Subjective Safety Analysis of Safety Requirements Specifications

J. Wang[1], A. Saeed[2] and R. de Lemos[2]

[1]Department of Engineering and Technology Management
Liverpool John Moores University L3 3AF, UK
[2]Centre for Software Reliability, Department of Computing Science
University of Newcastle upon Tyne NE1 7RU, UK

Key words: Evidential reasoning, fuzzy sets, subjective safety analysis and safety requirements specifications.

Summary: *This report presents a method for subjective safety analysis of safety requirements specifications of software for safety–critical systems, that are organised in an hierarchical structure. The methodology incorporates fuzzy set modelling and evidential reasoning to assess the safety associated with safety requirements specifications. Fuzzy set theory is used to model the primitive elements (i.e. safety rules) of the requirements specifications and an evidential reasoning approach is employed to synthesize the information produced. Three basic parameters – failure likelihood, consequence severity and failure consequence probability are used to analyse a safety rule in terms of membership functions. The subjective safety description associated with the safety rule is then mapped back to the defined safety expressions which are also characterised in terms of membership functions. Such a mapping results in the production of the safety evaluation associated with the safety rule, expressed in terms of the degrees to which the subjective safety description belongs to the safety expressions. Such degrees represent uncertainty in the safety evaluation associated with the safety rule. The information produced for all safety rules can then be synthesized using an evidential reasoning approach to obtain the safety evaluation associated with the safety requirements specifications. The developed method is capable of dealing with multiple safety analysts who make judgements on each safety rule. A case study based on a train set crossing is used to demonstrate the method.*

1. Introduction

In recent years, advances in computer technology have been increasingly used to fulfil control tasks to reduce human error and to provide operators with a better working environment. This has resulted in the development of more and more software intensive systems. However, the utilisation of software in control systems has introduced new failure modes and created problems in the development of safety–critical systems. When developing software for safety–critical systems, one has to achieve the following two complementary goals.

- To develop the software in such a way that it is impossible or extremely unlikely that its behaviour will lead to a catastrophic failure of the system.
- To provide evidence for both the developers and the assessment authorities that the risk associated with the software is acceptable within the overall system risk.

An effective approach to achieve the above goals, is to conduct the safety analysis of software in parallel with traditional software development activities. From all the phases of software development, the phase of the analysis of safety requirements plays the most vital role since any defects in the safety requirements specifications may corrupt the subsequent phases of software development. In this paper, the analysis of safety requirements includes: *requirements analysis* which produces the safety requirements specifications, and the *safety analysis* of the safety requirements specifications which aims to reduce risks to a reasonable and acceptable level (within both economic and technical constraints) and provide evidence to support certification.

1.1 Methodology for the Analysis of Safety Requirements

The approach for subjective safety analysis, presented in this paper, is described in the context of a systematic approach to the analysis of safety requirements /de Lemos 94/, /Saeed 95a/. The systematic approach partitions the analysis into smaller phases; each phase corresponds to a domain of analysis (i.e. part of the system) in which requirements analysis and safety analysis are conducted in parallel. The results of applying the approach are encoded in an hierarchical structure, the Safety Specification Graph (SSG), which records the safety requirements specifications obtained during each phase, such as 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. The SSG records three kinds of relationships:

- *Coverage*. The absence of all hazards associated with an accidents should ensure that the accident does not occur.

- *Exclusion*. A safety constraint should exclude all the associated hazards.

•*Refinement*. A safety strategy should maintain all the specifications of the previous layer to which it is linked.

An SSG is represented as a linear graph, in which a *node* represents a safety specification and an *edge* denotes that a relationship exists between a pair of safety specifications. For a system for which *I* accidents have been identified, the SSG consists of *I* component graphs, one for each accident, a sample SSG is depicted in figure 1.

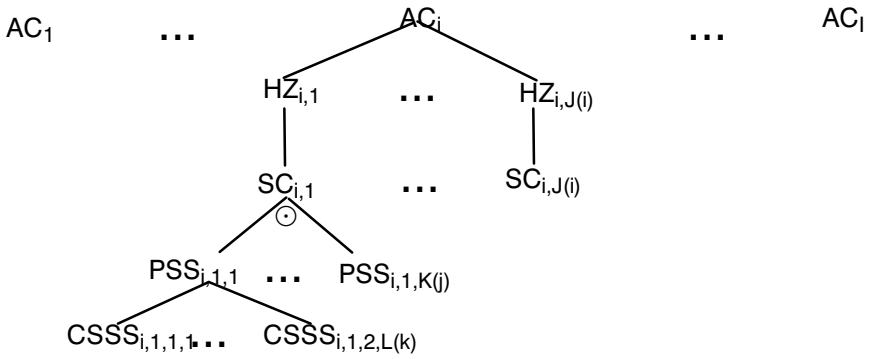

Figure 1. A sample of a Safety Specification Graph (SSG)

where AC_i represents accident i, I is the number of the possible accidents,
$HZ_{i,j}$ represents hazard j associated with AC_i , $J(i)$ is the number of the hazards.
$SC_{i,j}$ represents safety constraint j for $HZ_{i,j}$,
$PSS_{i,j,k}$ represents plant safety strategy k associated with $SC_{i,j}$, $K(j)$ is the number of plant safety strategies for $SC_{i,j}$.
$CSSS_{i,j,k,l}$ represents controlling system safety strategy l associated with $PSS_{i,j,k}$, $L(k)$ is the number of interface safety strategies for $PSS_{i,j,k}$.

1.2 Safety Analysis for Requirements Specifications

Safety analysis for the safety requirements specifications can be conducted on both qualitative and quantitative bases /Saeed 92/. Qualitative analysis has the aim to confirm that under normal circumstances the safety requirements specifications will prevent the system to enter a hazard state, identify possible violations of the requirements specifications and analyse their impact on safe behaviour. Quantitative safety analysis, however, deals with the uncertainty inherent in the evaluation of potential hazards and assessment of the safety associated with the safety requirements specifications. Quantitative safety analysis can be conducted on the basis of the probability distributions of basic failure events which affect the safety associated with the safety requirements specifications. Typical quantitative safety analysis techniques, such as Fault Tree Analysis (FTA), can be used to assess the safety associated with safety requirements specifications in terms of the probabilities of occurrence of serious system failures leading to catastrophic accidents.

However, in many cases, especially at the very early stages of software development, it may be difficult or even impossible to precisely determine probability distribution parameters for basic failure events due to the nature of software failure. Therefore, analysts may have to describe a basic failure event in terms of vague and imprecise descriptors like '*reasonably low*' or '*low*', terms that are commonly used by safety analysts /Wang 95/. These kinds of judgements are fuzzy in nature and may be more suitably studied using fuzzy set theory. Our literature search has shown that there is no application of subjective safety analysis incorporating fuzzy set modelling and evidential reasoning to requirements specifications of safety–critical software. The characteristics of the SSG that make it particularity amenable to a subjective analysis are as follows.

- The requirements specifications are expressed in a formal notation. This supports a better judgement over factors related to a single specification.

- The logical relationships between the different requirements specifications are explicitly encoded. Supporting a better judgement on factors dependent upon the interrelationships between specifications.

In this paper, the proposed methodology combines safety modelling of safety requirements specifications at the bottom level using fuzzy set theory and safety analysis of safety requirements specifications in a hierarchical process using an evidential reasoning approach.

2. A framework for Subjective Safety Analysis of Safety Specifications

The safety of a specification can be expressed by degrees to which it belongs to such linguistic variables as '*poor*', '*fair*', '*average*' and '*good*' – referred to as safety expressions. A fuzzy statement describing the extent to which the safety of a specification belongs to each safety expression, is referred to as the safety evaluation of that specification. The objective of subjective safety analysis for an SSG is to determine the safety evaluation of the specifications at the nodes of the SSG, thereby obtaining the safety evaluation associated with the SSG.

To conduct the subjective safety analysis for an SSG, issues related to the *boundaries* and *granularity* of the analysis need to be resolved. With regard to the boundaries, the starting layer for the subjective safety analysis depends on the phase of requirements analysis and the termination layer on the specification over which the safety targets are imposed. For example, if the safety targets are imposed over individual accidents, on completion of plant analysis the subjective safety analysis should start at the layer of the safety strategies and terminate at the accidents. The general scheme is to determine the safety evaluation of the specifications at the starting layer and then to propagate the safety evaluations through the layers of the SSG. At each step in the propagation the safety evaluation for the specifications of a new layer are determined, until the termination layer is reached. The approach used to propagate the safety evaluations is evidential reasoning, this avoids any information loss which may occur in the hierarchical evaluation of fuzzy information using fuzzy set theory as demonstrated in /Andersson 88//Keller 89/.

The safety evaluations for the specifications in the starting layer are determined by employing fuzzy set modelling. The granularity of the modelling depends upon the information available that describes the internal structure of the specifications at the starting layer (i.e. the extent to which they can be decomposed). In the case of safety strategies, as a minimum the analysis should be in terms of the safety rules that define the safety strategies. In general, it is appropriate to start the analysis at the most detailed level to allow the effective and efficient application of fuzzy set modelling. For example, if different failure modes were know for the safety rules these would provide a more appropriate starting point than the safety rules.

