12][13]:

$$\lambda_{i,j,k,l,n} = \varepsilon_{i,j,k,l} \frac{\xi_{i,j,k,l,n}}{\xi_{i,j,k,l,Max}}$$

$$\prod_{n=1}^{N} (1 - \varepsilon_{i,j,k,l} \frac{\xi_{i,j,k,l,n}}{\xi_{i,j,k,l,Max}}) \le 1 - \Omega$$

where $\xi_{i,j,k,l,n}$ (n = 1, …, or N) is the relative weight of the nth safety analyst; $\xi_{i,j,k,l,Max}$ is the largest value among $\xi_{i,j,k,l,n}$ (n = 1, …, and N); and $\varepsilon_{i,j,k,l}$ is a priority coefficient representing the importance of the role the most important safety analyst plays in the evaluation of the safety associated with $Rule_{i,j,k,l}$. Given all $\xi_{i,j,k,l,n}$ (n = 1, …, and N), $\varepsilon_{i,j,k,l}$ can be calculated and $\lambda_{i,j,k,l,n}$ can then be obtained.

Suppose $M^m_{i,j,k,l,n}$ (n = 1, …, or N) is a degree to which $S(S_{i,j,k,l,n})$ supports the hypothesis that the safety evaluation associated with $Rule_{i,j,k,l}$ is confirmed to H_m (m = 1, 2, 3 and 4). Then, $M^m_{i,j,k,l,n}$ can be obtained as follows [9][12]:

$$M^m_{i,j,k,l,n} = \lambda_{i,j,k,l,n} \times \beta^m_{i,j,k,l,n}$$

Suppose $M^H_{i,j,k,l,n}$ (n = 1, …, or N) is the remaining belief unassigned after commitment of belief to all H_m (m = 1, 2, 3 and 4) for $S(S_{i,j,k,l,n})$. $M^H_{i,j,k,l,n}$ can be obtained as follows [9][12]:

$$M^{H}_{i,j,k,l,n} = 1 - \sum_{m=1}^{4} M^{m}_{i,j,k,l,n}$$

Suppose $MM^{m}_{i,j,k,l,n}$ (m = *1, 2, 3* or *4; n = 1, …,* or *N*) represents the degree to which the safety associated with the $Rule_{i,j,k,l}$ belongs to H_m as a result of the synthesis of the judgments produced by safety analysts *1* to *n*. Suppose $MM^{H}_{i,j,k,l,n}$ represents the remaining belief unassigned after commitment of belief to all H_m (m = *1, 2, 3* and *4*) as a result of the synthesis of the judgments produced by safety analysts *1* to *n*. The recursive algorithm for synthesizing the analysts' judgments to obtain the safety evaluation associated with $Rule_{i,j,k,l}$ can be stated as follows [12][13]:

Initial conditions: $MM^{m}_{i,j,k,l,1} = M^{m}_{i,j,k,l,1}$ (m = *1, 2, 3, 4*) and $MM^{H}_{i,j,k,l,1} = M^{H}_{i,j,k,l,1}$

$\{H_m\}$ $$MM^{m}_{i,j,k,l,n+1} = K_{i,j,k,l,n+1}(MM^{m}_{i,j,k,l,n} M^{m}_{i,j,k,l,n+1} + MM^{m}_{i,j,k,l,n} M^{H}_{i,j,k,l,n+1} + MM^{H}_{i,j,k,l,n} M^{m}_{i,j,k,l,n+1}) \qquad m = 1, 2, 3, 4$$

{H} $$MM^{H}_{i,j,k,l,n+1} = K_{i,j,k,l,n+1} MM^{H}_{i,j,k,l,n} M^{H}_{i,j,k,l,n+1}$$

$$K_{i,j,k,l,n+1} = [1 - \sum_{T=1}^{4} \sum_{\substack{R=1 \\ R \neq T}}^{4} MM^{T}_{i,j,k,l,n} M^{R}_{i,j,k,l,n+1}]^{-1}$$

n = *1, …, N-1*

$MM^{m}_{i,j,k,l,N}$ is the safety evaluation associated with $Rule_{i,j,k,l}$.

The safety evaluation associated with $Rule_{i,j,k,l}$ can then be presented in the following form:

$S(S_{i,j,k,l}) = \{(\beta^{1}_{i,j,k,l}$, "*poor*"), ($\beta^{2}_{i,j,k,l}$, "*fair*"), ($\beta^{3}_{i,j,k,l}$, "*average*"), ($\beta^{4}_{i,j,k,l}$, "*good*")}

where $\beta^{m}_{i,j,k,l}$ (m = 1, 2, 3 and 4) is equal to $MM^{m}_{i,j,k,l,N}$.

2.4 Hierarchical Propagation for Safety Evaluation

After the safety evaluation associated with each safety rule has been obtained, it is required to synthesise the safety evaluations associated with all $Rule_{i,j,k,l}$ to obtain the safety evaluation associated with $SS_{i,j,k}$. Then the safety evaluations associated with $SS_{i,j,k}$ need to be synthesised to obtain the safety evaluation associated with $SC_{i,j}$. Such a hierarchical evaluation can finally be progressed up to the accident (AC_i) level to obtain the safety evaluation associated with the safety requirements specifications [11]. All such hierarchical evaluations can be conducted using the evidential reasoning approach in the same way as described above.

3. Subjective Cost Analysis

Safety and cost may be two conflicting criteria, with high safety leading to high costs. When studying safety requirements specifications, this means that if the safety associated with the safety requirements specifications is improved, then there may be a higher cost incurred. Since the cost incurred is determined by many factors, the level of uncertainty in cost estimation may be very high. Therefore, it is often difficult to model the cost incurred in safety improvement of safety requirements specifications on a numerical basis. It may be more appropriate to model the cost using fuzzy sets.

The cost incurred in safety improvement of safety requirements specifications can be described using such linguistic variables as "*Very low*", "*Low*", "*Moderately low*", "*Average*", "*Moderately high*", "*High*" and "*Very high*". Such linguistic variables are referred to as *cost expressions*. They can be described as shown in Table 5 in terms of membership values with respect to the seven categories already defined.

