Acknowledgements

At the end of this work, I would like to acknowledge all those who helped me finishing this master report.

First, I would like to acknowledge my advisors Boutheina Ben Yaghlane and Christophe Simon for their continuous guidance, encouragement and presence. I would like to express my sincere gratitude to them for introducing me to an interesting area of research and also for all valuable discussion we have had during this research.

I am also thankful to Zied Elouedi and Amel Ben Yaghlane for replying me each time I asked them any questions.

I would like to address my thanks to all professors of ISG Tunis, members of LARODEC laboratory for their help and kindness.

Heartfelt thanks to all of my friends for their encouragement especially Wafa for being always with me. I am also indebted to my friend mouna for her generous help.

I would like to thank all my family, especially my dear father, my beloved mother, my two sisters and my brother for their permanent support. I am also grateful to all members of families Ben Hariz, Haddad and Najar.

I am greatly indebted to my dear husband for giving me strength and motivation, for creating a pleasant environment at home and for supporting me during difficult periods. A very special thanks and excuses, to my little daughter Lamis.

Finally, I thank all the members of jury who accept to judge my dissertation.

Abstract

Risk analysis becomes very important especially with the increase of risk accidents in the industrial fields. In this context, we present in this master thesis a new approach based on belief functions theory for determining the safety integrity level of a safety instrumented system. This approach consists on collecting data from expert opinions by eliciting judgements using a qualitative method, dividing them in groups using the k-means algorithm and aggregating them by applying a hierarchical method. The output of the data collecting process will be integrated into a risk evaluation model in order to get the safety integrity level. As an evaluation method, we propose a new generalized risk graph named Evidential Risk Graph, which is able to deal with imperfect data modeled with the belief functions theory.

Résumé

L'analyse de risque devient de plus en plus importante avec l'augmentation rapide du nombre des accidents surtout dans le domaine industriel. Dans ce contexte, nous présentons dans ce rapport de master une nouvelle approche pour déterminer le niveau d'intégrité de sécurité d'un système instrumenté de sécurité. Cette approche est basée sur la collecte des données à partir des avis d'experts. Le processus de la collecte se caractérise par trois principales étapes : l'élicitation des avis d'experts avec une méthode qualitative, la division de ces avis à l'aide de l'algorithme de clustering k-moyenne et l'agrégation des avis d'experts en utilisant une méthode hiérarchique. Les résultats du processus de la collecte des données seront intégrés dans un modèle d'évaluation de risque afin d'obtenir le niveau d'intégrité de sécurité. Comme méthode d'évaluation, nous proposons une généralisation de la méthode du graphe de risque (Graphe de Risque Crédibiliste) capable de traiter les données imparfaites modélisées à l'aide des fonctions de croyance.

Contents

List of Figures

List of Tables

Introduction

Motivation and purpose

Currently, industrial facilities present different risks for persons, equipments and environment. Serious accidents are still caused by these risks. One of the solutions for dealing with these problems is having good safety systems. To design, implement and maintain these systems various standards can be used. For instance the IEC61508 standard (IEC61508, 2002) presents the Safety Instrumented Systems (SIS) whose main objective is reducing the occurrence probability of the risk.

The risk reduction process is based on the evaluation of the necessary risk reduction level according to the Safety Integrity Level (SIL) of the SIS. Several methods can be used for risk evaluation such as the risk graph (IEC61508, 2002) and the risk matrix (ISO14121-2, 2005).

Risk evaluation methods are based on various parameters. Getting these data becomes more and more difficult especially with the fast changes in the current society. Experts can be a good source of information to deal with these parameters. Collecting data from experts requires two basic steps: elicitation of expert opinions and aggregation of expert opinions.

There are many methods which can be used for the elicitation of expert opinions process. These methods are generally divided into two main approaches: the quantitative approaches and the qualitative approaches. In the quantitative approaches, experts' opinions are expressed as numbers according to an uncertainty theory. In the qualitative approaches (Ben Yaghlane et al., 2006a; Bryson and Mobolurin, 1999; Wong and Lingras, 1994), it is easier to experts to express their opinions as they can use the natural language.

Experts when giving their opinions can not be always sure and precise. Thus, data originating from experts are usually imperfect. Many mathematical theories are able to deal with this type of data such as probability theory, possibility theory (Zadeh, 1965) and evidence theory (Shafer, 1976).

The evidence theory becomes more and more popular. It is a simple and flexible way for modeling imperfect data. It is a powerful tool for combining data from different sources.

Data resulting from the elicitation process must be aggregated in order to get a unique, relevant and useful information. There are many combination rules that can be used for aggregating expert opinions in the evidence framework. We are interested in this work on a hierarchical method of aggregation (Ha-Duong, 2008).

The classic methods used for the risk evaluation are not able to deal with imperfect data resulting from expert opinions. To resolve this problem in the risk graph model, we propose a generalized risk graph based on belief functions theory.

Master contribution

In this work, we propose an approach for SIL allocation based on the belief functions theory. Our approach is based on two essential steps: collecting data from expert opinions and integrating these data into a risk evaluation method based on evidence theory in order to determine the safety integrity level of a SIS.

For collecting data, we elicit expert opinions using a qualitative method (Ben Yaghlane et al., 2006a), divide these opinions using the k-means algorithm (MacQueen, 1967) and aggregate them by means of a hierarchical method of aggregation of expert judgements (Ha-Duong, 2008). For SIL allocation we propose a generalized risk graph (IEC61508, 2002) based on the belief functions theory: Evidential Risk Graph.

Master organization

This report is organized as follows: Chapter 1 presents the risk evaluation process, it defines many concepts related to this process. In chapter 2, we present the treatment of uncertainty in the risk evaluation process. We detail the approach of collecting expert opinions in the evidence framework in chapter 3. In chapter 4, we describe the proposed evidential risk graph and the schema of the adopted approach and we present a case study to illustrate this approach. Finally, chapter 5 deals with the implementation and simulation tasks.

1
Risk evaluation process

1.1 Introduction

Many tasks in the industry fields induce high risk and cause serious accidents and injuries. Industrial facilities have to reduce the risk in order to avoid its consequences.

The risk reduction aims to reduce the occurrence probability of the risk. To achieve this aim, implementing a safety system will be very important. Many standards can be used to design these systems, one of the most used is the IEC standard (IEC61508, 2002).

Before reducing the risk, it is necessary to identify and evaluate it. The risk evaluation aims to identify the risk level in order to be able to reduce or eliminate the risk. Many risk evaluation methods can be adopted such as the risk graph (IEC61508, 2002) and the risk matrix (ISO14121-2, 2005).

In this chapter, we first introduce the concept of risk. Then we present some safety systems, the IEC standard and the risk reduction process. Finally, we detail some risk evaluation methods.

1.2 Risk concepts

1.2.1 Risk definition

The risk is not a new concept, it has been developed by several authors in the literature. According to (Villemeur, 1988), the risk is defined as "*a measure of a danger associat-*

ing a measure of the occurrence of an unwanted event and a measure of its effects or consequences".

Whereas Shaughnessy (O'Shaughnessy, 1992) proposed the following definition: "*The risk is established by the possibility that a fact having undesirable consequences occurs* ".

According to the IEC 61508 standard (IEC61508, 2002), the risk is "*A combination of the probability of a damage and its gravity*".

Gouriveau (Gouriveau, 2003) studied many definitions of this word and noticed that the risk can be defined as an association of the situation's causes and the related consequences. The causes can be characterized by their occurrence (P) and the effects by their impact (I). The correlation between P and I allows to build a risk indicator $R = f(P, I)$ (figure 1.1).

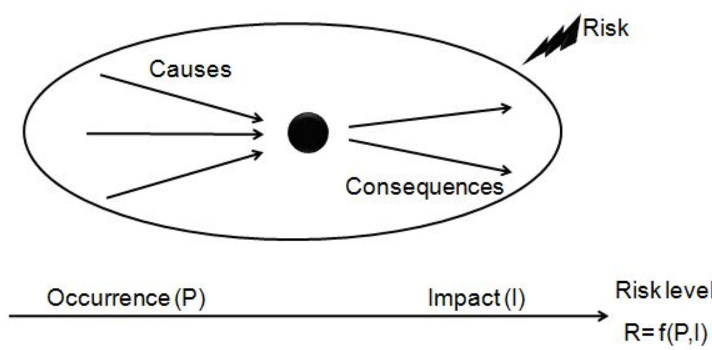

Figure 1.1: Risk components

1.2.2 Risk measure

The risk, as it is demonstrated in many of its definitions, is usually related to the couple (Gravity, Probability). Farmer (Farmer, 1967) has developed a relation between the risk and this couple in his curve shown in figure 1.2. Risks classified under the curve are considered to be acceptable, but those placed over the curve are not.

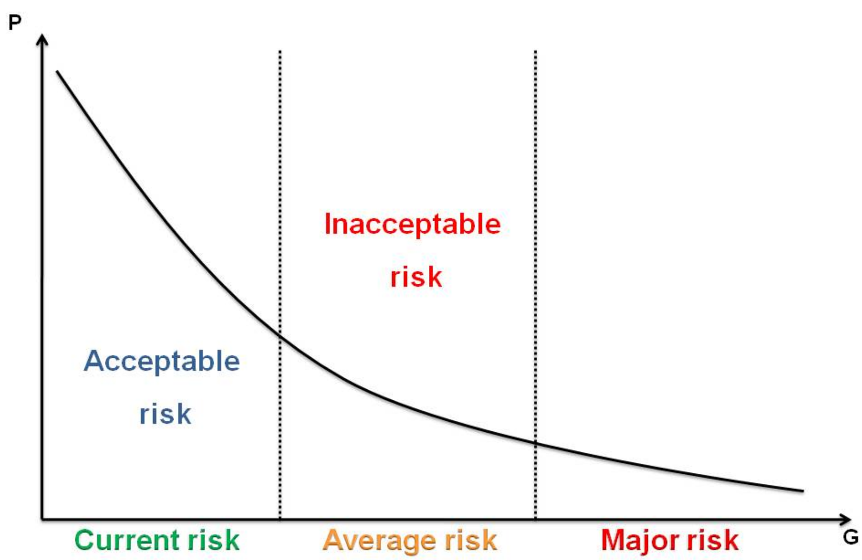

Figure 1.2: Farmer's curve (Farmer, 1967)

1.2.3 Risk types

The occurrence probability and the damage caused by the risk are different from a situation to another. Thus, different types of risk are deduced:

- **Tolerable risk:** According to the IEC standard (IEC61508, 2002) the tolerable risk is the risk accepted in a certain context and based on the current values of the company.

- **Major risk:** The major risk is characterized by its big number of victims, the cost of the equipment damage, and its impact on the environment (Tanzi and Delmer, 2003; Sallak, 2007).

- **Residual risk:** It is the remaining risk after taking all the prevention measures (IEC61508, 2002).

- **EUC risk:** Risk resulting from the EUC [1] or from the interaction of the EUC with its command system (IEC61508, 2002).

1.3 Safety systems

Safety is often defined by its opposite. It can be seen as the absence of danger, risk, accident or disaster (Sallak, 2007).

A safety system is a system aimed to achieve a safe state and maintain it for an equipment, a machine or any other device(IEC61508, 2002).

1.3.1 Electric/Electronic/Programmable Electronic Systems (E/E/PES)

Safety systems are based on different types of technologies: pneumatic, mechanic, hydraulic, electric, electronic, programmable electronic, etc...

