Contents lists available at ScienceDirect

Journal of Hazardous Materials

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

Modified risk graph method using fuzzy rule-based approach

R. Nait-Said[a,*], F. Zidani[b], N. Ouzraoui[a]

[a] LARPI Laboratory, Safety Department, Institute of Health and Occupational Safety, University of Batna, Road Med El-Hadi Boukhlouf, Batna, Algeria
[b] LSPIE Laboratory, Electrical Engineering Department, Faculty of Engineering, University of Batna, Road Med El-Hadi Boukhlouf, Batna 05000, Algeria

ARTICLE INFO

Article history:
Received 23 September 2007
Received in revised form 14 August 2008
Accepted 18 August 2008
Available online 30 August 2008

Keywords:
Risk graph method
Safety integrity level
Fuzzy rule-based system

ABSTRACT

The risk graph is one of the most popular methods used to determine the safety integrity level for safety instrumented functions. However, conventional risk graph as described in the IEC 61508 standard is subjective and suffers from an interpretation problem of risk parameters. Thus, it can lead to inconsistent outcomes that may result in conservative SILs. To overcome this difficulty, a modified risk graph using fuzzy rule-based system is proposed. This novel version of risk graph uses fuzzy scales to assess risk parameters and calibration may be made by varying risk parameter values. Furthermore, the outcomes which are numerical values of risk reduction factor (the inverse of the probability of failure on demand) can be compared directly with those given by quantitative and semi-quantitative methods such as fault tree analysis (FTA), quantitative risk assessment (QRA) and layers of protection analysis (LOPA).

1. Introduction

The purpose of a safety analysis is to ensure that the risks that could be a potential source of harm, damage of property and degradation of the environment, are sufficiently minimised by addressing all the relevant safety lifecycle stages including the design, implementation, operation and maintenance through to decommissioning. Reducing residual risk to an acceptable level is usually achieved by using a combination of safety protective systems, including safety instrumented systems, SIS (e.g. Emergency Shutdown Systems and Fire and Gas Systems), other technology safety-related systems (e.g. relief valves, bursting discs, firewalls and drain system) and external risk reduction facilities (e.g. work organization, procedures and separation). The SIS often represents an integral part of a safety management system [1]. It is made up of one or more safety instrumented functions (SIF) to sense abnormal situations and automatically return the process to a safe state. This is usually achieved by performing a partial or complete shutdown of the process, to prevent a hazardous event or mitigate its consequences. If the initial risk without SIS is high, the availability and integrity requirements for SIFs must be high.

Requirements for SIFs are addressed in the international standard IEC 61508 [2] and the process industry sector-specific version IEC 61511 [3] which are widely accepted as the basis for specification, design and operation of SISs. Each SIF is specified in terms of the action to be achieved and the required probability of failure on demand (PFD). The latter defines the required safety integrity level (SIL) for the SIF. The IEC standards provide a framework for establishing SILs although they do not specify the SILs required for specific applications. They propose various methods for determining the PFD or the amount of risk reduction needed.

The risk graph described in Part 5 of the IEC 61508 is one of the most popular methods that enables the SIL of a SIF to be determined from a knowledge on the risk factors related to the process. In particular, it has been extensively applied when determining SIL requirements for local safety functions such as process shutdown systems [4,5]. The principles of the risk graph method have been adopted in the UKOOA guidelines for process control and safety systems on offshore installations and other documents published by offshore operators [6,7].

An important issue faced by risk analysts is how to deal with uncertainties that arise in each phase of the risk assessment process. In particular, one should identify how to deal with the state of "incomplete/no knowledge" related to process safety functions. An underlying assumption is that "uncertainty increases risk", but this is a conservative approach requiring that, in the absence of meaningful data or the opportunity to assimilate all available data, risk should be overestimated rather than underestimated. So, higher ratings are assigned to risk parameters, reflecting the assumption of unfavorable conditions, in order to compensate the uncertainty. Although this approach results in a conservative outcome leading to a design of sufficient safety integrity, it leads also to higher installation and maintenance costs. Alternatively, more efforts are certainly needed to obtain a consistent and less conservative outcome using more refined SIL determination methods [4,8,9].

[*] Corresponding author. Tel.: +213 33868977; fax: +213 33868977.
E-mail addresses: r_nait_said@hotmail.com (R. Nait-Said), fati_zidani@lycos.com (F. Zidani), ouzraoui@yahoo.fr (N. Ouzraoui).

0304-3894/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2008.08.086

Fuzzy rule-based systems and fuzzy arithmetic [10,11] have emerged over the last years as a very appropriate tool in dealing with uncertainty in reliability and safety analysis [12–17]. In this paper, an approach of fuzzy rule-based risk graph is proposed in order to add more power features to the conventional calibrated risk graph method. In this perspective, the safety integrity assessment based on fuzzy logic allows the analyst to evaluate the SIL of SIFs in a natural way by using the notion of a linguistic variable for depicting information which is qualitative, imprecise and/or uncertain. The methodology we have used is the application of the fuzzy inference system with fuzzifier and defuzzifier on a calibrated risk graph. The outcomes of the fuzzy risk graph are numerical values of risk reduction factor (RRF = 1/PFD) which are computed from a defuzzification of "fuzzy SILs".

2. Conventional risk graph method

Safety-related systems are conceived to implement the safety functions necessary to achieve or maintain a safe state for the process in terms of specified risk reduction related to hazardous events. A safety function is thus expressed in terms of the action to be taken and the required probability to satisfactorily perform this action. This probability as a quantitative target defines the safety integrity. Four discrete safety integrity levels, namely SIL1, SIL2, SIL3 and SIL4, are defined in the IEC 61508 and quantitative targets to which they relate are based on whether the safety-related system is operating in low demand mode (e.g. shutdown system) or continuously (e.g. motor care brakes). In the first case, the appropriate measure of safety function performance is the PFD, or its inverse, risk reduction factor (RRF). For functions which operate continuously, it is the probability of a dangerous failure per hour which is of concern. Table 1 shows the definition of the four SILs for low demand mode. As shown, the higher the SIL, the more available the safety-related system, so the more stringent becomes the implementation of safety function.