The membership values describing the cost incurred may be given by safety analysts with reference to Table 5. Suppose there are multiple safety analysts. The cost $C(i)_n$ incurred in safety improvement of option i judged by safety analyst n can be described in terms of membership values as follows:

$$C(i)_n = [1/\mu^1_{C(i)_n}, 2/\mu^2_{C(i)_n}, 3/\mu^3_{C(i)_n}, 4/\mu^4_{C(i)_n}, 5/\mu^5_{C(i)_n}, 6/\mu^6_{C(i)_n}, 7/\mu^7_{C(i)_n}]$$

where each $\mu^j_{C(i)_n}$ (j = 1, 2, 3, 4, 5, 6, 7) represents a degree to which $C(i)_n$ belongs to the jth category.

4. Synthesis of Safety and Cost Evaluations

A framework for synthesis of safety and cost evaluations for option ranking is shown in Fig. 3. In the framework, multiple safety analysts can make their judgments on each rule in an option of safety requirements specifications in terms of three parameters and then the information produced can be synthesised to obtain the safety evaluation associated with the option of the safety requirements specifications. Multiple safety analysts can also make judgments on the cost incurred for the option of safety requirements specifications. Both safety and cost evaluations can then be synthesised in order to select the best option. The evidential reasoning approach can be used to synthesise safety and cost evaluations to produce the preference degree associated with each option of safety requirements specifications.

To synthesise both safety and cost aspects for decision-making purposes, it is necessary to define a utility space that can be used to evaluate safety and cost on the same scale [10]. Four exclusive utility expressions (i.e. "*slightly preferred*", "*moderately preferred*", "*preferred*" and "*greatly preferred*") are defined as shown in Table 6. The safety associated with and the cost incurred in each option of safety requirements specifications are then mapped onto the utility space and expressed in terms of the utility expressions.

Since the safety expressions and the utility expressions are defined by the same membership functions with respect to the seven categories, a safety description can be directly mapped onto the utility space. Given the membership values of a cost description with reference to Table 5, the Best-Fit method can also be used to map the subjective cost description onto the defined utility expressions. The cost $C(i)_n$ incurred in the ith option of safety requirements specifications judged by safety analysts n can be evaluated in terms of the utility expressions as follows:

$U(C(i)_n)$ = {($\mu^1_{C(i)_n}$, "*slightly preferred*"), ($\mu^2_{C(i)_n}$, "*moderately preferred*"), ($\mu^3_{C(i)_n}$, "*preferred*"), ($\mu^4_{C(i)_n}$, "*greatly preferred*")}

The evidential reasoning approach can be used to synthesise all $U(C(i)_n)$ (n = 1, ..., N) to obtain the utility expression associated with the ith option of safety requirements specifications as follows:

$U(C(i))$ = {($\mu^1_{C(i)}$, "*slightly preferred*"), ($\mu^2_{C(i)}$, "*moderately preferred*"), ($\mu^3_{C(i)}$, "*preferred*"), ($\mu^4_{C(i)}$, "*greatly preferred*")}

Suppose there are D options in hand. Given the relative importance of cost against safety, denoted by ω, $U(S(i))$ and $U(C(i))$ can be synthesised using the evidential reasoning approach to obtain a preference estimate associated with option i in terms of the utility expressions. The synthesised preference estimate $U(i)$ for an option can be expressed as follows:

$U(i)$ = {(μ^1_{Ui}, "*slightly preferred*"), (μ^2_{Ui}, "*moderately preferred*"), (μ^3_{Ui}, "*preferred*"), (μ^4_{Ui}, "*greatly preferred*")}

Preference degree P_i associated with option i can be obtained by:

$$P_i = \sum_{j=1}^{4} \mu^j_{U(i)} \times K_j + (1 - \sum_{j=1}^{4} \mu^j_{U(i)}) \times \frac{1}{4} \times \sum_{j=1}^{4} K_j$$

where $[K_1\ K_2\ K_3\ K_4] = [0.217\ 0.478\ 0.739\ 1]$; $(1-\sum_{j=1}^{4}\mu_{U(i)}^{j})$ describes the remaining belief unassigned after commitment of belief in the synthesis of cost and safety descriptions; and $\frac{1}{4}\times\sum_{j=1}^{4}K_j$ is the average value of the K_js.

Obviously, a larger P_i means that option i is more desirable. Each P_i ($i = 1, 2, \ldots D$) represents the comparison with others. The best option with the largest preference degree can be selected.

5. An Example

With the aim of exemplifying the proposed framework for making decisions on safety requirements specifications based on subjective safety and cost analyses, a case study based on a train set crossing is used in this paper. The detailed description of the train set crossing can be found in [8].

5.1 Safety Assessment

The train set crossing process consists of two track circuits C_p and C_s, and two types of trains, that is, primary (*Trp*) and secondary (*Trs*). The circuits are divided into sections and there are two separate crossing sections at which the two circuits intersect. It is assumed that trains of type *Trp* travel around circuit C_p and trains of type *Trs* travel around circuit C_s; both types of train travel in one direction (clockwise) only. The longest train is shorter than the smallest section. The circuits C_p and C_s, and the crossing sections are illustrated in Fig. 4 [8].

Suppose the type of circuit is denoted by $c \in L$, $L = \{p, s\}$, the crossing section by $r \in Trc = \{1, \ldots, Ntc\}$. Addition $\oplus$ and subtraction Θ on circuit section numbers are performed modulo the number of sections of the circuit. The danger zone on circuit C_c for *CC(c, r)* for a crossing section *CC(c, r)* are illustrated in Fig. 4 [8]. The behaviour of the physical process is captured by two state variables *Ptrain* and *Rtrain*. *Ptrain(c, x)* denotes the state variable for the position of train x on circuit C_c, and *Rtrain(c, x)* the reservation set of train x on circuit C_c.

