Implementation of Safety Instrumented Systems using Fuzzy Risk Graph Method

Nouara Ouzraoui, Bilal Rabah, Rachid Nait Said, and Mouloud Bourarech
Safety Department
Institute of Health and Occupational Safety, University of Batna
Road Med El-Hadi Boukhlouf, Batna, Algeria

Abstract

Although the risk graph method, described by the IEC 61508 standard is widely used for the determination of Safety Integrity Levels for the Safety Instrumented Functions (SIF) which performed by Safety Instrumented Systems (SIS). This technique has limits regarding the linguistic interpretation of the parameters of the risk analyzed. In addition, the calibration of the risk graph method as defined at the IEC61511 standard consists to use discrete intervals include also a problem of uncertainty in the calculation of Safety Integrity Levels. The purpose of this work is to improve of conventional risk graph in order to ensure a better implementation of safety instrumented systems (SIS). The proposed model based on fuzzy rules, considers the parameters defining the risk graph as inputs of a fuzzy inference systems and the Safety Integrity Level (SIL) as unique output. In order to validate the proposed model, a case study on an industrial system is carried out. The obtained results show a particular interest of fuzzy graph risk for estimating the appropriate Safety Integrity Level than that given by the risk graph conventional.

Keywords
Risk graph, Safety Instrumented Systems, Safety Integrity Levels, fuzzy rules.

1. Introduction

The main objective of safety analysis s related to the industrial process is the reduction of the risks identified and considered to be unacceptable to an acceptable level. These risks could be led to physical harms, damage of property or negative environmental impact. Risk reduction is usually achieved by several safety related systems (SRS) [3]. Each SRS is characterized by one or more safety functions with a factor of reduction (RRF) which is the inverse of the probability of failure on demand (PFD) of that SRS. These safety systems have different roles according to whether they intervene, prevention by reducing the probability that the hazardous event occurred or protection by mitigation the consequences of this event. Reducing risk is achieved by using several systems including shutdown systems known Safety Instrumented Systems (SIS) in order to make the process in safe state. The standards IEC 61508 and IEC 61511 define four safety integrity levels (SIL) for the safety function. The implementation of SIS requires defining the SIL which should be reached by the SIF. The assessment of integrity level could be calculated by qualitative and quantitative methods [IEC 61508 98], [IEC 61511 00], [SAL 06], [SAL 08].

The risk graph is the most qualitative method used to determine the safety integrity level of which described on part 5 of standard IEC 61508 [IEC 61508 98]. Although the risk graph is a relatively easy method for application and allowing a fast assessment of SIL, it has also some disadvantages in the interpretation of linguistic terms used to define the parameters C, F, P and W, which may differ between evaluators due of subjectivity related to the definition of these parameters.. Even we make quantitative definition to the parameters the numerical intervals used will still present uncertainty of information upon which the evaluators base their judgmentFuzzy logic due to L.A Zadah [ZAD 65] seems to provide an adequate environment for the treatment of uncertainty related to the different parameters of risk graph [NAI 09], [SIM 07]. In this work, a fuzzy approach of risk graph based on fuzzy rules is proposed in order to treat the ambiguity of parameters by using the operations of fuzzy logic, the calibrated a parameters of risk graph are introduced into the fuzzy inference system to determine the SIL required. The approach is validated experimentally on an operational industrial system " Heater".

2. Conventional risk graph

The most qualitative method used for determining the SIL is the one that called risk graph [IEC 61508 98]. The risk graph based on the following equation: R=F x G, or R is the risk during the absence of the related safety system F is the frequency of the dangerous event during the absence of the safety systems and C is the consequences of the dangerous event. The frequency of dangerous event supposed to be the result of three following factors:

- Probability that the exposed area is occupied ;
- The probability of avoiding the hazardous situation;
- Number of times per year that the hazardous situation would occur.

Finally, we take the following 4 measures of the risk:

- Consequence of the hazardous event (C) ;
- Occupancy (F) ;
- Probability of avoiding the hazardous event (P) ;
- Demand rate (W).

Combining these parameters, we obtain the risk graph which presented at the figure (1). The use of these parameters of risk C, F and P results at certain number of outputs (X1, X2, Xn). Each output is mapped in three scales (W1, W2 and W3). Each point of these scales indicates the required SIL that has to be generated by the system.
This method supposed to be qualitative, the most of criteria often remain qualitative, due the necessity to calibrate the graph and gives a numerical intervals to different parameters which described by linguistics terms(Table 2), Fig (2). The standard IEI 61511- 3 provides a semi-qualitative method that is the calibrated risk graph [6], [7], [20].