For determining the SIL, IEC standards have provided various methods that have been applied with differing degrees of success [4]. These methods range from using pure quantitative risk assessments (QRAs) to more qualitative methods, as follows:

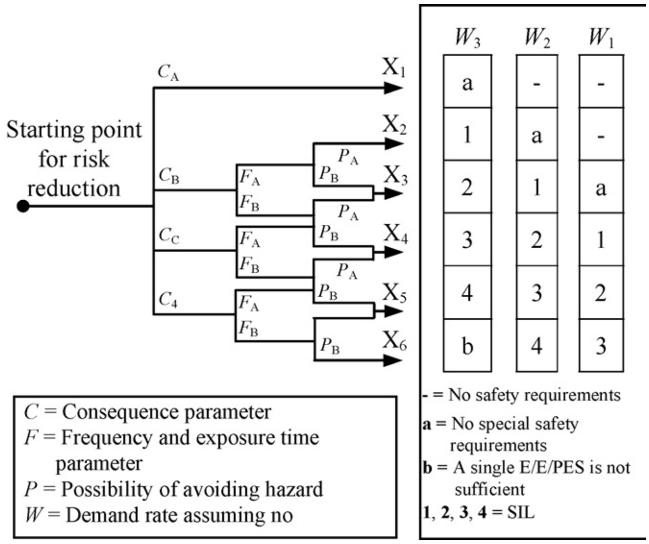
- Quantitative methods such as fault tree analysis (FTA) and Markov graphs.
- Semi-qualitative methods such as safety layer matrix, calibrated risk graph, and layers of protection analysis (LOPA).
- Qualitative methods like risk graph and hazardous event severity matrix.

Qualitative and semi-qualitative methods are generally less costly than the quantitative ones. They are technologically less demanding to develop, relatively intuitive to plant operators without requiring detailed risk assessment training, and do not make extensive use of historical failure-related data as a base of estimating failure probabilities.

The risk graph as a qualitative method can be described as a decision tree in which four risk parameters, considered to be sufficiently generic to deal with a wide range of applications, must be combined to arrive at the required SIL. These parameters are: consequence (C_i), frequency and exposure time (F_j), possibility of avoiding hazard (P_k), and probability of the unwanted occurrence (W_l). Fig. 1 gives an example of a risk graph implementation [2]. An explanation of this risk graph is the following:

Table 1
Definition of SILs for low demand mode from IEC 61508-1

SIL	Range of average PFD	Range of RRF
4	$[10^{-5}, 10^{-4}]$	$[10^{-4}, 10^{-5}]$
3	$[10^{-4}, 10^{-3}]$	$[10^{-3}, 10^{-4}]$
2	$[10^{-3}, 10^{-2}]$	$[10^{-2}, 10^{-3}]$
1	$[10^{-2}, 10^{-1}]$	$[10, 10^{2}]$



W_3	W_2	W_1
a	-	-
1	a	-
2	1	a
3	2	1
4	3	2
b	4	3

C = Consequence parameter
F = Frequency and exposure time parameter
P = Possibility of avoiding hazard
W = Demand rate assuming no

- = No safety requirements
a = No special safety requirements
b = A single E/E/PES is not sufficient
1, **2**, **3**, **4** = SIL

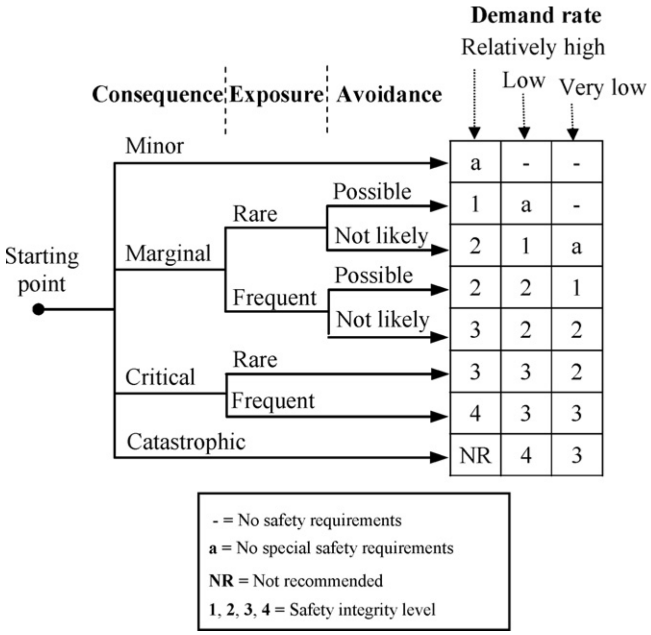
Fig. 1. Example of risk graph from IEC 61508-5.

- Use of the risk parameters C, F, and P leads to one of six outputs $X_1, X_2, \ldots, X_6$. Each one of these outputs is mapped onto one of three scales (W_1, W_2 and W_3). Each point on these scales gives an indication of the necessary safety integrity that has to be met by the E/E/PE safety-related system. The numbers 1, 2, 3 and 4 represent the four SILs. The point 'a' indicates the case of a system without special safety requirements, which corresponds to a probability of failure less than is indicated for SIL1. The point 'b' refers to situations when for specific consequences, a single safety-related system is not sufficient to give the necessary risk reduction.
- The mapping onto W_1, W_2 or W_3 allows the contribution of other risk reduction measures to be made. Scale W_3 provides the minimum risk reduction contributed by other measures (i.e. the highest probability of the unwanted occurrence), scale W_2 a medium contribution and scale W_1 the maximum contribution. Thus, the output of the risk graph as a measure of the required risk reduction for the E/E/PE safety-related system, together with the risk reductions achieved by other technology safety-related systems and external risk reduction facilities which are taken into account by the W_l scales, gives the overall risk reduction for the specific situation.

3. Shortcomings and alternatives

Although the risk graph method is relatively easy to be implemented and allows a fast assessment of SILs, it is less precise. Indeed, the interpretation of linguistic terms such as 'rare', 'possible', 'death of several persons', etc. can differ between evaluators since they could be the result of a subjective decision or from one industry sector to another [4,6,18].