Electric/electronic systems are used, for years, to execute safety functions in many sectors. Computer systems (usually called programmable electronic systems (PES)) become recently very important to fulfil functions related to the security or to any other field.

Thus, to use the electric/electronic systems and exploit the advantages of computing, the IEC 61508 standard (IEC61508, 2002) presents the Electric/Electronic/Programmable

[1] Equipment Under Control: equipment, machine, device or installation used for manufacturing, treatment, transport, medical or other activities (IEC61508, 2002).

Electronic Systems (E/E/PES) which are systems of command, protection or surveillance based on one or more Programmable Electronic devices. Figure 1.3 shows the structure of these systems according to the IEC 61508 standard.

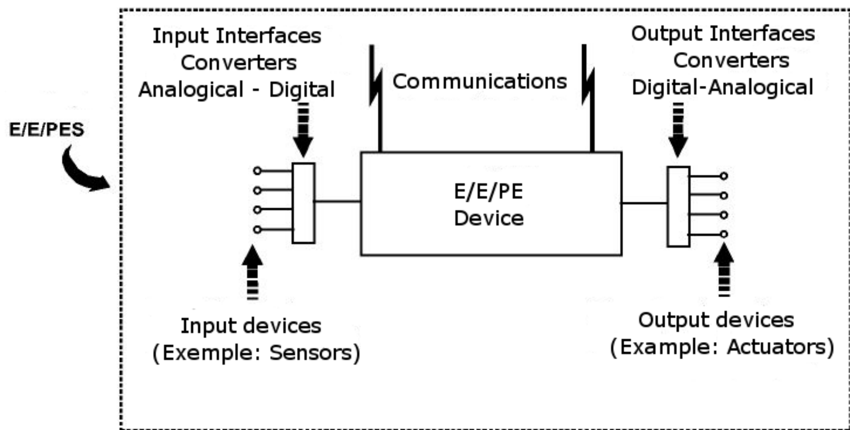

Figure 1.3: Structure and terminology of the electric/electronic/programmable electronic systems according to the IEC standard

1.3.2 Safety Instrumented Systems (SIS)

One of the most used E/E/PES is Safety Instrumented System (SIS). The main objective of this system is to take a process into a safe state when it is in a real risk situation.

A SIS is composed of three parts (figure 1.4). The *sensor part* is used to supervise the drift of a parameter towards a dangerous state. The *logic unit* is dedicated to collect the signal coming from the sensor, treat it and compute the actuator's input. The main objective of the third part (*actuator part*) is to put the process into a safe state and maintain it (Simon et al., 2006).

A SIS is used to implement Safety Instrumented Functions (SIF) that is intended to control parameters and implement actions in order to achieve or maintain a safe state for the supervised process with respect to the specific hazardous event (Indus-

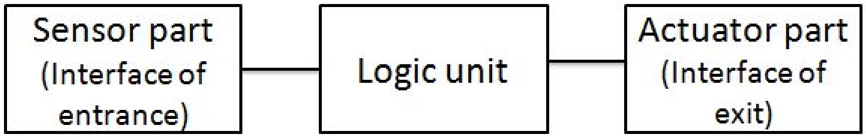

Figure 1.4: The structure of a SIS

tries, 2009).

Each SIF affords a measure of risk reduction indicated by its Safety Integrity Level (SIL). The IEC standard define the safety integrity level of a SIS according to the value of its average Probability of Failure on Demand (PFD_{avg}) for low demand systems (less than one solicitation per year) and its failure per hour for high demand systems or systems acting in continuous mode (table 1.1).

Table 1.1: SIL levels according to the IEC 61508

Solicitation	**Low Demand**	**High Demand**
SIL	PFD_{avg}	Failure/hour
1	$[10^{-2}, 10^{-1}[$	$[10^{-6}, 10^{-5}[$
2	$[10^{-3}, 10^{-2}[$	$[10^{-7}, 10^{-6}[$
3	$[10^{-4}, 10^{-3}[$	$[10^{-8}, 10^{-7}[$
4	$[10^{-5}, 10^{-4}[$	$[10^{-9}, 10^{-8}[$

1.4 IEC 61508 standard: Functional safety of E/E/PE Safety-related Systems

The IEC 61508 [2] standard (IEC61508, 2002) is an international standard designed for ensuring the functional safety of electrical / electronic / programmable electronic safety-related systems. This standard presents an approach for establishing E/E/PE

[2] International Electrotechnical Commission

systems by taking into account all the steps of the life cycle of these systems. It includes seven parts:

- **61508-1:** General requirements.
- **61508-2:** Requirements for E/E/PE safety-related systems.
- **61508-3:** Software requirements.
- **61508-4:** Definitions and abbreviations.
- **61508-5:** Examples of methods for the determination of safety integrity levels.
- **61508-6:** Guidelines on the application of parts 2 and 3.
- **61508-7:** Overview of techniques and measures.

The IEC standard is designed as a generic standard. It can be applied at any field where safety is treated using E/E/PE systems such as manufacturing industries, pharmaceutical processes, Nuclear, etc. The main objective of this standard is to be sure that the safety-related systems achieve correctly the required safety functions.

1.5 Risk reduction

The risk reduction concerns all the actions or measures aimed to decrease the probability or the gravity of the damage (INERIS-DRA-2006-P46055-CL47569:Omega7, 2006). The risk reduction becomes more important when the risk is considered unacceptable. The risk reduction process, according to the IEC standard, is shown in figure 1.5.

The measures adopted for risk reduction are divided, usually, on three types (INERIS-DRA-2006-P46055-CL47569:Omega7, 2006):

- **Prevention measure:** Measures to avoid or limit the probability of an unwanted event.
- **Limitation measure:** Measures to limit the intensity of the effects of a dangerous phenomenon.
- **Protection measure:** Measures to limit the consequences on the potential targets by decreasing the vulnerability.

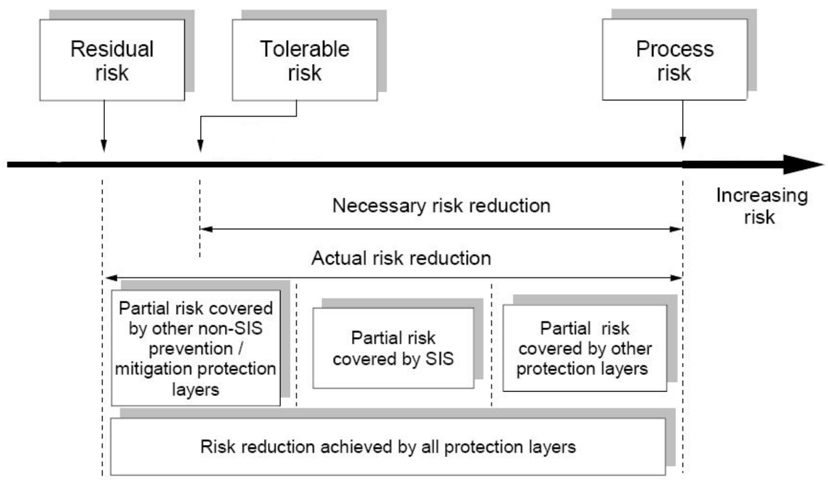

Figure 1.5: Risk reduction according to the IEC standard

1.6 Risk evaluation methods

1.6.1 Categories

Several methods are used to evaluate the risk level. These methods are divided on three categories (Simon et al., 2007):

- **Quantitative methods:** These methods compute the availability of a SIS using the failure rate and the repair failure rates of their components. The most widespread methods are: simplified equations (ISA-TR84.00.02-2002, 2002b); fault trees (ISA-TR84.00.02-2002, 2002a); markovian approaches (ISA-TR84.00.02-2002, 2002c).

- **Semi-quantitative methods:** The most widespread method is the matrix of risk. This matrix gives the level of SIL according to the gravity of the risk and the frequency of occurrence.

- **Qualitative methods:** They determine the level of SIL starting from the knowledge of the risks associated to the system.

In this work we are interested in semi-quantitative and qualitative methods which are generally less costly than the quantitative ones. Several semi-quantitative and qualitative methods have been proposed, the risk matrix and risk graph are among the most used ones.

1.6.2 Risk matrix

A risk matrix is a multidimensional table (in most of the cases a two dimension matrix) allowing the combination of any class of gravity of damage with any class of probability of occurrence of that damage (Etherton, 2007).

This method is very popular in system reliability and risk assessment fields. Its use is very simple. For every dangerous situation, a category (or a value) is allocated to every input parameter. The level of risk of the studied dangerous situation is obtained by projection of the categories of the parameters given in input on the risk matrix.

Figure 1.6 shows an example of a risk matrix according to (ISO14121-2, 2005; J.Marsot and L.Claudon, 2006). This matrix has four input parameters: the Severity (S), the Frequency of exposure (F), the probability of Occurrence (O) and the possibility of Avoidance (A).

Example 1.1
Let us consider a dangerous situation with a high gravity (S2), low exposure (F1), high probability of occurrence (O3) and low possibility of avoidance (A1).
The intersection between (S2, F1) and (O3, A1) gives the risk level: 3. ■

1.6.3 Risk graph

An other representation for determining the risk level is the risk graph. It is a graphical representation of the relation between the risk and its components. The risk graph is a good way to show visually and quickly the effect of a protective measure on the reduction of the studied risk.

An example of a risk graph used by the IRSST [3] is shown in figure 1.7. This graph is based on four parameters: the gravity of the risk, the frequency of exposure, the probability of occurrence and the possibility of avoidance.

[3] Institut de Recherche en Santé et en Sécurité du Travail en France

		Risk index calculation					
		O1		O2		O3	
		A1	A2	A1	A2	A1	A2
S1	F1	1				2	
	F2						
S2	F1	2			3		4
	F2	3	4		5		6

Figure 1.6: Risk matrix

The use of the risk graph is similar to a decision tree (Quinlan, 1986). According to the value of each parameter, a path is built. The risk level is, then, obtained by following this path.

Example 1.2
Let us consider a dangerous situation with a high gravity (severe injury), rare frequency of exposure, low probability of occurrence and possibility of avoidance of the dangerous situation. According to the graph, the path built with these values gives the risk level: 1 as shown in figure 1.7. ■

1.7 Conclusion

In this chapter, we have presented the basic concepts of the risk evaluation process. We have described how can reduce the risk by using safety systems such as the safety instrumented systems and adopting a risk evaluation method such as the risk graph.

In the next chapter we will study the treatment of uncertain data in the risk evaluation process.