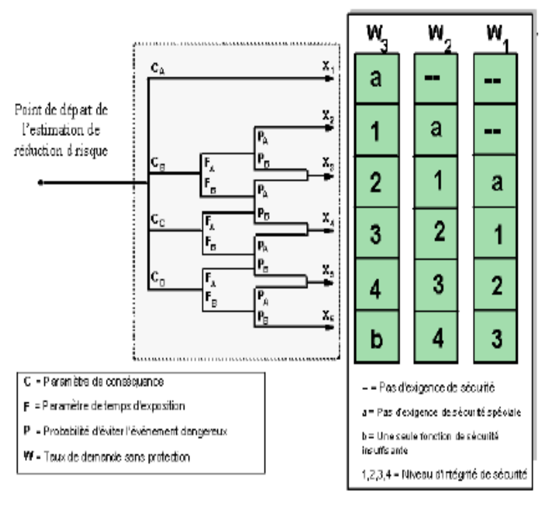


Figure 1: Risk graph example [IEC61508-5 98]

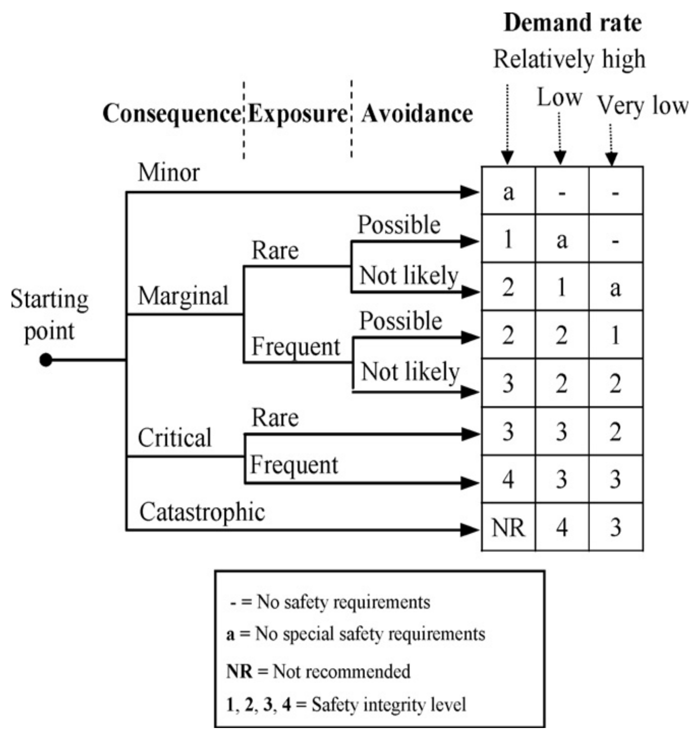


Figure 2: Risk graph with qualitative description of parameters

SIL	Range of average PFD	Range of RRF

Table 1: Definitions of SIL for
low-demand mode
[IEC61508 98]

4	$[10^{-5}, 10^{-4}[$	$]10^{-4}, 1$
3	$[10-4, 10^{-3}[$	$]10^{-3}, 10^{-4}]$
2	$[10^{-3}, 10^{-2}[$	$]10^{-2}, 10^{-3}]$
1	$[10^{-2}, 10^{-1}[$	$]10^{-1}, 10^{-2}]$

Table 2 : Exemple of qualitativ
definitions of paran

Parameter	Qualitative description	Quantitative description
Consequence (C)	Minor	[10-2,10-1]
	Marginal	[10-2,10-1]
	Critical	[10-1,1]
	Catastrophic	> 1
Exposure (F)	Rare	< 10% de temps
	Frequent	≥10% de temps
Avoidance (P)	Possible	90% probabilité d'évitement de danger
	Impossible	≤90% probabilité d'évitement de danger
Demand rate (W)	Very low	<1dans 30 ans≈<0.03/an
	Low	1 dans [3,30] ans ≈ [0.03, 0.3] par an
	High	1 dans [0.3,3] ans≈[0.3,3] par an

The faults noticed are originally incoherences of results and eventually of conservatism, which may translate by overestimation of SIL. In consideration of insufficiencies established on the conventional risk graph, this work proposes to develop a calibrated risk graph more flexible which based on fuzzy inference system.