There is therefore the need to calibrate the graph and to give guidance on the meanings of linguistic terms using orders of magnitude via numerical scales so that the resulting SIL rating will bring down the residual risk to the acceptable level. Otherwise, the risk reduction will be principally subjective with substantial limitations



Relatively high	Low	Very low
a	-	-
1	a	-
2	1	a
2	2	1
3	2	2
3	3	2
4	3	3
NR	4	3

- = No safety requirements
a = No special safety requirements
NR = Not recommended
1, **2**, **3**, **4** = Safety integrity level

Fig. 2. Risk graph with qualitative description of parameters.

for safety-related decision making [19]. In this sense, the IEC 61511-Part 3 provides a semi-qualitative method which is the calibrated risk graph. Although not specifically and absolutely fixed by the standard, the risk graph is usually calibrated such that each decision differs from another by a factor of ten ($10^{-1}, 10^{-2}, \ldots$). Fig. 2 and Table 2 respectively show an example of a risk graph as used in the UKOOA guidelines and quantitative definitions of risk parameters [6,7,20].

Against a tolerable target risk, managing the inherent uncertainty in the range of the risk parameters of a risk graph is problematic [7,20,21]. Although crisp intervals as means of characterizing uncertainty are an acceptable part of the usual calibrated risk graphs, the sufficient robustness in the SIL value may not be reached against the ambiguity of the information upon which the assessors base their judgment.

This type of knowledge elicitation presents two major disadvantages: first, it is in discordance with the gradual transition from one interval to another, well known in real-world applications. Indeed, a measurement that falls into a close neighbourhood of each precisely defined border between two adjacent intervals is taken as evidential support for only one of them, in spite of the inevitable uncertainty involved in the computing of the SIL, i.e. the safety integrity will be more or less one with of course different requirements. Second, it fails to reflect the fact that in most human reasoning and concept formation the decomposition of whole into parts is fuzzy rather than crisp [22–24]. In fact, there is an incompatibility between the uncertainty characterizing human perception and the crispness of the response mode. Thus, we need a representation of numbers, which is tolerant of imprecision and partial truths. Linguistic terms defined on numerical universes and supported by fuzzy sets, provide a rather natural tool for numeric/symbolic interfaces and would be a very adequate alternative when available information is imprecise and/or uncertain.

Table 2
Example of qualitative and quantitative definitions of parameters

Risk parameter	Qualitative descriptions	Quantitative descriptions
Consequence (*C*)	Minor injury	No deaths per event
	Marginal: one death or permanent injury	$[10^{-2}, 10^{-1}]$ probable deaths per event
	Critical: several deaths	$[10^{-1}, 1]$ probable deaths per event
	Catastrophic: many deaths	>1 probable deaths per event
Exposure (*F*)	Rare	<10% of time
	Frequent	≥10% of time
Avoidance (*P*)	Possible	90% probability of avoiding hazard
	Not likely	≤90% probability of avoiding hazard
Demand rate (*W*)	Very low	<1 in 30 years ≈ <0.03 per year
	Low	1 in [3, 30] years ≈ [0.03, 0.3] per year
	Relatively high	1 in [0.3, 3] years ≈ [0.3, 3] per year

Furthermore, compared to *C* and *W* parameters *F* and *P* have only two ranges each and so the calibration will be dominated by the two first. As an alternative solution, Blackmore [21] developed for an offshore project an alternative graph format by introducing four categories for *F* against reducing those of *C* to two only (injury or death). As reported, the proposed approach has resulted in improved effectiveness in the SIL determination. For a best calibration, Dean [7] suggested also the introduction of additional consequence and frequency bands in some cases. Recently, Baybutt [8] has developed an improved risk graph with the following four parameters: initiating cause frequency, enabling events/conditions, safeguards failure probability and consequences of the hazardous event. He introduces more than two levels for the first and the two last parameters to overcome both conservative and optimistic choices that respectively may result in an overestimation and underestimation of the SIL.

Another alternative proposed by Ormos and Ajtonyi [25] concerns the use of a fuzzy rule-based system in determining the SIL value by applying hazardous event severity matrix and conditional catastrophe theory. By application to three subsystems of steam production, the results of this approach compared with those provided by the quantitative method (as described by the IEC 61508) are very encouraging. For two subsystems the same result is obtained, SIL3 and SIL2 and for the third the result is SIL1 by fuzzy approach against SIL2 by the quantitative method. This difference is interpreted by the fact that severity parameter qualitatively estimated as low is not taken into consideration by the quantitative method. In the same way, Simon et al. [26] propose a fuzzy rule-based approach of the risk graph as well as a subjective evaluation of risk parameters by aggregation of expert judgments. Allocation of required SIL is determined by considering the risk graph as a fuzzy decision tree. Both risk parameters and SIL are represented by fuzzy partitions with linguistic descriptors, defined on ordinal measurement scales. The proposed approach is applied to equipment issued from the literature: a vessel containing a volatile flammable liquid. A SIF is considered to protect against a gas release greater than the admissible rate which is 10^{-4} per year. Each risk parameter is assessed by aggregating expert judgments given as possibility distributions, and fuzzy inference system provides after difuzzification the SIL value which is SIL2. Referring to these works, we attempt in this paper to develop a more flexible calibrated risk graph using fuzzy logic system, with two main differences compared to the above approaches: first, calibration problem is taken into consideration and so, scales supporting fuzzy partitions of the SIL and parameters *C*, *F*, *P*, and *W* are numeric rather ordinal with the orders of magnitude given by Tables 1 and 2. Second, fuzzy intervals defined on the RRF universe particularly allow a SIL value to be between two successive classes with differing membership degrees. In practice, when the availability data for a SIF indicates a requirement “just between” two SIL classes, generally the stricter SIL requirement is chosen [5]. This conservative solution involves a more substantial increment of effort and competence with the major difference occurring when moving from SIL2 to SIL3 [6]. The fuzzy integrity levels may be an alternative to resolve this kind of problems. For example, a value of RRF (1/PFD) as an outcome of the fuzzy risk graph model may belong simultaneously to two fuzzy sets “SIL2” and “SIL3” but with a little higher membership degree to the latter (equal to 0.7 for example). It would be reasonable to say that we are in presence of “rather SIL3” requirements which clearly involve less cost and time than “conventional SIL3”, according to the proportion given by the membership degree. For example, 70% of the cost and time devoted to the “conventional SIL3”.