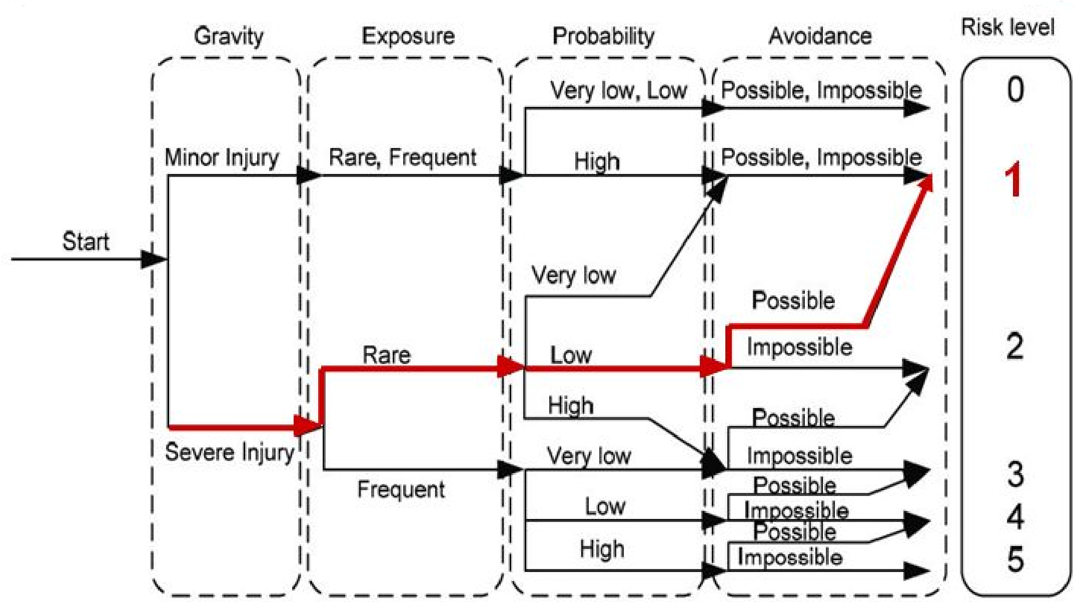

Figure 1.7: Risk Graph used by IRSST

2

Risk evaluation under uncertainty

2.1 Introduction

Risk evaluation methods are based on several parameters. Usually, these parameters are imperfect. Indeed, they can be incoherent, imprecise or/and uncertain. Many theories can be used for dealing with imperfect data, such as probability theory, possibility theory (Zadeh, 1965) and evidence theory (Shafer, 1976).

The evidence theory becomes more and more popular. It is a simple and flexible framework for dealing with imperfect information. It generalizes the probabilistic framework by its capacity to model the total and partial ignorance. Also, it is a powerful tool for combining data. Thus we are interested on the treatment of uncertainty using the evidence theory.

Several methods of risk evaluation have been proposed to deal with imperfect data. One of these methods is the fuzzy risk graph which extends the risk graph method.

In this chapter, we first introduce the basic concepts of the evidence theory. Then we present some risk evaluation methods able to deal with uncertainty.

2.2 Basic concepts of evidence theory

The evidence theory also known as *belief functions theory* or *Dempster-Shafer theory* was first introduced by Dempster in 1967 and Shafer in 1976. Several models have been proposed from this theory. One of the most used is the Transferable Belief Model developed by Smets to represent quantified beliefs. In the following, we remind some basic concepts of the TBM. More details can be found in (Shafer, 1976; Smets and Kennes, 1994; Smets and Gabbay, 1998).

2.2.1 Frame of discernment

Let Ω a finite set of exclusive and exhaustive elements called the frame of discernment and 2^Ω its power set defined by:

$$2^\Omega = \{A : A \subseteq \Omega\} \tag{2.1}$$

Example 2.1 Let us consider a variable W which can be one of the risk graph parameters. This variable can take three values: W_1, W_2 or W_3. Therefore its frame of discernment Ω is constituted of W_1, W_2 and W_3:

$\Omega = \{W_1,\ W_2,\ W_3\}$.

The corresponding power set is:

$2^\Omega = \{\emptyset,\ W_1,\ W_2,\ W_3,\ W_1 \cup W_2,\ W_1 \cup W_3,\ W_2 \cup W_3,\ W_1 \cup W_2 \cup W_3\}$. ■

2.2.2 Basic belief assignment

A basic belief assignment (*bba*) also named belief mass, is a function $2^\Omega \to [0, 1]$, such that:

$$\sum_{A \subseteq \Omega} m(A) = 1 \tag{2.2}$$

$m(A)$ is the portion of belief supporting exactly A. Any subset A of Ω such that $m(A) > 0$ is called a focal element. Let $\mathcal{F}(m) \subseteq 2^\Omega$ denotes the set of focal elements.

Example 2.2 The following belief masses are defined on the frame of discernment $\Omega = \{W_1,\ W_2,\ W_3\}$:

$m(W_1) = 0.2$

$m(W_2 \cup W_3) = 0.4$

$m(\emptyset) = 0.4$

The set of focal elements is $\mathcal{F}(m) = \{\{\emptyset\},\ \{W_1\},\ \{W_2 \cup W_3\}\}$. ■

If $m(\emptyset) = 0$, the related belief function is assumed to be normalized. In the TBM, the mass of the empty set can be non null. This mass is interpreted as a consequence of the open-world assumption. It is considered to be the expert's degree of belief that the variable's value is not an hypothesis belonging to Ω. The related belief function is then unnormalized.

An unnormalized belief mass m can be transformed into a normalized one $m\prime$ using the normalization operator defined as follows:

$$\begin{cases} m\prime(A) = \frac{m(A)}{1-m(\emptyset)} & \forall A \subseteq \Omega,\ m(\emptyset) \neq 1 \\ m\prime(\emptyset) = 0 \end{cases} \tag{2.3}$$

Example 2.3 The belief masses presented in 2.2 are an example of an unnormalized belief masses. Applying the normalization operator gives:
$m\prime(W_1) = 0.2/(1-0.4) = 0.33$
$m\prime(W_2 \cup W_3) = 0.4/(1-0.4) = 0.67$
$m\prime(\emptyset) = 0$

■

The mass $m(\Omega)$ is the degree of belief assigned to the whole frame of discernment. It represents the amount of the total ignorance.

2.2.3 Belief function

The belief function (or credibility function) corresponding to a belief mass m is a function $bel : 2^{\Omega} \to [0, 1]$, defined as:

$$bel(A) = \sum_{\emptyset \neq B \subseteq A} m(B) \tag{2.4}$$

$bel(A)$ gives the amount of support given to A.

Example 2.4 Suppose that an expert gave these belief masses:
$m(W_1) = 0.6$
$m(W_1 \cup W_3) = 0.2$
$m(W_1 \cup W_2) = 0.2$
The corresponding credibility function is:
$bel(W_1) = 0.6$

$bel(W_1 \cup W_2) = 0.8$
$bel(W_1 \cup W_3) = 0.8$
$bel(\Omega) = 1$

■

$m(A)$ may be derived from $bel(A)$ as follows:

$$\begin{cases} m(A) = \sum_{A \subseteq B} (-1)^{|B|-|A|} bel(A) \\ m(\emptyset) = 1 - bel(\Omega) \end{cases} \tag{2.5}$$

Some belief functions can have particular values. In the following, we present some of these special belief functions:

- *Categorical belief function:* A categorical belief function is a normalized belief function, it is characterized by an unique focal element which is different from Ω and $\emptyset$. This belief function can be defined as follows:

$$m^{\Omega}(A) = \begin{cases} 1 & \text{if } A = A^{\star} \subset \Omega \\ 0 & \forall A \subseteq \Omega \text{ and } A \neq A^{\star} \end{cases} \tag{2.6}$$

Example 2.5 The following belief function is categorical:
$m(W_1 \cup W_2) = 1$

■

- *Vacuous belief function (VBF):* A vacuous belief function is a normalized belief function having an unique focal element which is Ω. Its corresponding belief function is defined as follows:

$$m^{\Omega}(A) = \begin{cases} 1 & \text{if } A = \Omega \\ 0 & \text{otherwise} \end{cases} \tag{2.7}$$

This belief function is used to express the total ignorance of an expert. Thus, when an expert have no idea about the real value of the variable, he attributes the unit to the Ω meaning that all hypotheses can be the variable's real value.

Example 2.6 The following belief function is vacuous:
$m(\Omega) = 1$

■

- *Contradictory belief function:* A contradictory belief function is a belief function having the contradictory belief function is a non normalized belief function having an unique focal element which is the empty set $\emptyset$. Its corresponding bba is defined as follows:

$$m^{\Omega}(A) = \begin{cases} 1 & \text{if } A = \emptyset \\ 0 & \text{otherwise} \end{cases} \tag{2.8}$$

Example 2.7 The following belief function is contradictory:
$m(\emptyset) = 1$

■

- *Dogmatic belief function:* A dogmatic belief function is a belief function such that Ω is not a focal element:

$$m^{\Omega}(\Omega) = 0 \tag{2.9}$$

Example 2.8 The following belief function is dogmatic:
$m(W_1) = 0.6$
$m(W_1 \cup W_3) = 0.2$
$m(W_1 \cup W_2) = 0.2$

■

- *Bayesian belief function:* A Bayesian belief function is a bba such that all focal elements are singletons:

$$\begin{cases} m^{\Omega}(A) \in [0,1] & \text{if } \mid A \mid = 1 \\ m^{\Omega}(A) = 0 & \text{otherwise} \end{cases} \tag{2.10}$$

Example 2.9 The following belief function is bayesian:
$m(W_1) = 0.6$
$m(W_2) = 0.2$
$m(W_3) = 0.2$

■

This belief function corresponds to a probability distribution.

- *Certain belief function:* A certain belief function is a categorical belief function such that its unique focal element is a singleton. This bba represents the total certainty. Its corresponding bba is defined as follows:

$$\begin{cases} m^{\Omega}(A) = 1 & \text{if } A \in \Omega \\ m^{\Omega}(B) = 0 & B \subseteq \Omega \text{ and } B \neq A \end{cases} \tag{2.11}$$

Example 2.10 Let us assume that the experts affirmed that the value of W is W_1, then we get:
$m(W_1) = 1.$ ■

- *Consonant belief function:* A consonant belief function is a belief function where the focal elements are nested ($A_1 \subset A_2 \subset \ldots \subset \Omega$).

Example 2.11 The following belief function is consonant:
$m(W_1) = 0.2$
$m(W_1 \cup W_2) = 0.3$
$m(W_1 \cup W_2 \cup W_3) = 0.5$

■

2.2.4 Plausibility function

The plausibility function associated with m is a function $pl : 2^{\Omega} \rightarrow [0, 1]$, defined by:

$$pl(A) = \sum_{\emptyset \neq B \cap A} m(B) \tag{2.12}$$

$pl(A)$ represents the maximum amount of potential specific support that could be given to A, it contains parts of belief that do not contradict A.

Example 2.12 Suppose that an expert gave these belief masses as an attribute's value:
$m(W_1) = 0.2$
$m(W_1 \cup W_3) = 0.5$
$m(W_1 \cup W_2) = 0.3$
The corresponding credibility function is:
$pl(W_1) = 1$
$pl(W_2) = 0.3$
$pl(W_1 \cup W_2) = 1$

$pl(W_3) = 0.5$
$pl(W_1 \cup W_3) = 1$
$pl(W_2 \cup W_3) = 0.8$
$pl(\Omega) = 1$

■

$m(A)$ may be obtained from $pl(A)$ as follows:

$$\begin{cases} m(A) = \sum_{A \subseteq B} (-1)^{|B|-|A|+1} pl(\bar{A}) \\ m(\emptyset) = 1 - pl(\Omega) \end{cases} \tag{2.13}$$

2.2.5 Commonality function

The commonality function has no significant meaning but it is used to simplify computations. A commonality function associated to a *bba* m is a function $q : 2^{\Omega} \rightarrow [0, 1]$, defined by:

$$q(A) = \sum_{A,B \subseteq \Omega, B \supseteq A} m(B) \tag{2.14}$$

Example 2.13 Suppose that an expert gave these belief masses as an attribute's value:

$m(W_2 \cup W_3) = 0.4$
$m(W_1 \cup W_3) = 0.3$
$m(W_1 \cup W_2) = 0.3$

The corresponding commonality function is:

$q(\emptyset) = 1$
$q(W_1) = 0.6$
$q(W_2) = 0.7$
$q(W_1 \cup W_2) = 0.3$
$q(W_3) = 0.7$
$q(W_1 \cup W_3) = 0.3$
$q(W_2 \cup W_3) = 0.4$

■

$m(A)$ may be obtained from $q(A)$ as follows:

$$m(A) = \sum_{A \subseteq B} (-1)^{|B-A|} q(B) \tag{2.15}$$

2.2.6 Combination of belief functions

The belief function theory is a strong tool for combining data originating from many sources of information.