An example of an hierarchical subjective safety analysis of safety requirements specifications is shown in Figure 2. In this figure, an ellipse represents the safety evaluation of the named specification or rule (R(k) represents the number of safety rules that define the safety strategy $PSS_{i,j,k}$) and an arrow gives the propagation direction of safety analysis from one level to another.

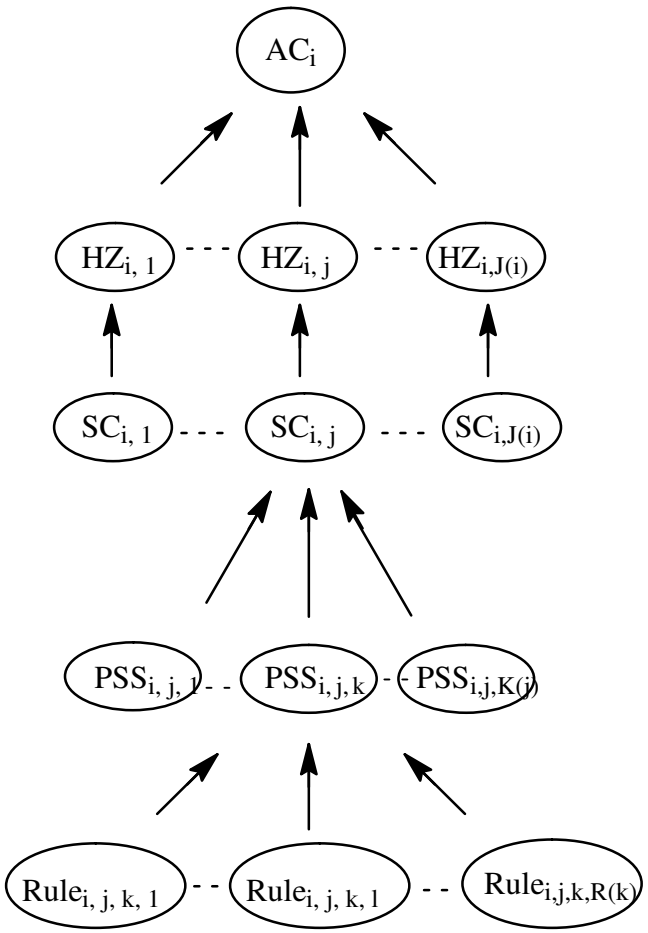

Figure 2. A hierarchical framework for subjective safety analysis

The subjective safety associated with a safety rule is modelled in terms of three basic parameters (i.e. failure likelihood, consequence severity and failure consequence probability) that are typically used to assess the safety associated with an event on a subjective basis /Karwowski 86/. 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. The subjective safety description associated with a safety

rule can be obtained by synthesizing the three associated basic parameters /Karwowski 86//Wang 95/. The subjective safety description can then be mapped back to the defined safety expressions and stated in terms of the extents to which it belongs to them. In this way, the uncertain safety evaluations associated with all safety rules can be produced. The uncertain safety evaluations associated with the safety rules can be combined to produce the safety evaluations for the safety strategies. This kind of synthesis can be progressed through the layers of the SSG. In the following sections, we discuss the concepts in more detail in the context of the scenario of figure 2.

3. Fuzzy Set Modelling

3.1 Fuzzy Safety Definition

The safety associated with $Rule_{i,\ j,\ k,\ l}$ can be modelled by studying the associated failure likelihood, consequence severity and failure consequence probability as described earlier. These three parameters can be described by linguistic variables which can be further described by membership functions. A membership function is a description which consists of membership values to categories. The typical linguistic variables for describing failure likelihood, consequence severity and failure consequence probability may be defined in terms of membership degrees belonging to the seven categories (shown in Tables 1, 2 and 3). The reasons for employing seven categories are: experience has shown that the number of categories should be limited to seven in order to produce reasonable results /Karwowski 86/, and seven categories have been most widely used by safety researchers. The membership degrees of the typical linguistic variables in each table are not exclusive with respect to a category, this makes it easier for safety analysts to make judgements on a safety rule. It is obviously possible to have some flexibility in the definition of membership functions for the typical linguistic variables to suit different situations.

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 judgements. The three parameters can be grouped into two categories.

3.1.1 Local Safety Parameter

The failure likelihood can be assigned by a safety analysts examining the safety rule, specifically by estimating the likelihood the safety rule will be violated. To estimate the failure likelihood, for example, an analyst would use such variables as *'highly frequent', 'frequent', 'reasonably frequent', 'average', 'reasonably low', 'low'* and '*very low'*.

3.1.2 Global Safety Parameters

The consequence severity and the failure consequence probability are parameters derived from specifications at higher layers. To estimate the consequence severity, an analyst would use such variables as '*catastrophic', 'critical', 'marginal*' and '*negligible*'. The consequence severity can be assigned studying the severity class of the potential accident caused by the violation of the safety rule (in fact, it should be the same for all safety rules connected to an accident). However, it may be comparatively difficult for safety analysts to assign membership degrees for the failure consequence probability,

Table 1 Failure likelihood

μ_L Linguistic variables	Categories 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 Linguistic variables	Categories 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

described using variables, such as '*definite', 'highly likely', 'reasonably likely', 'likely', 'reasonably unlikely', 'unlikely'* and '*highly* unlikely'. This is because it may be required to study the logical relations between safety strategies and between hazards leading to the accident. Suppose $E_{i,\,j,\,k,\,l}$ represents the fuzzy set of the failure consequence probability. Following factors need to be synthesized to assign $E_{i,\,j,\,k,\,l}$:

- the conditional probability $e_{i,\,j,\,k,\,l}$ that $PSS_{i,\,j,\,k}$ is violated given that $Rule_{i,\,j,\,k,\,l}$ is violated,

Table 3 Failure consequence probability

μ_E Linguistic variables	Categories 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

- the conditional probability $e_{i,\,j,\,k}$ that $SC_{i,\,j}$ is violated given that $PSS_{i,\,j,\,k}$ is violated, and
- the conditional probability $e_{i,\,j}$ that hazard j associated with accident i occurs given that $SC_{i,\,j}$ is violated, and
- the conditional probability $e_{i,\,j}^{HZ}$ that accident i happens given that hazard i associated with accident i occurs.

Multiple analysts may be involved in the identification of the individual conditional probabilities. The failure consequence probability is estimated on the basis of the individual probabilities; for example, if $e_{i,\,j,\,k,\,l}$, $e_{i,\,j,\,k}$, $e_{i,\,j}$ and $e_{i,\,j}^{HZ}$ are all estimated as '*low*', then the literal estimate for $E_{i,\,j,\,k,l}$ would be '*low*'. Obviously, experience together with an appreciation of the logical structure of the SSG would enable a more informed assignment of membership degrees of the failure consequence probability.

3.1.3 Combination of Parameters

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) and $C_{i,\,j,\,k,\,l}$ represents the fuzzy set of the consequence severity. The subjective safety description $S_{i,\,j,\,k,\,l}$ associated with $Rule_{i,\,j,\,k,\,l}$ can be defined as follows /Karwowski 86/:

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

where 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*:*

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

3.2 Fuzzy Safety Identification

It is commonly understood that 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 characterize them using membership degrees with respect to the same categories used in order to project the obtained subjective safety description back to the safety expressions. When characterizing the safety expressions, the conditions such as $\mu_{S^{poor}_{i,j,k,l}} = \mu_{C^{catastrophic}_{i,j,k\,l}} \; o \; \mu_{E^{definite}_{i,j,k,l}} \times \mu_{L^{frequent}_{i,j,k,l}}$ need to be satisfied to confine the safety expression space within the certain extent. The safety expressions also need to be defined to be exclusive to allow the evidential reasoning approach to be applied, and to be defined in such a way that a subjective safety description can be mapped back to them easily and effectively. The four safety expressions are defined as shown in Table 4.

Table 4 Four safety expressions

$\mu_{Si,j,k,l}$ Linguistic expressions	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

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 obtained using the Best–Fit method /Schmucker 84//Wang 95/ and is described by $\beta^{m}_{i,j,k,l}$ (*m = 1, 2, 3* or *4*), this can be calculated as follows /Wang 95/:

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 *m*th safety expression /Wang 95/:

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

$$\alpha^{m}_{i,\,j,\,k,\,l} = \frac{1}{d^{m}_{i,\,j,\,k,\,l} / d^{M}_{i,\,j,\,k,\,l}}$$

where $d^{m}_{i,\,j,\,k,\,l}$ is the Euclidean distance between $S_{i,\,j,\,k,\,l}$ and the *m*th 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*).

