ELSEVIER

0951-8320(94)00053-0

Reliability Engineering and System Safety **47** (1995) 103–118

0951-8320/95/$9.50

Safety analysis and synthesis using fuzzy sets and evidential reasoning

J. Wang, J. B. Yang & P. Sen

Engineering Design Centre, University of Newcastle upon Tyne, Newcastle upon Tyne, NE1 7RU, UK

(Received 28 December 1993; accepted 29 August 1994)

This paper presents a new methodology for safety analysis and synthesis of a complex engineering system with a structure that is capable of being decomposed into a hierarchy of levels. In this methodology, fuzzy set theory is used to describe each failure event and an evidential reasoning approach is then employed to synthesise the information thus produced to assess the safety of the whole system. Three basic parameters—failure likelihood, consequence severity and failure consequence probability, are used to analyse a failure event. These three parameters are described by linguistic variables which are characterised by a membership function to the defined categories. As safety can also be clearly described by linguistic variables referred to as the safety expressions, the obtained fuzzy safety score can be mapped back to the safety expressions which are characterised by membership functions over the same categories. This mapping results in the identification of the safety of each failure event in terms of the degree to which the fuzzy safety score belongs to each of the safety expressions. Such degrees represent the uncertainty in safety evaluations and can be synthesised using an evidential reasoning approach so that the safety of the whole system can be evaluated in terms of these safety expressions. Finally, a practical engineering example is presented to demonstrate the proposed safety analysis and synthesis methodology.

1 INTRODUCTION

The growing technical complexity of large engineering systems and the public concern regarding their safety have aroused great interest in the development of scientific and objective methods of demonstrating system safety.

The safety of a large engineering system is affected by many factors regarding its design, manufacturing, installation, commissioning, operation and maintenance. Consequently, it may be extremely difficult, if not impossible, to construct an accurate and complete mathematical model for the system in order to assess the safety because of inadequate knowledge about the basic failure events. This leads inevitably to problems of uncertainty in representation.

Problems of uncertainty in safety analysis can be treated using two principal types of method involving probability and possibility, respectively. Probability methods deal with uncertainty which is essentially random in nature but of an ordered kind. Probabilistic methods are based on a mature scientific theory.[2] Possibility methods (non-probabilistic methods) study problems which are not really probabilistic but cause uncertainty due to imprecision associated with the complexity of a system as well as vagueness of human judgement. Possibility methods are still developing and often use fuzzy sets, possibility theory and belief functions.[2]

Traditionally, safety analysis is carried out on a probabilistic basis. Probability distributions are used to describe a set of states for a system and to deal with uncertainty in order to evaluate potential hazards and assess system safety. In many cases, however, it may be difficult or even impossible to precisely determine the parameters of a probability distribution for a given event due to lack of evidence or due to the inability of the safety engineer to make firm assessments. Therefore, one may have to describe a given event in terms of vague and imprecise descriptors such as '*likely*' or '*impossible*', terms that are commonly used by safety analysts. Such judgements are obviously fuzzy and non-probabilistic, and hence non-probabilistic methods such as fuzzy set modelling may

be more appropriate to analyse the safety of systems with incomplete information of the kind described above.

The last two decades have seen an explosion in research and publications in the areas of non-probabilistic theories and their applications.[2] A few of these may be briefly outlined as follows:

(i) Bayesian modelling with imprecise prior probabilities.[5] An extension of the standard Bayesian approach based on the theory of imprecise probabilities and intervals of measures is developed to reflect expert opinions using prior distributions. The opinions of several experts can be combined using the approach developed.
(ii) Modelling of risk using approximate reasoning and fuzzy sets.[9] Linguistic variables are used to assess the risk of an event.
(iii) Identification of hazardous events using fuzzy set theory.[10,11] A survey of the possible applications of fuzzy logic is carried out with respect to the analysis of hazardous events.
(iv) Application of fuzzy sets and possibility theory for risk analysis and decision making.[1] Subjective linguistic assignments are modelled for risk analysis using fuzzy set theory.
(v) Use of fuzzy set theory for uncertainty analysis.[4] The potential applicability of fuzzy set theory to uncertainty analysis of accident progression event trees with imprecise and uncertain branch probabilities and/or with a number of phenomenological uncertainty issues is examined as a possible alternative procedure to that used in the current probabilistic risk assessments.

Example (i) suffers from the numerical stability problems involved in Bayesian modelling, as indicated in Ref. 6. Examples (ii)–(iv) mainly focus on safety assessment of a single failure event, and are not concerned either with safety synthesis of many events at a single level or with safety synthesis at different levels (component level, subsystem level and system level). Example (v) causes the loss of safety information due to the use of min-max operations in the process of safety synthesis. Such information loss could be rather serious in safety analysis of large and complex engineering systems.

The safety of a system is determined by the constituent subsystems and the safety of each subsystem is, in turn, determined by the associated components and their possible failure modes. In a hierarchical structure, it is usually the case that safety analysis at a high level makes use of the information produced at lower levels. There is therefore a need to develop a framework for hierarchical system safety analysis. Such a framework could be established by developing an approach using fuzzy sets and belief functions in an integrated manner, and it is largely the aim of this paper to present such an approach.

Figure 1 shows a diagram of a framework for safety analysis of an engineering system. Safety analysis of an engineering system should be carried out by taking into account such an evaluation hierarchy. In Fig. 1, a failure mode at the bottom level can be initially analyzed and described using fuzzy sets. The fuzzy safety score of the failure mode can thus be obtained. On the other hand, a set of linguistic variables may be used to express various safety levels. Such linguistic variables may be referred to as safety expressions, which can also be described using fuzzy sets. The obtained fuzzy safety description of the failure mode could then be mapped back to the defined safety expressions using the so-called best-fit method.[14] In the mapping, each of the safety expressions may be confirmed to some extent, depending upon the obtained fuzzy safety description of the failure mode as well as the defined fuzzy descriptions of the safety expressions. The degree of confirmation to a safety expression representing a safety level could then be viewed as a degree of confidence with which the safety associated with a failure mode is evaluated to the given safety level. Such uncertainty can conveniently be handled using an evidential reasoning approach, which has been developed on the basis of the Dempster-Shafer theory to deal with hierarchical evaluation problems with uncertainty.[17–19,21]

In this way, the safety associated with all failure modes can be evaluated with respect to the safety levels defined. Then, these uncertain evaluations of the failure modes associated with a component can be combined to produce an evaluation of the safety of the component using the evidential reasoning algorithm. Similarly, the uncertain evaluations for the components of a subsystem can be synthesised to evaluate subsystem safety. The safety of the whole system can finally be assessed by synthesising the safety information of the subsystems.

In this paper, the proposed methodology combines safety modelling of failure modes at the bottom level using fuzzy set theory and safety assessment of the whole system using the evidential reasoning approach.

2 SYSTEM MODELLING FOR SAFETY ANALYSIS AND SYNTHESIS

Section 1 has examined how an engineering system may be composed of several subsystems which can be further broken down to the component level. Traditionally, the safety of a system is estimated by analysing each of its constituent components. Such analyses could be carried out by identifying the

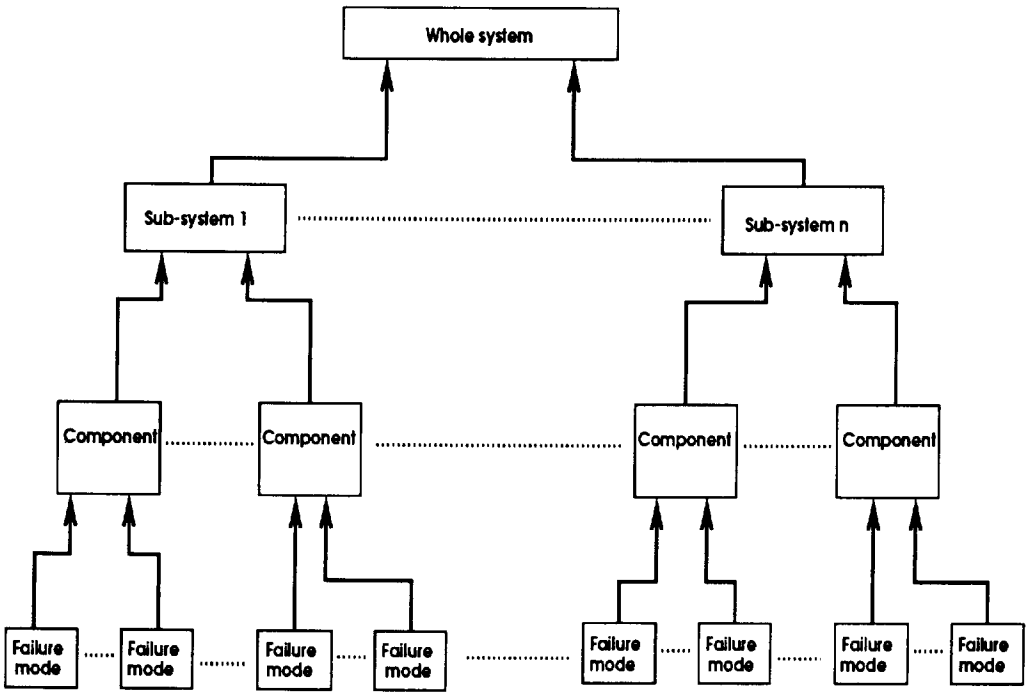

Fig. 1. The diagram of a safety analysis for an engineering system.

following information for each component using a Failure Mode, Effects and Criticality Analysis (FMECA).[16]

(i) Each failure mode.
(ii) Failure likelihood of occurrence of each identified failure mode.
(iii) Possible consequences, described by the severity class of the resulting effects where such a severity class may be defined by one of the following linguistic variables:

catastrophic: involving death and/or system loss;
critical: involving severe injury and/or major system damage;
marginal: involving minor injury and/or minor system damage;
negligible: involving no injury and negligible damage to the system.

(iv) Failure consequence probability defining the likelihood that the failure effects of the identified failure mode will occur, given that the failure mode has taken place.

Given the above information, the component failure mode criticality number (C) under a particular severity class can be calculated as follows:[13]

$$C = \sum_{i=1}^{N} E_i L_i t$$

where E_i = failure consequence probability of failure mode i,
L_i = likelihood of occurrence of failure mode i,
N = number of the failure modes of the component, which fall under a particular severity classification,
t = duration of applicable mission phase.