4. Fuzzy inference system methodology

Fuzzy logic-based method is a powerful tool for modeling the behavior of systems which are too complex or too ill-defined to admit of conventional quantitative techniques or when the available information from the systems is qualitative, imprecise and/or uncertain. In contrast to classical logical systems, fuzzy logic aims at modeling the imprecise modes of reasoning that play an essential role in the human ability to give judgments or to make decisions in an environment of uncertainty and imprecision. Thus, unlike quantitative approaches that require accurate equations to model real-world behaviors, fuzzy logic can accommodate the ambiguities of real-world human with the concept of fuzzy sets and fuzzy inference techniques and consequently, possess a natural capability to express and deal with judgment and measurement uncertainties.

Fuzzy inference systems have found numerous applications in fields such as automatic control, data classification, decision analysis, expert systems, reliability engineering, and system safety. Among these systems, the fuzzy logic controller proposed by Mamdani and Assilian [27] is the most encountered in fuzzy rule-based problems. It was the first implementation dedicated to the control of a steam engine by synthesizing a set of fuzzy rules provided by experienced human operators. Based on a simple technique using the max–min inference, Mamdani’s method has been successfully applied in many fields ranging from processes control to medical diagnosis. Specific details for each step of this method are explained briefly below [28].

Let us consider a rule base constituted of n fuzzy IF-THEN rules with multiple inputs and single output (MISO). Each rule R_i (i = 1, . . ., n) is therefore of the form:

$$R_i: \text{ IF } X_1 \text{ is } A_{i1} \text{ and} \ldots \text{and } X_m \text{ is } A_{im} \text{ THEN } Y \text{ is } B_i \tag{1}$$

where the, X_j’s, j = 1, . . ., m, and Y are linguistic variables defined on the universes $U = U_1 \times \cdots \times U_m$ and V, respectively. The fuzzy sets A_{ij} are elements of a linguistic partition T_j of U_j (universe of variable X_j). For a crisp input vector $u^0 = (u_1^0, \ldots, u_m^0)$, the output value is determined by the following three-step method.

4.1. Fuzzification

It is the process of converting an input data u_j^0 into its symbolic representation, i.e. a fuzzy set A_{ij}^*, using the fuzzy partition T_j of U_j, by computing the membership degree $\mu_{A_{ij}}(u_j^0)$ of u_j^0 to each A_{ij}. Then, a matching degree $\alpha_i = \min_j \mu_{A_{ij}}(u_j^0)$ is computed for each rule R_i.

4.2. Fuzzy inference

The process for obtaining the fuzzy output using the max–min inference method consists of the following sub-steps:

- Finding the firing level of each rule: The truth value for the premise of each rule R_i is computed and applied to the conclusion part of this rule. It is computed as follows:

$$\alpha_i = \min_j \mu_{A_{ij}}(u_j^0) \tag{2}$$

- If a rule’s premise has non-zero degree of truth, i.e. when the input matches partially the premise of the rule, then the rule is fired.
- Inferencing: In the inference step, the output B_i' of each rule R_i is computed using a conjunction operator, the min. Then, $B_i' = \alpha_i \wedge B_i$ is given by:

$$\mu_{B_i'}(v) = \min(\alpha_i, \mu_{B_i}(v)) \tag{3}$$

- Aggregation: For obtaining the overall system output, all the individual rule outputs are combined using the union operator. Then, $B' = \bigcup_i B_i' = \bigcup_i \alpha_i \wedge B_i$ with as membership function:

$$\mu_{B'}(v) = \max_{i=1,\ldots,n} \mu_{B_i'}(v) \tag{4}$$

4.3. Defuzzification

It produces a representative value v_0 of Y in B'. Among defuzzification methods, the center of gravity is the most commonly used, and it is given by:

$$v^0 = \frac{\int_{v \in V} \mu_{B'}(v) v \, dv}{\int_{v \in V} \mu_{B'}(v) \, dv} \tag{5}$$

5. Fuzzy safety integrity assessment

The overall procedure for making a fuzzy safety integrity assessment is shown in Fig. 3. The analysis uses fuzzy partitions to describe both risk parameters and SILs. The membership functions are determined by a fuzzification, i.e. a fuzzy information granulation according to Zadeh [24], of data of a typical calibrated risk graph. Thus, crisp intervals are replaced by fuzzy intervals with trapezoidal membership functions. The basic idea of this transformation is to consider the boundaries of an ordinary interval as a mean value of a fuzzy number under the form of upper and lower expectations [29]. Details concerning the different steps of the proposed fuzzy model are presented below.

5.1. Selection of input variables

Referring to the IEC standards, the fuzzy rule-based system associated with conventional risk graph considers the four risk parameters C, F, P, and W as input variables and the SIL as the unique output variable. The parameters C, F, P, and W allow a meaningful graduation of the risks to be made, and contain the key risk assessment factors. Obviously, other factors or conditions could be considered but with reduced number because two major disadvantages may emerge: first, the higher the number of parameters is, the more additional SILs should be necessarily added but certainly without corresponding requirements. Second, further input variables do not allow the fuzzy system to be at a reasonable size and may complicate the test of the model.

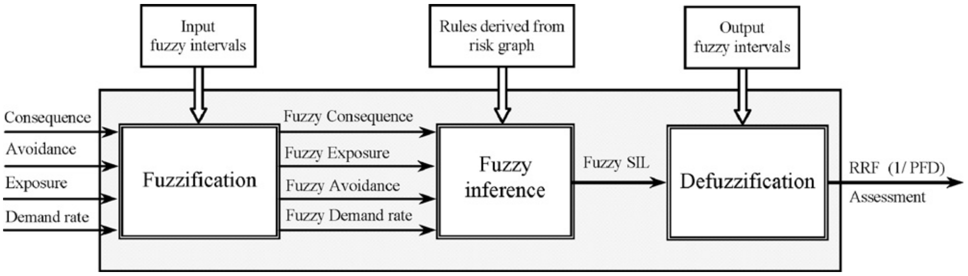


Fig. 3. Overall procedure of fuzzy safety integrity assessment.