4. Hierarchical Propagation for Safety Synthesis

4.1 Fuzzy Set Modelling by Multiple Safety Analysts

If multiple safety analysts are involved in the safety analysis process, their judgements need to be synthesized. A diagram for synthesizing the judgements on a safety rule produced by multiple safety analysts is shown in Figure 3. Suppose there are *N* safety analysts who assign membership degrees for three basic safety parameters associated with a safety rule. Suppose $L_{i,\,j,\,k,\,l,\,n}$, $C_{i,\,j,\,k,\,l,\,n}$ and $E_{i,\,j,\,k,\,l,\,n}$ 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 back to the defined safety expressions to identify the uncertainty safety evaluation $S(S_{i,\,j,\,k,\,l,\,n})$ associated with $Rule_{i,\,j,\,k,\,l}$, as 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 *m*th safety expression. $S(S_{i,\,j,\,k,\,l,\,n})$ can be expressed in the following form:

$$S(S_{i,\,j,\,k,\,l,\,n}) = \{(\beta^{1}_{i,\,j,\,k,\,l,\,n},\ \text{'Poor'}),\ (\beta^{2}_{i,\,j,\,k,\,l,\,n},\ \text{'Fair'}),\ (\beta^{3}_{i,\,j,\,k,\,l,\,n},\ \text{'Average'}),\ (\beta^{4}_{i,\,j,\,k,\,l,\,n},\ \text{'Good'})\}$$

It is required to synthesize all $S(S_{i,\,j,\,k,\,l,\,n})$ (*n = 1,* · · ·, and *N*) to obtain the safety evaluation associated with $Rule_{i,\,j,\,k,\,l}$. An evidential reasoning approach can be employed to synthesize $S(S_{i,\,j,\,k,\,l,\,n})$ (*n = 1,* · · ·, and *N*) and take into account the weight of each safety analyst in such a synthesis process without losing any useful safety information.

The evidential reasoning approach is well suited for handling uncertain and inconsistent safety evaluations /Yang 94a//Yang 94b/. This approach 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. In Figure 2, whether the safety

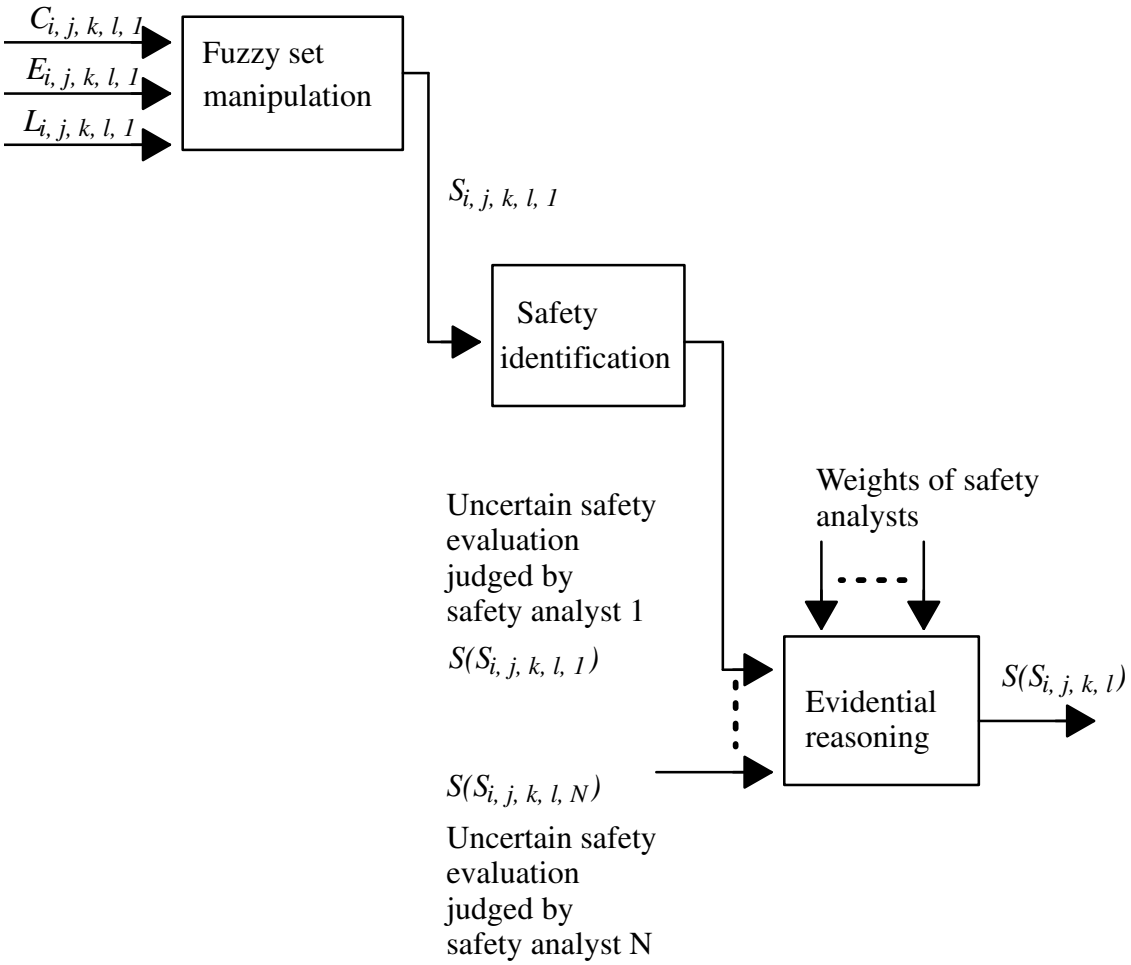

Figure 3 A diagram for synthesising the judgements produced by multiple safety analysts

evaluation associated with a safety rule belongs to '*poor*', '*fair*', '*average*' or '*good'* can be regarded as a hypothesis. If the judgement on a safety rule produced by a safety analyst is to some extent evaluated as '*good'*, for example, then the safety associated with the safety rule would be to some extent evaluated as '*good',* depending on the judgement itself and the weight of the safety analyst in the evaluation process. The application of the evidential reasoning approach provides a systematic way of synthesizing such uncertain safety evaluations involving multiple analysts' judgements to produce the safety evaluation for a safety rule.

4.2 Synthesis of the Judgements of Multiple Safety Analysts

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 $\lambda_{i,j,k,l,n}$ ($n = 1, \cdots$, or N) be the normalized relative weight of safety analyst n in the safety evaluation process where $0 \leq \lambda_{i,j,k,l,n} \leq 1$.The weight $\lambda_{i,j,k,l,n}$ ($n = 1, \cdots$, 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 confidence degree Ω of over 99.5 percent. The following formula can be used to obtain the value of $\lambda_{i,j,k,l,n}$ ($n = 1, \cdots$, or N) /Yang 94a/ /Yang 94b/:

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

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

where $\zeta_{i,j,k,l,n}$ ($n = 1, \cdots$, or N) is the relative weight of the nth safety analyst; $\zeta_{i,j,k,l,Max}$ is the largest value among $\zeta_{i,j,k,l,n}$ ($n = 1, \cdots$, 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 $\zeta_{i,j,k,l,n}$ ($n = 1, \cdots$, and N), $\varepsilon_{i,j,k,l}$ can be calculated and $\lambda_{i,j,k,l,n}$ can then be obtained.

Suppose $M^m_{i,j,k,l,n}$ ($n = 1, \cdots$, 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 ($m = 1, 2, 3$ or 4). Then, $M^m_{i,j,k,l,n}$ can be obtained as follows /Wang 95//Yang 94b/:

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

Suppose $M^H_{i,j,k,l,n}$ ($n = 1, \cdots$, 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 /Wang 95/:

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

Suppose $MM^m_{i,j,k,l,n}$ ($m = 1, 2, 3$ or 4; $n = 1, \cdots$, 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 synthesis of the judgements produced by safety analysts $1, \cdots$, and 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 synthesis of the judgements produced by safety analysts $1, \cdots$, and n. The algorithm for synthesizing the analysts' judgements to obtain the safety evaluation associated with $Rule_{i,j,k,l}$ can be stated as follows /Yang 94b/:

Initial conditions: $MM^{m}_{i,\,j,\,k,\,l,\,1} = M^{m}_{i,\,j,\,k,\,l,\,1}$ $\qquad MM^{H}_{i,\,j,\,k,\,l,\,1} = M^{H}_{i,\,j,\,k,\,l,\,1}$

$$\{H_m\} \quad MM^{m}_{i,j,k,l,n+1} = K_{i,j,k,l,n+1}(MM^{m}_{i,j,k,l,n}\ M^{m}_{i,j,k,l,n+1} +$$

$$MM^{m}_{i,j,k,l,n}\ M^{H}_{i,j,k,l,n+1} + MM^{H}_{i,j,k,l,n}\ M^{m}_{i,j,k,l,n+1})$$

$$m = 1,\ 2,\ 3,\ 4$$

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

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

$$n = 1, \cdots, N-1$$

N–1 iterations of the above algorithm are required to obtain the degree (i.e. $MM^{m}_{i,\,j,\,k,\,l,N}$) to which the safety evaluation associated with $Rule_{i,\,j,\,k,\,l}$ belongs to H_m *(m = 1, 2, 3* or *4)*.