Let m_1 and m_2 two $bba's$ representing two sources of information and having the same frame of discernment Ω. Different rules can be used to combine these pieces of information. Here are some of the commonly used rules:

- *Dempster's rule of combination*: (Dempster, 1967) this rule is denoted by $\oplus$, it is defined by the following formula:

$$(m_1 \oplus m_2)(A) = \begin{cases} \dfrac{\sum\limits_{B \cap C = A} m_1(B)\ .\ m_2(C)}{1 - \sum\limits_{B \cap C = \emptyset} m_1(B)\ .\ m_2(C)} & \forall A \subseteq \Omega,\ A \neq \emptyset \\ 0 & \text{if } A = \emptyset \end{cases} \tag{2.16}$$

- *The conjunctive rule of combination (CRC)*: denoted by $\ocap$ and defined as follows:

$$(m_1 \ocap m_2)(A) = \sum_{B,C \subseteq \Omega:\ \ B \cap C = A} m_1(B).m_2(C) \tag{2.17}$$

- *The disjunctive rule of combination (DRC)*: denoted by $\ocup$ and defined as:

$$(m_1 \ocup m_2)(A) = \sum_{B,C \subseteq \Omega:\ \ B \cup C = A} m_1(B).m_2(C) \tag{2.18}$$

- *The cautious conjunctive rule*: It is an extension of the conjunctive rule of combination (Denœux, 2008). This rule is denoted by $\owedge$ and obtained by the following formula:

$$m_1 \owedge m_2 = \cap_{A \subsetneq \Omega} A^{\omega_1(A) \wedge \omega_2(A)} \tag{2.19}$$

where $\wedge$ denotes the minimum operator and $\omega(A)$ is the weight of every $A \in 2^{\Omega} \setminus \{\Omega\}$ obtained by:

$$\omega(A) = \prod_{B \supseteq A} q(B)^{(-1)^{|B|-|A|+1}} \tag{2.20}$$

where $|A|$ is the cardinality of A, and A^{ω} denotes the Generalized Simple BBA (GSBBA). It is a function $\mu : 2^{\Omega} \longrightarrow \Re$ verifying:

$$\begin{aligned} &\mu(A) = 1 - \omega \\ &\mu(\Omega) = \omega \\ &\mu(B) = 0,\ \ \forall B \in 2^{\Omega}\ A, \Omega \end{aligned} \tag{2.21}$$

for $A \neq \Omega$ and $\omega \in [0, +\infty)$.

Example 2.14 In table 2.1, we present two $bba's$ m_1 and m_2 given by two different sources of information, these $bba's$ are combined using the different combination rules presented previously.

Table 2.1: Combining information using different rules of combination

	$\mathbf{m_1}$	$\mathbf{m_2}$	$\mathbf{m_{1\oplus 2}}$	$\mathbf{m_{1 \bigcirc\!\!\!\!\cap\, 2}}$	$\mathbf{m_{1 \bigcirc\!\!\!\!\cup\, 2}}$	$\mathbf{m_{1 \bigcirc\!\!\!\!\wedge\, 2}}$
$\emptyset$	0.1	0	0	0.292	0	0.4226
W_1	0.05	0.3	0.209	0.148	0.045	0.1279
W_2	0.3	0.4	0.5819	0.412	0.16	0.2789
$W_1 \cup W_2$	0.2	0.1	0.1102	0.078	0.315	0.0620
W_3	0.06	0	0.0169	0.012	0	0.0186
$W_3 \cup W_1$	0.01	0	0.0028	0.002	0.021	0.0031
$W_3 \cup W_2$	0.1	0	0.0282	0.02	0.064	0.031
Ω	0.18	0.2	0.0508	0.036	0.395	0.0558

■

The use of all these rules of combination depends on the dependency and reliability of the data sources. This problem will be discussed in 3.3.1.

2.2.7 Refinement and vacuous extension of belief functions

Let $m\prime$ be a *bba* defined on a frame of discernment $\Omega\prime$ and Ω a refinement ρ of $\Omega\prime$. It means that for every proposition $\omega\prime \in \Omega\prime$ is associated one or more elements in Ω. The *bba* $m\prime$ can be extended to a larger frame Ω using the vacuous extension (Shafer, 1976) denoted by $m^{\Omega\prime\uparrow\Omega}$. The values of $m^{\Omega\prime\uparrow\Omega}$ are given by:

$$m^{\Omega\prime\uparrow\Omega}(\omega) = \begin{cases} m^{\Omega\prime}(\omega\prime); & if\ \ \omega = \rho(\omega\prime) \\ 0 & otherwise \end{cases} \tag{2.22}$$

where $\rho(\omega\prime)$ is the image of $\omega\prime$ under ρ.

Example 2.15 Let $\Omega\prime = \{W, P\}$ and $\Omega = \{W_1, W_2, W_3, P_1, P_2\}$ its refinement such that $\rho(W) = \{W_1, W_2, W_3\}$ and $\rho(P) = \{P_1, P_2\}$.

Let $m\prime$ be a *bba* defined on $\Omega\prime$ by:
$m\prime(\{W\}) = 0.2$; $m\prime(\Omega\prime) = 0.8$
The vacuous extension of $m\prime$ to Ω is a *bba* defined as follows:
$m^{\Omega\prime\uparrow\Omega}(\{W_1, W_2, W_3\}) = 0.2$; $m^{\Omega\prime\uparrow\Omega}(\Omega) = 0.8$ ■

2.2.8 Discounting

The discounting is needed when sources of information are not considered fully reliable. Suppose that a source of a belief m is considered reliable at a level α and not reliable at a level $1 - \alpha$, thus the belief m is transformed into m^* using the following formula (Smets, 2000):

$$\begin{cases} m^*(A) = \alpha m(A), \ \forall A \neq \Omega \\ m^*(\Omega) = 1 - \alpha + \alpha m(\Omega) \end{cases} \tag{2.23}$$

where $\alpha \in]0, 1]$.

2.2.9 The pignistic transformation

The problem of making decisions from beliefs is resolved in the TBM by the pignistic transformation which gives a probability measure denoted by $BetP$ in order to use it for decision making. The pignistic transformation is defined as follows:

$$BetP(A) = \sum_{B \subseteq \Omega} \frac{|A \cap B|}{|B|} \frac{m(B)}{1 - m(\emptyset)} \quad \forall A \subseteq \Omega \tag{2.24}$$

where $|A|$ denotes the cardinality of A.

Example 2.16 Let us finish with the same example 2.2 and suppose that an expert gave these $bba's$:
$m^{\Omega}(\{W_1\}) = 0.2$
$m^{\Omega}(\{W_2\}) = 0.4$
$m^{\Omega}(\{W_1 \cup W_3\}) = 0.3$
$m^{\Omega}(\Omega) = 0.1$
After applying the pignistic transformation, we obtain:
$BetP\{W_1\} = 0.38$
$BetP\{W_2\} = 0.44$
$BetP\{W_3\} = 0.18$
We note that the most probable value of the risk graph parameter W is $W2$. Thus, if we have to decide, we will choose this hypothesis. ■

2.3 Risk evaluation methods under uncertainty: State of Art

As we previously said the risk evaluation methods are based on several parameters which are usually imperfect. Classical methods are not able to deal with uncertainty. Several works have been developed to resolve this problem.

2.3.1 Works related to risk evaluation methods under uncertainty

For dealing with uncertainty, many classical methods of risk evaluation have been extended using an uncertainty theory such as probability theory, possibility theory and evidence theory.

Some of these methods are summarized in table 2.2. The first column in this table includes the classical method of risk evaluation and the second indicates the uncertainty representation used for dealing with imperfect data. More details about these methods can be found in references in the third column.

Table 2.2: Works related to risk evaluation methods under uncertainty

Evaluation method	Uncertainty representation	Reference
Risk graph	Fuzzy sets	(Nait-Said and Ouzraoui, 2008)
Risk graph	Fuzzy sets	(Simon et al., 2007)
Fault tree	Possibility theory and Fuzzy sets	(Sallak and Simon, 2006)
Fault tree	Probability theory and Fuzzy sets	(Sallak and Aubry, 2005)
Fault tree	Belief functions	(Schön and Denoeux, 2004)

As we previously mentioned, we are interested in this work in semi-quantitative and qualitative methods and more especially on the risk graph method. Therefore, we present in the following an example of risk graph able to deal with imprecise data.

2.3.2 Fuzzy risk graph

The fuzzy risk graph (Simon et al., 2007) is based on the same parameters of the standard risk graph. These parameters are modeled using fuzzy numbers and possibility theory.

The fuzzy risk graph is based on three main steps:

1. **Fuzzy partition and fuzzyfication:** this step consists on defining the fuzzy partitions (figure 2.1) of the four parameters used in the fuzzy risk graph. These partitions must be in the reference scales provided to the experts.

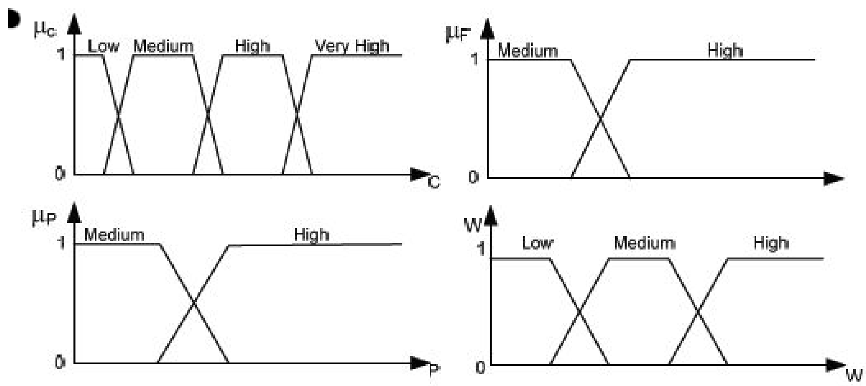

Figure 2.1: Evaluation scale partitions

2. **Inference system:** to take into account the uncertainty of data, the fuzzy risk graph uses a fuzzy inference system which is able to establish the relation between inputs fuzzy variables and output one (Simon et al., 2007).

   Two main operators are used in this context: the *T-norms* (conjunctive operators AND) and the *T-conorms* (disjunctive operator OR). To define these operators in the fuzzy logic Simon et al. used the product and the probabilistic sum operators (Simon et al., 2007).

Thus, the fuzzy inference system of the fuzzy risk graph is constituted of a set of $if..then$ rules (figure 2.2).