5.2. Development of the fuzzy scales

Fuzzy logic uses the concept of linguistic variable to describe the premise and conclusion of a fuzzy rule [11]. This concept provides a tool of approximate characterization of situations which are too complex or too ill-defined for the application of conventional quantitative techniques. A linguistic variable differs from a numerical variable in that its values are not numbers but words in a natural language. The fuzzy sets, with their boundaries not sharply defined, play the role of values of the linguistic variable and may be viewed as summaries of various subclasses of elements in a universe of discourse. In the present step, the fuzzy sets for the description of the parameters C, F, P, and W and the SIL are derived from corresponding crisp partitions, referring to an experienced model, the calibrated risk graph presented in Fig. 2. Transforming an ordinary interval to a fuzzy interval may be considered as the converse problem of determining the mean value of a fuzzy interval. However, consistently with the well-known definition of expectation in probability theory, Dubois and Prade [29] have suggested a relevant definition of the mean value of a fuzzy interval as follows: “the mean value of a fuzzy interval Q is a closed interval bounded by the expectations calculated from its upper and lower distribution functions”, i.e.:

$$E(Q) = [E_*(Q), E^*(Q)] \tag{6}$$

where

$$E_*(Q) = \inf E(Q) = \int_{-\infty}^{+\infty} u \; \mathrm{d}F^*(u) \tag{7}$$

$$E^*(Q) = \sup E(Q) = \int_{-\infty}^{+\infty} u \; \mathrm{d}F_*(u) \tag{8}$$

F_* and F^* are the lower and upper distribution functions of P, respectively, and P belongs to the set of probability measures, $P(Q)$, which is defined on the support of Q. Let Q be a fuzzy interval with a trapezoidal membership function μ_Q, and let $S(Q) = [s_-, s_+]$ and $C(Q) = [q_-, q_+]$ be the support and core of Q respectively, i.e. $\mu_{S(Q)}(\mu) > 0$ and $\mu_{C(Q)}(u) = 1$. Let α and β be called the left and right spreads, respectively. Under the condition $\lim_{x\to-\infty} u^k F(u) = \lim_{x\to+\infty} u^k (1 - F(u)) = 0$ for $k \geq 1$, it follows that

$$\begin{aligned} E_*(Q) &= \int_0^{+\infty} (1 - F^*(u)) \; \mathrm{d}u - \int_{-\infty}^{0} F^*(u) \, \mathrm{d}u \\ &= q_- - \int_{-\infty}^{q_-} \mu_Q(u) \, \mathrm{d}u \end{aligned} \tag{9}$$

$$\begin{aligned} E^*(Q) &= \int_0^{+\infty} (1 - F_*(u)) \; \mathrm{d}u - \int_{-\infty}^{0} F_*(u) \, \mathrm{d}u \\ &= q_+ + \int_{q_+}^{+\infty} \mu_Q(u) \, \mathrm{d}u \end{aligned} \tag{10}$$

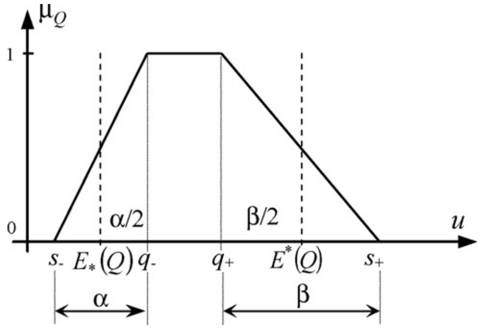


Fig. 4. Upper and lower mean values of Q.

By integration (see Fig. 4):

$$E_*(Q) = q_- - \frac{\alpha}{2} \tag{11}$$

and

$$E^*(Q) = q_+ + \frac{\beta}{2} \tag{12}$$

These results are in concordance with the fact that the width of the mean value is a linear function of the spreads α and β [29]. In our case, given E_* and q_- (respectively E^* and q_+) of an unknown fuzzy interval Q, α (respectively β) will be determined using Eq. (11) (respectively Eq. (12)). E_* and E^* as mean values are given by the boundaries of crisp intervals. The calculation of α and β is as follows: first, one computes the mean value, m, of the interval $[E_*, E^*]$. Next, the core boundaries, q_- and q_+, are computed using the mean value of the subdivisions $[E_*, m]$ and $[m, E^*]$, respectively. Both for m, q_- and q_+, one uses either arithmetic mean or geometric mean according to whether or not the universe scale is linear. Fig. 5 illustrates the transformation of an ordinary interval into a fuzzy one

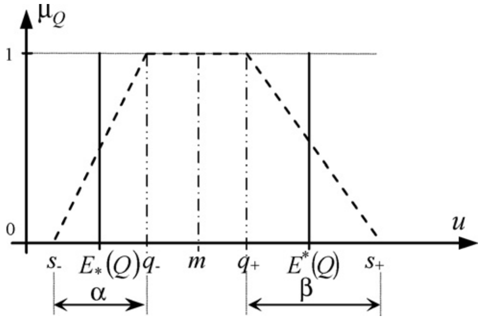


Fig. 5. Transformation of a crisp interval into a fuzzy one.