For example, if $S(S_{1,1,1,1,1}) = \{(0.1, \text{'poor'}), (0.2, \text{'fair'}), (0.5, \text{'average'}), (0.2, \text{'good'})\}$ and $S(S_{1,1,1,1,2}) = \{(0.2, \text{'poor'}), (0.2, \text{'fair'}), (0.4, \text{'average'}), (0.2, \text{'good'})\}$, the combination of these two safety evaluations can be obtained as follows:

Suppose $\lambda_{1,\,1,\,1,\,1,\,1} = 0.8$ and $\lambda_{1,\,1,\,1,\,1,\,2} = 0.4$. $M^{m}_{1,1,1,1,1}$, $M^{m}_{1,1,1,1,2}$ and $MM^{m}_{1,1,1,1,1}$ (*m = 1, 2, 3* and *4*) can be obtained as follows:

$$[\ M^{1}_{1,1,1,1,1}\quad M^{2}_{1,\,1,\,1,\,1,\,1}\quad M^{3}_{1,1,1,1,1}\quad M^{4}_{1,1,1,1,1}\ ] = [0.08\ \ 0.16\ \ 0.4\ \ 0.16]$$

$$[\ M^{1}_{1,1,1,1,2}\quad M^{2}_{1,1,1,1,2}\quad M^{3}_{1,1,1,1,2}\quad M^{4}_{1,1,1,1,2}\ ] = [0.08\ \ 0.08\ \ 0.16\ \ 0.08]$$

$$[\ MM^{1}_{1,1,1,1,1}\quad MM^{2}_{1,1,1,1,1}\quad MM^{3}_{1,1,1,1,1}\quad MM^{4}_{1,1,1,1,1}\ ]$$

$$= [\ M^{1}_{1,1,1,1,1}\quad M^{2}_{1,\,1,\,1,\,1,\,1}\quad M^{3}_{1,1,1,1,1}\quad M^{4}_{1,1,1,1,1}\ ] = [0.08\ \ 0.16\ \ 0.4\ \ 0.16]$$

$MM^{H}_{1,1,1,1,1}$ and $M^{H}_{1,1,1,1,2}$ can be obtained by:

$MM^{H}_{1,1,1,1,1} = 0.2 \quad M^{H}_{1,1,1,1,2} = 0.6$

$K_{1,1,1,1,2}$ and $MM^{H}_{1,1,1,1,2}$ can then be obtained as follows:

$K_{1,1,1,1,2} = 1.289 \quad MM^{H}_{1,1,1,1,2} = 0.155$

$MM^{m}_{1,1,1,1,2}$ ($m = 1, 2, 3$ and 4) can finally be obtained as follows:

$[\ MM^{1}_{1,1,1,1,2} \ \ MM^{2}_{1,1,1,1,2} \ \ MM^{3}_{1,1,1,1,2} \ \ MM^{4}_{1,1,1,1,2}\ ] = [0.09\ 0.161\ 0.433\ 0.161]$

The above result means that the combination of the two safety evaluations has a degree of 15.5 percent as remaining belief unassigned, 9 percent to which it is confirmed to '*Poor*', 16.1 percent to '*fair*', 43.3 percent to '*average*' and 16.1 percent to '*good*'.

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

4.3 Hierarchical Propagation of Safety Evaluations

After the safety evaluation associated with each safety rule has been obtained, it is required to synthesize the safety evaluations associated with all $Rule_{i,j,k,l}$ ($l = 1, \cdots, R(K)$) to obtain the safety evaluation associated with $SS_{i,j,k}$. Then the safety evaluations produced for all $SS_{i,j,k}$ ($k = 1, \cdots,$ and $K(j)$) need to be synthesized 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 a component graph. The detailed evaluation is described as follows with respect to each level shown in Figure 2.

4.3.1. Safety Evaluation for Safety Strategies

The fact that the safety associated with $Rule_{i,j,k,l}$ is confirmed to H_m ($m = 1, 2, 3$ or 4) to the extent of $\beta^{m}_{i,j,k,l}$ (i.e. $MM^{m}_{i,j,k,l,N}$) can be viewed as a piece of evidence when the safety associated with $PSS_{i,j,k}$ is evaluated to H_m. Evidential reasoning can then be used to combine the different pieces of evidence using the process is discussed in section 4.2.

he normalized relative weight for a rule ($\lambda_{i,j,k,l}$) is different from the one of $\lambda_{i,j,k,l,n}$. The latter reflects the importance of safety analyst n who estimates the safety associated with $Rule_{i,j,k,l}$, whereas the former reflects a correlation factor between the rules; for example, if the violation of $Rule_{i,j,k,l}$ is likely to cause violations in the other rules than a high relative weight will be associated with the rule. The normalised

weight $\lambda_{i,j,k,l}$ can be calculated on the basis of the relative weights of the safety rules for $PSS_{i,j,k}$ using a formula similar to that for calculating $\lambda_{i,j,k,l,n}$. Suppose $\zeta_{i,j,k,l}$ represents the relative weight of $Rule_{i,j,k,l}$. $\zeta_{i,j,k,l}$ can be assigned by studying the logical relations between $Rule_{i,j,k,l}$ and other safety rules for $PSS_{i,j,k}$ and studying the relative confidence in safety analysis of $Rule_{i,j,k,l}$. Suppose $M^m_{i,j,k,l}$ is a degree to which the safety evaluation associated with $Rule_{i,j,k,l}$ supports the hypothesis that the safety evaluation associated with $PSS_{i,j,k}$ is confirmed to H_m. Suppose $M^H_{i,j,k,l}$ is the remaining belief unassigned after commitment of belief to all H_m ($m = 1, 2, 3$ and 4) for $S(S_{i,j,k,l})$. The problem can be solved in a way similar to that described in the last subsection if $\lambda_{i,j,k,l}$ is treated as $\lambda_{i,j,k,l,n}$, $M^m_{i,j,k,l}$ as $M^m_{i,j,k,l,n}$, $M^H_{i,j,k,l}$ as $M^H_{i,j,k,l,n}$, l as n, $R(K)$ as N, $MM^H_{i,j,k,l}$ as $M^H_{i,j,k,l,n}$, $MM^m_{i,j,k,l}$ as $MM^m_{i,j,k,l,n}$ and $\beta^m_{i,j,k,l}$ as $\beta^m_{i,j,k,l,n}$. The safety evaluation associated with $PSS_{i,j,k}$ can then be obtained as follows:

$$S(S_{i,j,k}) = \{(\beta^1_{i,j,k}, \text{'Poor'}), (\beta^2_{i,j,k}, \text{'Fair'}), (\beta^3_{i,j,k}, \text{'Average'}), (\beta^4_{i,j,k}, \text{'Good'})\}$$

where $\beta^m_{i,j,k}$ ($m = 1, 2, 3$ or 4) represents the extent to which the safety evaluation associated with $PSS_{i,j,k}$ belongs to the mth safety expression and is equal to $MM^H_{i,j,k,L(k)}$ which can be obtained using the evidential reasoning algorithm.

4.3.2. Safety Evaluation for Safety Constraints

The fact that the safety associated with $PSS_{i,j,k}$ is confirmed to H_m ($m = 1, 2, 3$ or 4) to the extent of $\beta^m_{i,j,k}$ can be viewed as a piece of evidence when the safety associated with $SC_{i,j}$ is evaluated to H_m. Suppose $\lambda_{i,j,k}$ is the normalized relative weight of $SS_{i,j,k}$ in the evaluation of the safety associated with $SC_{i,j}$. In a similar way, $\lambda_{i,j,k}$ can be calculated on the basis of the relative weights of safety strategies for $SC_{i,j}$. Suppose $\zeta_{i,j,k}$ ($k = 1, \cdots,$ or $K(j)$) is the relative weight of safety strategy k. $\zeta_{i,j,k}$ can be assigned by studying the relations between safety strategy k and other safety strategies for $SC_{i,j}$ and studying the relative confidence in safety analysis of safety strategy k. Evidential reasoning can then be used to combine the different pieces of evidence using the process for safety strategies (in section 4.3.1). The result will be:

$$S(S_{i,j}) = \{(\beta^1_{i,j}, \text{'Poor'}), (\beta^2_{i,j}, \text{'Fair'}), (\beta^3_{i,j}, \text{'Average'}), (\beta^4_{i,j}, \text{'Good'})\}$$

where $\beta^m_{i,j}$ ($m = 1, 2, 3$ or 4) represents the extent to which the safety evaluation associated with $SC_{i,j}$ belongs to the mth safety expression and is equal to $MM^m_{i,j,K(j)}$.

4.3.3. Safety Evaluation for Hazards

From Figure 2, it can be observed that the safety evaluation associated with $HZ_{i,j}$ is completely determined by the safety evaluation associated with $SC_{i,j}$. Suppose $\lambda_{i,j}^{HZ}$ is the normalized relative weight of $SC_{i,j}$ in the evaluation of the safety associated with $HZ_{i,j}$. The safety evaluation $S(S_{i,j}^{HZ})$ associated with $HZ_{i,j}$ can be obtained as follows:

$$S(S_{i,j}^{HZ}) = \{(\beta_{i,j}^{1}(HZ), \text{ 'Poor'}), (\beta_{i,j}^{2}(HZ), \text{ 'Fair'}), (\beta_{i,j}^{3}(HZ), \text{ 'Average'}), (\beta_{i,j}^{4}(HZ), \text{ 'Good'})\}$$

where $\beta_{i,j}^{m}(HZ)$ *(m = 1, 2, 3* or *4)* represents the extent to which the safety evaluation associated with $HZ_{i,j}$ belongs to the *m*th safety expression and is equal to $\lambda_{i,j}^{HZ} \times \beta_{i,j}^{m}$.