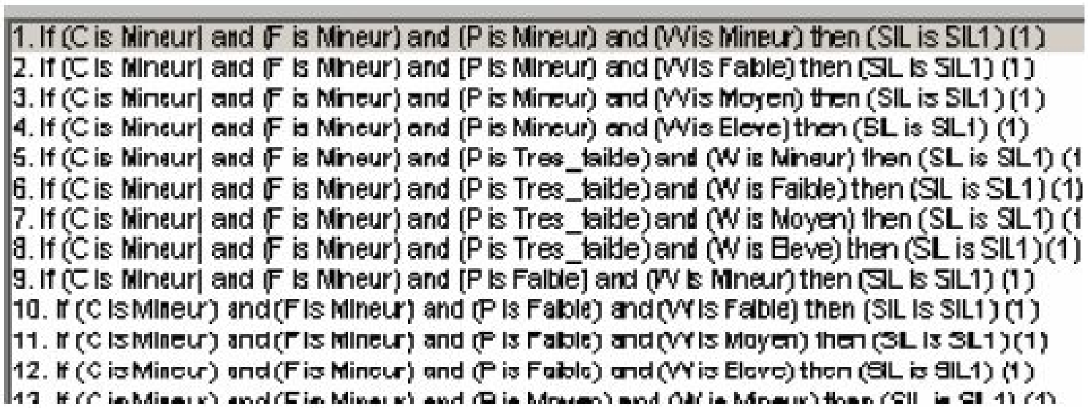
1. If (C is Mineur) and (F is Mineur) and (P is Mineur) and (W is Mineur) then (SIL is SIL1) (1)
2. If (C is Mineur) and (F is Mineur) and (P is Mineur) and (W is Faible) then (SIL is SIL1) (1)
3. If (C is Mineur) and (F is Mineur) and (P is Mineur) and (W is Moyen) then (SIL is SIL1) (1)
4. If (C is Mineur) and (F is Mineur) and (P is Mineur) and (W is Eleve) then (SIL is SIL1) (1)
5. If (C is Mineur) and (F is Mineur) and (P is Tres_faible) and (W is Mineur) then (SIL is SIL1) (1
6. If (C is Mineur) and (F is Mineur) and (P is Tres_faible) and (W is Faible) then (SIL is SIL1) (1)
7. If (C is Mineur) and (F is Mineur) and (P is Tres_faible) and (W is Moyen) then (SIL is SIL1) (1
8. If (C is Mineur) and (F is Mineur) and (P is Tres_faible) and (W is Eleve) then (SIL is SIL1) (1)
9. If (C is Mineur) and (F is Mineur) and (P is Faible) and (W is Mineur) then (SIL is SIL1) (1)
10. If (C is Mineur) and (F is Mineur) and (P is Faible) and (W is Faible) then (SIL is SIL1) (1)
11. If (C is Mineur) and (F is Mineur) and (P is Faible) and (W is Moyen) then (SIL is SIL1) (1)
12. If (C is Mineur) and (F is Mineur) and (P is Faible) and (W is Eleve) then (SIL is SIL1) (1)

Figure 2.2: Fuzzy inference system

3. **Output fuzzy partition and defuzzyfication:** The SIL levels are obtained after performing the inference system of the fuzzy risk graph. These levels are modeled in a continuous scale. Thus, the decision is made using the defuzzification operation based on the center of gravity.

2.4 Conclusion

In this chapter, we have presented the belief function theory which is a good tool to deal with uncertain data in the risk evaluation process.

Then, we have given an example of a risk evaluation method which is able to take into account uncertain data using the fuzzy numbers and the possibility theory.

In chapter 3, we will study the process of collecting data from expert opinions. This process depends on two essential steps: the elicitation and the aggregation of expert opinions.

3

Collecting expert opinions

3.1 Introduction

As we previously mentioned, risk evaluation methods are based on different parameters. The process of collecting these parameters is very important to get correct and relevant results.

However, getting needed information is currently very difficult. Experiences are not always possible and they can not give at all times the expected and useful results. So, experts' opinions can be a good solution for these problems.

Data provided by experts can not be always perfect, thus several methods of elicitation and aggregation have been proposed in order to deal with this type of data.

We are interested in this work on the elicitation and aggregation of expert opinions using the belief function theory. Many methods are proposed in this context such as the qualitative method for eliciting expert judgements proposed by Ben Yaghlane et al. (Ben Yaghlane et al., 2006a) and the hierarchical method for aggregating expert opinions proposed by Ha-Duong (Ha-Duong, 2008).

In this chapter, we first present the process of elicitation of expert opinions. Then, we introduce the adopted method for aggregating expert judgements. Finally, we present the k-means (MacQueen, 1967) algorithm used for dividing expert opinions into groups.

3.2 Elicitation of expert opinions

Getting efficient information from expert opinions needs to model them in a proper way. Two main approaches are generally adopted for elicitation of expert opinions: the quantitative approaches and the qualitative approaches.

3.2.1 Quantitative approaches

In the quantitative approaches, the expert is asked to give his judgement using numbers. Depending on the problem, these numbers can be modeled according to the probability, possibility or evidence theory.

For example in the probability theory, experts are generally asked to give (Sandri and Kalfsbeek, 1995):

- The 5%, 50% and the 95% quantiles.
- The mean, the mode or the median of the distribution.
- The distribution function.

In the possibility theory, experts can give:

- Several intervals using fuzzy numbers.
- Possibility distributions.

It is possible to transform these opinions (expressed in probability or possibility theory) into evidence theory using the following formula (Ha-Duong, 2008):

- Any probability function $p :\rightarrow [0, 1]$ naturally defines a *bba* m by:

$$\begin{cases} m(\omega) = p(\omega) \quad \text{for any } \omega \in \Omega \\ m(X) = 0 \quad \text{if } |X| \neq 1 \end{cases} \tag{3.1}$$

- A normalized possibility distribution is a function $\pi : \Omega \rightarrow [0, 1]$ such that $max_{\omega \in \Omega} \pi(\omega) = 1$. Given such π, a BBA m naturally associated with π can be computed via its commonality function as follows:

$$q(A) = min_{\omega \in A} \pi(\omega) \tag{3.2}$$

$$m(A) = \sum_{B \supseteq A} (-1)^{|B|-|A} q(B) \tag{3.3}$$

In this approach, it is very difficult to experts to express their opinions especially when they are not familiar with the theory used in the elicitation problem. Then, the qualitative approach can be more suitable to elicit experts' opinions.

3.2.2 Qualitative approaches

In this approach, experts can easily express their opinions using natural language. Several methods have been proposed for eliciting qualitatively expert opinions.

Wong and Lingras' method

Wong and Lingras (Wong and Lingras, 1994) proposed a method for representing preferences by quantitative belief functions. This method is based on modeling expert opinions using two binary relations: the preference relation denoted by $\gtrdot$ and the indifference relation denoted by $\sim$.

Let A and B two propositions in the frame of discernment Ω. If the expert prefers A to B, then $A \gtrdot B$. If he is indifferent, then $A \sim B$. These preference relations are represented by a belief function as follows:

$$A \gtrdot B \Leftrightarrow bel(A) > bel(B) \tag{3.4}$$

$$A \sim B \Leftrightarrow bel(A) = bel(B) \tag{3.5}$$

The process of generating the belief function from the preference relations is based on two steps:

1. **Determination of the focal elements:** considering initially that all the propositions in Ω are focal elements and then eliminating some propositions according to the following condition: if $A \sim B$ and $B \subset A$ then A is not a focal element.

2. **Computation of the basic belief assignment:** this step consists on the resolution of a system of equalities and inequalities defined by equations (3.4) and (3.5).

Bryson and Mobolurin's method

Bryson and Mobolurin (Bryson and Mobolurin, 1999) proposed a method for generating belief function from qualitative preferences. This method is based on several steps:

1. Qualitative scoring: each proposition in the frame of discernment is assigned first to a $BROAD$ category bucket, then to a corresponding $INTERMEDIATE$ bucket and finally to a corresponding $NARROW$ bucket according to a qualitative scoring table.
2. Identifying and removing non-focal elements using the qualitative scoring table.
3. Providing numeric intervals to indicate his beliefs on the relative truthfulness of the proposition.
4. Checking the beliefs provided in step 3.
5. Generating belief function by providing a *bba* interval and a belief interval for each focal element.
6. Checking the $bba's$ and beliefs generated in the previous step. If they are acceptable then the process is stopped, else the process is repeated.

Ben Yaghlane et al.' method

Ben Yaghlane et al. (Ben Yaghlane et al., 2006a; Ben Yaghlane et al., 2006b) proposed a method for constructing belief functions from qualitative expert opinions. The main idea of this method is generating belief functions from expert opinions using the preference relations proposed in (Wong and Lingras, 1994) and defined by equations (3.4) and (3.5). These relations will be transformed as follows:

$$A \gtrdot B \Leftrightarrow bel(A) - bel(B) \geq \varepsilon \tag{3.6}$$

$$A \sim B \Leftrightarrow -\varepsilon \leq bel(A) - bel(B) \leq \varepsilon \tag{3.7}$$

where $\varepsilon > 0$ is a constant given by an expert. It is considered to be the smallest gap that the expert may discern between the degrees of belief in two propositions A and B.

Relations defined in equations (3.6) and (3.7) will constitute the constraints of an optimization problem. The objective function of this optimization problem is to maximize an uncertainty measure (UM) of the belief functions generated.

In order to take into account more than one objective in the optimization problem, Ben Yaghlane et al. proposed different multi-objective optimization models using goal programming. More details can be found in (Ben Yaghlane et al., 2006a; Ben Yaghlane et al., 2006b).

Ben Yaghlane et al. proposed an easier way to elicit expert opinions: instead of expressing their opinions using binary relations, experts can order their preferences by giving a rank for each focal element in the frame of discernment. Then, this order will built the constraints of an optimization problem which has also as an objective function maximizing an uncertainty measure.

This method has the advantage of taking into account the quality of the constructed belief functions and the inconsistency of the preference relations provided by the expert.

3.3 Aggregation of expert opinions

Once the elicitation step is achieved, an aggregation process will be very important in order to get a unique and reliable information that represents all experts' opinions. Here, we are interested in aggregating data using the belief functions framework.

3.3.1 Combination of expert opinions in the belief functions theory

As mentioned previously, many rules in evidence theory can be used for the fusion of expert judgements. The efficiency of these rules depends on the reliability and dependence of the sources of information.

For instance, the conjunctive rule is usually used for combining two *bbas* produced by distinct and reliable sources of information. For the fusion of evidences provided by sources which are distinct but not considered all reliable, the disjunctive rule is generally used. The cautious conjunctive rule is suitable when sources are correlated

(Denœux, 2008; Smets, 2000).

Then, it will be interesting to have a combination method based on more than one rule of combination which can be able to combine different types of information sources.

3.3.2 Hierarchical method for aggregation of expert opinions

Ha-Duong (Ha-Duong, 2008) proposed a hierarchical method for aggregating expert opinions based on two rules of combination of expert opinions. The main idea of this method is to combine conjunctively coherent sources of information and then combining disjunctively partially aggregated opinions. It is based on three essential steps:

1. Dividing expert opinions into schools of thought, i. e. experts which have similar opinions will be in the same group.
2. Combining information within each group using the cautious conjunctive rule assuming that sources in each group are reliable but not independent.
3. Combining the different results of the second step using the disjunctive rule supposing that the groups of experts are independent but not all reliable.

These steps are presented by the following formula:

$$m_{Hierarchical} = \textcircled{\cup}_{k=1..N} \ \textcircled{\wedge}_{i \in G_k} discount(m_i, 0.999) \tag{3.8}$$

where N denotes the number of groups and $G_1 ... G_N$ represent the different groups of experts.