If only two possible accidents on the train set are considered, the safety specification hierarchy for the train set crossing is shown in Fig. 5 [8][11]. The details of the rules are not discussed any further in this paper. The subjective safety analysis of the safety requirements specifications in the safety specification hierarchy is carried out as follows:

Suppose there are four safety analysts who make judgments on each rule in terms of failure likelihood, consequence severity and failure consequence probability. The safety description of each rule judged by a safety expert can be obtained using fuzzy manipulations. Then the safety

description can be mapped onto the safety definitions to be presented in terms of the safety definitions and the extent to which it belongs to each of the safety definitions. Such safety evaluations for rule 1 are as follows:

$\underline{Rule_{1,1,1,1}}$

$S(S_{1,1,1,1,1})$ = {(0.175496, "*poor*"), (0.184576, "*fair*"), (0.364160, "*average*"), (0.275768, "*good*")}

$S(S_{1,1,1,1,2})$ = {(0.177419, "*poor*"), (0.186412, "*fair*"), (0.364218, "*average*"), (0.271953, "*good*")}

$S(S_{1,1,1,1,3})$ = {(0.175134, "*poor*"), (0.183683, "*fair*"), (0.367365, "*average*"), (0.273818, "*good*")}

$S(S_{1,1,1,1,4})$ = {(0.124688, "*poor*"), (0.156304, "*fair*"), (0.584837, "*average*"), (0.134171, "*good*")}

where $S(S_{i,\ j,\ k,\ l,\ n})$ is the subjective safety evaluation associated with $Rule_{i,\ j,\ k,\ l}$ judged by safety analyst *n*.

Suppose the relative weights of the four safety analysts are 2, 1, 2 and 1, respectively. Then $[\xi_{i,j,k,l,1}\ \xi_{i,j,k,l,2}\ \xi_{i,j,k,l,3}\ \xi_{i,j,k,l,4}]^T = [2\ 1\ 2\ 1]^T$ where $i = 1$ or 2; $j = 1$; $k = 1$; and $l = 1$ or 2. $\lambda_{i,j,k,l,n}$ (n = 1, 2, 3, and 4) are calculated as follows [7][9]:

$$\lambda_{i,j,k,l,1} = 0.8744 \quad \lambda_{i,j,k,l,2} = 0.4372 \quad \lambda_{i,j,k,l,3} = 0.8744 \quad \lambda_{i,j,k,l,4} = 0.4372$$

Using the evidential reasoning algorithm, the safety evaluations associated with $Rule_{1,1,1,1}$ is obtained as follows:

$S(S_{1,1,1,1})$ = {(0.115318, "*poor*"), (0.127214, "*fair*"), (0.503492, "*average*"), (0.231790, "*good*")}

In a similar way, the safety evaluations associated with $Rule_{1,1,1,2}$, $Rule_{2,1,1,1}$ and $Rule_{2,1,1,2}$ are obtained as follows:

$S(S_{1,1,1,2})$ = {(0.115431, "*poor*"), (0.127229, "*fair*"), (0.504863, "*average*"), (0.230315, "*good*")}

$S(S_{2,1,1,1})$ = {(0.115318, "*poor*"), (0.127214, "*fair*"), (0.503492, "*average*"), (0.231790, "*good*")}

$S(S_{2,1,1,2})$ = {(0.084500, "*poor*"), (0.103661, "*fair*"), (0.658630, "*average*"), (0.1331126, "*good*")}

Suppose $[\xi_{1,1,1,1}\ \xi_{1,1,1,2}]^T$ is obtained as $[1.5\ 1]^T$ by studying the relations between $Rule_{1,1,1,1}$ and $Rule_{1,1,1,2}$ and studying the relative confidence in safety analysis of each safety rule. $\lambda_{1,1,1,1}$ and $\lambda_{1,1,1,2}$ are calculated as follows:

$\lambda_{1,1,1,1} = 0.9855 \qquad \lambda_{1,1,1,2} = 0.6570$

Suppose $[\xi_{2,1,1,1}\ \xi_{2,1,1,2}]^T$ is obtained as $[1\ 1]^T$ by studying the relations between $Rule_{2,1,1,1}$ and $Rule_{2,1,1,2}$ and studying the relative confidence in safety analysis of each safety rule. $\lambda_{2,1,1,1}$ and $\lambda_{2,1,1,2}$ are calculated as follows:

$\lambda_{2,1,1,1} = 0.9293$ $\lambda_{2,1,1,2} = 0.9293$

The safety evaluations associated with $SS_{1,1,1}$ and $SS_{2,1,1}$ are obtained as follows:

$S(S_{1,1,1})$ = {(0.068534, "*poor*"), (0.078407, "*fair*"), (0.696841, "*average*"), (0.137151, "*good*")}

$S(S_{2,1,1})$ = {(0.049794, "*poor*"), (0.060850, "*fair*"), (0.760025, "*average*"), (0.113180, "*good*")}

$\lambda_{1,1,1}$ and $\lambda_{2,1,1}$ are calculated as follows:

$\lambda_{1,1,1} = 0.9950$ $\lambda_{2,1,1} = 0.9950$

The safety evaluations associated with $SC_{1,1}$ and $SC_{2,1}$ are obtained as follows:

$S(S_{1,1})$ = {(0.068191, "*poor*"), (0.078015, "*fair*"), (0.693357, "*average*"), (0.136546, "*good*")}

$S(S_{2,1})$ = {(0.049545, "*poor*"), (0.060546, "*fair*"), (0.756225, "*average*"), (0.112614, "*good*")}

$\lambda_{1,1}^{HZ}$ and $\lambda_{2,1}^{HZ}$ are calculated as follows:

$\lambda_{1,1}^{HZ} = 0.9950$ $\lambda_{2,1}^{HZ} = 0.9950$

The safety evaluations associated with $HZ_{1,1}$ and $HZ_{2,1}$ are obtained as follows:

$S(S_{1,1}^{HZ})$ = {(0.067850, "*poor*"), (0.077625, "*fair*"), (0.689890, "*average*"), (0.135780, "*good*")}

$S(S_{2,1}^{HZ})$ = {(0.049297, "*poor*"), (0.060243, "*fair*"), (0.752444, "*average*"), (0.112051, "*good*")}

$\lambda_{1,1}$ and $\lambda_{2,1}$ are calculated as follows:

$\lambda_{1,1} = 0.9950$ $\lambda_{2,1} = 0.9950$

The safety evaluations associated with AC_1 and AC_2 are obtained as follows:

$S(S_1)$ = {(0.067511, "*poor*"), (0.077237, "*fair*"), (0.686441, "*average*"), (0.135104, "*good*")}

$S(S_2)$ = {(0.049051, "*poor*"), (0.059942, "*fair*"), (0.748681, "*average*"), (0.111491, "*good*")}

Suppose $[\xi_1\ \xi_2]^T$ is obtained by $[1\ 2]^T$ by studying the relations between AC_1 and AC_2 and studying the relative confidence in safety analysis of each accident. λ_1 and λ_2 are calculated as follows:

$\lambda_1 = 0.4951$ $\lambda_2 = 0.9901$

The safety evaluation associated with option 1 of the safety requirements specifications is finally obtained as follows:

$S(S(1))$ = {(0.035199, "*poor*"), (0.043240, "*fair*"), (0.811309, "*average*"), (0.084147, "*good*")}

Suppose there are two other options of safety requirements specifications in which rule $Rule_{1,1,1,1}$ is changed and the other three remain unchanged. The modification of a rule may change the safety associated with the option of safety requirements specifications. This may be demonstrated by an example in which a rule is that if one train is at the crossing section, other trains on the tracks should keep a distance from it for at least 2 miles. If the distance is increased to 5 miles, the safety may be increased and if the distance is reduced to 1 mile, the safety may be reduced. It can also be understood that the costs incurred in the above three options may be different since those three options require different speeds of other trains on the tracks, track structure, etc. Therefore, different options of safety requirements specifications may correspond to different levels of cost.

In a similar way, the safety evaluations associated with options 2 and 3 of the safety requirements specifications are obtained as follows:

$S(S(2))$ = {(0.040887, "*poor*"), (0.064904, "*fair*"), (0.782754, "*average*"), (0.092668, "*good*")}

$S(S(3))$ = {(0.040153, "*poor*"), (0.049232, "*fair*"), (0.787313, "*average*"), (0.105124, "*good*")}

5.2 Cost Assessment

Suppose the four safety analysts make the cost estimates as follows:

Option 1

$C(1)_1$ = [1/0, 2/0, 3/0.5, 4/1, 5/0.5, 6/0, 7/0]

$U(C(1)_1)$ = {(0.169984, "*slightly preferred*"), (0.330016, "*moderately preferred*"), (0.330016, "*preferred*"), (0.169984, "*greatly preferred*")}

$C(1)_2$ = [1/0, 2/0, 3/0.5, 4/1, 5/0.5, 6/0, 7/0]

$U(C(1)_2)$ = {(0.169984, "*slightly preferred*"), (0.330016, "*moderately preferred*"), (0.330016, "*preferred*"), (0.169984, "*greatly preferred*")}

$C(1)_3$ = [1/0, 2/0.25, 3/1, 4/0.75, 5/0, 6/0, 7/0]

$U(C(1)_3)$ = {(0.102234, "*slightly preferred*"), (0.685810, "*moderately preferred*"), (0.115923, "*preferred*"), (0.09603, "*greatly preferred*")}

$C(1)_4$ = [1/0, 2/0, 3/0, 4/0.75, 5/1, 6/0.25, 7/0]

$U(C(1)_4)$ = {(0.096033, "*slightly preferred*"), (0.115923, "*moderately preferred*"), (0.685810, "*preferred*"), (0.102234, "*greatly preferred*")}

The judgments produced can then be synthesised to obtain the utility description of the cost incurred in design option 1.

$U(C(1))$ = {(0.08133, "*slightly preferred"*), (0.576404, "*moderately preferred*"), (0.240367, "*preferred*"), (0.07915, "*greatly preferred*")}

The four safety analysts can also make the cost estimations on options 2 and 3 and in a similar way the utility descriptions of the costs incurred in those two options are obtained as follows:

Option 2

$U(C(2))$ = {(0.078148, "*slightly preferred"*), (0.706781, "*moderately preferred*"), (0.127187, "*preferred*"), (0.068324, "*greatly preferred*")}

Option 3

$U(C(3))$ = {(0.068324, "*slightly preferred"*), (0.127187, "*moderately preferred*"), (0.706781, "*preferred*"), (0.078148, "*greatly preferred*")}

5.3 Synthesis of Safety and Cost Evaluations

If safety and cost aspects are considered to be of equal importance, then the utility descriptions of the three options are obtained as follows using the evidential reasoning approach:

Option 1

$U(1)$ = {(0.033499, "*slightly preferred"*), (0.198317, "*moderately preferred*"), (0.690426, "*preferred*"), (0.056197, "*greatly preferred*")}

$P_1 = 0.033499 \times 0.217 + 0.198317 \times 0.478 + 0.690426 \times 0.739 + 0.056197 \times 1 + 0.02156 \times 0.6085 = 0.681607$

Option 2

$U(2)$ = {(0.04138, "*slightly preferred"*), (0.339518, "*moderately preferred*"), (0.531463, "*preferred*"), (0.061776, "*greatly preferred*")}

$P_2 = 0.04138 \times 0.217 + 0.339518 \times 0.478 + 0.531463 \times 0.739 + 0.061776 \times 1 + 0.025862 \times 0.6085 = 0.641534$

Option 3

U(3) = {(0.016937, "*slightly preferred"*), (0.029856, "*moderately preferred*"), (0.908145, "*preferred*"), (0.033337, "*greatly preferred*")}

$P_3 = 0.016937 \times 0.217 + 0.029856 \times 0.478 + 0.908145 \times 0.739 + 0.033337 \times 1 + 0.011725 \times 0.6085 = 0.729537$

The ranking of the three options is as follows:

Ranking	Options	Preference degrees
1	Option 3	0.729537
2	Option 1	0.681607
3	Option 2	0.641534

The ranking of the three options varies with the change of the relative importance of cost against safety. For different relative weights of cost against safety, the ranking of the three options is obtained as shown in Table 7, Table 8 and Fig. 6.

From Table 8 and Fig. 6, it can be seen that the ranking order of the three options is consistently option 3, option 1 and option 2 when the relative weights of cost against safety are set to 0.1, 0.2, 0.5, 1, 2, 5, 10. It can be noted that when the relative weights of cost against safety are small, the preference degrees associated with the three options are close. For example, when the relative weight of cost against safety is equal to 0.1, the preference degrees associated with options 1, 2 and 3 are 0.728208, 0.720426 and 0.730045, respectively. As the relative weight of cost against safety increases, the differences among the preference degrees associated with the three options are widened. For example, when the relative weight of cost against safety is equal to 5, the preference degrees associated with options 1, 2 and 3 are 0.572936, 0.535429 and 0.693896, respectively. In this particular example, the best option is option 3 in terms of both safety and cost.