After all criticality numbers of a component under all severity classes have been obtained, a criticality matrix can be constructed which provides a means of identifying and comparing each failure mode to all others with respect to the same severity class. The resulting matrix display shows the distributions of criticality of component failure modes and provides a tool for assigning priorities for corrective action.

From the above, it can be seen that there are three basic parameters (i.e. failure likelihood, consequence severity and failure consequence probability) which are used in assessing the safety associated with each failure mode of a component. The safety level associated with a particular failure mode is determined by these three parameters and the product of these three parameter values is called the 'safety score'[7,9] if consequence severity can be described numerically. Safety scores are often used in the judgement of safety where a high safety score represents poor safety and a low safety score represents good safety. The safety score of a component is the sum of the safety scores of the associated failure modes and the safety score of a system can be synthesised by similarly processing the information produced for each of its constituent components.

In the traditional method discussed above, it is

implicitly assumed that the consequence severity of a failure mode is described by linguistic variables, and the failure likelihood and the failure consequence probability are assumed to take numerical values. However, the failure likelihood and the failure consequence probability are affected by so many factors in real life that it may be difficult to define them precisely in numerical terms as the probabilities may often be made on the basis of subjective judgements. Such subjective judgements are especially meaningful when one deals with non-numerical data. In fact, it has sometimes been argued that although human beings find quantitative prediction of safety difficult they may be comparatively efficient at qualitative assessments using linguistic variables.[14] To describe the likelihood of occurrence of a failure mode, for example, one may often use linguistic variables such as 'highly frequent', 'frequent', 'reasonably frequent', 'average', 'reasonably low', 'low' and 'very low'. To describe a failure consequence probability, linguistic variables such as 'definite', 'highly likely', 'reasonably likely', 'likely', 'reasonably unlikely', 'unlikely' and 'highly unlikely' may be used.

It may also be noted that in the above discussion it is assumed that the consequence severity, the failure likelihood or the failure consequence probability of a failure mode only belongs to one of the linguistic descriptions used to describe the respective extent. For instance, the consequence severity of a failure mode only belongs to one of the four severity classes: 'catastrophic', 'critical', 'marginal' and 'negligible'. However, such a description may at times be inadequate. For example, the consequence severity of failure mode may be something between 'catastrophic' and 'critical' or even between 'catastrophic' and 'negligible'.

Fuzzy set theory is well suited to model such subjective linguistic variables. In fuzzy set theory, linguistic variables used in describing failure likelihood, consequence severity and failure consequence probability can be characterised by their membership functions to a set of categories which describe the degrees of failure likelihood, severity class and failure consequence probability and which are usually graduated from low to high. For instance, if $U = \{1, 2, 3, \ldots n-1, n\}$ represents a set of categories, the linguistic variables 'catastrophic', 'very low' and 'highly likely' may be modelled by:

'catastrophic' = $\{1/0, \ldots, n-3/0,\ n-2/0,$
$n-1/0{\cdot}75,\ n/1{\cdot}0\}$
'very low' = $\{1/1{\cdot}0,\ 2/0{\cdot}75,\ 3/0,\ 4/0, \ldots, n/0\}$
'highly likely' = $\{1/0, \ldots, n-4/0,\ n-3/0,$
$n-2/0{\cdot}75,\ n-1/1{\cdot}0,\ n/0{\cdot}25\}$

where the integers in the numerators of each term within the brackets represent the categories and the real numbers in the denominators stand for the membership degrees.

The membership values for the components in U belonging to each of the linguistic variables 'catastrophic', 'very low' and 'highly likely' can thus be denoted as follows:

$$\mu_{\text{catastrophic}} = (0, \ldots, 0, 0{\cdot}75, 1{\cdot}0)$$

$$\mu_{\text{very low}} = (1{\cdot}0, 0{\cdot}75, 0, \ldots, 0)$$

$$\mu_{\text{highly likely}} = (0, \ldots, 0, 0{\cdot}75, 1{\cdot}0, 0{\cdot}25).$$

The fuzzy safety score of a failure mode of a component can be estimated by the product of the fuzzy descriptions of the corresponding failure likelihood, consequence severity and failure consequence probability. If L, C and E represent the fuzzy sets of the failure likelihood, consequence severity and failure consequence probability of a failure mode, the fuzzy safety score S can be defined as follows using fuzzy set manipulation:[14]

$$S = C \circ E \times L$$

$$\mu_S = \mu_{C \circ E \times L} = (\mu_S^1, \ldots, \mu_S^j, \ldots)$$

where symbol 'o' represents composition operation and '$\times$' the Cartesian product operation in fuzzy set theory as will be stated later.

μ_S is the description function of safety score S in terms of membership degrees μ_S^j $(j = 1, 2, \ldots, n)$ representing the extent to which S belongs to the elements in U. Each element in μ_S can be obtained using the max-min method as will be shown in the next section. It should be pointed out that the fuzzy safety score of a failure mode obtained using this method is the maximal possible one because of characteristics of Cartesian and composition rules.

In the above, S represents a fuzzy description for the safety score of a failure mode while the relevant fuzziness is described by μ_S. To express the safety of the failure mode in a clear way, linguistic variables such as 'poor', 'average', 'good' and 'excellent' may be used. For instance, it may be quite clear to state that the safety of a failure mode is to a large extent 'good'. Such linguistic variables may be referred to as safety expressions. The safety expressions may also be characterised by membership degrees to each element in U so that the fuzzy safety score of the failure mode could be identified in terms of these expressions. For instance, 'poor' could be defined as follows:

'poor' = $\{1/0, \ldots, n-2/0,\ n-1/0{\cdot}75,\ n/1{\cdot}0\}$.

Such a definition needs to be consistent with the ones for other linguistic variables. Thus, if a failure mode occurs 'highly frequently' and if it may cause 'definite' failure effect classified to be 'catastrophic', then the safety of the failure mode should be 'poor'.

When fuzzy descriptions for the safety scores of the failure modes of each component are evaluated in terms of the safety expressions, it is desirable, as shown in Fig. 1, to synthesise them to assess the safety for each component, then for each subsystem if necessary, and finally for the system being investigated. A novel synthesis approach is therefore required for such a hierarchical evaluation propagation without any loss of useful information generated for each failure mode of each component. The evidential reasoning approach is one such method which is capable of combining uncertain evaluations at a single level and implementing hierarchical propagation of such evaluations between different levels.

Following a brief introduction of fuzzy operations, the rest of the paper will present how to describe, evaluate and identify the safety associated with a failure mode of a component. Then, the evidential reasoning approach will be employed to synthesise assessments of safety for each component and the system.

3 SAFETY ANALYSIS USING FUZZY SETS

3.1 Fuzzy operations

Let U be a set and A and B subsets of U where $U = \{u_1, u_2, \ldots, u_n\}$. Suppose the membership values for the elements in U belonging to the subsets A and B are denoted by $\mu_A = (u_A^1, \mu_A^2, \ldots, \mu_A^n)$ and $\mu_B = (\mu_B^1, \mu_B^2, \ldots, \mu_B^n)$, respectively. Then, some typical fuzzy operations such as union, intersection, complement, Cartesian product and composition of fuzzy sets are described as follows.

(i) Complement. Complement of A is defined by:

$$\mu_{\bar{A}} = (\mu_{\bar{A}}^j)_{1\times n}$$

where $\mu_{\bar{A}}^j = 1 - \mu_A^j$, $j = 1, 2, \ldots, n$.

(ii) Intersection. Intersection of A and B is defined by:

$$\mu_{A\cap B} = (\mu_{A\cap B}^j)_{1\times n}$$

where $\mu_{A\cap B}^j = \min(\mu_A^j, \mu_B^j)$, $j = 1, 2, \ldots, n$.

(iii) Union. Union of A and B is defined by:

$$\mu_{A\cup B} = (\mu_{A\cap B}^j)_{1\times n}$$

where $\mu_{A\cup B}^j = \max(\mu_A^j, \mu_B^j)$, $j = 1, 2, \ldots, n$.

(iv) Cartesian product. Cartesian product of A and B is defined by:

$$\mu_{A\times B} = (\mu_{A\times B}^{ij})_{n\times n}$$

where $\mu_{A\times B}^{ij} = \min(\mu_A^i, \mu_B^j)$. For example, if $\mu_A = 1, 0{\cdot}5, 0{\cdot}1, 0, 0, 0, 0)$ and $\mu_B = (0, 0, 0, 0, 0{\cdot}1, 0{\cdot}5, 1)$, then

$$\mu_{A\times B} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0{\cdot}1 & 0{\cdot}5 & 1 \\ 0 & 0 & 0 & 0 & 0{\cdot}1 & 0{\cdot}5 & 0{\cdot}5 \\ 0 & 0 & 0 & 0 & 0{\cdot}1 & 0{\cdot}1 & 0{\cdot}1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

(v) Composition. Given the membership functions for the set A and for the Cartesian product of the sets A and B, the membership functions for B can be obtained as follows using the composition rule of inference.

$$\mu_B = \mu_{A\circ A\times B} = (\mu_B^j)_{1\times n}$$

where $\mu_B^j = \max(\min(\mu_A^1, \mu_{A\times B}^{1j}), \ldots, \min(\mu_A^n, \mu_{A\times B}^{nj}))$, $j = 1, 2, \ldots, n$. For example, given μ_A and $\mu_{A\times B}$, μ_B can be calculated as follows using the max-min method.

$$\mu_B = (0, 0, 0, 0, 0{\cdot}1, 0{\cdot}5, 1)$$

where, for example, $\mu_B^6 = \max[\min(1, 0{\cdot}5), \min(0{\cdot}5, 0{\cdot}5), \min(0{\cdot}1, 0{\cdot}1), \min(0, 0), \min(0, 0), \min(0, 0), \min(0, 0)] = 0{\cdot}5$.

3.2 Fuzzy safety description

As discussed before, linguistic variables can be used to describe failure likelihood, consequence severity and failure consequence probability. A linguistic variable may then be characterised by a membership function to a set of categories with regard to the particular condition. It is often recommended that the number of categories be restricted to no more than seven to remain within the practical bounds of human discrimination.[9] The use of categorical judgements has been quite successful in many practical situations.[3,14] It is usually convenient for engineers to use categories to articulate safety information. The typical linguistic variables for failure likelihood, consequence severity and failure consequence probability of a failure event may be defined and characterised as shown in Tables 1–3. It is obviously possible to have some flexibility in the definition of membership functions to suit different situations.