This approach is extremely dependent on the step of dividing experts. This step becomes more difficult when the number of experts is very large. So, we propose to divide them automatically using a clustering algorithm.

Example 3.1 Lets consider the opinions of three experts concerning the parameter W expressed in the frame of discernment $\Omega = \{W_1,\ W_2,\ W_3\}$. The opinions of these experts are given in table 3.1:

The opinions of these experts can be divided into two groups. The first group contains expert1 and expert2 and the second group contains expert3.

Table 3.1: Expert opinions expressed using the evidence theory

Expert	**Opinion**
Expert1	$m(W_1) = 0.1; m(W_1 \cup W_2) = 0.7; m(\Omega) = 0.2$
Expert2	$m(W_2) = 0.2; m(W_1 \cup W_2) = 0.5; m(\Omega) = 0.3$
Expert3	$m(W_1) = 0.7; m(W_1 \cup W_3) = 0.3$

The result of combining the opinions within each group is summarized in the second and fourth column of table 3.2. After aggregating the $bba's$ of each group of experts, the final result of the hierarchical method of aggregation is given in column four. ■

Table 3.2: Results of aggregation within each group of experts

Elements	**Result of group1**	**Result of group2**	**Final result**
$m(\emptyset)$	0	0.02	0
$m(W_1)$	0	0	0
$m(W_2)$	0	0.1798	0
$m(W_3)$	0	0	0
$m(W_1 \cup W_2)$	0.6993	0.0799	0.0699
$m(W_1 \cup W_3)$	0.2997	0	0.0299
$m(W_2 \cup W_3)$	0	0.6599	0.5872
$m(\Omega)$	0.001	0.0604	0.3130

3.4 Clustering method for dividing expert opinions

The clustering is the process of organizing objects into groups (clusters) by maximizing the similarity of objects within the same group and maximizing the dissimilarity of objects belonging to different clusters (San et al., 2004).

One of the well spread techniques of clustering is the k-means algorithm (MacQueen,

1967) proposed by MacQueen in 1967. As described in (Jain, 2009), the k-means algorithm is based on the following steps:

1. Select arbitrarily an initial partition with K clusters (figure 3.1);

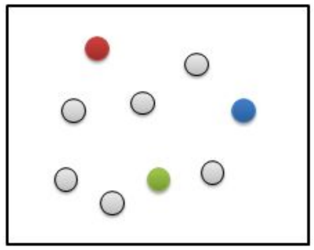

Figure 3.1: First step of k-means algorithm

2. Compute cluster centers (figure 3.2);

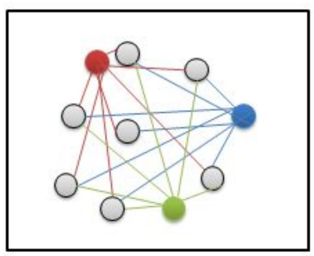

Figure 3.2: Second step of k-means algorithm

3. **Repeat**:

   (a) Generate a new partition by assigning each object to its nearest cluster center.

   (b) Compute new cluster centers.

   Until cluster membership stabilizes (clusters do not change from an iteration to another) (figure 3.3);

Example 3.2 Let us consider a set T containing 7 clusters: $T = \{1,\ 2,\ 3,\ 6,\ 7,\ 8,\ 13,\ 15,\ 17\}$. The results of k-means algorithm application using Euclidean distance (for simplicity)

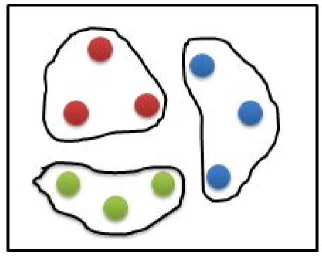

Figure 3.3: Third step of k-means algorithm

and choosing $k = 3$ are given in table 3.3.

■

Two parameters are essential in this algorithm: the number of clusters K and the metric used to measure the similarity (distance) between objects. In our work, we assume that K is given by a manager. For the metric used in this algorithm we need one able to measure the distance between two bodies of evidence. The distance of Jousselme et al. (Jousselme et al., 2001) is widely used in the belief functions framework. This distance takes into account the specificity of the belief function by inducing the cardinalities of the focal elements in the distance's calculation. It is defined as follows:

$$d_{BPA}(m_1, m_2) = \sqrt{\frac{1}{2}(\overrightarrow{m_1} - \overrightarrow{m_2})^T D(\overrightarrow{m_1} - \overrightarrow{m_2})} \tag{3.9}$$

where m_1 and m_2 are two bodies of evidence defined on the same frame of discernment Ω. $\overrightarrow{m_1}$ and $\overrightarrow{m_2}$ are vectors containing the $bba's$ of m_1 and m_2. D is a $2^{|\Omega|} \times 2^{|\Omega|}$ matrix whose elements are defined as:

$$D(A, B) = \begin{cases} 1 & \text{if A=B=}\emptyset \\ \frac{|A \cap B|}{|A \cup B|} & \forall A, B \in 2^{\Omega} \end{cases} \tag{3.10}$$

where $|A|$ denotes the cardinality of A.

Example 3.3 Suppose that two sources S_1 and S_2 provide us two $bba's$ m_1 and m_2, respectively:

$m_1(W_1) = 0.5$, $m_1(W_2) = 0.5$.

$m_2(W_1) = 0.3$, $m_2(W_3) = 0.3$, $m_2(W_2) = 0.4$.

The distance between m_1^{Ω} and m_2^{Ω} using Jousselme distance is:

$d_{BPA}(m_1, m_2) = 0.26$ ■

Table 3.3: Application of K-means algorithm

Step	**Clusters**	**Means**
1	$C_1 = \{1\}$ $C_2 = \{2\}$ $C_3 = \{3\}$	$M_1 = 1$ $M_2 = 2$ $M_3 = 3$
2	$C_1 = \{1\}$ $C_2 = \{2\}$ $C_3 = \{3,\ 6,\ 7,\ 8,\ 13,\ 15,\ 17\}$	$M_1 = 1$ $M_2 = 2$ $M_3 = 9.86$
3	$C_1 = \{1\}$ $C_2 = \{2,\ 3\}$ $C_3 = \{6,\ 7,\ 8,\ 13,\ 15,\ 17\}$	$M_1 = 2$ $M_2 = 2.5$ $M_3 = 11$
4	$C_1 = \{1\}$ $C_2 = \{2,\ 3,\ 6\}$ $C_3 = \{7,\ 8,\ 13,\ 15,\ 17\}$	$M_1 = 1$ $M_2 = 3.67$ $M_3 = 12$
5	$C_1 = \{1,\ 2\}$ $C_2 = \{3,\ 7,\ 8\}$ $C_3 = \{8,\ 13,\ 15,\ 17\}$	$M_1 = 1.5$ $M_2 = 5.34$ $M_3 = 13.25$
6	$C_1 = \{1,\ 2,\ 3\}$ $C_2 = \{6,\ 7,\ 8\}$ $C_3 = \{13,\ 15,\ 17\}$	$M_1 = 2$ $M_2 = 7$ $M_3 = 15$

3.5 Conclusion

In this chapter, we have presented some qualitative methods for eliciting expert opinions. Ben Yaghlane et al.'s method has the advantage of taking into account the quality of the constructed belief functions and the inconsistency of the preference relations provided by the experts.

For the aggregation of expert judgements, we presented a hierarchical method proposed by Ha-Duong. This method is based on dividing experts into groups of thought. In order to make this step easier, faster and more relevant, we proposed to use a clustering algorithm based on Jousselme's distance.

The information resulting from the collecting data process will be used in the evidential risk graph, a generalization of the risk graph method proposed in the next chapter.

4

Evidential risk graph process

4.1 Introduction

The main objective of the process of collecting expert opinions is to prepare the different parameters that will be the input of the adopted risk evaluation method.

Experts can not always provide perfect data. The classic methods of risk evaluation are not able to treat this type of data.

Thus, we propose in this chapter a new method for Safety Integrity Level (SIL) allocation based on the belief functions theory as it is a flexible way to model uncertainty and a strong tool for combining data. This method is a generalization of the standard risk graph called the Evidential Risk Graph. Then, the whole process of determining safety integrity level of a SIS is described. At the end of this chapter we present a case study in order to illustrate this process.

4.2 Risk graph for determining safety integrity level

In this work we are interested in the risk graph model, given by the IEC standard, for determining the safety integrity level. This model will be adapted to deal with imperfect data modeled with the belief functions theory.

4.2.1 Standard risk graph according to the IEC standard

As we have already mentioned, the risk graph is a popular method used in industry problems. It is a simple and clear way to model the relation between the risk and its components. This method is used to measure the risk reduction level by determining the safety integrity level of a safety instrumented function in a safety instrumented system. Figure 4.1 shows an example of a risk graph for SIL allocation according to the IEC standard (IEC61508, 2002). This model is based on four parameters, C, F, P and W. The meaning of each parameter is given by table 4.1.

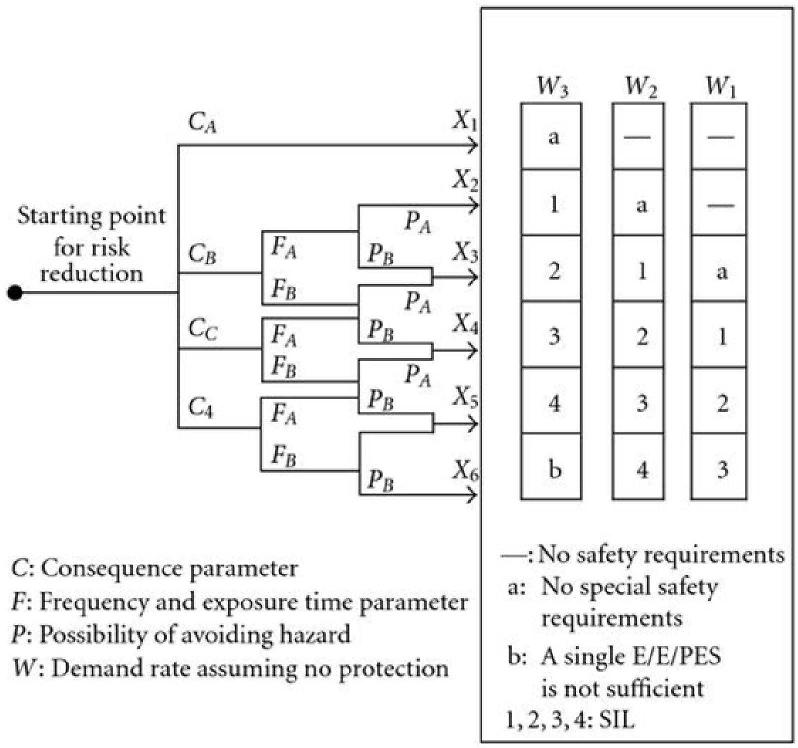

Figure 4.1: Risk Graph in IEC 61508 for SIL allocation

This graph is explained as follows: the use of parameters C, F, and P gives as a result several exits (X_1, X_2, X_3..., X_n). Each exit is recorded in one of three scales (W_1, W_2, W_3). Each scale gives the SIL allocation level for the SIS. There are four levels of risk reduction ($SIL \in 1, 2, 3, 4$). Level a means that a SIF is not necessary, level b indicates that only one safety system is not sufficient, and " $---$ " means that there is no need for a safety requirement.