It should be mentioned that the options can only be compared with respect to the same relative weight of cost against safety. In this example, the ranking order of the options does not change with the relative weight of cost against safety. In practice, the ranking order of options in hand may change with the relative weight of cost against safety. The best option may be chosen by considering the particular requirements on safety and cost.

6. Concluding Remarks

This paper presents a modelling approach for subjective analysis of both safety and cost criteria associated with safety requirements specifications. If there are several options of safety requirements specifications in hand, the best one can be selected by synthesising subjective safety and cost evaluations. The approach presented in this paper combines fuzzy set modelling and evidential reasoning to avoid any possible information loss which often happens when traditional subjective techniques are used. This approach is particularly useful in situations where the level of uncertainty involved in safety and cost analyses is high. It can be used as an alternative approach for safety analysts to make decisions based on safety and cost analyses of safety requirements specifications in safety-critical software development. Since the uncertainty involved in safety and cost assessment in the software domain is often high, the proposed approach offers significant potential to aid the development of safety-critical systems.

Acknowledgement

This work forms part of the project jointly supported by the UK Engineering and Physical Sciences Research Council (EPSRC) and Health & Safety Executive (HSE) under Grant References GR/M24967 and D3727. The second author is partially supported by the EPSRC under the Grant Reference GR/N65615/01.

References

1. De Lemos R., Saeed A., Anderson T., *On the safety analysis of requirements specifications*, Proceedings of 3th International Conference on Computer Safety, Reliability and Security (SAFECOMP'94), Ed. Victor Maggioli, Anaheim, CA, 17-227, 1994.
2. Karwowski W., Mital A., *Potential applications of fuzzy sets in industrial safety engineering*, Fuzzy Sets and Systems, Vol. 19, 1986, 105-120.
3. Keller A. Z, Kara-Zaitri, *Further application of fuzzy logic to reliability assessment and safety analysis*", Micro Reliab., Vol. 29, No.3, 1989, 399-404.
4. Leveson N. G., Harvey P. R., *Analyzing software safety*, IEEE Transactions on Software Engineering, Vol. SE-9, No. 5, 1983, 569-579.
5. Leveson N. G., Cha S. S., Shimeall T. J., *Safety verification of ADA programs using software fault trees*, IEEE Software, 1991, 48-59.
6. Leveson N. G., *Software safety in embedded computer systems*, Communications of the ACM, Vol. 34, No. 2, 1991, 35-46.
7. McDermid J. A., *Formal methods: use and relevance for the development of safety-critical systems*, Safety Aspects of Computer Control, Ed. P. Bennett, 1993.

8. Saeed A., De Lemos R., Anderson T., *An approach to the risk analysis of safety specifications*, Proceedings of 9th Annual Conference on Computer Assurance (COMPASS'94), Gaithersburg, MD, 1994, 209-222.

9. Wang J., Yang. J. B., Sen P., *Safety analysis and synthesis using fuzzy set modelling and evidential reasoning*, Reliability Engineering and System Safety, Vol.47, No.3, 1995, 10-118.

10. Wang J., Yang. J. B., Sen P., *Multi-person and multi-attribute design evaluations using evidential reasoning based on subjective safety and cost analyses*, Reliability Engineering and System Safety, Vol. 52, No. 2,1996, 113-129.

11. Wang J., "*A subjective methodology for safety analysis of safety requirements specifications*", IEEE Transactions on Fuzzy Systems, Vol.5, No.3, 1997, 418-430.

12. Yang J. B., Singh M. G., *An evidential reasoning approach for multiple attribute decision making with uncertainty*, IEEE Transactions on Systems, Man and Cybernetics, Vol. 23, No.1, 1994, 1-18.

13. Yang J. B., Sen P., *A general multi-level evaluation process for hybrid MADM with uncertainty*, IEEE Transactions on Systems, Man and Cybernetics, Vol. 24, No. 10, 1994, 1458-1473.

Table 1 Failure likelihood

μ_L	Categories						
Linguistic variables	1	2	3	4	5	6	7
Highly frequent	0	0	0	0	0	0.75	1
Frequent	0	0	0	0	0.75	1	0.25
Reasonably frequent	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Reasonably low	0	0.25	1	0.75	0	0	0
Low	0.25	1	0.75	0	0	0	0
Very low	1	0.75	0	0	0	0	0

Table 2 Consequence severity

μ_C	Categories						
Linguistic variables	1	2	3	4	5	6	7
Catastrophic	0	0	0	0	0	0.75	1
Critical	0	0	0	0.75	1	0.25	0
Marginal	0	0.25	1	0.75	0	0	0
Negligible	1	0.75	0	0	0	0	0

Table 3 Failure consequence probability

μ_E	Categories						
Linguistic variables	1	2	3	4	5	6	7
Definite	0	0	0	0	0	0.75	1
Highly likely	0	0	0	0	0.75	1	0.25
Reasonably likely	0	0	0	0.75	1	0.25	0
Likely	0	0	0.5	1	0.5	0	0
Reasonably unlikely	0	0.25	1	0.75	0	0	0
Unlikely	0.25	1	0.75	0	0	0	0
Highly unlikely	1	0.75	0	0	0	0	0

Table 4 Safety expression

μ_S Linguistic variables	Categories 1	2	3	4	5	6	7
1. Poor	0	0	0	0	0	0.75	1
2. Fair	0	0	0	0.5	1	0.25	0
3. Average	0	0.25	1	0.5	0	0	0
4. Good	1	0.75	0	0	0	0	0

Table 5 Cost expressions

μ_C Linguistic variables	Categories 1	2	3	4	5	6	7
Very high	0	0	0	0	0	0.75	1
High	0	0	0	0	0.75	1	0.25
Moderately high	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Moderately low	0	0.25	1	0.75	0	0	0
Low	0.25	1	0.75	0	0	0	0
Very low	1	0.75	0	0	0	0	0

Table 6 Utility expressions

μ Linguistic variables	Categories 1	2	3	4	5	6	7
1. Slightly preferred	0	0	0	0	0	0.75	1
2. Moderately preferred	0	0	0	0.5	1	0.25	0
3. Preferred	0	0.25	1	0.5	0	0	0
4. Greatly preferred	1	0.75	0	0	0	0	0

Table 7 Summary of the three options with the relative importance of cost against safety