From the fuzzy descriptions of failure likelihood, consequence severity and failure consequence probability, it may be observed that the linguistic variables are not exclusive, so that the sum of the membership degrees for the linguistic variables belonging to a category may be greater than 1. For example, the sum of the elements in column 1 of Table 1 is 1·25. This is because there are intersections among the defined linguistic variables describing failure likelihood,

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	0·25	1	0·75	0	0
Low	0·25	1	0·75	0	0	0	0
Very low	1	0·75	0	0	0	0	0

consequence severity and failure consequence probability. Inclusive expressions may make it more convenient for the safety analyst to judge a failure mode.

Given a failure mode i, the failure likelihood, consequence severity and failure consequence probability, denoted by L_i, C_i and E_i, respectively, may be characterised by their membership functions with respect to the seven categories. Such membership functions need to be assigned by safety analysts with reference to the given three tables.

The safety score S_i of the ith failure mode of a component can be expressed by $S_i = C_i \circ B_i \times L_i$. The membership function of S_i is thus described by $\mu_{S_i} = \mu_{C_i \circ E_i \times L_i}$.

3.3 Fuzzy safety evaluation

The safety score S_i characterised by μ_{S_i} provides a fuzzy description of the safety of the ith failure mode of a component. However, the safety may be expressed more clearly in terms of linguistic variables. For instance, it is commonly understood that the safety of a failure mode of a component can be expressed by degrees to which it belongs to such linguistic variables as 'poor', 'average', 'good', and 'excellent'. Each of these linguistic variables may be referred to as a safety expression. To evaluate S_i in terms of these linguistic variables, it is necessary to characterise them using membership values with respect to the seven categories defined. These safety expressions need to be defined to be exclusive for each category. The reasons for doing so are stated as follows.

(i) Exclusive expressions can more clearly represent safety than inclusive ones although it may be slightly more difficult for the safety analyst to make direct judgment using the former.

(ii) It makes it easier for the obtained fuzzy safety score to be mapped back to one (or all) of the defined exclusive safety expressions.

(iii) It facilitates the implementation of the evidential reasoning approach to synthesise the safety of a large complex system.

The extent to which each safety expression belongs to each of the seven categories is defined by a membership value. The sum of membership values for each expression with respect to the seven categories is assigned to be the same. The purpose of doing so is to make a rational projection of the obtained fuzzy safety score description back to the defined safety expressions. In addition, the following conditions also need to be satisfied:

(i) $S_{\text{poor}} = C_{\text{catastrophic}} \circ E_{\text{definite}} \times L_{\text{highly frequent}}$
(ii) $S_{\text{average}} = C_{\text{critical}} \circ E_{\text{reasonably likely}} \times L_{\text{reasonably frequent}}$
(iii) $S_{\text{good}} = C_{\text{marginal}} \circ E_{\text{reasonably unlikely}} \times L_{\text{reasonably low}}$
(iv) $S_{\text{excellent}} = C_{\text{negligible}} \circ E_{\text{highly unlikely}} \times L_{\text{very low}}$.

Considering the above requirements, the four safety expressions are defined on the basis of Tables 1, 2 and 3, as shown in Table 4.

The four defined safety expressions in Table 4 have the following characteristics:

(i) 'poor' is described only by the membership values with regard to categories 6 and 7;
(ii) 'excellent' is described only by the membership values with regard to categories 1 and 2;
(iii) the membership functions of 'good' and

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

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
High 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

'average' are not symmetric with respect to categories 3 and 5, respectively, and actually they lay slightly more weight on category 4.

3.4 Safety identification

Using the best-fit method,[14] the obtained fuzzy safety score description S_i of failure mode i of a component can be mapped back to one (or all) of the defined safety expressions (i.e. 'excellent', 'good', 'average' and 'poor'). The method uses the distance between S_i and each of the safety expressions to represent the degree to which S_i is confirmed to each of them. For instance, the distance between the obtained fuzzy safety score description S_i and the expression 'poor' is defined as follows:

$$d_{i1}(S_i, \text{poor}) = \left[\sum_{j=1}^{7} (\mu^j_{S_i} - \mu^j_{\text{poor}})^2\right]^{1/2}.$$

Similarly, we can define:

$$d_{i2}(S_i, \text{average}) = \left[\sum_{j=1}^{7} (\mu^j_{S_i} - \mu^j_{\text{average}})^2\right]^{1/2}$$

$$d_{i3}(S_i, \text{good}) = \left[\sum_{j=1}^{7} (\mu^j_{S_i} - \mu^j_{\text{good}})^2\right]^{1/2}$$

$$d_{i4}(S_i, \text{excellent}) = \left[\sum_{j=1}^{7} (\mu^j_{S_i} - \mu^j_{\text{excellent}})^2\right]^{1/2}.$$

It should be noted that each d_{ij} $(j = 1, 2, 3, 4)$ is an unscaled distance. The closer S_i is to the jth expression, the smaller d_{ij} is. More specifically, d_{ij} is equal to zero if S_i is just the same as the jth expression in terms of the membership functions. In such a case, S_i should not be evaluated to other expressions at all due to the exclusiveness of these expressions. To embody such features, new indices need to be defined based on d_{ij} $(j = 1, 2, 3, 4)$.

Suppose d_{iJ} $(1 \leq J \leq 4)$ is the smallest among the obtained distances for S_i and let α_{i1}, α_{i2}, α_{i3} and α_{i4} represent the reciprocals of the relative distances between the identified fuzzy safety description S_i and each of the defined safety expressions with reference to d_{iJ}. Then, α_{ij} $(j = 1, 2, 3, 4)$ can be defined as follows:

$$\alpha_{ij} = \frac{1}{d_{ij}/d_{iJ}} \qquad j = 1, 2, 3, 4.$$

If $d_{iJ} = 0$ it follows that α_{iJ} is equal to 1 and the others are equal to 0. Then, α_{ij} $(j = 1, 2, 3, 4)$ can be normalised by:

$$\beta_{ij} = \frac{\alpha_{ij}}{\sum_{m=1}^{4} \alpha_{im}} \qquad j = 1, 2, 3, 4.$$

Each β_{ij} $(j = 1, 2, 3, 4)$ represents the extent to which S_i belongs to the jth defined safety expression. It can be noted that if S_i completely belongs to the jth expression then β_{ij} is equal to 1 and the others are equal to 0. The sum of values of these indices for S_i is equal to 1, i.e. $\sum_{j=1}^{n} \beta_{ij} = 1$. Thus β_{ij} could be viewed as a degree of confidence that S_i belongs to the jth safety expression.

The following example shows the developed method for the obtained safety score description to be mapped back to the defined safety expressions.

Table 4. Safety expressions

μ_{S_i} Linguistic variables	Categories 1	2	3	4	5	6	7
1. Poor	0	0	0	0	0	0·75	1
2. Average	0	0	0	0·5	1	0·25	0
3. Good	0	0·25	1	0·5	0	0	0
4. Excellent	1	0·75	0	0	0	0	0

Suppose $\mu_{S_i} = (0, 0, 0, 0, 0{\cdot}1, 0{\cdot}5, 1)$. Then, d_{ij} and α_{ij}, $(j = 1, 2, 3, 4)$ can be calculated by:

$$d_{i1} = \sqrt{0^2 + 0^2 + 0^2 + 0^2 + 0{\cdot}1^2 + 0{\cdot}25^2 + 0^2} = 0{\cdot}269,$$

$$d_{i2} = 1{\cdot}457,\ d_{i3} = 1{\cdot}604,\ d_{i4} = 1{\cdot}680$$

and

$$\alpha_{i1} = 1{\cdot}000,\ \alpha_{i2} = 0{\cdot}185,\ \alpha_{i3} = 0{\cdot}168,\ \alpha_{i4} = 0{\cdot}160.$$

β_{i1}, β_{i2}, β_{i3} and β_{i4} can then be calculated by:

$$\beta_{i1} = 0{\cdot}661,\ \beta_{i2} = 0{\cdot}122,\ \beta_{i3} = 0{\cdot}111,\ \beta_{i4} = 0{\cdot}106.$$

Thus, S_i is identified to belong to 'poor' with a confidence level of 66·1 percent, to 'average' with 12·2 percent, to 'good' with 11·1 percent and to 'excellent' with 10·6 percent. Such an evaluation may be summarized by the following expectation:

$$S_{(S_i)} = \{(0{\cdot}661, \text{'poor'}), (0{\cdot}122, \text{'average'}), (0{\cdot}111, \text{'good'}), (0{\cdot}106, \text{'excellent'})\}.$$

4 SYNTHESIS OF SAFETY EVALUATION BY HIERARCHICAL EVIDENTIAL REASONING

4.1 Evidential reasoning scheme

As discussed above, the safety of a component is determined by the associated failure modes. If a component only has one failure mode whose safety is absolutely evaluated as 'good', then the safety of the component will be 'good'. Generally, a component may have several failure modes. If the safety levels associated with the failure modes are all absolutely evaluated as 'good', then the safety of the component should also be 'good'. Unfortunately, such certain and consistent evaluations can hardly be expected in real life safety analysis. Problems may then arise as to how uncertain and inconsistent evaluations of safety analysis of all the failure modes of a component may be synthesised in a rational way so as to attain an (often uncertain) evaluation of the safety of the component. The problems may be ultimately generalised as one of determining how the safety of a system with a hierarchy as shown in Fig. 1 could be evaluated. As argued before a hierarchical evaluation process may be expected to provide a reasonable way of dealing with such problems.[17–19,21]

This evaluation process is based on the Dempster-Shafer (D-S) theory which is well suited for handling incomplete assessment of uncertainty. The D-S theory can model the narrowing of the hypothesis set with the accumulation of evidence. In other words, it will become more likely that a given hypothesis is true if more pieces of evidence support that hypothesis. In Fig. 1, whether the safety of a component is 'excellent', 'good', 'average' or 'poor' would be regarded as a hypothesis. The obtained safety evaluation of a failure mode may be viewed as a single piece of evidence. If the safety associated with a failure mode is to a certain extent evaluated as 'good', then the safety of the associated component would be to some degree 'good'. The hierarchical evaluation process provides a systematic way of synthesising such uncertain safety evaluations of multiple failure modes to produce an evaluation for a component.