4.3.4. Safety Evaluation for Accidents

The fact that the safety associated with $HZ_{i,j}$ is confirmed to H_m to the extent of $\beta_{i,j}^{m}(HZ)$ can be viewed as a piece of evidence when the safety associated with AC_i is evaluated to H_m. Further suppose the analysts determine $\lambda_{i,j}$ is the normalized relative weight of $HZ_{i,j}$ in the evaluation of the safety associated with AC_i. Evidential reasoning can then be used to combine the different pieces of evidence using the process for safety strategies. The safety evaluation associated with AC_i can then be obtained as follows:

$$S(S_i) = \{(\beta_i^1, \text{ 'Poor'}), (\beta_i^2, \text{'Fair'}), (\beta_i^3, \text{ 'Average'}), (\beta_i^4, \text{ 'Good'})\}$$

where β_i^m (*m = 1, 2, 3* or *4*) represents the extent to which the safety evaluation associated with AC_i belongs to the *m*th safety expression and is equal to $MM_{i,1}^{m}$.

4.3.5. Composition of Safety Evaluations of Component Graphs

The fact that the safety associated with AC_i is confirmed to H_m to the extent of β_i^m can be viewed as a piece of evidence when the safety associated with the SSG is evaluated to H_m. Suppose MM_i^m is a degree of confidence that the safety associated with the safety requirements specifications is confirmed to H_m as a result of the synthesis of all AC_p (p = *1,* · · ·, and i). Suppose MM_i^H 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 all AC_p (p = *1,* · · ·, and i). The problem then becomes how to obtain MM_i^m and MM_i^H from β_i^m (i = *1,* · · ·, and I; m = *1, 2, 3* and *4*). Suppose λ_i is the normalized relative weight of AC_i in the evaluation of the safety associated with the safety requirements specifications. In a similar way, λ_i can be calculated on the basis of the relative weights of accidents (i.e. based on the relative likelihood that a particular accident will cause

another accident). Suppose M_i^m is the degree to which the safety evaluation associated with AC_i supports the hypothesis that the safety evaluation associated with the safety requirements specifications is confirmed to H_m. Suppose M_i^H is the remaining belief unassigned after commitment of belief to all H_m (m = *1, 2, 3* and *4*) for AC_i. The problem can be solved in a way similar to that for synthesizing the safety evaluation for each component graph if λ_i is treated as $\lambda_{i,j}$, and β_i^m as $\beta_{i,j}^m$. The safety evaluation associated with the SSG can then be obtained as follows:

$$S(S) = \{(\beta^1, \text{'Poor'}), (\beta^2, \text{'Fair'}), (\beta^3, \text{'Average'}), (\beta^4, \text{'Good'})\}$$

5. An Example

With the aim of exemplifying the proposed framework for analysing safety requirements specifications on a subjective basis, 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 /Saeed 92//Saeed 94/. In this paper, the proposed subjective safety analysis framework is demonstrated on the basis of the safety requirements specifications produced in /Saeed 92/.

5.1 Process Description and Safety Specification Graph

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 Cp and trains of type Trs travel around circuit Cs; both types of train travel in one direction (clockwise) only. The longest train is shorter than the smallest section. The circuits Cp and Cs, and the crossing sections are illustrated in Figure 3

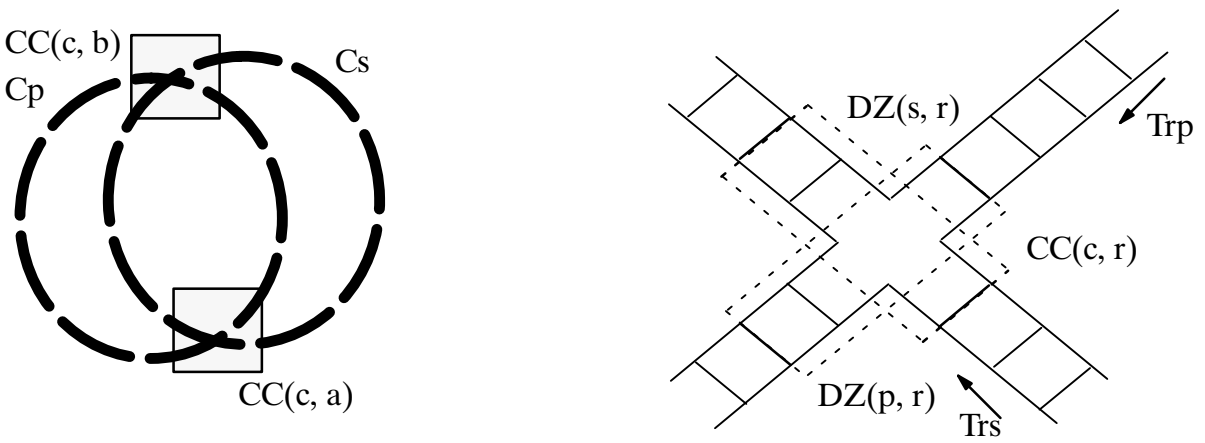

Figure 3 The train set circuits and the crossing section

Suppose the type of circuit is denoted by c ∈ L, L = {p, s}, the crossing section by r ∈ R, R ={a, b}, and suppose the trains which run on Cc are denoted by x, y ∈ Trc = {1, · · · , Ntc}. Addition ⊕ and

subtraction $\ominus$ on circuit section numbers are performed modulo the number of sections of the circuit. The danger zone on circuit Cc for CC(c, r) is defined as: DZ(c, r)={CC(c, r), CC(c, r)$\oplus$1}. The danger zones DZ(p, r) and DZ(s, r) for a crossing section CC(c, r) are illustrated in Figure 3. 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 Cc, and Rtrain(c, x) the reservation set of train x on circuit Cc.

For the purposes of this case study we will consider only two types of accidents on the train set. The safety specification graph for the train set crossing over which the approach to subjective safety analysis will be applied, is presented in Figure 4.

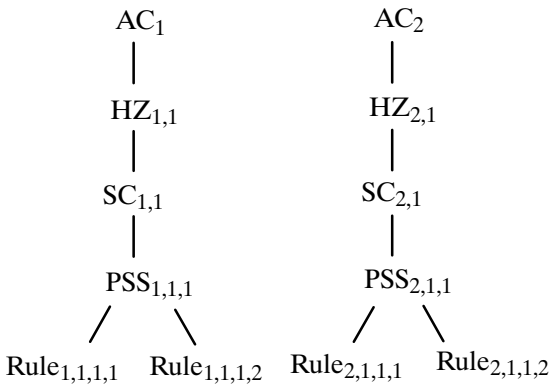

Figure 4 Safety specification graph of train set example

Accidents

AC_1 − trains of the same type collide;
AC_2 − trains of different type collide.

Hazards

$HZ_{1,1}$ − some part of any two trains are in the same section.
$HZ_{2,1}$ − some part of a primary train and a secondary train are in the same crossing section.

Safety Constraints

$SC_{1,1}$ − for any two trains there must be at least one section between the sections containing the fronts of the trains.

$SC_{2,1}$ − either the front of no primary train is in a danger zone DZ(p, r) or the front of no secondary train is in the danger zone DZ(s, r).

Plant Safety Strategies

$PSS_{1,1,1}$ − the basic rules for the strategy for $SC_{1,1}$ are:

$Rule_{1,1,1,1}$. for any train, the current section (i.e. the position of the front of the train) and the section behind the current section must always be reserved;
$Rule_{1,1,1,2}$. no section can be reserved by more than one train.

$PSS_{2,1,1}$ − the basic rules for the strategy for $SC_{2,1}$ are:

$Rule_{2,1,1,1}$. if any train x on circuit Cc is in a danger zone then the crossing section contained within that danger zone is reserved (on circuit Cc);
$Rule_{2,1,1,1}$. section CC(p, r) and section CC(s, r) cannot both be reserved.

5.2 Safety Rule Modelling

Four safety rules $Rule_{1,1,1,1}$, $Rule_{1,1,1,2}$, $Rule_{2,1,1,1}$ and $Rule_{2,1,1,2}$ can be modelled using the developed fuzzy set modelling method. Suppose there are four safety analysts who make judgements on each safety rule. $Rule_{1,1,1,1}$ is modelled in detail as shown below. Other three safety rules are modelled in a similar way. The assignments of the basic failure consequence probabilities of the safety rules are based upon the conditional probabilities for the failure consequences of the safety specifications. The evaluations presented in this section are for illustrative purposes only.

$Rule_{1,1,1,1}$

Suppose safety analyst *1* makes the judgement on $Rule_{1,1,1,1}$ as follows:

- The associated failure likelihood is approximately '*reasonably low*' and may vary about '*reasonably low*'.
- The associated consequence severity is '*critical*'.
- The conditional probability that $PSS_{1,1,1}$ is violated given that $Rule_{1,1,1,1}$ is violated, is '*highly likely*' and may vary about '*highly likely'*, the conditional probability that $SC_{1,1}$ is violated given that $PSS_{1,1,,1}$ is violated, is '*highly likely*', the conditional probability that $HZ_{1,1}$ happens given that $SC_{1,1}$ is violated, is '*highly likely*', and the conditional probability that AC_1 happens given that $HZ_{1,1}$ occurs, is '*highly likely*' and may vary about '*highly likely*'. The associated failure consequence probability can then be judged to be approximately '*highly likely*' and may vary about '*highly likely*'.