Safety is twice as important as cost. Option 1 *U(1)* = {(0.033823, "*slightly preferred"*), (0.068841, "*moderately preferred*"), (0.793887, "*preferred*"), (0.081854, "*greatly preferred*")} P_1 = 0.721923 Option 2 *U(2)* = {(0.038883, "*slightly preferred"*), (0.108353, "*moderately preferred*"), (0.743788, "*preferred*"), (0.084864, "*greatly preferred*")} P_2 = 0.709426 Option 3 *U(3)* = {(0.028102, "*slightly preferred"*), (0.036948, "*moderately preferred*"), (0.844841, "*preferred*"), (0.072491, "*greatly preferred*")} P_3 = 0.731308 Ranking Options Preference degrees 1 Option 3 0. 731308 2 Option 1 0. 721923 3 Option 2 0. 709426	**Safety is five times as important as cost.** Option 1 *U(1)* = {(0.036203, "*slightly preferred"*), (0.052299, "*moderately preferred*"), (0.800072, "*preferred*"), (0.089827, "*greatly preferred*")} P_1 = 0.727078 Option 2 *U(2)* = {(0.040144, "*slightly preferred"*), (0.076687, "*moderately preferred*"), (0.769663, "*preferred*"), (0.090142, "*greatly preferred*")} P_2 = 0.718508 Option 3 *U(3)* = {(0.035755, "*slightly preferred"*), (0.044683, "*moderately preferred*"), (0.805505, "*preferred*"), (0.093315, "*greatly preferred*")} P_3 = 0.730322 Ranking Options Preference degrees 1 Option 3 0. 730322 2 Option 1 0. 727078 3 Option 2 0. 718508
Safety is ten times as important as cost. Option 1 *U(1)* = {(0.036795, "*slightly preferred"*), (0.048776, "*moderately preferred*"), (0.801361, "*preferred*"), (0.091701, "*greatly preferred*")} P_1 = 0.728208 Option 2 *U(2)* = {(0.040456, "*slightly preferred"*), (0.070089, "*moderately preferred*"), (0.775176, "*preferred*"), (0.091318, "*greatly preferred*")} P_2 = 0.720426 Option 3 *U(3)* = {(0.037953, "*slightly preferred"*), (0.046936, "*moderately preferred*"), (0.794475, "*preferred*"), (0.099234, "*greatly preferred*")} P_3 = 0.730045 Ranking Options Preference degrees 1 Option 3 0. 730045 2 Option 1 0. 728208 3 Option 2 0. 720426	**Cost is twice as important as safety.** Option 1 *U(1)* = {(0.067648, "*slightly preferred"*), (0.477762, "*moderately preferred*"), (0.358159, "*preferred*"), (0.070655, "*greatly preferred*")} P_1 = 0.594069 Option 2 *U(2)* = {(0.069416, "*slightly preferred"*), (0.634316, "*moderately preferred*"), (0.206607, "*preferred*"), (0.064917, "*greatly preferred*")} P_2 = 0.550923 Option 3 *U(3)* = {(0.045338, "*slightly preferred"*), (0.084643, "*moderately preferred*"), (0.795569, "*preferred*"), (0.055986, "*greatly preferred*")} P_3 = 0.705445 Ranking Options Preference degrees 1 Option 3 0. 705445 2 Option 1 0. 594069 3 Option 2 0. 550923
Cost is five times as important as safety. Option 1 *U(1)* = {(0.076984, "*slightly preferred"*), (0.545301, "*moderately preferred*"), (0.274753, "*preferred*"), (0.076326, "*greatly preferred*")} P_1 = 0.572936 Option 2 *U(2)* = {(0.075410, "*slightly preferred"*), (0.684200, "*moderately preferred*"), (0.149193, "*preferred*"), (0.067102, "*greatly preferred*")} P_2 = 0.535429 Option 3 *U(3)* = {(0.060030, "*slightly preferred"*), (0.111856, "*moderately preferred*"), (0.736110,	**Cost is ten times as important as safety.** Option 1 *U(1)* = {(0.079155, "*slightly preferred"*), (0.560876, "*moderately preferred*"), (0.255691, "*preferred*"), (0.077677, "*greatly preferred*")} P_1 = 0.568095 Option 2 *U(2)* = {(0.076734, "*slightly preferred"*), (0.695019, "*moderately preferred*"), (0.136917, "*preferred*"), (0.067617, "*greatly preferred*")} P_2 = 0.532099 Option 3 *U(3)* = {(0.064199, "*slightly preferred"*), (0.119563, "*moderately preferred*"), (0.719447,

"*preferred*"), (0.070070, "*greatly preferred*")} P_3 = 0.693896 Ranking Options Preference degrees 1 Option 3 0. 693896 2 Option 1 0. 572936 3 Option 2 0. 535429	"*preferred*"), (0.074101, "*greatly preferred*")} P_3 = 0.690662 Ranking Options Preference degrees 1 Option 3 0. 690662 2 Option 1 0. 568095 3 Option 2 0. 532099

Table 8 Ranking of the design options

Relative importance of cost against safety	Option 3	Option 1	Option 2
0.1	1	2	3
0.2	1	2	3
0.5	1	2	3
1	1	2	3
2	1	2	3
5	1	2	3
10	1	2	3