To apply the D-S theory, the mutual exclusiveness and exhaustiveness of all hypotheses have to be satisfied. It is therefore necessary that all the linguistic variables for expression of system safety be defined as distinct grades. In other words, if one of the variables is absolutely confirmed, all the others must not be confirmed at all; if more than one variable is confirmed simultaneously, the total degree of confidence must be one or smaller than one. In addition to this requirement, the variables must cover all possible grades the safety analyst may need to use for evaluation of system safety. The linguistic variables defined in Section 3.3 satisfy the requirements of exclusiveness and exhaustiveness. This enables us to employ the evidential reasoning algorithm developed to synthesise the uncertain safety evaluations generated for failure modes using fuzzy sets.

4.2 Algorithm

Suppose H represents a set of linguistic variables for safety expressions and H_j the jth linguistic variable such as 'good'. Then, H is defined by:

$$H = \{H_1, \ldots, H_j, \ldots, H_N\}$$

where N is the number of the linguistic variables defined. In Section 3.3, for example, H is defined by:

$$H = \{\text{Poor, average, good, excellent}\}.$$

Suppose there are L_k failure modes associated with the kth component. Let e_{ki} denote failure mode i associated with component k, denoted by c_k. The set of the failure modes for the component can then be defined by:

$$E_k = \{e_{k1}, \ldots, e_{ki}, \ldots, e_{kL_k}\}.$$

Let λ_{ki} be the normalised relative weight of failure mode i in evaluation of the safety of component k where $0 \leq \lambda_{ki} \leq 1$. The way of assigning λ_{ki} can be found in Refs 17–19 and will be briefly outlined in the next section. Suppose $m^j_{ki} = m(H_j/e_{ki})$ $(m^j_k \leq 1)$ is a real number, referred to as a basic probability assignment, which represents a degree to which the obtained safety evaluation of the ith failure mode supports a hypothesis that the safety of the kth

component is confirmed to H_j. Then, m_{ki}^j may be obtained as follows:

$$m_{ki}^j = \lambda_{ki}\beta_{ij}$$

where β_{ij} is given with respect to the kth component, as discussed in Section 3.4.

As $0 \le \lambda_{ki} \le 1$ and $\sum_{j=1}^{N} \beta_{ij} = 1$, then $\sum_{j=1}^{N} m_{ki}^j \le 1$. Suppose $m_{ki}^H = m(H/e_{ki})$ is the basic probability assignment to H, which is the remaining belief unassigned after commitment of belief to all H_j $(j = 1, \ldots, N)$, that is, $m_{ki}^H = 1 - \sum_{j=1}^{N} m_{ki}^j$. A basic probability assignment matrix $m(c_k/E_k)$ for evaluation of the safety of the component c_k through the associated failure modes E_k may then be formulated by:

$$M(c_k/E_k) = \begin{bmatrix} m_{k1}^1 & \cdots & m_{k1}^j & \cdots & m_{k1}^N & m_{k1}^H \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ m_{ki}^1 & \cdots & m_{ki}^j & \cdots & m_{ki}^N & m_{ki}^H \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ m_{kL_k}^1 & \cdots & m_{kL_k}^j & \cdots & m_{kL_k}^N & m_{kL_k}^H \end{bmatrix} \begin{matrix} \{e_{k1}\} \\ \cdots \\ \{e_{ki}\} \\ \cdots \\ \{e_{kL_k}\} \end{matrix}$$

Suppose m_{ck}^j is a degree of confidence to which the safety of the kth component is evaluated to H_j. Then, m_{ck}^j can be obtained by synthesising the basic probability assignments as listed in $M(c_k/E_k)$ using the evidential reasoning algorithm as described below.

Suppose Ψ is a subset of H. Define a subset $e_{I_k(i)}$ of E_k and a combined probability assignment $m_{I_k(i)}^{\Psi}$ as follows:

$$e_{I_k(i)} = \{e_k^1 \cdots e_k^i\},\ 1 \le i \le L_k; \qquad m_{I_k(i)}^{\Psi} = m(\Psi_{I_k(i)})$$

where $m(\Psi/e_{I_k(i)})$ is a combined probability assignment to Ψ confirmed by $e_{I_k(i)}$. Then, the algorithm can be stated as follows:

$$\{H_j\}:\ m_{I_k(i+1)}^j = K_{I_k(i+1)}(m_{I_k(i)}^j m_{k,i+1}^j + m_{I_k(i)}^j m_{k,i+1}^H + m_{I_k(i)}^H m_{k,i+1}^j),\ j = 1, \ldots, N$$

$$\{H\}:\ m_{I_k(i+1)}^H = K_{I_k(i+1)} m_{I_k(i)}^H m_{k,i+1}^H$$

$$K_{I_k(i+1)} = \left[1 - \sum_{\tau=1}^{N} \sum_{\substack{j=1 \\ j \ne \tau}}^{N} m_{I_k(i)}^{\tau} m_{k,i+1}^j\right]^{-1}$$

$$i = 1, \ldots, L_k - 1.$$

4.3 Hierarchical propagation

It can be proven from the algorithm that $m_{I_k(L_k)}^{\Psi}$ is the overall probability assignment to $\Psi(\subseteq H)$ confirmed by E_k and $m_{I_k(L_k)}^{\Psi} = 0$ for any $\Psi \subseteq H$ other than $\Psi = H_j (j = 1, \ldots, N)$ and H, or

$$m_{ck}^j = m(H_j/E_k) = m_{I_k(L_k)}^j,\ j = 1, \ldots, N,$$

and

$$m_{ck}^H = m(H/E_k) = m_{I_k(L_k)}^H$$

$$m(\Psi/E_k) = m_{I_k(L_k)}^{\Psi} = 0 \quad \text{for any} \quad \Psi \subseteq H$$

but

$$\Psi \ne H_j\ (j = 1, \ldots, N) \text{ and } H.$$

Consequently, the safety of the kth component can be evaluated in terms of the safety expressions defined in H by the following expectation:

$$S(c_k) = \{(m_{ck}^j, H_j),\ j = 1, \ldots, N)$$

that is, the kth component is evaluated to H_j with a degree of confidence of m_{ck}^j, $j = 1, \ldots, N$. Such an evaluation is generated by synthesising the given safety evaluations of the relevant failure modes.

In a similar way, the safety evaluation of each component could be obtained. A further problem is then to produce an evaluation on the safety of a subsystem which is composed of several components. Suppose there are L_l components associated with the lth subsystem. The set of the components in subsystem l is defiend by:

$$F_l = \{c_{l1}, \ldots, c_{lk}, \ldots, c_{lL_l}\}$$

At this stage, the safety evaluations of components have been generated. So, the fact that the safety of the kth component is confirmed to H_j to an extent of m_{ck}^j $(j = 1, \ldots, N)$ could be viewed as a piece of evidence while the safety of the lth subsystem may be assumed to be evaluated to any of H_j $(j = 1, \ldots, N)$. Suppose m_{sl}^j is a degree of confidence that the safety of the lth subsystem is confirmed to H_j. The problem then becomes how to obtain m_{sl}^j from m_{ck}^j $(j = 1, \ldots, N;\ k = 1, \ldots, L_l)$. This problem can be solved in the same way as described in the last subsection if c_{lk} is treated as e_{ki}, m_{ck}^j as β_{ij} and m_{sl}^j as m_{ck}^j.

The safety of the lth subsystem can then be evaluated by:

$$S(s_l) = \{(m_{sl}^j, H_j),\ j = 1, \ldots, N\}$$

Let m^j be the degree of confidence to which the safety of the whole system is confirmed to H_j. Then, m^j can be obtained from m_{sl}^j $(j = 1, 2, \ldots, N;\ l = 1, 2, \ldots, S_l$ where S_l is the number of the subsystems) using the evidential reasoning algorithm. The safety of the whole system can thus be evaluated by:

$$S(s) = \{(m^j, H_j),\ j = 1, \ldots, N\}.$$

5 AN EXAMPLE: THE HYDRAULIC HOISTING TRANSMISSION SYSTEM OF A MARINE CRANE

The hydraulic hoisting transmission system of a marine crane is functionally shown in Fig. 2. This

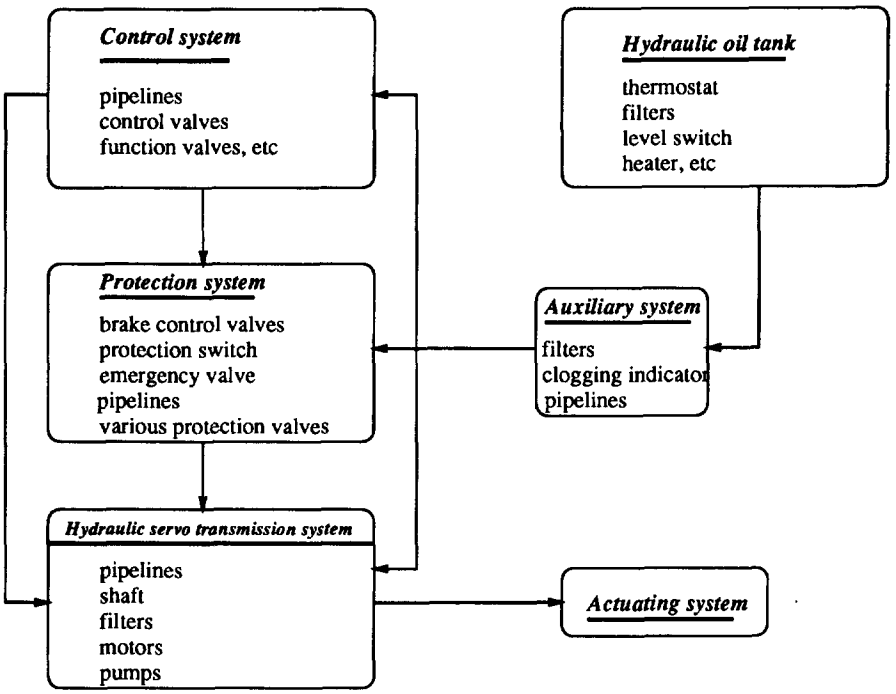

Fig. 2. Diagram of the hydraulic hoisting transmission system.

system is used to control the crane motions such as hoisting up or hoisting down loads as required by the operator.[12,16] It consists of five subsystems, namely hydraulic oil tank, auxiliary system, control system, protection system and hydraulic servo transmission system. Each subsystem is associated with several failure modes. The occurrence of each failure mode associated with a subsystem may result in a range of possible consequences with associated severity class and failure consequence probability, depending on the nature of the failure mode and the interactions of the subsystems. Examples of possible consequences or effects caused by the occurrence of the failure modes of the subsystems are degradation of the crane, damage to the boom ranging from minor distortion to total collapse (bucking), rupture of hoisting rope resulting in dropped load, damage to the surrounding structures and other goods within the operating radius and possible death or severe injuries to personnel. The precise values of the three variables used to describe the safety associated with a failure mode of each subsystem (i.e. the failure likelihood, consequence severity and failure consequence probability) are often difficult to estimate as the marine crane is working in a changing environment. However, it could be comparatively easier to use fuzzy subjective judgments to describe these three variables in order to evaluate the safety of this crane hydraulic hoisting transmission system.