3. Fuzzy risk graph

3.1 Proposed risk graph model

The proposed fuzzy risk graph is a model which takes in a count the problem of calibration, the fuzzy scales of SIL and the parameters *C*, *F*, *P* and *W* are numerical with the orders of grandeur given by the tables I and II. The fuzzy intervals defines on the univers RRF allow the value of SIL to be between two successive sections with different memberships. The global structure of fuzzy risk graph proposed is given at figure 3.

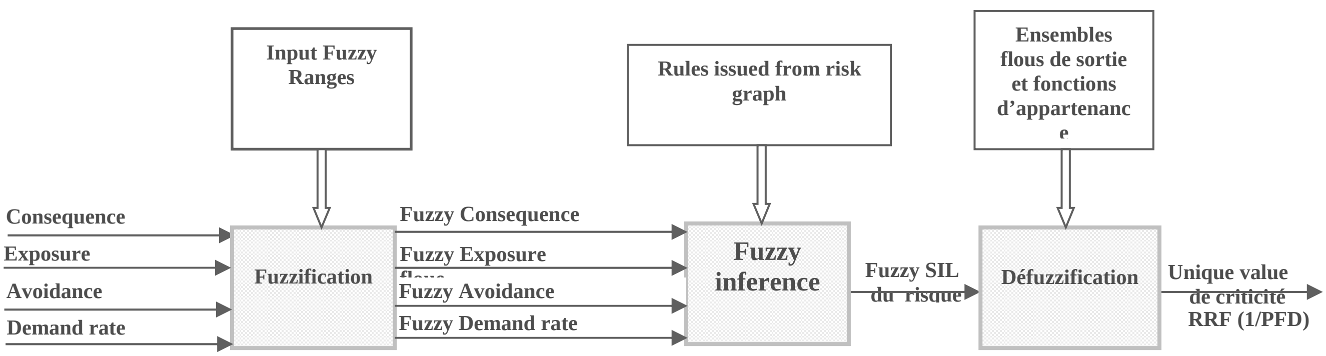


Figure 3: Global procedure of SIL assessment using fuzzy approach

The implementation of fuzzy risk graph model based on three principal units:

- Fuzzification : this step requires the transformation of real inputs to another fuzzy ones

- Fuzzy Inference *:* The process for obtaining the fuzzy output using the maxmin inference method consists of the following substeps :

(i) Finding the firing level of each rule: the truth value for the premise of each rule Ri is computed and applied to the conclusion part of this rule. It is computed as follows:

$$\alpha i = \min_{j} \mu_{Ai\,j}\,(u^0_j)$$

(ii) Inferencing: in the inference step, the output of each rule is computed using a conjunction operator min. Then , B_i = αi ^Bi is given by :

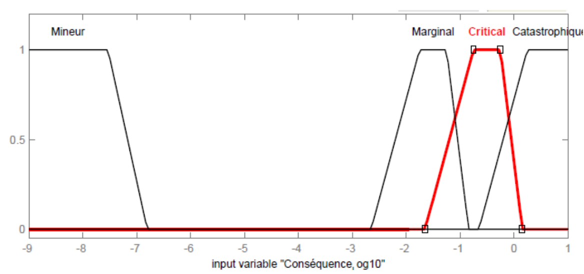
$$\mu B_i\,(v) = \min(\alpha_i, \mu B_i\,(v)).$$

(iii) Aggregation: for obtaining the overall system output, all the individual rule outputs are combined using the union operator. Then, $B' = \cup_i B'_i = \cup_i \alpha_i \wedge B_i$ with membership function :

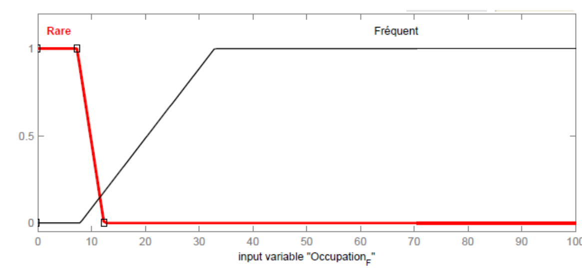
$$\mu_{B'}\,(v) = \max_{i=1,\ldots,n} \mu B'_i\,(v).$$

- 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 following equation :