With respect to Tables 1, 2 and 3, safety analyst *1* may assign failure likelihood $L_{1,1,1,1,1}$, consequence severity $C_{1,1,1,1,1}$ and failure consequence probability $E_{1,1,1,1,1}$ as follows:

$L_{1,1,1,1,1}$ = {1/0, 2/0.3, 3/1.0, 4/0.7, 5/0, 6/0, 7/0}
$C_{1,1,1,1,1}$ = {1/0, 2/0, 3/0, 4/0.75, 5/1, 6/0.25, 7/0}
$E_{1,1,1,1,1}$ = {1/0, 2/0, 3/0, 4/0, 5/0.7, 6/1, 7/0.3}

Subjective safety description $S_{1,1,1,1,1}$ can be obtained as follows:

$S_{1,1,1,1,1} = C_{1,1,1,1,1} \circ E_{1,1,1,1,1} \times L_{1,1,1,1,1} = \{1/0, 2/0.3, 3/0.7, 4/0.7, 5/0, 6/0, 7/0\}$

Mapping back to the safety expressions, $S(S_{1,1,1,1,1})$ can be obtained as follow:

$S(S_{1,1,1,1,1}) = \{(0.128099, \text{'poor'}), (0.160233, \text{'fair'}), (0.570981, \text{'average'}), (0.140687, \text{'good'})\}$

Suppose safety analyst *2* makes the judgement on $Rule_{1,1,1,1}$ that

- the associated failure likelihood is '*reasonably low*',
- the associated consequence severity is approximately '*critical*' and may vary about '*critical*' and
- the associated failure consequence probability is approximately '*highly likely*' and may vary about '*highly likely*'.

With respect to Tables 1, 2 and 3, safety analyst *2* may assign $L_{1,1,1,1,2}$, $C_{1,1,1,1,2}$ and $E_{1,1,1,1,2}$ as follows:

$L_{1,1,1,1,2} = \{1/0, 2/0.25, 3/1.0, 4/0.75, 5/0, 6/0, 7/0\}$
$C_{1,1,1,1,2} = \{1/0, 2/0, 3/0, 4/0.8, 5/1, 6/0.2, 7/0\}$
$E_{1,1,1,1,2} = \{1/0, 2/0, 3/0, 4/0, 5/0.7, 6/1, 7/0.3\}$

The safety can be evaluated as follows:

$S_{1,1,1,1,2} = C_{1,1,1,1,2} \circ E_{1,1,1,1,2} \times L_{1,1,1,1,2} = \{1/0, 2/0.25, 3/0.7, 4/0.7, 5/0, 6/0, 7/0\}$
$S(S_{1,1,1,1,2}) = \{(0.128011, \text{'poor'}), (0.160602, \text{'fair'}), (0.573031, \text{'average'}), (0.138356, \text{'good'})\}$

Suppose safety analyst *3* makes the judgement on $Rule_{1,1,1,1}$ that

- the associated failure likelihood is '*reasonably low*',
- the associated consequence severity is '*critical*' and
- the associated failure consequence probability is approximately '*highly likely*' and may vary about '*highly likely*'.

With respect to Tables 1, 2 and 3, safety analyst *3* may assign $L_{1,1,1,1,3}$, $C_{1,1,1,1,3}$ and $E_{1,1,1,1,3}$ as follows:

$L_{1,1,1,1,3} = \{1/0, 2/0.25, 3/1, 4/0.75, 5/0, 6/0, 7/0\}$
$C_{1,1,1,1,3} = \{1/0, 2/0, 3/0, 4/0.75, 5/1, 6/0.25, 7/0\}$
$E_{1,1,1,1,3} = \{1/0, 2/0, 3/0, 4/0, 5/0.8, 6/1, 7/0.2\}$

The safety can be evaluated as follows:

$S_{1,1,1,1,3} = C_{1,\,1,\,1,\,1,\,3} \circ E_{1,\,1,\,1,\,1,\,3} \times L_{1,\,1,\,1,\,1,\,3} = \{1/0, 2/0.25, 3/0.8, 4/0.75, 5/0, 6/0, 7/0\}$
$S(S_{1,1,1,1,3}) = \{(0.116689, \text{'poor'}), (0.145145, \text{'fair'}), (0.612872, \text{'average'}), (0.125293, \text{'good'})\}$

Suppose safety analyst *4* makes the judgement on $Rule_{1,\,1,\,1,\,1}$ that

- the associated failure likelihood is between '*low*' and '*reasonably low*',
- the associated consequence severity is approximately '*critical*' and may vary about '*critical*' and
- the associated failure consequence probability is between '*reasonably likely*' and '*highly likely*'.

With respect to Tables 1, 2 and 3, safety analyst *4* may assign $L_{1,\,1,\,1,\,1,\,4}$, $C_{1,\,1,\,1,\,1,4}$ and $E_{1,\,1,\,1,\,1,\,4}$ as follows:

$L_{1,\,1,\,1,\,1,\,4} = \{1/0.1, 2/0.7, 3/0.8, 4/0.4, 5/0, 6/0, 7/0\}$
$C_{1,\,1,\,1,\,1,\,4} = \{1/0, 2/0, 3/0, 4/0.6, 5/0.9, 6/0.4, 7/0.1\}$
$E_{1,\,1,\,1,\,1,\,4} = \{1/0, 2/0, 3/0, 4/0.6, 5/0.9, 6/0.4, 7/0.1\}$

The safety can be evaluated as follows:

$S_{1,\,1,\,1,\,1,\,4} = C_{1\,,\,1,\,1,\,1,\,4} \circ E_{1,\,1,\,1,\,1,\,4} \times L_{1,\,1,\,1,\,1,\,4} = \{1/0.1, 2/0.7, 3/0.8, 4/0.4, 5/0, 6/0, 7/0\}$
$S(S_{1,\,1,\,1,\,1,\,4}) = \{(0.147666, \text{'poor'}), (0.167962, \text{'fair'}), (0.487627, \text{'average'}), (0.196745, \text{'good'})\}$

$Rule_{1,\,1,\,1,\,2}$

$L_{1,\,1,\,1,\,2,\,1} = \{1/0.25, 2/1, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$
$C_{1,\,1,\,1,\,2,\,1} = \{1/0, 2/0, 3/0, 4/0.75, 5/1, 6/0.25, 7/0\}$
$E_{1,\,1,\,1,\,2,\,1} = \{1/0, 2/0, 3/0, 4/0, 5/0.7, 6/1, 7/0.3\}$
$S_{1,1,1,2,1} = C_{1,\,1,\,1,\,2,\,1} \circ E_{1\,,1,\,1,\,2,\,1} \times L_{1,\,1,\,1,\,2,\,1} = \{1/0.25, 2/0.7, 3/0.7, 4/0, 5/0, 6/0, 7/0\}$
$S(S_{1,1,1,2,1}) = \{(0.175496, \text{'poor'}), (0.184576, \text{'fair'}), (0.364160, \text{'average'}), (0.275768, \text{'good'})\}$

$L_{1,\,1,\,1,\,2,\,2} = \{1/0, 2/0.3, 3/1, 4/0.7, 5/0, 6/0, 7/0\}$
$C_{1,\,1,\,1,\,2,\,2} = \{1/0, 2/0, 3/0, 4/0.8, 5/1, 6/0.2, 7/0\}$
$E_{1,\,1,\,1,\,2,\,2} = \{1/0, 2/0, 3/0, 4/0, 5/0.75, 6/1, 7/0.25\}$
$S_{1,1,1,2,2} = C_{1,\,1,\,1,\,2,\,2} \circ E_{1,\,1,\,1,\,2,\,2} \times L_{1,\,1,\,1,\,2,\,2} = \{1/0, 2/0.3, 3/0.75, 4/0.7, 5/0, 6/0, 7/0\}$
$S(S_{1,1,1,2,2}) = \{(0.118872, \text{'poor'}), (0.147588, \text{'fair'}), (0.603353, \text{'average'}), (0.130194, \text{'good'})\}$

$L_{1,\,1,\,1,\,2,\,3} = \{1/0.2, 2/1, 3/0.7, 4/0, 5/0, 6/0, 7/0\}$
$C_{1,\,1,\,1,\,2,\,3} = \{1/0, 2/0, 3/0, 4/0.75, 5/1, 6/0.25, 7/0\}$
$E_{1,\,1,\,1,\,2,\,3} = \{1/0, 2/0, 3/0, 4/0, 5/0.75, 6/1, 7/0.25\}$
$S_{1,1,1,2,3} = C_{1,\,1,\,1,\,2,\,3} \circ E_{1,\,1,\,1,\,2,\,3} \times L_{1,\,1,\,1,\,2,\,3} = \{1/0.2, 2/0.75, 3/0.7, 4/0, 5/0, 6/0, 7/0\}$
$S(S_{1,1,1,2,3}) = \{(0.177418, \text{'poor'}), (0.186412, \text{'fair'}), (0.364218, \text{'average'}), (0.271952, \text{'good'})\}$