In this section, this system is examined to demonstrate the proposed methodology incorporating fuzzy set modelling and evidential reasoning.

5.1 Failure mode modelling

1. Hydraulic oil tank

Four failure modes of this subsystem are identified. These are:

(i) level gauge failure
(ii) oil temperature too high or too low
(iii) major leak
(iv) minor leak.

The safety associated with each of these failure modes is analysed using the methodology described above. The detailed analysis for the first failure mode is presented. The analyses for other failure modes are conducted in a similar manner.

(i) Level gauge failure

For this failure mode, the failure likelihood is considered to be approximately 'reasonably low' and may vary about 'reasonably low'. With reference to Table 1, the failure likelihood L_{11} is modelled as follows:

$$L_{11} = \{1/0{\cdot}1,\ 2/0{\cdot}3,\ 3/1{\cdot}0,\ 4/0{\cdot}8,\ 5/0{\cdot}1,\ 6/0,\ 7/0\}.$$

The consequence severity is considered to be approximately 'marginal' and may vary about 'marginal'. With reference to Table 2, the failure likelihood C_{11} is modelled as follows:

$$C_{11} = \{1/0,\ 2/0{\cdot}25,\ 3/1{\cdot}0,\ 4/0{\cdot}8,\ 5/0{\cdot}1,\ 6/0,\ 7/0\}.$$

The failure consequence probability is considered to be approximately 'unlikely' and may vary about

'unlikely'. With reference to Table 3, the failure likelihood E_{11} is modelled as follows:

$$E_{11} = \{1/0{\cdot}25,\ 2/1{\cdot}0,\ 3/0{\cdot}8,\ 4/0{\cdot}1,\ 5/0,\ 6/0,\ 7/0\}.$$

The fuzzy safety score S_{11} of this failure mode is calculated as follows:

$$S_{11} = C_{11} \circ E_{11} \times L_{11}$$
$$= \{1/0{\cdot}1,\ 2/0{\cdot}3,\ 3/0{\cdot}8,\ 4/0{\cdot}8,\ 5/0{\cdot}1,\ 6/0,\ 7/0\}.$$

The obtained fuzzy safety score of the failure mode can be mapped back to the defined safety expressions (i.e. 'poor', 'average', 'good' and 'excellent'). The safety associated with this failure mode is identified as follows:

$$S(s_{11}) = \{(0{\cdot}127399,\ \text{'poor'}),\ (0{\cdot}167771,\ \text{'average'}),$$
$$(0{\cdot}560565,\ \text{'good'}),\ (0{\cdot}144265,\ \text{'excellent'})\}.$$

It can be noted that the failure likelihood, the consequence severity and the failure consequence probability of this failure mode are estimated approximately as 'reasonably low', 'marginal' and 'unlikely', respectively. Therefore, the evaluation of this failure mode should be identified to belong to 'good' and 'excellent' to a large extent. this is confirmed by the above results.

λ_{kj} is a normalised relative weight for the jth failure mode of the kth subsystem and can be assigned using the method described in.[17,19] It is assumed that if all the failure modes of the hydraulic tank are absolutely evaluated as 'excellent' the hydraulic oil tank is judged as 'excellent' with a confidence degree of over 99·5 percent. The following formulae can be used to assign the value of λ_{kj} as shown in:[17,19]

$$\lambda_{kj} = \alpha_k \frac{\zeta_k^j}{\zeta_k^I}, \quad \prod_{j=1}^{4} \left(1 - \alpha_k \frac{\zeta_k^j}{\zeta_k^I}\right) \leq \delta$$

where $\delta = 1 - 0{\cdot}995 = 0{\cdot}005$

ζ_k^j = the relative weight of the j failure mode of the hydraulic oil tank ($k = 1$),

ζ_k^I = the largest value among the weights of the failure modes of the hydraulic oil tank ($k = 1$),

α_k = a priority coefficient representing the importance of the role the most importance factor plays in evaluation of the safety of the hydraulic oil tank ($k = 1$).

Given $\zeta_1 = (\zeta_1^1\ \zeta_1^2\ \zeta_1^3\ \zeta_1^4)^T = (2\ 4\ 4\ 1)^T$, λ_{11} can thus be calculated by $\lambda_{11} = 0{\cdot}46$.

(ii) Oil temperature too high or too low

$$L_{12} = \{1/0,\ 2/0,\ 3/0{\cdot}3,\ 4/1{\cdot}0,\ 5/0{\cdot}8,\ 6/0{\cdot}1,\ 7/0\}$$
$$C_{12} = \{1/1{\cdot}0,\ 2/0{\cdot}75,\ 3/0{\cdot}1,\ 4/0,\ 5/0,\ 6/0,\ 7/0\}$$
$$E_{12} = \{1/0,\ 2/0{\cdot}25,\ 3/1{\cdot}0,\ 4/0{\cdot}75,\ 5/0,\ 6/0,\ 7/0\}$$
$$S_{12} = C_{12} \circ E_{12} \times L_{12} = \{1/0,\ 2/0,\ 3/0{\cdot}25,\ 4/0{\cdot}25,\ 5/0{\cdot}25,\ 6/0{\cdot}1,\ 7/0\}$$
$$S(s_{12}) = \{(0{\cdot}203344,\ \text{'poor'}),\ (0{\cdot}306207,\ \text{'average'}),\ (0{\cdot}295963,\ \text{'good'}),\ (0{\cdot}194486,\ \text{'excellent'})\}$$

(iii) Major leak

$$L_{13} = \{1/0{\cdot}3,\ 2/1{\cdot}0,\ 3/0{\cdot}8,\ 4/0{\cdot}1,\ 5/0,\ 6/0,\ 7/0\}$$
$$C_{13} = \{1/0,\ 2/0{\cdot}25,\ 3/1{\cdot}0,\ 4/0{\cdot}75,\ 5/0{\cdot}1,\ 6/0,\ 7/0\}$$
$$E_{13} = \{1/0,\ 2/0{\cdot}1,\ 3/0{\cdot}9,\ 4/1{\cdot}0,\ 5/0{\cdot}9,\ 6/0{\cdot}1,\ 7/0\}$$
$$S_{13} = C_{13} \circ E_{13} \times L_{13} = \{1/0{\cdot}3,\ 2/0{\cdot}9,\ 3/0{\cdot}8,\ 4/0{\cdot}1,\ 5/0,\ 6/0,\ 7/0\}$$
$$S(s_{13}) = \{(0{\cdot}172777,\ \text{'poor'}),\ (0{\cdot}183395,\ \text{'average'}),\ (0{\cdot}36116,\ \text{'good'}),\ (0{\cdot}282711,\ \text{'excellent'})\}$$

(iv) Minor leak

$$L_{14} = \{1/0{\cdot}3,\ 2/1{\cdot}0,\ 3/0{\cdot}75,\ 4/0,\ 5/0,\ 6/0,\ 7/0\}$$
$$C_{14} = \{1/1{\cdot}0,\ 2/0{\cdot}75,\ 3/0,\ 4/0,\ 5/0,\ 6/0,\ 7/0\}$$
$$E_{14} = \{1/1{\cdot}0,\ 2/0{\cdot}75,\ 3/0,\ 4/0,\ 5/0,\ 6/0,\ 7/0\}$$
$$S_{14} = C_{14} \circ E_{14} \times P_{14} = \{1/0{\cdot}3,\ 2/1{\cdot}0,\ 3/0{\cdot}75,\ 4/0,\ 5/0,\ 6/0,\ 7/0\}$$
$$S(s_{14}) = \{(0{\cdot}179706),\ \text{'poor'}),\ (0{\cdot}187129,\ \text{'average'}),\ (0{\cdot}328012,\ \text{'good'}),\ (0{\cdot}305152,\ \text{'excellent'})\}$$
$$\lambda_{14} = 0{\cdot}23$$
$$\lambda_1 = 0{\cdot}24$$

2. Auxiliary system

Six failure modes of this subsystem are identified and evaluated as follows:

(i) Failure allowing contaminant into system

$$L_{21} = \{1/0,\ 2/0,\ 3/0{\cdot}2,\ 4/0{\cdot}8,\ 5/1{\cdot}0,\ 6/0{\cdot}25,\ 7/0\}$$
$$C_{21} = \{1/0{\cdot}1,\ 2/0{\cdot}4,\ 3/1{\cdot}0,\ 4/0{\cdot}8,\ 5/0{\cdot}1,\ 6/0,\ 7/0\}$$
$$E_{21} = \{1/0{\cdot}4,\ 2/1{\cdot}0,\ 3/0{\cdot}8,\ 4/0{\cdot}1,\ 5/0,\ 6/0,\ 7/0\}$$
$$S_{21} = C_{21} \circ E_{21} \times P_{21} = \{1/0,\ 2/0,\ 3/0{\cdot}2,\ 4/0{\cdot}8,\ 5/0{\cdot}8,\ 6/0{\cdot}25,\ 7/0\}$$
$$S(s_{21}) = \{(0{\cdot}140185,\ \text{'poor'}),\ (0{\cdot}545059,\ \text{'average'}),\ (0{\cdot}183801,\ \text{'good'}),\ (0{\cdot}130956,\ \text{'excellent'})\}$$
$$\lambda_{21} = 0{\cdot}5$$

(ii) Filter blocked

$$L_{22} = \{1/0{\cdot}25,\ 2/1{\cdot}0,\ 3/0{\cdot}75,\ 4/0,\ 5/0,\ 6/0,\ 7/0\}$$
$$C_{22} = \{1/0{\cdot}1,\ 2/0{\cdot}4,\ 3/1{\cdot}0,\ 4/0{\cdot}8,\ 5/0{\cdot}1,\ 6/0,\ 7/0\}$$
$$E_{22} = \{1/0{\cdot}4,\ 2/1{\cdot}0,\ 3/0{\cdot}8,\ 4/0{\cdot}1,\ 5/0,\ 6/0,\ 7/0\}$$
$$S_{22} = C_{22} \circ E_{22} \times P_{22} = \{1/0{\cdot}25,\ 2/0{\cdot}8,\ 3/0{\cdot}75,\ 4/0,\ 5/0,\ 0,\ 7/0\}$$