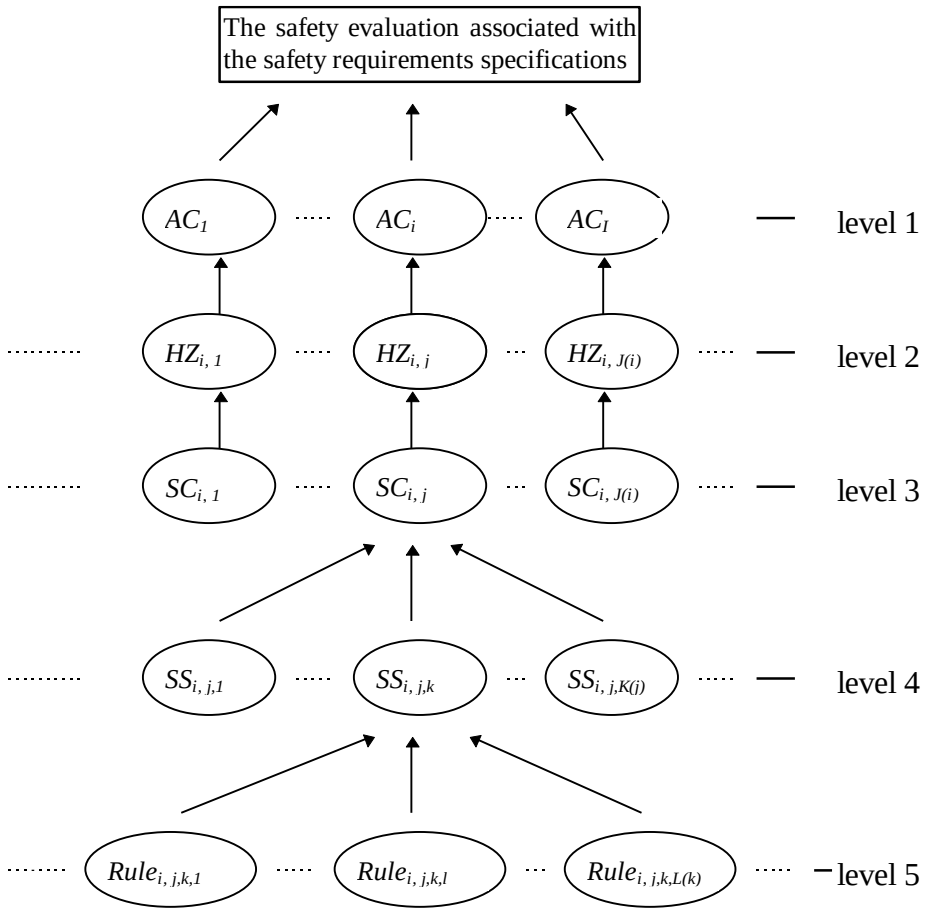

Fig. 1 A hierarchical framework for subjective safety analysis of safety requirements specifications

where AC_i represents the modelling of accident i;

I is the number of the possible accidents;

$HZ_{i,j}$ represents the modelling of hazard j associated with AC_i;

$J(i)$ is the number of the hazards associated with accident i;

$SC_{i,j}$ represents safety constraint j for $HZ_{i,j}$;

$SS_{i,j,k}$ represents safety strategy k for $SC_{i,j}$;

$K(j)$ is the number of the safety strategies for $SC_{i,j}$;

$Rule_{i,j,k,l}$ represents safety rule l associated with $SS_{i,j,k}$; and

$L(k)$ is the number of the safety rules for $SS_{i,j,k}$.

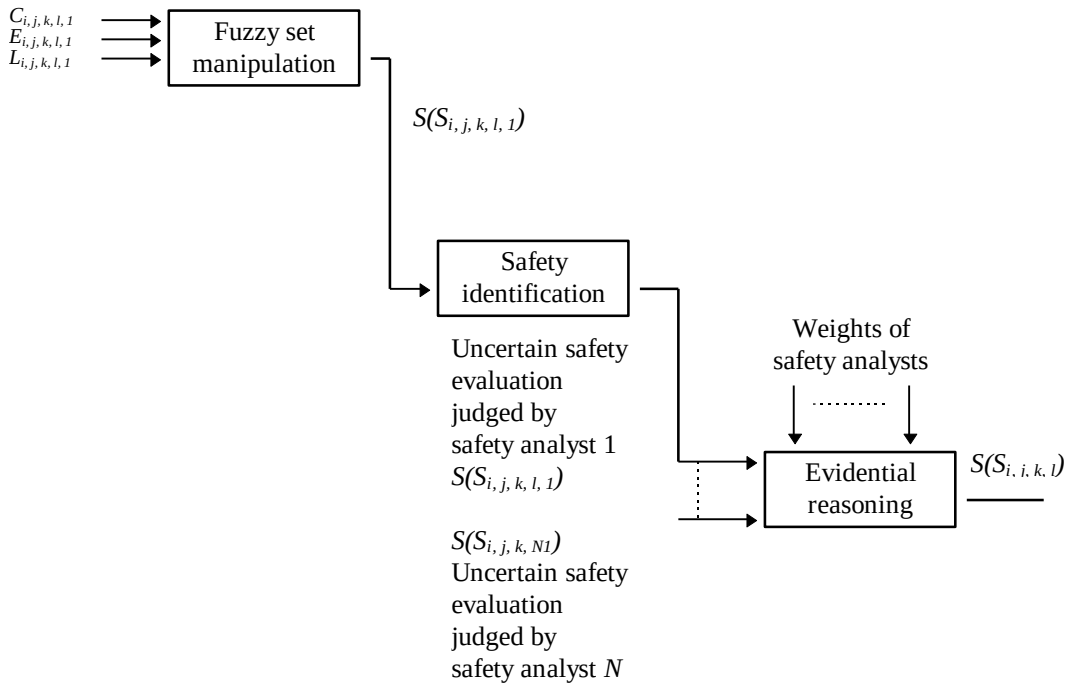

Fig. 2 A diagram for synthesising the judgments produced by multiple safety analysts