Table 3
Transformation of crisp intervals into fuzzy intervals

	E^*	E^*	M	q_-	q_+	α	β	s_-	s_-^*	s_+	s_+^*
Consequence											
Minor	1.0E−09	1.0E−07	1.0E−08	3.162E−09	3.162E−08	4.325E−09	1.368E−07	−1.162E−09	1.0E−09	1.684E−07	–
Marginal	0.01	0.1	3.162E−02	1.778E−02	5.623E−02	1.557E−02	8.753E−02	2.217E−03	–	1.438E−01	–
Critical	0.1	1	3.162E−01	1.778E−01	5.623E−01	1.557E−01	8.753E−01	2.217E−02	–	1.438E+00	–
Catastrophic	1	10	3.162E+00	1.778E+00	5.623E+00	1.557E+00	8.753E+00	2.217E−01	–	1.438E+01	10
Exposure											
Rare	0	10	5.0E+00	2.50E+00	7.50E+00	5.0E+00	5.0E+00	−2.50E+00	0	1.250E+01	–
Frequent	10	100	5.50E+01	3.250E+01	7.750E+01	4.50E+01	4.50E+01	−1.250E+01	7.50E+00	1.225E+02	100
Avoidance											
Not likely	0	90	4.50E+01	2.250E+01	6.750E+01	4.50E+01	4.50E+01	−2.250E+01	0	1.125E+02	9.250E+01
Possible	90	100	9.50E+01	9.250E+01	9.750E+01	5.0E+00	5.0E+00	8.750E+01	–	1.025E+02	100
Demand rate											
Very low	1.0E−05	0.03	5.477E−04	7.401E−05	4.054E−03	1.280E−04	5.189E−02	−5.401E−05	1.0E−05	5.595E−02	–
Low	0.03	0.3	9.487E−02	5.335E−02	1.687E−01	4.670E−02	2.626E−01	6.652E−03	–	4.313E−01	–
Relatively high	0.3	1	5.477E−01	4.054E−01	7.401E−01	2.107E−01	5.198E−01	1.946E−01	–	1.260E+00	1
SIL (RRF = 1/PFD)											
NSSR (a)	1	10	3.162E+00	1.778E+00	5.623E+00	1.557E+00	8.753E+00	2.217E−01	1	1.438E+01	–
SIL1	10	100	3.162E+01	1.778E+01	5.623E+01	1.557E+01	8.753E+01	2.217E+00	–	1.438E+02	–
SIL2	1.0E+02	1.0E+03	3.162E+02	1.778E+02	5.623E+02	1.557E+02	8.753E+02	2.217E+01	–	1.438E+03	–
SIL3	1.0E+03	1.0E+04	3.162E+03	1.778E+03	5.623E+03	1.557E+03	8.753E+03	2.217E+02	–	1.438E+04	–
SIL4	1.0E+04	1.0E+05	3.162E+04	1.778E+04	5.623E+04	1.557E+04	8.753E+04	2.217E+03	–	1.438E+05	–
NR	1.0E+05	1.0E+06	3.162E+05	1.778E+05	5.623E+05	1.557E+05	8.753E+05	2.217E+04	–	1.438E+06	1.0E+06

Note: s_-^* and s_+^* are modified values of $s-$ and s_+, respectively.

on a linear scale. For instance, α and s_- are determined as follows:

$$\begin{aligned} \alpha &= 2(q_- - E_*) \\ &= 2\left(\frac{E_* + m}{2} - E_*\right) \\ &= \frac{E^* - E_*}{2} \\ s_- &= q_- - \alpha \end{aligned} \tag{13}$$

Extreme fuzzy sets within a linguistic partition are derived from the transformation by assuming infinitespreads, i.e. taking $\alpha = -\infty$, for $\mu_{Q_{el}}(u) = 1$ for $u \le q_-$ and $\beta = +\infty$, and $\beta = +\infty$, $\mu_{Q_{er}}(u) = 1$ for $u \ge q_+$ ('el' is for extreme left and 'er' for extreme right). Furthermore, transforming an irregular crisp partition into a fuzzy partition may involve linguistic labels with meaningless values (incompatibility problem). In this case, the slope of the increasing or decreasing part of these fuzzy sets needs to be reasonably modified. Table 3 shows numerical results of the different transformations based on data of Tables 1 and 2. The fuzzy partitions of risk parameters and SILs, which are derived from the fuzzy intervals $Q = [q_-, [s_-, s_+], q_+]$, are given by Figs. 6a–d and 7. A more detailed description of these partitions is presented in the following:

- *Consequence*: Four fuzzy sets, namely 'Minor', 'Moderate', 'Critical', and 'Catastrophic' were defined on the input space of this variable (Fig. 6a). The values varying from 10^{-9} to 10 are represented on a logarithmic scale. To the linguistic value 'Minor' defined in risk graph as 'no deaths' is assigned the crisp interval $[10^{-9}, 10^{-7}]$ which suitably represents an unlikely event. This interval is transformed into a fuzzy one with the omission of the negative part. The interval [1, 10] is selected to be the mean value of the fuzzy set 'Catastrophic' with the possibility to change its upper bound according to the hazardous situation. The increasing part of 'Catastrophic' is adjusted by taking the upper bound of the core of the fuzzy set 'Critical' as its beginning point. This adjustment has double purpose: first, it removes the negative part of the fuzzy interval associated with the term 'catastrophic', which is meaningless from a point of view 'number of fatalities'. Second, it avoids the overlapping between more than two fuzzy sets, which involves many meaningless values for the class 'catastrophic'. For instance, the degree of membership of the zero value in the non-adjusted fuzzy interval is 0.27.
- *Frequency and exposure time*: Two fuzzy sets, namely 'Rare' and 'Frequent' were defined on a linear scale ranging from 0% to 100% (Fig. 6b). The boundaries of their cores are derived from arithmetic means of crisp interval subdivisions. As in the previous risk parameter, the negative part of the first set 'Rare' is removed, and the upper bound of its core has served as a lower bound of the support of the second set 'Frequent'. The membership function of the latter is obviously right open.
- *Possibility of avoiding hazard*: As in the previous input parameter, two fuzzy sets named respectively 'Not likely' and 'Possible' were defined on the universe [0, 100] (Fig. 6c). For the first set 'Not likely', the negative part is removed and the upper bound of its support takes the lower bound value of the core of the set 'Possible'. The values of the latter are limited to 100 with a right open membership function.
- *Probability of the unwanted occurrence*: Three fuzzy sets, namely 'Very low', 'Low' and 'Relatively high' were defined on a probability space ranging from 10^{-5} pa to 1 pa (Fig. 6d). As for the first risk parameter, the probability values are represented on a logarithmic scale. The choice of 10^{-5} pa (or 1.14×10^{-9} ph) as a lower bound of the interval $[10^{-5}, 0.03]$, refers to an unlikely event. Only the first and the last fuzzy set were adjusted by removing the negative part and the values greater then one, respectively. The intermediate fuzzy set 'Low' is remaining unchanged.
- *Safety integrity level* (*SIL*): The SIL as a unique output variable is defined on a RRF scale. The universe of discourse of the latter consists of the interval $[1, 10^6]$ with a regular crisp partition, i.e. there is a factor of 10 between 2 successive subintervals. Seven fuzzy sets were defined on the output space (Fig. 7): four sets are associated with the four SILs, with the same labels as levels themselves, namely 'SIL1', 'SIL2', 'SIL3' and 'SIL4', and two sets named 'NSSR' and 'NR' refer to the cases 'no special safety requirements' and 'Single SRS not recommended, respectively. Except the delimitation of the set 'NR', no adjustment is made for all these labels.