$S(s_{22}) = \{(0{\cdot}176247, \text{'poor'}), (0{\cdot}184596, \text{'average'}), (0{\cdot}360054, \text{'good'}), (0{\cdot}279103, \text{'excellent'})\}$

$\lambda_{22} = 0{\cdot}25$

(iii) Blocking indicator fails to operate

$L_{23} = \{1/0, 2/0{\cdot}3, 3/1{\cdot}0, 4/0{\cdot}8, 5/0{\cdot}1, 6/0, 7/0\}$

$C_{23} = \{1/0, 2/0{\cdot}25, 3/1{\cdot}0, 4/0{\cdot}75, 5/0{\cdot}1, 6/0, 7/0\}$

$E_{23} = \{1/0{\cdot}25, 2/1{\cdot}0, 3/0{\cdot}75, 4/0, 5/0, 6/0, 7/0\}$

$S_{23} = C_{23} \circ E_{23} \times P_{23} = \{1/0, 2/0{\cdot}3, 3/0{\cdot}75, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S(s_{23}) = \{(0{\cdot}126268, \text{'poor'}), (0{\cdot}167319, \text{'average'}), (0{\cdot}568525, \text{'good'}), (0{\cdot}13788, \text{'excellent'})\}$

$\lambda_{23} = 0{\cdot}25$

(iv) Minor leak

$L_{24} = \{1/0, 2/0{\cdot}2, 3/0{\cdot}6, 4/1{\cdot}0, 5/0{\cdot}5, 6/0, 7/0\}$

$C_{24} = \{1/1{\cdot}0, 2/0{\cdot}75, 3/0{\cdot}1, 4/0, 5/0, 6/0, 7/0\}$

$E_{24} = \{1/0{\cdot}25, 2/1{\cdot}0, 3/0{\cdot}75, 4/0, 5/0, 6/0, 7/0\}$

$S_{24} = C_{24} \circ E_{24} \times P_{24} = \{1/0, 2/0{\cdot}2, 3/0{\cdot}6, 4/0{\cdot}75, 5/0{\cdot}5, 6/0, 7/0\}$

$S(s_{24}) = \{(0{\cdot}157031, \text{'poor'}), (0{\cdot}297143, \text{'average'}), (0{\cdot}352437, \text{'good'}), (0{\cdot}166276, \text{'excellent'})\}$

$\lambda_{24} = 0{\cdot}25$

(v) Major leak

$L_{25} = \{1/0{\cdot}25, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$C_{25} = \{1/0{\cdot}1, 2/0{\cdot}3, 3/1{\cdot}0, 4/0{\cdot}8, 5/0{\cdot}1, 6/0, 7/0\}$

$E_{25} = \{1/0, 2/0{\cdot}25, 3/1{\cdot}0, 4/0{\cdot}75, 5/0{\cdot}1, 6/0, 7/0\}$

$S_{25} = C_{25} \circ E_{23} \times P_{25} = \{1/0{\cdot}25, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S(s_{25}) = \{(0{\cdot}176890, \text{'poor'}), (0{\cdot}187174, \text{'average'}), (0{\cdot}352436, \text{'good'}), (0{\cdot}283500, \text{'excellent'})\}$

$\lambda_{25} = 0{\cdot}8$

(vi) No output from control pump

$L_{26} = \{1/0{\cdot}2, 2/1{\cdot}0, 3/0{\cdot}9, 4/0{\cdot}2, 5/0, 6/0, 7/0\}$

$C_{26} = \{1/0{\cdot}1, 2/0{\cdot}4, 3/1{\cdot}0, 4/0{\cdot}8, 5/0{\cdot}1, 6/0, 7/0\}$

$E_{26} = \{1/0, 2/0{\cdot}1, 3/0{\cdot}6, 4/1{\cdot}0, 5/0{\cdot}6, 6/0{\cdot}1, 7/0\}$

$S_{26} = C_{26} \circ E_{26} \times P_{26} = \{1/0{\cdot}2, 2/0{\cdot}8, 3/0{\cdot}8, 4/0{\cdot}2, 5/0, 6/0, 7/0\}$

$S(s_{26}) = \{(0{\cdot}164996, \text{"poor'}), (0{\cdot}179384, \text{'average'}), (0{\cdot}410346, \text{'good'}), (0{\cdot}245275, \text{'excellent'})\}$

$\lambda_{26} = 0{\cdot}8$

$\lambda_2 = 0{\cdot}24$

3. Control system

Five failure modes of this subsystem are identified and evaluated as follows:

(i) Major leak

$L_{31} = \{1/0{\cdot}3, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$C_{31} = \{1/0, 2/0, 3/0{\cdot}1. 4/0{\cdot}8, 5/1{\cdot}0, 6/0{\cdot}4, 7/0{\cdot}1\}$

$E_{31} = \{1/0, 2/0, 3/0{\cdot}2, 4/0{\cdot}8, 5/1{\cdot}0, 6/0{\cdot}3, 7/0\}$

$S_{31} = C_{31} \circ E_{31} \times P_{31} = \{1/0{\cdot}3, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S(s_{31}) = \{(0{\cdot}175962, \text{'poor'}), (0{\cdot}186099, \text{'average'}), (0{\cdot}346332, \text{'good'}), (0{\cdot}291607, \text{'excellent'})\}$

$\lambda_{31} = 0{\cdot}8$

(ii) Minor leak

$L_{32} = \{1/0, 2/0, 3/0, 4/0{\cdot}75, 5/1, 6/0{\cdot}25, 7/0\}$

$C_{32} = \{1/1{\cdot}0, 2/0{\cdot}75, 3/0, 4/0, 5/0, 6/0, 7/0\}$

$E_{32} = \{1/0{\cdot}25, 2/1{\cdot}0, 3/0{\cdot}75, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S_{32} = C_{32} \circ E_{32} \times P_{32} = \{1/0, 2/0, 3/0, 4/0{\cdot}1, 5/0{\cdot}8, 6/0{\cdot}8, 7/0{\cdot}3\}$

$S(s_{32}) = \{(0{\cdot}272065, \text{'poor'}), (0{\cdot}37796, \text{'average'}), (0{\cdot}180610, \text{'good'}), (0{\cdot}169529, \text{'excellent'})\}$

$\lambda_{32} = 0{\cdot}2$

(iii) No output when required

$L_{33} = \{1/0, 2/0, 3/0{\cdot}1, 4/0{\cdot}8, 5/1{\cdot}0, 6/0{\cdot}3, 7/0\}$

$C_{33} = \{1/0{\cdot}1, 2/0{\cdot}3, 3/1{\cdot}0, 4/0{\cdot}75, 5/0, 6/0, 7/0\}$

$E_{33} = \{1/0, 2/0, 3/0{\cdot}6, 4/1{\cdot}0, 5/0{\cdot}6, 6/0, 7/0\}$

$S_{33} = C_{33} \circ E_{33} \times P_{33} = \{1/0, 2/0, 3/0{\cdot}1, 4/0{\cdot}75, 5/0{\cdot}75, 6/0{\cdot}3, 7/0\}$

$S(s_{33}) = \{(0{\cdot}137888, \text{'poor'}), (0{\cdot}568525, \text{'average'}), (0{\cdot}167319, \text{'good'}), (0{\cdot}126268, \text{'excellent'})\}$

$\lambda_{33} = 0{\cdot}4$

(iv) Control output for lowering motion cannot be closed when required

$L_{34} = \{1/0, 2/0{\cdot}25, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$C_{34} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{34} = \{1/0, 2/0{\cdot}1, 3/0{\cdot}7, 4/1{\cdot}0, 5/0{\cdot}7, 6/0{\cdot}1, 7/0\}$

$S_{34} = C_{34} \circ E_{34} \times P_{34} = \{1/0, 2/0{\cdot}1, 3/0{\cdot}1, 4/0{\cdot}1, 5/0{\cdot}1, 6/0{\cdot}1, 7/0\}$

$S(s_{34}) = \{(0{\cdot}227082, \text{'poor'}), (0{\cdot}272918, \text{'average'}), (0{\cdot}272918, \text{'good'}), (0{\cdot}227082, \text{'excellent'})\}$

$\lambda_{34} = 0{\cdot}8$

(v) Control output for hoisting up motion can not be closed when required

$L_{35} = \{1/0, 2/0{\cdot}1, 3/0{\cdot}7, 4/1{\cdot}0, 5/0{\cdot}7, 6/0{\cdot}1, 7/0\}$

$C_{35} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{35} = \{1/0, 2/0{\cdot}1, 3/0{\cdot}7, 4/1{\cdot}0, 5/0{\cdot}7, 6/0{\cdot}1, 7/0\}$

$S_{35} = C_{35} \circ E_{35} \times P_{35} = \{1/0, 2/0{\cdot}1, 3/0{\cdot}1, 4/0{\cdot}1, 5/0{\cdot}1, 6/0{\cdot}1, 7/0\}$

$S(s_{35}) = \{(0{\cdot}227082, \text{'poor'}), (0{\cdot}272918, \text{'average'}), (0{\cdot}272918, \text{'good'}), (0{\cdot}227082, \text{'excellent'})\}$

$\lambda_3 = 0{\cdot}8$

4. Protection system

Eight failure modes of this subsystem are identified and evaluated as follows:

(i) Failure of switch when energised

$L_{41} = \{1/0, 2/0{\cdot}3, 3/0{\cdot}6, 4/1{\cdot}0, 5/0{\cdot}6, 6/0{\cdot}1, 7/0\}$

$C_{41} = \{1/0, 2/0{\cdot}25, 3/1{\cdot}0, 4/0{\cdot}75, 5/0, 6/0, 7/0\}$

$E_{41} = \{1/0, 3/0{\cdot}1, 4/0{\cdot}8, 5/1{\cdot}0, 6/0{\cdot}4, 7/0{\cdot}1\}$

$S_{41} = C_{41} \circ E_{41} \times P_{41} = \{1/0, 2/0{\cdot}3, 3/0{\cdot}6, 4/0{\cdot}75, 5/0{\cdot}6, 6/0{\cdot}1, 7/0\}$