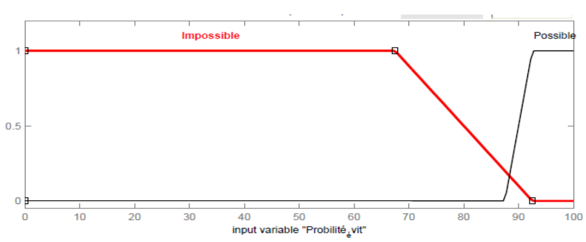
$$v0 = \_v \in V\, \mu B\_\,(v)\cdot v\cdot dv\_v \in V\, \mu B\_\,(v)\cdot dv$$



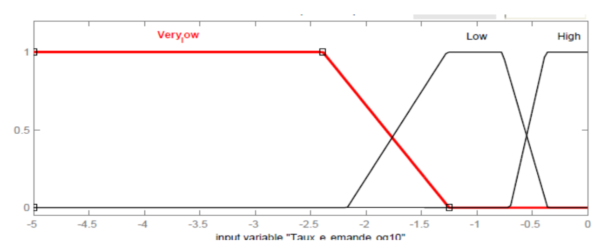
(a)



(b)



(c)



(d)

Figure 4: Membership functions generated for risk parameters:

(a) Consequence, (b) Occuppancy, (c) Avoidance, and (d) demand rate.

The SIL is the unique output, it is defined on RRF range .the values between 1 and 10^{-6} and represented on logarithmic scale with regular partition figure (5).

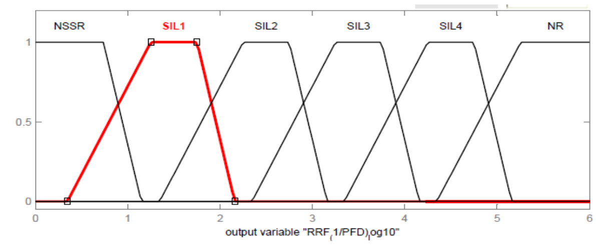


Figure 5: Membership functions generated for SIL

3.2 Establishment of fuzzy rules

Fuzzy sets are associated to make in conclusions of rules to make the fuzzy rules base (table 3).

Rule	Consequence	Occupancy	Avoidance	Demand rate	SIL
1	Minor	/	/	High	a
2	Minor	/	/	Low	/
3	Minor	/	/	Very low	/
4	Marginale	Rare	Possible	high	1
5	Marginale	Rare	Possible	Low	a
6	Marginale	Rare	Possible	Very low	/
…	…	…	…	…	…

Table 3 : Combined rules of parameters

The previous table present the rules generated by combining the different parametres C, F, P et W obtained from risk graph. The rule number 4, for example, should be given as :

If the Consequence is marginale and occuppancy israre and avoidance is possible and demand rate is high so the SIL is 1.

The issued surface from fuzzy rules is given by the figure (6).

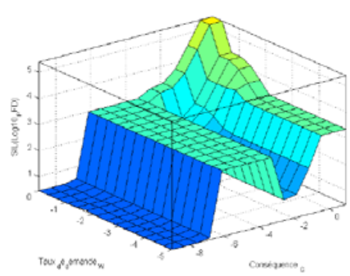


Figure 6: Issued surface

4. Case study

4.1 Presentation of process

In order to demonstrate the applicability of the proposed fuzzy risk graph model, our case study has focused on a heater of the MPP3-plant at sensitive plant of the company SONATRACH, which is considered one of the most critical systems that can generate, in the case of failure, a critical and even catastrophic material, human and environmental consequences.

Figure (4) shows in a simplified diagram the furnace rebouilor Four H-101 system and its various components.

The furnace rebouillor is operational in a permanent way, its main role is to produce fuels gas, which are mainly composed of methane and ethane.

The condensate from the bottom of column C-101, is sent by means of the pump P-101 A / B, to furnace rebouilor H-101 with 150°C for reheating, then the outgoing fluid of the heated rebouillor with 180 °C, is returned to the column like hot backward flow in order to extract gases

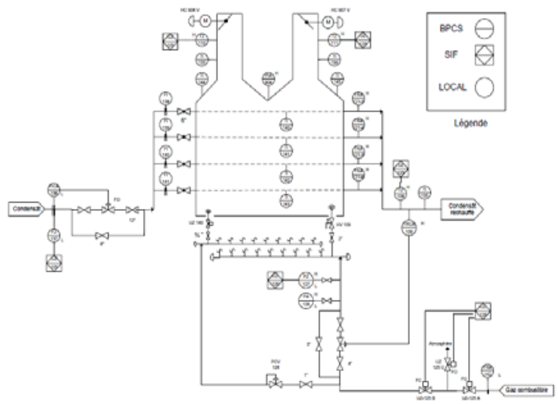


Figure 7: Heataer process H101 (SONATRACH)