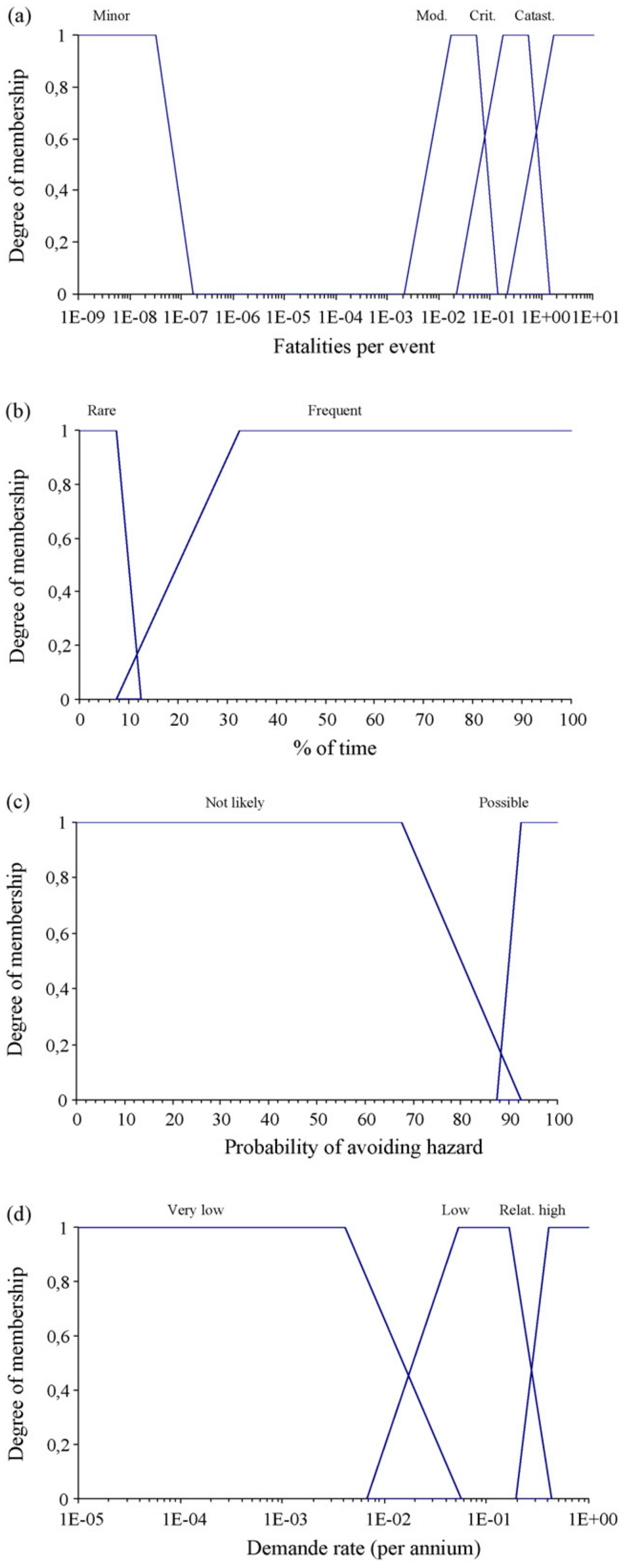


Fig. 6. Membership functions generated for risk parameters. (a) Consequence, (b) exposure, (c) avoidance, (d) demand rate.

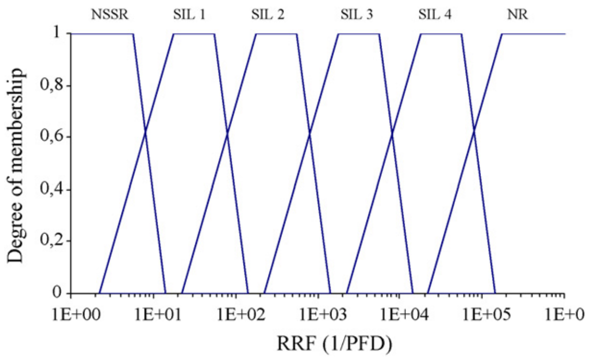


Fig. 7. Membership functions generated for SIL.

5.3. Derivation of the fuzzy rules

A number of fuzzy IF-THEN rules are extracted following the risk graph logic and using the linguistic descriptors associated with risk parameters and SIL. In this case, the rule base can be understood as a translation of the risk graph which is mainly based on the knowledge and experience of analysts regarding the process nature and required risk reduction. Both the number of rules and input variables involved in premise parts depend on the risk graph implementation, i.e. the decomposition level of risk graph. In the premise and conclusion parts of rules, the linguistic value meaning of input and output variables are described by the fuzzy sets defined in step 2. The general form of the derived fuzzy rules is:

$$R_i : \text{IF } C \text{ is } A_{iC} \text{ and } F \text{ is } A_{iF} \text{ and } P \text{ is } A_{iP} \text{ and } W \text{ is } A_{iW} \quad \text{THEN SIL is } B_i \tag{14}$$

where the risk parameters C, F, P, and W stand for input variables; A_{ic}, A_{iF}, A_{iP}, and A_{iW} are their linguistic values, respectively. The SIL is an output variable with B_i as its linguistic value. The fuzzy vector $(A_{ic}, A_{iF}, A_{iP}, A_{iW})$ and the fuzzy set B_i are elements of the universes $U_{\text{RP}} = U_C \times U_F \times U_P \times U_W$ (RP for risk parameters) and U_{SIL}, respectively. According to the risk graph reduction, the premise part of the above rule may be reduced to two or three input variables. Referring to the calibrated risk graph of Fig. 2, two examples of fuzzy rules are the following:

IF C is *Marginal* and F is *Frequent* and P is *Possible*
and W is *Low*
THEN *SIL* is *SIL*2
IF C is *Critical* and F is *Rare* and W is *Low*
THEN *SIL* is *SIL*3

5.4. Fuzzy rule base application

As explained in Section 4: fuzzy inference system methodology, when the fuzzy inference system is to be applied to a set of input parameter values the information flows through the fuzzification–inference–defuzzification process in order to generate the output value. Given any combination of input values which cover the specific context of risk parameters, the fuzzy rule-based risk graph will compute the RRF value that the SIF must achieve within the specific context. The fuzzifier maps crisp input vector $u^0_{\text{RP}} = (u^0_C, u^0_F, u^0_P, u^0_W)$ in U_{RP} to fuzzy sets in U_{RP}, and the defuzzifier maps fuzzy sets in U_{SIL}. If one or more risk parameters are not considered for a given rule, they will not have any effect on the matching degree α_i.