$L_{1,1,1,2,4} = \{1/0.25, 2/1, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$
$C_{1,1,1,2,4} = \{1/0, 2/0, 3/0, 4/0.6, 5/0.9, 6/0.3, 7/0.1\}$
$E_{1,1,1,2,4} = \{1/0, 2/0, 3/0, 4/0, 5/0.7, 6/1, 7/0.3\}$
$S_{1,1,1,2,4} = C_{1,1,1,2,4} \circ E_{1,1,1,2,4} \times L_{1,1,1,2,4} = \{1/0.25, 2/0.7, 3/0.7, 4/0, 5/0, 6/0, 7/0\}$
$S(S_{1,1,1,2,4}) = \{(0.175496, \text{'poor'}), (0.184576, \text{'fair'}), (0.364160, \text{'average'}), (0.275768, \text{'good'})\}$

$\underline{Rule_{2,1,1,1}}$

$L_{2,1,1,1,1} = \{1/0.25, 2/1, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$
$C_{2,1,1,1,1} = \{1/0, 2/0, 3/0, 4/0, 5/0, 6/0.75, 7/1\}$
$E_{2,1,1,1,1} = \{1/0, 2/0, 3/0, 4/0, 5/0.75, 6/1, 7/0.25\}$
$S_{2,1,1,1,1} = C_{2,1,1,1,1} \circ E_{2,1,1,1,1} \times L_{2,1,1,1,1} = \{1/0.25, 2/0.75, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$
$S(S_{2,1,1,1,1}) = \{(0.175496, \text{'poor'}), (0.184576, \text{'fair'}), (0.364160, \text{'average'}), (0.275768, \text{'good'})\}$

$L_{2,1,1,1,2} = \{1/0.2, 2/1, 3/0.7, 4/0, 5/0, 6/0, 7/0\}$
$C_{2,1,1,1,2} = \{1/0, 2/0, 3/0, 4/0, 5/0, 6/0.75, 7/1\}$
$E_{2,1,1,1,2} = \{1/0, 2/0, 3/0, 4/0, 5/0.75, 6/1, 7/0.25\}$
$S_{2,1,1,1,2} = C_{2,1,1,1,2} \circ E_{2,1,1,1,2} \times L_{1,1,1,1,2} = \{1/0.2, 2/0.75, 3/0.7, 4/0, 5/0, 6/0, 7/0\}$
$S(S_{2,1,1,1,2}) = \{(0.177419, \text{'poor'}), (0.186412, \text{'fair'}), (0.364218, \text{'average'}), (0.271953, \text{'good'})\}$

$L_{2,1,1,1,3} = \{1/0.25, 2/1, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$
$C_{2,1,1,1,3} = \{1/0, 2/0, 3/0, 4/0, 5/0, 6/0.75, 7/1\}$
$E_{2,1,1,1,3} = \{1/0, 2/0, 3/0, 4/0, 5/0.75, 6/1, 7/0.25\}$
$S_{2,1,1,1,3} = C_{2,1,1,1,3} \circ E_{2,1,1,1,3} \times L_{2,1,1,1,3} = \{1/0.25, 2/0.75, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$
$S(S_{2,1,1,1,3}) = \{(0.175134, \text{'poor'}), (0.183683, \text{'fair'}), (0.367365, \text{'average'}), (0.273818, \text{'good'})\}$

$L_{2,1,1,1,4} = \{1/0, 2/0.25, 3/1.0, 4/0.75, 5/0, 6/0, 7/0\}$
$C_{2,1,1,1,4} = \{1/0, 2/0, 3/0, 4/0, 5/0, 6/0.75, 7/1\}$
$E_{2,1,1,1,4} = \{1/0, 2/0, 3/0, 4/0.1, 5/0.8, 6/0.9, 7/0.2\}$
$S_{2,1,1,1,4} = C_{2,1,1,1,4} \circ E_{2,1,1,1,4} \times L_{2,1,1,1,4} = \{1/0, 2/0.25, 3/0.75, 4/0.75, 5/0, 6/0, 7/0\}$
$S(S_{2,1,1,1,4}) = \{(0.124688, \text{'poor'}), (0.156304, \text{'fair'}), (0.584837, \text{'average'}), (0.134171, \text{'good'})\}$

$\underline{Rule_{2,1,1,2}}$

$L_{2,1,1,2,1} = \{1/0, 2/0.25, 3/1.0, 4/0.75, 5/0, 6/0, 7/0\}$
$C_{2,1,1,2,1} = \{1/0, 2/0, 3/0, 4/0, 5/0, 6/0.75, 7/1\}$
$E_{2,1,1,2,1} = \{1/0, 2/0, 3/0, 4/0, 5/0.75, 6/1, 7/0.25\}$
$S_{2,1,1,2,1} = C_{1,1,1,2,1} \circ E_{2,1,1,2,1} \times L_{2,1,1,2,1} = \{1/0, 2/0.25, 3/0.75, 4/0.75, 5/0, 6/0, 7/0\}$
$S(S_{2,1,1,2,1}) = \{(0.124688, \text{'poor'}), (0.156304, \text{'fair'}), (0.584837, \text{'average'}), (0.134171, \text{'good'})\}$

$L_{2,1,1,2,2} = \{1/0.25, 2/1, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$
$C_{2,1,1,2,2} = \{1/0, 2/0, 3/0, 4/0, 5/, 6/0.75, 7/1\}$
$E_{2,1,1,2,2} = \{1/0, 2/0, 3/0, 4/0.3, 5/0.8, 6/0.7, 7/0.2\}$

$S_{2,1,1,2,2} = C_{2,1,1,2,2} \circ E_{2,1,1,2,2} \times L_{2,1,1,2,2} = \{1/0.25, 2/0.7, 3/0.7, 4/0, 5/0, 6/0, 7/0\}$
$S(S_{2,1,1,2,2})$= {(0.175496, 'poor'), (0.184576, 'fair'), (0.364160, 'average'), (0.275286, 'good')}

$L_{2,1,1,2,3} = \{1/0.25, 2/1, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$
$C_{2,1,1,2,3} = \{1/0, 2/0, 3/0, 4/0, 5/0, 6/0.75, 7/1\}$
$E_{2,1,1,2,3} = \{1/0, 2/0, 3/0, 4/0.3, 5/0.8, 6/0.7, 7/0.2\}$
$S_{2,1,1,2,3} = C_{2,1,1,2,3} \circ E_{2,1,1,2,3} \times L_{2,1,1,2,3} = \{1/0.25, 2/0.7, 3/0.7, 4/0, 5/0, 6/0, 7/0\}$
$S(S_{2,1,1,2,3})$= {(0.175496, 'poor'), (0.184576, 'fair'), (0.364160, 'average'), (0.275786, 'good')}

$L_{2,1,1,2,4} = \{1/0, 2/0.25, 3/1, 4/0.75, 5/0, 6/0, 7/0\}$
$C_{2,1,1,2,4} = \{1/0, 2/0, 3/0, 4/0, 5/0, 6/0.75, 7/1\}$
$E_{2,1,1,2,4} = \{1/0, 2/0, 3/0, 4/0, 5/0.75, 6/1, 7/0.25\}$
$S_{2,1,1,2,4} = C_{2,1,1,2,4} \circ E_{2,1,1,2,4} \times L_{2,1,1,2,4} = \{1/0, 2/0.25, 3/0.75, 4/0.75, 5/0, 6/0, 7/0\}$
$S(S_{2,1,1,2,4})$ = {(0.124688, 'poor'), (0.156304, 'fair'), (0.584873, 'average'), (0.134171, 'good')}

5.3 Safety Synthesis

Synthesis of the judgements of the safety analysts

Suppose the relative weights of four safety analysts in evaluation of safety are 2, 1, 2 and 1, respectively. Then $[\zeta_{i,j,k,l,1}\ \zeta_{i,j,k,l,2}\ \zeta_{i,j,k,l,3}\ \zeta_{i,j,k,l,4}]^T = [2\ \ 1\ \ 2\ \ 1]^T$ where $i = 1$ or 2; $j = 1$; and $k = 1$.