$S(s_{41}) = \{(0{\cdot}160484, \text{'poor'}), (0{\cdot}321832, \text{'average'}), (0{\cdot}347827, \text{'good'}), (0{\cdot}169858, \text{'excellent'})\}$

$\lambda_{41} = 0{\cdot}32$

(ii) Failure of return for hoisting up when de-energised

$L_{42} = \{1/0{\cdot}3, 2/1{\cdot}0, 3/0{\cdot}75, 4/0, 5/0, 6/0, 7/0\}$

$C_{42} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}2, 6/0{\cdot}9, 7/1{\cdot}0\}$

$E_{42} = \{1/0, 2/0{\cdot}1, 3/0{\cdot}8, 4/1{\cdot}0, 5/0{\cdot}8, 6/0{\cdot}1, 7/0\}$

$S_{42} = C_{42} \circ E_{42} \times P_{42} = \{1/0{\cdot}2, 2/0{\cdot}2, 3/0{\cdot}2, 4/0, 5/0, 6/0, 7/0\}$

$S(s_{42}) = \{(0{\cdot}211166, \text{'poor'}), (0{\cdot}228852, \text{'average'}), (0{\cdot}283647, \text{'good'}), (0{\cdot}276335, \text{'excellent'})$

$\lambda_{42} = 0{\cdot}32$

(iii) Minor leak

$L_{43} = \{1/0, 2/0, 3/0{\cdot}1, 4/0{\cdot}75, 5/1, 6/0{\cdot}4, 7/0{\cdot}1\}$

$C_{43} = \{1/11{\cdot}0, 2/0{\cdot}75, 3/0{\cdot}1, 4/0, 5/0, 6/0, 7/0\}$

$E_{43} = \{1/0{\cdot}25, 2/1, 3/0{\cdot}75, 4/0, 5/0, 6/0, 7/0\}$

$S_{43} = C_{43} \circ E_{43} \times P_{43} = \{1/0, 2/0, 3/0{\cdot}1, 4/0{\cdot}75, 5/0{\cdot}75, 6/0{\cdot}4, 7/0{\cdot}1\}$

$S(s_{43}) = \{(0{\cdot}154418, \text{'poor'}), (0{\cdot}542517, (\text{'average'}), (0{\cdot}171944, \text{'good'}), (0{\cdot}131120, \text{'excellent'})\}$

(iv) Major leak

$L_{44} = \{1/0{\cdot}3, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 6/0, 7/0\}$

$C_{44} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{44} = \{1/0, 2/0, 3/0{\cdot}1, 4/0{\cdot}2, 5/0{\cdot}75, 6/1{\cdot}0, 7/0{\cdot}3\}$

$S_{44} = C_{44} \circ E_{44} \times P_{44} = \{1/0{\cdot}3, 2/0{\cdot}8, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S(s_{44}) = \{(0{\cdot}169529, \text{'poor'}), (0{\cdot}180610, \text{'average'}), (0{\cdot}377796, \text{'good'}), (0{\cdot}272065, \text{'excellent'})\}$

$\lambda_{44} = 0{\cdot}64$

(v) Failure of emergency stop

$L_{45} = \{1/0{\cdot}3, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$C_{45} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{45} = \{1/0, 2/0, 3/0{\cdot}1, 4/0{\cdot}75, 5/1{\cdot}0, 6/0{\cdot}3, 7/0\}$

$S_{45} = C_{45} \circ E_{45} \times P_{45} = \{1/0{\cdot}3, 2/0{\cdot}3, 3/0{\cdot}3, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S(s_{45}) = \{(0{\cdot}169529, \text{'poor'}), (0{\cdot}180610, \text{'average'}), (0{\cdot}377796, \text{'good'}), (0{\cdot}272062, \text{'excellent'})\}$

$\lambda_{45} = 0{\cdot}16$

(vi) Failure of hoisting up limit

$L_{46} = \{1/0{\cdot}3, 2/1{\cdot}0, 3/0{\cdot}75, 4/0, 5/0, 6/0, 7/0\}$

$C_{46} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{46} = \{1/0, 2/0, 3/0{\cdot}6, 4/1{\cdot}0, 5/0{\cdot}6, 6/0, 7/0\}$

$S_{46} = C_{46} \circ E_{46} \times P_{46} = \{1/0{\cdot}1, 2/0{\cdot}1, 3/0{\cdot}1, 4/0, 5/0, 6/0, 7/0\}$

$S(s_{46}) = \{(0{\cdot}225805, \text{'poor'}), (0{\cdot}245933, \text{'average'}), (0{\cdot}272623, \text{'good'}), (0{\cdot}255638, \text{'excellent'})\}$

$\lambda_{46} = 0{\cdot}64$

(vii) Failure of hoisting down limit

$L_{47} = \{1/0{\cdot}3, 2/1{\cdot}0, 3/0{\cdot}75, 4/0, 5/0, 6/0, 7/0\}$

$C_{47} = \{1{\cdot}0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{47} = \{1/0{\cdot}1, 2/0{\cdot}3, 3/1{\cdot}0, 4/0{\cdot}8, 5/0{\cdot}1, 6/0, 7/0\}$

$S_{47} = C_{47} \circ E_{47} \times P_{47} = \{1/0{\cdot}1, 2/0{\cdot}1, 3/0{\cdot}1, 4/0, 5/0, 6/0, 7/0\}$

$S(s_{47}) = \{(0{\cdot}225805, \text{'poor'}), (0{\cdot}245933, \text{'average'}), (0{\cdot}272623, \text{'good'}), (0{\cdot}255638, \text{'excellent'})\}$

$\lambda_{47} = 0{\cdot}64$

(viii) Low boost pressure switch fails to open

$L_{48} = \{1/1{\cdot}0, 2/0{\cdot}9, 3/0{\cdot}2, 4/0, 5/0, 6/0, 7/0\}$

$C_{48} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{48} = \{1/0, 2/0{\cdot}1, 3/0{\cdot}75, 4/1{\cdot}0, 5/0{\cdot}75, 6/0, 7/0\}$

$S_{48} = C_{48} \circ E_{48} \times P_{48} = \{1/0{\cdot}1, 2/0{\cdot}1, 3/0{\cdot}1, 4/0, 5/0, 6/0, 7/0\}$

$S(s_{48}) = \{(0{\cdot}225805, \text{'poor'}), (0{\cdot}245933, \text{'average'}), (0{\cdot}272623, \text{'good'}), (0{\cdot}255638, \text{'excellent'})\}$

$\lambda_4 = 0{\cdot}48$

5. Hydraulic servo transmission system

Seven failure modes of this subsystem are identified and evaluated as follows:

(i) Major leak

$L_{51} = \{1/0{\cdot}1, 2/0{\cdot}3, 3/1{\cdot}0, 4/0{\cdot}8, 5/0{\cdot}1, 6/0, 7/0\}$

$C_{51} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{51} = \{1/0, 2/0, 3/0{\cdot}1, 4/0{\cdot}7, 5/1{\cdot}0, 6/0{\cdot}3, 7/0\}$

$S_{51} = C_{51}$ o $E_{51} \times P_{51} = \{1/0{\cdot}1, 2/0{\cdot}3, 3/0{\cdot}3, 4/0{\cdot}3, 5/0{\cdot}1, 6/0, 7/0\}$

$S(s_{51}) = \{(0{\cdot}186270, \text{'poor'}), (0{\cdot}241453, \text{'average'}), (0{\cdot}341080, \text{'good'}), (0{\cdot}231196, \text{'excellent'})\}$

$\lambda_{51} = 0{\cdot}88$

(ii) Minor leak

$L_{52} = \{1/0, 2/0, 3/0{\cdot}1, 4/0{\cdot}8, 5/1{\cdot}0, 6/0{\cdot}3, 7/0\}$

$C_{52} = \{1/1{\cdot}0, 2/0{\cdot}75, 3/0{\cdot}2, 4/0, 5/0, 6/0, 7/0\}$

$E_{52} = \{1/0{\cdot}25, 2/1{\cdot}0, 3/0{\cdot}75, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S_{52} = C_{52}$ o $E_{52} \times P_{52} = \{1/0, 2/0, 3/0{\cdot}1, 4/0{\cdot}75, 5/0{\cdot}75, 6/0{\cdot}3, 7/0\}$

$S(s_{52}) = \{(0{\cdot}137888, \text{'poor'}), (0{\cdot}568525, \text{'average'}), (0{\cdot}167319, \text{'good'}), (0{\cdot}126268, \text{'excellent'})\}$

$\lambda_{52} = 0{\cdot}21$

(iii) Shaft failure

$L_{53} = \{1/0{\cdot}25, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$C_{53} = \{1/0, 2/0, 3/0, 4/0{\cdot}1, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{53} = \{1/0, 2/0, 3/0, 4/0{\cdot}1, 5/0{\cdot}8, 6/1{\cdot}0, 7/0{\cdot}3\}$

$S_{53} = C_{53}$ o $E_{53} \times P_{53} = \{1/0{\cdot}25, 2/0{\cdot}8, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S(s_{53}) = \{(0{\cdot}169884, \text{'poor'}), (0{\cdot}181104, \text{'average'}), (0{\cdot}385875, \text{'good'}), (0{\cdot}263138, \text{'excellent'})\}$

$\lambda_{53} = 0{\cdot}44$

(iv) No output from the package motor

$L_{54} = \{1/0, 2/0, 3/0, 4/0{\cdot}1, 5/0{\cdot}9, 6/1{\cdot}0, 7/0{\cdot}3\}$

$C_{54} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{54} = \{1/0, 2/0, 3/0{\cdot}6, 4/1{\cdot}0, 5/0{\cdot}6, 6/0, 7/0\}$

$S_{54} = C_{54}$ o $E_{54} \times P_{54} = \{1/0, 2/0, 3/0, 4/0{\cdot}1, 5/0{\cdot}1, 6/0{\cdot}1, 7/0{\cdot}1\}$

$S(s_{54}) = \{(0{\cdot}249886, \text{'poor'}), (0{\cdot}279311, \text{'average'}), (0{\cdot}249886, \text{'good'}), (0{\cdot}220917, \text{'excellent'})\}$

$\lambda_{54} = 0{\cdot}44$

(v) Hydraulic short circuit

$L_{55} = \{1/0{\cdot}3, 2/1.0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$C_{55} = \{1/0, 2/0, 3/0, 4/0{\cdot}1, 5/0{\cdot}3, 6/0{\cdot}8, 7/1{\cdot}0\}$