Example 4.1
Let us consider a dangerous situation with the following values of parameters:
$C = C_B$, $F = F_A$, $P = P_B$ and $W = W_3$.
By following the risk graph given in figure 4.1, the safety integrity level corresponding to these values is SIL2. ■

Table 4.1: Risk graph parameters

Parameter	**Values**	**Meaning of each value**
C: Consequence of the dangerous event	C_A	Minor incident
	C_B	Reversible effects
	C_C	Lethal effects limited to the site
	C_D	Lethal effects outside the site
F: Frequency and exposure time	F_A	Rare exposure in the considered zone
	F_B	Frequent exposure in the considered zone
P: Possibility of avoiding the dangerous event	P_A	Possible under certain conditions
	P_B	Impossible
W: Probability of the unwanted occurrence	W_1	Low probability
	W_2	Medium probability
	W_3	High probability

4.2.2 Risk graph vs decision tree

The risk graph has the structure of a decision tree that we read from left to right as shown in figure 4.2 (J.Marsot and L.Claudon, 2006; ISO14121-2, 2005). Nodes of the tree represent factors or parameters and edges correspond to the classes or values of each factor.

For each dangerous situation, a value is assigned to every factor given in input. A path is then drawn according to the values of the different parameters and the risk level

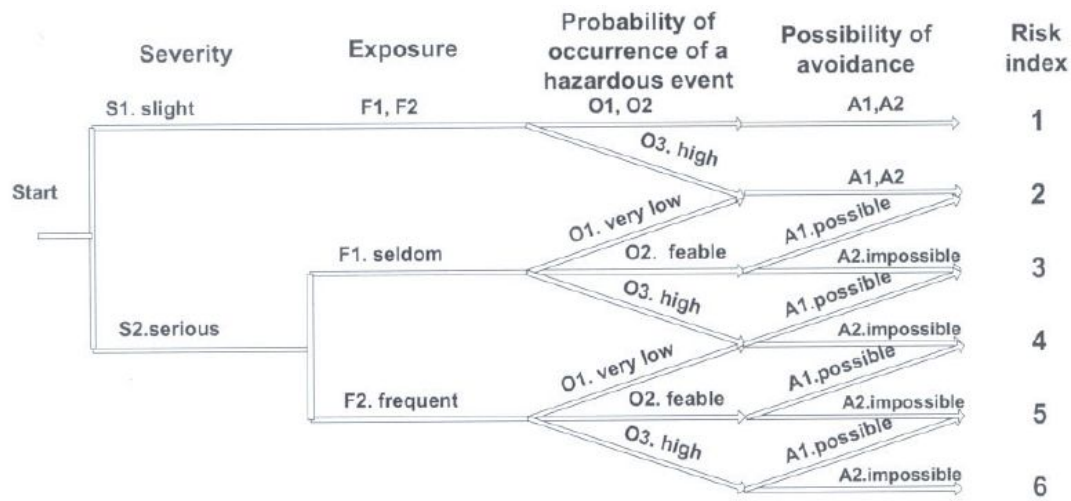

Figure 4.2: Risk Graph according to (ISO14121-2, 2005)

of the dangerous situation will be deduced from this path.

Table 4.2 summarizes the similarity between the risk graph and the decision tree.

Table 4.2: Risk graph vs decision tree

	Decision tree	**Risk graph**
Application fields	General method: different fields	Risk analysis
Main objective	Classification of a new objective	Risk evaluation: SIL allocation
Tree construction	Depends on the classification problem	Given by a standard, ex: IEC, ISO...
Attributes	Depends on the classification problem	Risk factors, ex: C, P, F, W
Leafs	Depends on the classification problem	Risk levels

4.2.3 Evidential risk graph

For dealing with imprecise and uncertain data, we proposed in this work a generalization of the risk graph method based on the belief functions theory: an *evidential risk graph*.

The evidential risk graph is based on the same parameters as the standard risk graph described in the IEC 61508 standard: C, F, P and W. These parameters are now considered imperfect and elicited using evidence theory.

As mentioned previously, the standard risk graph is very similar to a decision tree. Thus, for the propagation of parameters in the evidential risk graph we simulate the same inference engine (classification procedure) of the Belief Decision Trees (BDT) proposed by Elouedi et al. (Elouedi et al., 2001).

The different steps of the BDT's classification process are adopted in the inference task of the evidential risk graph in order to determine the safety integrity level of a SIS.

Inference system in the evidential risk graph

Let m_C be the *bba* representing the part of belief that supports parameter C defined on the frame of discernment Ω_C, m_F be the *bba* of parameter F defined on Ω_F, m_P be the *bba* of parameter P defined on Ω_P and m_W be the *bba* assigned to parameter W defined on Ω_W.
Let Ω_{SIL} be the frame of discernment of the safety integrity levels (classes) and m_{SIL} be the *bba* representing the part of belief committed to the SIL levels.

The inference task of the evidential risk graph is based on several steps (Elouedi et al., 2001):

Step 1: Generate a global frame of discernment Ω_G relative to all the parameters using the cross-product of the different frames of discernment:

$$\Omega_G = \Omega_C \times \Omega_F \times \Omega_P \times \Omega_W \tag{4.1}$$

Step 2: Extend the $bba's$ (m_C; m_F; m_P; m_W) of the different parameters to the global frame of discernment Ω_G. The extended $bba's$ are denoted by: $m_{C\uparrow G}$; $m_{F\uparrow G}$; $m_{P\uparrow G}$; $m_{W\uparrow G}$

Step 3: Calculate the body of evidence corresponding to the global frame of discernment m_G by aggregating the different extended $bba's$ using the conjunctive rule of combination:

$$m_G = m_{C\uparrow G} \bigcirc\!\!\!\!\cap\, m_{F\uparrow G} \bigcirc\!\!\!\!\cap\, m_{P\uparrow G} \bigcirc\!\!\!\!\cap\, m_{W\uparrow G} \tag{4.2}$$

Step 4: Calculate the belief function $bel^{\Omega_{SIL}}[x]$ of each focal element x of the bba m_G generated by the third step. As in the belief decision tree, this calculation depends on the cardinality of the treated focal element x:

- If the focal element is a singleton ($|x| = 1$), then $bel^{\Omega_{SIL}}[x]$ is equal to the belief function of the leaf attached to the treated focal element.
- If the focal element is not a singleton ($|x| > 1$), then $bel^{\Omega_{SIL}}[x]$ depends on the different paths corresponding to the values of parameters:
  - if all paths bring to the same leaf, then $bel^{\Omega_{SIL}}[x]$ is given by the belief function of the leaf related to these paths.
  - if paths lead to distinct leaves, then $bel^{\Omega_{SIL}}[x]$ is computed by combining the belief functions corresponding to each leaf using the disjunctive rule of combination.

Step 5: Compute the belief functions of the different classes (SIL levels) by averaging the belief functions computed in the previous step using the following formula:

$$bel^{\Omega_{SIL}}[\Omega_G](\omega) = \sum_{x \subseteq \Omega_G} m_G(x) \ . \ bel^{\Omega_{SIL}}[x](\omega) \quad for \ \ \omega \in \Omega_{SIL} \tag{4.3}$$

Step 6: Transform the beliefs resulting from the fifth step to probabilities using the pignistic transformation in order to make a decision. The adopted SIL will be the SIL having the highest probability value.

Figure 4.3 shows the decision tree that corresponds to the risk graph given by the IEC standard. Each leaf of this tree defines a safety level that represents the path attached to this leaf.

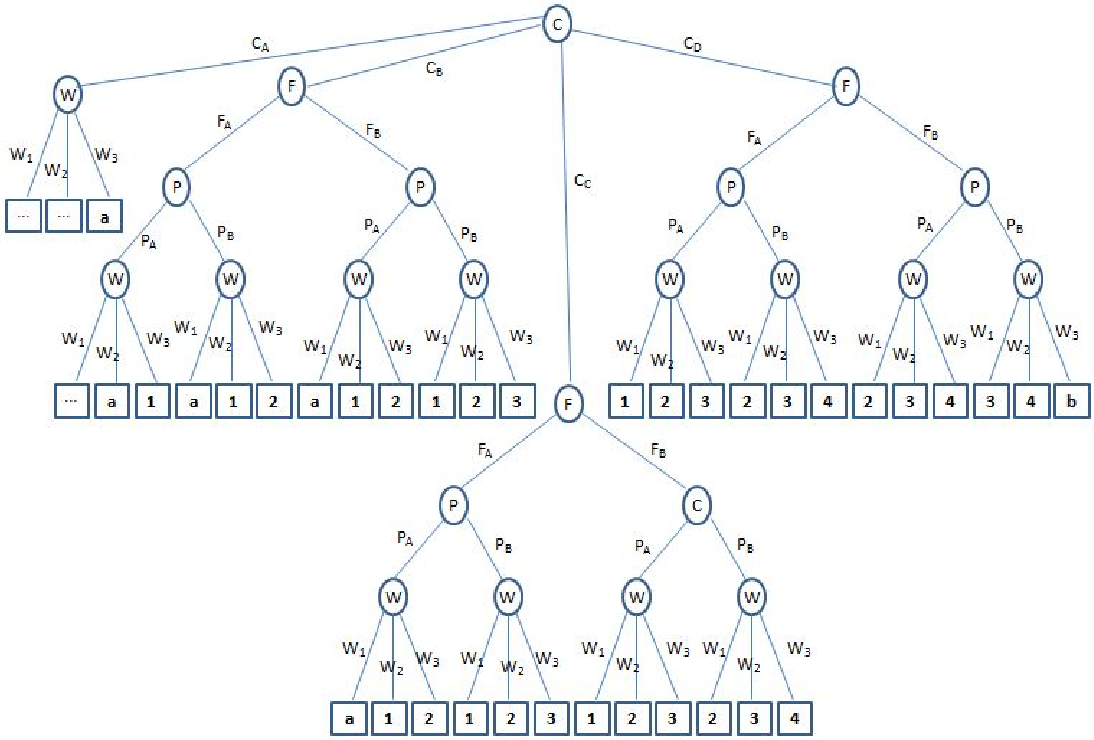

Figure 4.3: Transformation of the risk graph into a decision tree

In this work we are interested in the case where the levels are certain and described in the standard risk graph. Thus, each leaf in the evidential risk graph is characterized by a categorical belief function where the focal element refers to the safety integrity level defined by this leaf.

Example 4.2

Let us consider a path drawn according to following values of parameters:
$C = C_B$, $F = F_A$, $P = P_B$ and $W = W_3$.
The leaf attached to this path defines the safety integrity level 2, this leaf is characterized by the categorical belief function defined as follows:

$$m^{\Omega}(A) = \begin{cases} 1 & \text{if } A = SIL2 \\ 0 & \forall A \subseteq \Omega_{SIL} \text{ and } A \neq SIL2 \end{cases}$$

■

4.3 General scheme of the proposed process

We now introduce the general process summarized in figure 4.4. The first step in this process is the elicitation of expert opinions by the qualitative method of Ben Yaghlane et al.

Expert can express his opinion by ordering the propositions considered as focal elements. According to this order we generate the *bba* corresponding to the expert's opinion by resolving an optimization problem. In this work we did not focus on a particular uncertainty measure to be maximized. This may be the object of future works.