6. Conclusion

Although conventional risk graphs are relatively simple to be implemented, they can lead to inconsistent results and possibly conservatism that may result in SIL overestimation. Indeed, the use of qualitative definitions for risk parameters is highly subjective and their meaning can be misunderstood. On the other hand, numerical interpretation of risk parameters and SILs by means of crisp intervals violates gradual transition between intervals which is more realistic.

The proposed fuzzy risk graph model is a fuzzy rule-based-risk graph. Its main advantages may include:

- It preserves the four parameters used in the standard risk graph and can be adapted easily to improved risk graphs.
- Fuzzy scales with fuzzy linguistic values are used to assess risk parameters and calibration of the model may be made by varying risk parameters values.

The outcomes of the model which are numerical values of RRF (1/PFD) can be compared directly with those given by more refined methods like FTA, QRA and LOPA.

References

[1] C.R. Timms, IEC 61511-an aid to COMAH and safety case regulations compliance, Meas. Cont. J. 37 (2004) 115–122.

[2] IEC 61508 Standard, Functional Safety of Electrical/Electronic/Programmable Electronic Safety related Systems, Parts 1–6, First edition, 1998.

[3] IEC 61511 Standard, Functional Safety-Safety Instrumented Systems for the Process Industry Sector, Parts 1–3, First edition, 2003.

[4] Kirkwood, B. Tibbs, Developments in SIL determination, Comput. Cont. Eng. J. 16 (2005) 21–27.

[5] S. Hauge, P. Hokstad, T. Onshus, The introduction of IEC 61511 in Norwegian offshore industry, ESREL, 2001, pp. 483–490.

[6] D.J. Smith, K.J.L. Simpson, Functional Safety: A Straightforward Guide to Applying IEC 61508 and related Standards, Elsevier Butterworth-Heinemann, 2004.

[7] S. Dean, IEC 61508-Assessing the Hazard and Risk, Sauf Consulting Ltd., 1999. Available: http://www.sauf.co.uk.

[8] P. Baybutt, An improved risk graph approach for determination of safety integrity levels (SILs), Proc. Safety Prog. J. 26 (1) (2007) 66–76.

[9] W.K. Muhlbauer, Pipeline Risk Management Manual: Ideas, Techniques and Resources, Elsevier Inc, 2004.

[10] L.A. Zadeh, Outline of a new approach to the analysis of complex systems and decision processes, IEEE Trans. Syst. Man Cyb. 3 (1973) 28–44.

[11] L.A. Zadeh, The concept of a linguistic variable and its application to approximate reasoning. Parts I and II, Inf. Sci. 8 (1975) 199–249, 301–357.

[12] J.B. Bowles, C.E. Pelaez, Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis, Reliab. Eng. Syst. Safety 50 (1995) 203–213.

[13] K. Xu, L.C. Tang, M. Xie, S.L. Ho, M.L. Zhu, Fuzzy assessment of FMEA for engine systems, Reliab. Eng. Syst. Safety 75 (2002) 17–29.

[14] A. Pillay, J. Wang, Modified failure mode and effects analysis using approximate reasoning, Reliab. Eng. Syst. Safety 79 (2003) 69–85.

[15] A.C.F. Guimaraes, C.M.F. Lapa, Hazard and operability study using approximate reasoning in light-water reactors passive systems, Nucl. Eng. Des. 236 (2006) 1256–1263.

[16] A.C.F. Guimaraes, C.M.F. Lapa, Fuzzy inference to risk assessment on nuclear engineering systems, Appl. Soft Comput. 7 (2007) 17–28.

[17] A.S. Markowski, M.S. Mannan, A. Bigoszewska, Fuzzy logic for process safety analysis, in: International Symposium of Process Safety Center, 2007.

[18] F. Redmill, IEC 61508: principles and use in the management of safety, Comput. Cont. Eng. J. (1998) 205–213.

[19] K.T. Kosmowski, Functional safety concept for hazardous systems and new challenges, J. Loss Prev. Proc. Ind. 19 (2006) 298–305.

[20] W.G. Gulland, Methods of determining safety integrity level (SIL) requirements—Pros and Con, in: Safety-Critical Systems Symposium, 2004, pp. 105–122.

[21] L. Blackmore, IEC 61508-Practical experience in increasing the effectiveness of SIL assessments, ISA EXPO, 2000, ISBN/ID TP00ISA6023.

[22] D.W. Massaro, Broadening the domain of the fuzzy logical model of perception, in: H.L. Pick, J.R.P. Van Den Broek, D.C. Knill (Eds.), Cognition: Conceptual and Methodological Issues, APA, Washington, DC, 1992.

[23] S.A. Sandri, D. Dubois, H.W. Kalfsbeek, Elicitation, assessment, and pooling of expert judgments using possibility theory, IEEE Trans. Fuzzy Syst. 3 (1995) 313–335.

[24] L.A. Zadeh, Toward a theory of fuzzy information granulation and its centrality in human reasoning and fuzzy logic, Fuzzy Sets Syst. 90 (2) (1997) 111–127.

[25] L. Ormos, I. Ajtonyi, Soft computing method for determining the safety of technological system by 1EC 61508, in: Romanian–Hungarian Joint Sympsiom on Applied Computational Inelligence, Timisoara, 2004.

[26] C. Simon, M. Sallak, J.F. Aubry, SIL allocation of SIS by aggregation of experts' opinions, in: Safety and Reliability Conference, Stavanger (Norway), 2007.

[27] Mamdani, S. Assilian, An experiment in linguistic synthesis with a fuzzy logic controller, Int. J. Man-Mach. Stud. 7 (1975) 1–13.

[28] H.Prade Dubois, L. Ughetto, Fuzzy logic, control engineering and artificial intelligence, in: H.B. Verbruggen, H.J. Zimmerman, R. Babuska (Eds.), Fuzzy Algorithms for Control, Kluwer Academic Publishers, 1999.

[29] Dubois, H. Prade, The mean value of a fuzzy number, Fuzzy Sets Syst. 24 (1987) 279–300.