$E_{55} = \{1/0, 2/0, 3/0, 4/0{\cdot}1, 5/0{\cdot}5, 6/0{\cdot}8, 7/1{\cdot}0\}$

$S_{55} = C_{55}$ o $E_{55} \times P_{55} = \{1/0{\cdot}3, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S(s_{55}) = \{(0{\cdot}175962, \text{'poor'}) (0{\cdot}186099, \text{'average'}), (0{\cdot}346332, \text{'good'}), (0{\cdot}291607, \text{'excellent'})\}$

$\lambda_{55} = 0{\cdot}44$

(vi) Motor seizure

$L_{56} = \{1/0{\cdot}3, 2/1{\cdot}0, 3/0{\cdot}8, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$C_{56} = \{1/0, 2/0{\cdot}25, 3/1{\cdot}0, 4/0{\cdot}75, 5/0, 6/0, 7/0\}$

$E_{56} = \{1/0{\cdot}3, 2/0{\cdot}7, 3/1{\cdot}0, 4/0{\cdot}7, 5/0{\cdot}3, 6/0{\cdot}1, 7/0\}$

$S_{56} = C_{56}$ o $E_{56} \times P_{56} = \{1/0{\cdot}3, 2/0{\cdot}75, 3/0{\cdot}75, 4/0{\cdot}1, 5/0, 6/0, 7/0\}$

$S(s_{56}) = \{(0{\cdot}169055, \text{'poor'}), (0{\cdot}180786, \text{'average'}), (0{\cdot}376335, \text{'good'}), (0{\cdot}273824, \text{'excellent'})\}$

$\lambda_{56} = 0{\cdot}44$

(vii) Pipe burst

$L_{57} = \{1/1{\cdot}0, 2/0{\cdot}75, 3/0{\cdot}1, 4/0, 5/0, 6/0, 7/0\}$

$C_{57} = \{1/0, 2/0, 3/0, 4/0, 5/0{\cdot}1, 6/0{\cdot}75, 7/1{\cdot}0\}$

$E_{57} = \{1/0, 2/0, 3/0, 4/0{\cdot}1, 5/0{\cdot}8, 6/1{\cdot}0, 7/0{\cdot}25\}$

$S_{57} = C_{57}$ o $E_{57} \times P_{57} = \{1/0{\cdot}75, 2/0{\cdot}75, 3/0{\cdot}1, 4/0, 5/0, 6/0\ 7/0\}$

$S(s_{57}) = \{(0{\cdot}106954, \text{'poor'}), (0{\cdot}112284, \text{'average'}), (0{\cdot}128371, \text{'good'}), (0{\cdot}652392, \text{'excellent'})\}$

$\lambda_{57} = 0{\cdot}21$

$\lambda_5 = 0{\cdot}98$

5.2 Safety synthesis

Uncertain evaluations of subsystems and the whole system are then obtained using the evidential reasoning approach and proceed as follows:

Subsystems

1. Hydraulic oil tank

$S_1 = \{(0{\cdot}134298, \text{'poor'}), (0{\cdot}210362, \text{'average'}), (0{\cdot}451697, \text{'good'}), (0{\cdot}20029, \text{'excellent'})\}$

2. Auxiliary system

$S_2 = \{(0{\cdot}116894, \text{'poor'}), (0{\cdot}200282, \text{'average'}), (0{\cdot}437804, \text{'good'}), (0{\cdot}202550, \text{'excellent'})\}$

3. Control system

$S_3 = \{(0{\cdot}162497, \text{'poor'}), (0{\cdot}299497, \text{'average'}), (0{\cdot}299230, \text{'good'}), (0{\cdot}211705, \text{'excellent'})\}$

4. Protection system

$S_4 = \{(0{\cdot}166221, \text{'poor'}), (0{\cdot}224034, \text{'average'}), (0{\cdot}325006, \text{'good'}), (0{\cdot}237506, \text{'excellent'})\}$

5. Hydraulic servo transmission system

$S_5 = \{(0{\cdot}141912, \text{'poor'}), (0{\cdot}207604, \text{'average'}), (0{\cdot}362763, \text{'good'}), (0{\cdot}246110, \text{'excellent'})\}$

The whole system

$S = \{(0{\cdot}115566, \text{'poor'}), (0{\cdot}203768, \text{'average'}), (0{\cdot}425980, \text{'good'}), (0{\cdot}223201, \text{'excellent'})\}$

From the above results, it is obvious that four subsystems (i.e. the hydraulic oil tank, auxiliary system, protection system and hydraulic servo transmission system) have to a large extent been assessed as 'good'. For example, the hydraulic oil tank has been assessed as 'good' with a belief of 45·1697 percent; as 'excellent' with 20·0029 percent; as 'average' with 20·1362 percent; and as 'poor' with 13·4298 percent. The control system has been evaluated to a slightly larger extent as 'average' and 'good'. Since the safety of the hydraulic transmission system is determined by the safety of each of the constituent subsystems, the system safety should be evaluated as 'good' to a large extent. This is in harmony with the results obtained above as the safety of this hydraulic transmission system has been assessed as 'good' and 'excellent' to the extents of 42·5980 percent and 22·3201 percent, respectively.

The above information provides an analysis of safety of the crane hydraulic transmission system and an idea of the potential problem areas. From this information, the design engineer can have an insight into system safety and may then decide if design actions need to be taken to improve matters.

6 CONCLUSIONS

A new methodology is proposed in this paper for safety analysis and synthesis based on fuzzy set theory and an evidential reasoning approach. In this methodology, the safety of a failure event is analysed using fuzzy set modelling. This provides the safety analyst with flexibility in articulating judgements about such parameters as failure likelihood, consequences severity and failure consequence probability which are often used in safety analysis. The examination of the safety of a complex system with a hierarchical evaluation structure is carried out using an evidential reasoning approach, based on the information produced. Such a reasoning framework provides the safety analyst with a rational tool to make full use of the information generated at the lowest level in design to evaluate the safety of the whole system.

The proposed methodology can be used as an alternate approach for safety analysts to carry out safety analysis particularly in those situations where distributions of variables for use in probabilistic risk studies are difficult or impossible to obtain. Furthermore, since human reasoning is intrinsically fuzzy, it is believed that the proposed approach will be potentially useful in safety analysis and synthesis in many industrial environments.

ACKNOWLEDGEMENT

This work forms part of the projects on design for safety and multiple criteria decision making supported by the UK Science and Engineering Research Council under Grant No. GR/F 95306.

REFERENCES

1. Andersson, L., The theory of possibility and fuzzy sets: new ideas for risk analysis and decision making. Swedish Council for Building Research, 1988.
2. Apostolakis, G. E., Guedes Soares, C., Kondo, S. & Mancini, G., Are reliability and risk assessment ready for fuzzy methods? *Reliab. Engng System Safety*, **42,** (1993) 65.
3. Baldwin, J. F. & Pilsworth, B. W., A model of fuzzy reasoning through multi-valued logic and set theory. *Int. J. Man-Machine Studies*, **11,** (1979) 351–380.
4. Chun, M. H. & Ahn, K. I., Assessment of the potential applicability of fuzzy set theory to accident progression event trees with phenomenological uncertainties. *Reliab. Engng System Safety*, **37,** (1992) 237–252.
5. Coolen, F. P. A. & Newby, M. J., Bayesian reliability analysis with imprecise prior probabilities. *Reliab. Engng System Safety*, **43,** (1994) 75–85.
6. Dubois, D. & Prade, H., On the relevance of non-standard theories of uncertainty in modeling and pooling expert opinions. *Reliab. Engng System Safety*, **36,** (1992) 95–107.
7. Fine, W. T., *Mathematical Evaluations for Controlling Hazards*. Academic Press, Macon, GA, 1973.
8. Kaufmann, A., *Introduction to the Theory of Fuzzy Subsets*, Academic Press, Macon, GA, 1975.
9. Karwowski, W. & Mital, A., Potential applications of fuzzy sets in industrial safety engineering. *Fuzzy sets and systems*, **19** (1986), 105–120.
10. Keller, A. Z. & Kara-Zaitri, Application of fuzzy logic to reliability assessment. Reliability '87, Warrington, 14–16 April 1987, **3A/3/**1–11.
11. Keller, A. Z. & Kara-Zaitri, Further applications of

fuzzy logic to reliability assessment and safety analysis. *Micro Reliab.* **29,** (1989) 399–404.
12. NEL, FMECA of NEI pedestral crane, Report No. NECL/01, May 1987.
13. Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1629A, Military Standard, Department of Defense, Washington, 1980.
14. Schmucker, K. J., *Fuzzy Sets, Natural Language Computations, and Risk Analysis*, Computer Science Press, Rockville, MD, 1984.
15. Singer, D., Fault tree analysis based on fuzzy logic. *Computers Chem. Engng,* **14,** (1990) 259–266.
16. Wang, J. & Ruxton, T., Design for safety of Made-To-Order (MTO) products. ASME Publication, 93-DE-1, 1993 National Design Conference, March 7–11, Chicago, IL, USA, 1–12.
17. Yang, J. B. & Singh, M. G., An evidential reasoning approach for multiple attribute decision making with uncertainty. *IEEE Transactions on Systems, Man, and Cybernetics,* **24,** (1994) 1–18.
18. Yang, J. B. & Sen, P., A hierarchical evaluation process for multiple attribute design selection with uncertainty. In Industrial and Engineering Applications of Artificial Intelligence and Expert systems (IEA/AIE-93), P. W. H. Chung, G. Lovegrove and M. Ali (eds) Godon and Breach Science Publisher, Switzerland, 1993, 484–483.
19. Yang, J. B. & Sen, P., A general multi-level evaluation process for hybrid MADM with uncertainty. *IEEE Transactions on Systems, Man, and Cybernetics,* **24,** (1994) 1458–73.
20. Zadeh, L. A., *Fuzzy Sets and their Applications to Cognitive and Decision Processes,* Academic Press, Macon, GA, 1975.
21. Zhang, Z. J., Yang, J. B. & Xu, D. L., A hierarchical analysis model for multiobjective decision making. In Analysis, Design and Evaluation of Man-Machine Systems 1989, Selected Papers from the 4th IFAC/IFIP/IFORS/IEA Conference (Xi'an, China, September 1989), Pergamon, Oxford, U.K., 1990, 13–18.