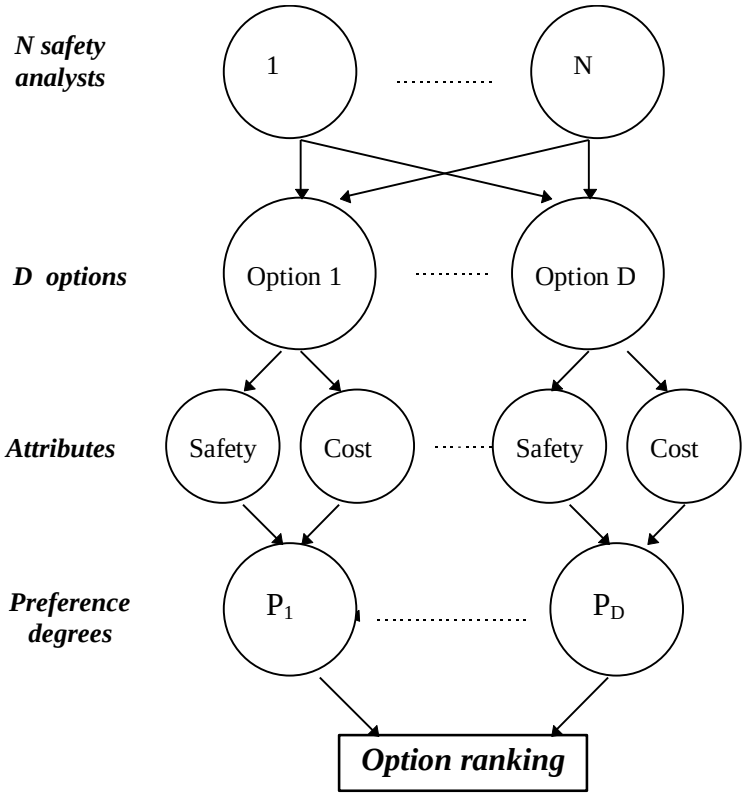

Fig. 3 A diagram for synthesis of safety and cost evaluations for option ranking

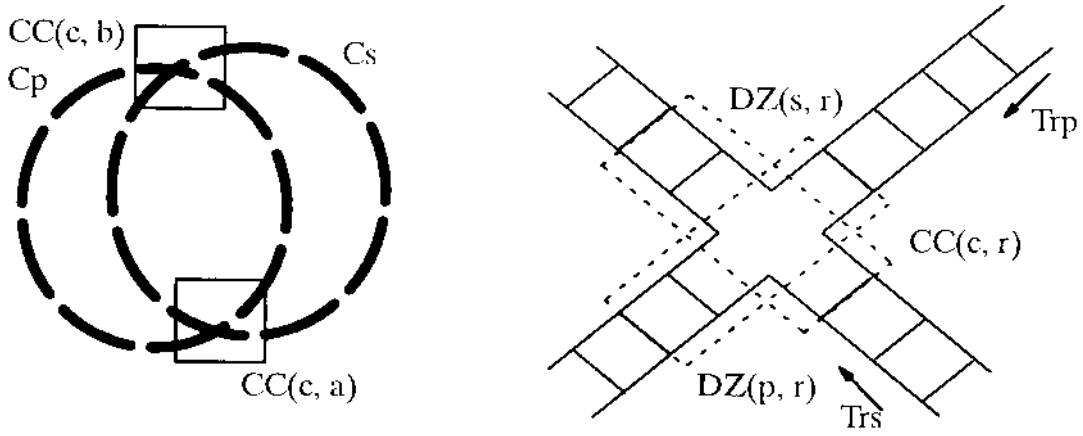

Fig. 4 The train set circuits and the crossing section

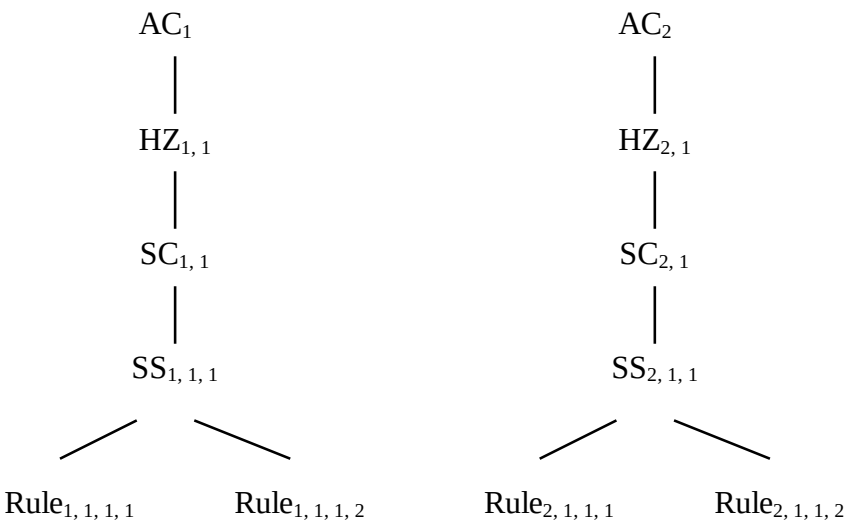

Fig. 5 Safety specification hierarchy of a train set example

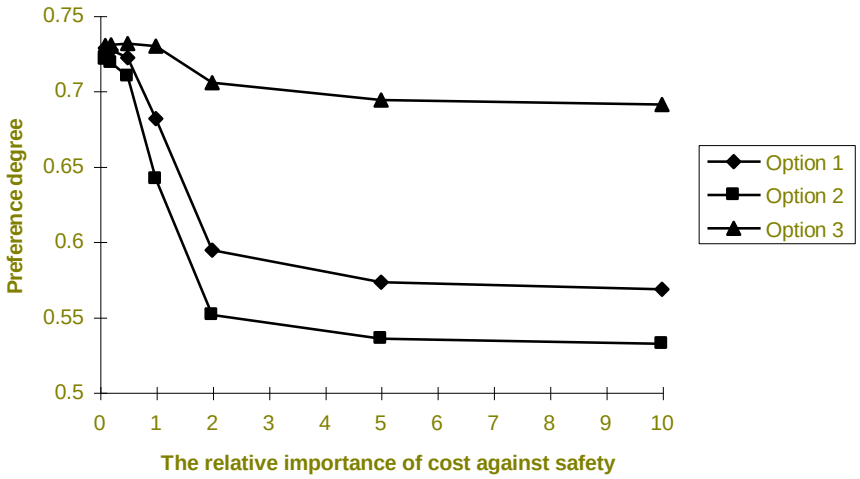

Fig. 6 The relative importance of cost against safety

Biography

Dr. Wang is Reader in Marine Engineering at Liverpool John Moores University (LJMU). He undertook two UK EPSRC and one EU (European Union) funded safety and reliability engineering research projects at Newcastle University from 1991 to 1995. He has been involved in marine and offshore engineering safety research for the past twelve years with support from the EPSRC, HSE, etc. His publications include over 80 technical papers in conference proceedings and international journals related to marine and offshore engineering safety assessment. He is currently directing a research group of 7 postdoctoral and doctoral research members in the areas of marine and offshore engineering safety/reliability assessment.

Dr. Yang is Senior Lecturer in Decision and System Sciences at the Manchester School of Management (MSM) of UMIST. Prior to this employment, he worked as Associate Professor in Systems Engineering at Shanghai Jiao Tong University of China in 1987-1989, Post-Doctoral Research Fellow at UMIST in 1990, Senior Research Fellow at the Engineering Design Centre of Newcastle University in 1991-1995, and Lecturer in Manufacturing Engineering and Operational Research at the University of Birmingham in 1995-1997. Dr Yang's research has been supported by many sources including the UK EPSRC. Dr. Yang has published three books and over 100 papers in national and international journals and conferences.