4.2 Scenarios of accidents

In order to develop the scenarios of potentials accidents that may present in the heater H-321, we proceed with an inductive analysis by HAZOP (Hazard and Operability). this method allows to identify the causes, the consequences and the safety barriers of systems already implemented to prevent the development of these scenarios. Although the system is equipped of BPCS for the control of fuel gas pressure and oil flow, the results of this analysis displays that the scenarios of major accident which can be happened on this system are:

- Explosion of the furnace caused by the elevation of fuel gas pressure (SC1)

- Fire caused by low flow of oil circulated inside the heater (SC 2)

The control system (BPCS) can not always be enough to manage these hazards , Shutdown system with instrumented nature fully independent of control and regulation system seems mandatory in order to make the heater in safe state. To implement this system, the required SIL should be calculated.

The values of parameters C,F,P,W related to the our system are given by the following table (Tab 4).

Table 4 : Values of parameters C, F, P, W

Scenario	Consequence	Occupation	Avoidance	Demand rate
1	CC	FA	PA	W2
2	CB	FA	PB	W2

The SIL required for the two scenarios is given in the following table (Table 5).

Table 5: Obtained SIL using classic and fuzzy models

Scenario	Input				Output (SIL)		
	C	F	P	W	*Classic Model*	*Fuzzy Model*	*RRF*
High pressure of fuel gas	[0,1- 1]	[0-25]	[90-100]	0,2	SIL 3	SIL2- 0,8/SIL3-0.4	3,89
Low flow of hot oil	[0,01-0,1]	[0-25]	[0-10]	1,1	SIL 2	SIL1- 0,7/SIL2-0.5	1.8

4.3 Interpretation of obtained results

The results comparison of the two assessments approaches of SIL, show a difference of values of SIL. We noticed that the SIL determined by the fuzzy risk graph is characterized by a progressive membership more than one level. In the case of the first scenario, the SIL belongs to level 2 and 3 with a degrees of respectively memberships 0 .8 and 0.4. The same, for the scenario 2, the SIL obtained belongs to two levels 1 and 2 with a degrees of respectively memberships 0 .7 and 0.5. This comparison shows that there is overestimation of SIL in the case of two scenarios. Although that this overestimation leads to conservative results, which requires high costs of installation and maintenance of the SIS.

5. Conclusion

The objective of this work is to show the importance of fuzzy approach for determining of SIL. The concepts of fuzzy sets, linguistic variables and fuzzy rules issued from this logic which allows us to take in consideration:

- The issue of interpretation of parameters related to graph (C,F,P et W). Indeed, the fuzzy scales have the capacity to describe the continuity of categories with progressive transition from one to another ;
- The problem of SIL classification: the SIL could belong to more than one level with various memberships degrees.

The fuzzy risk graph model has the flexibility which allows us to treat the linguistic parameters. The input parameters introduced in inference system were obtained from expertise, or the results of analyse risk model such as fault tree

References

IEC61508, Functional safety of electrical/electronic/programmable electronic (e/e/pe) safety related systems. International Electrotechnical Commission (IEC), 1998.

IEC61511, Functional safety : Safety instrumented systems for the process industry sector. International Electrotechnical Commission (IEC), 2000.

Nait-Saïd R., Zidani F. and Ouzraoui N., Modified risk graph method using fuzzy rule-based approach, *Journal of Hazardous Materials*, vol. 164, no. 2-3, pp. 651-658, 2009.

Sallak, M., Simon, C., and Aubry., J.-F, Evaluating safety integrity level in presence of uncertainty. *The 4th International Conference on Safety and Reliability*, Krakow, Poland, 2006.

Sallak, M., Simon, C., and Aubry, J.-F, A fuzzy probabilistic approach for determining safety integrity level. *IEEE Transactions on Fuzzy Systems*, 16(1) :239-248, 2008.

Simon, C., Sallak, M., and Aubry., J.-F, SIL allocation of sis by aggregation of experts opinions. *In ESREL, Safety and Reliability Conference*, Stavanger, Norvège, 2007.

Zadeh L, Fuzzy sets, Information and Control, vol. 8, pp. 338–353, 1965.