$\lambda_{i,j,k,l,n}$ (n =1, 2, 3 and 4) are calculated as follows:

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

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

Using the evidential reasoning algorithm, the safety evaluations associated with $Rule_{1,1,1,1}$, $Rule_{1,1,1,2}$, $Rule_{2,1,1,1}$ and $Rule_{2,1,1,2}$ are obtained as follows:

$S(S_{1,1,1,1})$ = {(0.050260, 'poor'), (0.069216, 'fair'), (0.806370, 'average'), (0.058581, 'good')}
$S(S_{1,1,1,2})$ = {(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'), (0.133126, 'good')}

Safety Evaluation for Safety Strategies

Suppose $[\zeta_{1,1,1,1}\ \zeta_{1,1,1,2}]^T$ 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:

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

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:

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

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

$S(S_{1,1,1}) = \{(0.068534, \text{'poor'}), (0.078407, \text{'fair'}), (0.696841, \text{'average'}), (0.137151, \text{'good'})\}$
$S(S_{2,1,1}) = \{(0.049794, \text{'poor'}), (0.060850, \text{'fair'}), (0.760025, \text{'average'}), (0.113180, \text{'good'})\}$

Safety Evaluation for Safety constraints

$\lambda_{1,1,1}$ 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:

$S(S_{1,1}) = \{(0.068191, \text{'poor'}), (0.078015, \text{'fair'}), (0.693357, \text{'average'}), (0.136456, \text{'good'})\}$
$S(S_{2,1}) = \{(0.049545, \text{'poor'}), (0.060546, \text{'fair'}), (0.756225, \text{'average'}), (0.112614, \text{'good'})\}$

Safety Evaluation for Hazards

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

$$\lambda^{HZ}_{1,1} = 0.9950 \ ; \ \lambda^{HZ}_{2,1} = 0.9950$$

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

$S(S^{HZ}_{1,1}) = \{(0.067850, \text{'poor'}), (0.077625, \text{'fair'}), (0.689890, \text{'average'}), (0.135780, \text{'good'})\}$
$S(S^{HZ}_{2,1}) = \{(0.049297, \text{'poor'}), (0.060243, \text{'fair'}), (0.752444, \text{'average'}), (0.112051, \text{'good'})\}$

Safety Evaluation for Accidents

$\lambda_{1,1}$ 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:

$S(S_1) = \{(0.067511, \text{'poor'}), (0.077237, \text{'fair'}), (0.686441, \text{'average'}), (0.135104, \text{'good'})\}$
$S(S_2) = \{(0.049051, \text{'poor'}), (0.059942, \text{'fair'}), (0.748681, \text{'average'}), (0.111491, \text{'good'})\}$

Combination of Safety Analysis for the Component Graphs

Suppose $[\zeta_1\ \zeta_2]^T$ is obtained as $[1\ \ 2]^T$ 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 the safety requirements specifications is finally obtained as follows:

$$S(S) = \{(0.035199, \text{'poor'}), (0.043240, \text{'fair'}), (0.811309, \text{'average'}), (0.084147, \text{'good'})\}$$

5.4. Discussion of Results

It can be seen that the four safety rules have been to a large extent judged as '*average*' by four safety analysts. For example, $Rule_{1,1,1,2}$ has been judged as '*poor*' with a belief of 11.8872 percent, as '*fair*' with 14.7548 percent, as '*average*' with 60.3353 percent and as '*good*' with 13.0159 percent by safety analyst *2*. The safety evaluations of the four safety rules should to a large extent belong to '*average*'. This is consistent with the results produced for the four safety rules. For example, the safety of $Rule_{1,1,1,1}$ has been evaluated as '*poor*' with a belief of 5.0260 percent, as '*fair*' with 6.9216 percent, as '*average*' with 80.6370 percent and as '*good*' with 5.8581 percent. The safety associated with each safety strategy should also be evaluated to a large extent as '*average*'. This is also consistent with the results produced for the two safety strategies. Since in this example the safety evaluation associated with $PSS_{i,j,k}$ ($i=1$ or 2; $j=1$; $k=1$) determines the safety evaluation associated with $SC_{i,j}$ and the safety evaluation associated with $HZ_{i,j}$ determines the safety evaluation associated with AC_i, $S(S_{i,j,k})$ and $S(S^{HZ}_{i,j})$ should be approximately equal to $S(S_{i,j})$ and $S(S_i)$, respectively. This is in harmony with the results produced for $PSS_{i,j,k}$, $SC_{i,j}$, $HZ_{i,j}$ and AC_i ($i=1$ or 2; $j=1$; $k=1$). The slight differences are caused by the fact that the confidence degree Ω is not equal to 100 percent. Since the safety associated with each AC_i ($i=1$ and 2) has been evaluated to a large extent as '*average*' the safety associated with the safety requirements specifications should also be evaluated to a large extent as '*average*'. This is also in harmony with the produced safety evaluation associated with the safety requirements specifications, which has been evaluated as '*poor*' with a belief of 3.5199 percent, as '*fair*' with 4.3240 percent, as '*average*' with 81.1309 percent and as '*good*' with 8.4147 percent.

The above information provides an exposition of the safety evaluation of the software requirements specifications for the software designers. This exposition supports the localization of modifications to the software requirements specifications by providing safety information at the different levels of the specification hierarchy.

6. Concluding Remarks

A methodology incorporating fuzzy set modelling and evidential reasoning is proposed for subjective safety analysis of safety requirements specifications of software for safety–critical systems. In this

methodology, a fuzzy set modelling method is used to analyse the safety associated with a safety rule, which is judged in terms of three basic parameters (i.e. failure likelihood, consequence severity and failure consequence probability) by multiple safety analysts. An evidential reasoning approach is then used to synthesize the information produced to obtain the safety evaluation associated with the safety requirements specifications. The combination of fuzzy set modelling and evidential reasoning provides safety–critical software analysts with flexibility in articulating judgements about the safety assessments associated with safety rules and with a rational tool for processing the safety information for hierarchical safety evaluation. The proposed methodology can be used as an alternative approach for analysts to conduct safety analysis of safety requirements specifications of software for safety–critical systems, especially in the situations where there is a lack of quantitative safety data for use in probabilistic risk analysis and where non–numerical safety data is dealt with.

It should be noted that in this paper this methodology is applied to carry out safety analysis of safety requirements specifications initially at the safety rule level. It may be more suitable to carry out a Failure Mode, Effects and Criticality Analysis (FMECA) of each safety rule and then to apply the proposed methodology initially at the failure mode level. This may make it more effective and efficient for safety analysts to make judgements. Other factors such as assumptions on the basis of which safety strategies are produced may also need to be taken into account to increase the effectiveness of the methodology in order to facilitate more practical applications.

The presented methodology can be enhanced with the introduction of a comparative analysis stage, to examine the safety evaluation for the safety requirements specifications against stipulated safety values. This comparison can be conducted most effectively between stipulated values for the hazards and estimated values for the safety constraints. Modifications to the approach presented here would include: the introduction of a procedure to allocate stipulated values to the hazards derived from their associated accidents and a procedure for the comparison of the estimated and stipulated values.

This report has provided some support for the feasibility of the application of subjective safety analysis for requirements specifications. However, the issue of how to integrate the approach with traditional safety analysis techniques and the other techniques emerging from ISAT has yet to be addressed. It is expected that the main vehicle for the technical integration will be the safety specification graph. Provided it is possible to project an SSG from the modelling abstraction employed for the requirements specification, the methodology described here can be applied to the specifications. Elsewhere our work /de Lemos 95/, /Saeed 95a/ has illusrated that an SSG can be projected from a number of modellling abstractions, including object–oriented models. Other factors, that will support integration are the work on a general framework and case studies to be prepared by IASE and JSI.

7. Acknowledgement

The authors would like to acknowledge the financial support of COPERNICUS Joint Research Project 1594. The authors would also like to thank Dr. J. B. Yang of Birmingham University for allowing the authors to use his software.

8. References

/Andersson 88/ L. Andersson, *The theory of possibility and fuzzy sets: new ideas for risk analysis and decision making*, Swedish Council for Building Research, 1988.

/de Lemos 94/ R. de Lemos, A. Saeed and T. Anderson, *On the safety analysis of requirements specifications*, Proceedings of 13th International Conference on Computer Safety, Reliability and Security (SAFECOMP'94), Ed. Victor Maggioli, Anaheim, CA, October 1994, 217–227.

/de Lemos 95/ R. de Lemos, B. Fields, A. Saeed. "*Analysis of Safety Requirements in the Context of System Faults and Human Errors*". Proceedings of the IEEE International Symposium and Workshop on Systems Engineering of Computer Based Systems. Tucson, Arizona. March 1995.

/Karwowski 86/ W. Karwowski and A. Mital, *Potential applications of fuzzy sets in industrial safety engineering,* Fuzzy Sets and Systems, Vol. 19, 1986, 105–120.

/Keller 89/ A. Z. Keller and Kara–Zaitri, *Further application of fuzzy logic to reliability assessment and safety analysis,* Micro Reliab., Vol. 29, No. 3, 1989, 399–404.

/Saeed 92/ A. Saeed, R. de Lemos and T. Anderson, *An approach to the assessment of requirements specifications for safety–critical systems*, TR–381, Department of Computing Science, University of Newcastle upon Tyne, April 1992, 21p

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

/Saeed 95a/ A. Saeed, R. de Lemos and T. Anderson. "*Safety Analysis for Requirements Specifications: Methods and Techniques*". Proceedings of IFAC Workshop SAFECOMP' 95. Beligirate, Italy. October 1995. pp. 27–41.

/Saeed 95b/ A. Saeed. R. de Lemos, T. Anderson. "On the Safety Analysis of Requirements Specifications for Safety–Critical Software". *ISA Transactions.* Vol. 34. No. 4. November 1995. pp. 283–295.

/Schmucker 84/ K. J. Schmucker, *Fuzzy sets, natural language computations and risk analysis*, Computer Science Press, 1984.

/Wang 95/ J. Wang, J. B. Yang and P. Sen, *Safety analysis and synthesis using fuzzy set modelling and evidential reasoning,* Reliability Engineering and System Safety, Vol. 47, 1995, 103–118.

/Yang 94a/ J. B. Yang and M. G. Singh, *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.

/Yang 94b/ J. B. Yang and P. Sen, *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.