The second step is dividing expert opinions using a clustering algorithm. We adopted in this step a k-means algorithm based on Jousselme's distance in order to be able to classify data modeled in the evidence framework.

The output of the clustering step will be the input of the third step which is aggregating expert judgements by means of the hierarchical method of fusion of expert opinions proposed by Ha-Duong (Ha-Duong, 2008).

These steps will be performed for each parameter (C, F, P, W) in order to get $bba's$ corresponding to these parameters. The resulting $bba's$ will be integrated in the evidential risk graph which will generate the safety integrity level of the SIS.

4.4 Case study

In order to illustrate the proposed approach for SIL allocation we present in the following a case study detailing its different steps.

4.4.1 Problem's description

Let us consider an example from the IEC standard. A process composed of a pressurized vessel containing volatile flammable liquid (see figure 4.5) can reject material in the environment. The acceptable risk is defined, it has an average level of gas rejection less than 10 year. An hazard analysis has shown that the current protection systems (alarm and protection layers) are insufficient to warrant the risk level. Our goal is to determine the SIL level of a safety integrated function that allows to reach the acceptable level of

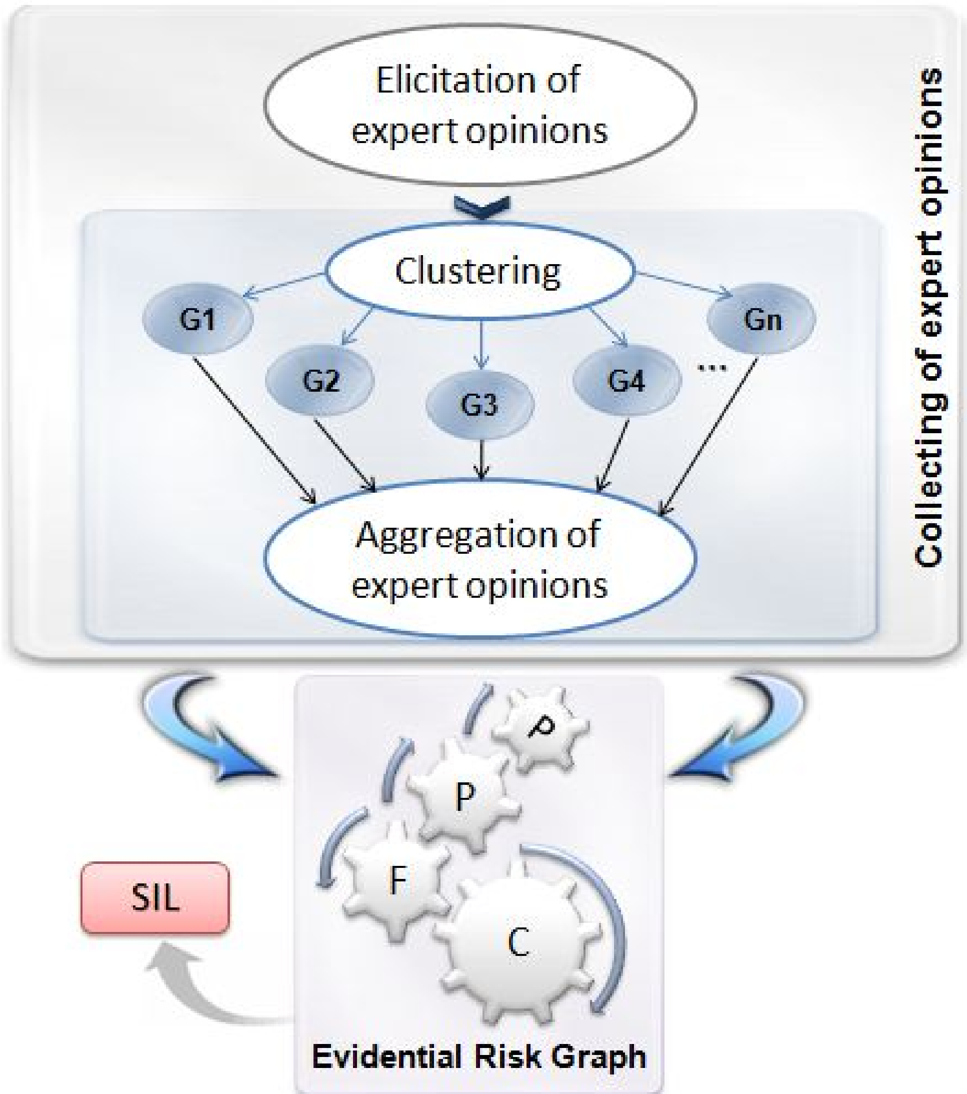

Figure 4.4: SIL allocation by elicitation and aggregation of expert opinions using evidential risk graph

risk. This determination is based on the known risk about the vessel (IEC61508, 2002; Simon et al., 2006). Below are the different values of the risk parameters used in this case study :

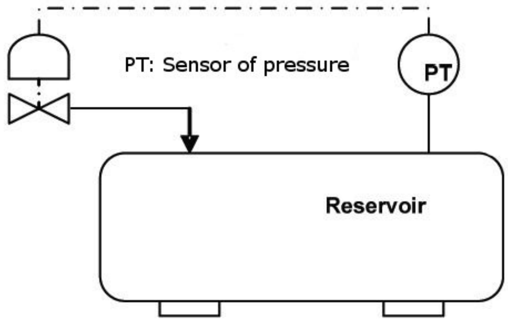

Figure 4.5: Vessel under pressure

- Significance of parameter C:
  - Low : minor harm
  - Medium: serious harm affecting one or more persons
  - High: Death of several people
  - Very High: Several killed people
- Significance of parameter F:
  - Medium: exposure from rare to frequent in a dangerous area
  - High: exposure from frequent to permanent in a dangerous zone
- Significance of parameter P:
  - Medium: Possible under some conditions
  - High: Almost impossible
- Significance of parameter W:
  - Low: A very weak probability that undesired events occur or only some undesired occurrences is probable
  - Medium: A weak probability that undesired events occur or only some undesired occurrences is probable
  - High: A high probability that undesired events occur or it is probable that undesired events frequently occur

Table 4.3: Possible values of parameters

Parameter	**Possible values**	**Frame of discernment**
C	Low (L_C); Medium (M_C); High (H_C); Very High (VH_C)	$\Omega_C = \{L_C; M_C; H_C; VH_C\}$
F	Medium (M_F); High (H_F)	$\Omega_F = \{M_F; H_F\}$
P	Medium (M_P); High (H_P)	$\Omega_P = \{M_P; H_P\}$
W	Low (L_W); Medium (M_W); High (H_W)	$\Omega_W = \{L_W; M_W; H_W\}$

The frame of discernment of each parameter is presented in table 4.3.

4.4.2 Collecting expert opinions

For data collecting process, we consider the opinions of five experts.

Elicitation of expert opinions

As we previously said, each expert expresses his opinion by ordering the propositions that he consider as focal elements. The judgement of each expert concerning each parameter is summarized in table 4.4.

Thus, according to the opinion provided by an expert, a rank is affected to each focal element. The proposition having the highest preference will have the highest rank. If the expert is indifferent between two propositions, they will take the same rank.

Example 4.3 Let us consider the opinion of the fifth expert about parameter W. Ranks are affected to the focal elements as follows:

$$\begin{array}{ccccccc} \{L_W \cup H_W\} & \gtrdot & \{L_W\} & \gtrdot & \{M_W\} & \sim & \{H_W\} \\ \Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\ 3 & & 2 & & 1 & & 1 \end{array}$$

■

After resolving the different optimization problems formed by expert preferences for each parameter, the result of the elicitation step will be the $bba's$ of the different

Table 4.4: Expert opinions

Expert	**C**	**F**	**P**	**W**
Expert1	$\{M_C\}$	$\{H_F \cup M_F\} \sim \{H_F\}$	$\{H_P\}$	$\{L_W \cup M_W \cup H_W\} \gtrdot \{L_W \cup H_W\} \gtrdot \{L_W\}$
Expert2	$\{M_C\}$	$\{H_F \cup M_F\} \gtrdot \{H_F\}$	$\{H_P\}$	$\{L_W\}$
Expert3	$\{M_C\}$	$\{H_F \cup M_F\} \gtrdot \{M_F\} \gtrdot \{H_F\}$	$\{H_P\}$	$\{L_W \cup H_W\} \gtrdot \{L_W\} \gtrdot \{M_W\}$
Expert4	$\{M_C\}$	$\{M_F\}$	$\{H_P\}$	$\{L_W\}$
Expert5	$\{M_C\}$	$\{H_F \cup M_F\}$	$\{H_P\}$	$\{L_W \cup H_W\} \gtrdot \{L_W\} \gtrdot \{M_W\} \sim \{H_W\}$

Table 4.5: The result of the elicitation step for the parameter C

Expert1	**Expert2**	**Expert3**	**Expert4**	**Expert5**
$m(\{M_C\}) = 1$	$m(\{M_C\}) = 1$	$m(\{M_C\}) = 1$	$m(\{M_C\}) = 1$	$m(\{M_C\}) = 1$

parameters. The $bba's$ of the focal elements for each parameter are shown in tables 4.5, 4.6, 4.7 and 4.8.

Clustering

The next step in our approach consists on dividing the different opinions given by experts for each parameter using the clustering algorithm.

Table 4.6: The result of the elicitation step for the parameter F

Expert1	**Expert2**	**Expert3**	**Expert4**	**Expert5**
$m(\{H_F\}) = 1$	$m(\{H_F\}) = 0.242$ $m(\{H_F \cup M_F\}) = 0.758$	$m(\{H_F\}) = 0.16$ $m(\{M_F\}) = 0.44$ $m(\{H_F \cup M_F\}) = 0.4$	$m(\{H_F\}) = 1$	$m(\{H_F \cup M_F\}) = 1$

Table 4.7: The result of the elicitation step for the parameter P

Expert1	**Expert2**	**Expert3**	**Expert4**	**Expert5**
$m(\{H_P\}) = 1$	$m(\{H_P\}) = 1$	$m(\{H_P\}) = 1$	$m(\{H_P\}) = 1$	$m(\{H_P\}) = 1$

Table 4.8: The result of the elicitation step for the parameter W

Expert1	**Expert2**	**Expert3**	**Expert4**
$m(\{L_W\}) = 0.22$ $m(\{L_W \cup H_W\}) = 0.38$ $m(\{\Omega_W\}) = 0.4$	$m(\{L_W\}) = 1$	$m(\{M_W\}) = 0.1$ $m(\{L_W\}) = 0.46$ $m(\{L_W \cup H_W\}) = 0.44$	$m(\{L_W\}) = 1$
Expert5			
$m(\{H_W\}) = 0.14$ $m(\{M_W\}) = 0.14$ $m(\{L_W\}) = 0.4$ $m(\{L_W \cup H_W\}) = 0.32$			

The graphical representation of the opinion of each expert (figure 4.6) can be helpful for choosing the number of clusters k.

It is clear for both parameters P and C that we have one cluster that contains all experts. Assuming that we have three groups of experts for F and two groups for parameter W, the result of the clustering step is as follows:

Parameter F

$Expert1;\ Expert4\ \in\ Cluster1$

$Expert2;\ Expert5\ \in\ Cluster2$

$Expert3\ \in\ Cluster3$

Parameter W

$Expert1;\ Expert3;\ Expert5\ \in\ Cluster1$

$Expert2;\ Expert4\ \in\ Cluster2$

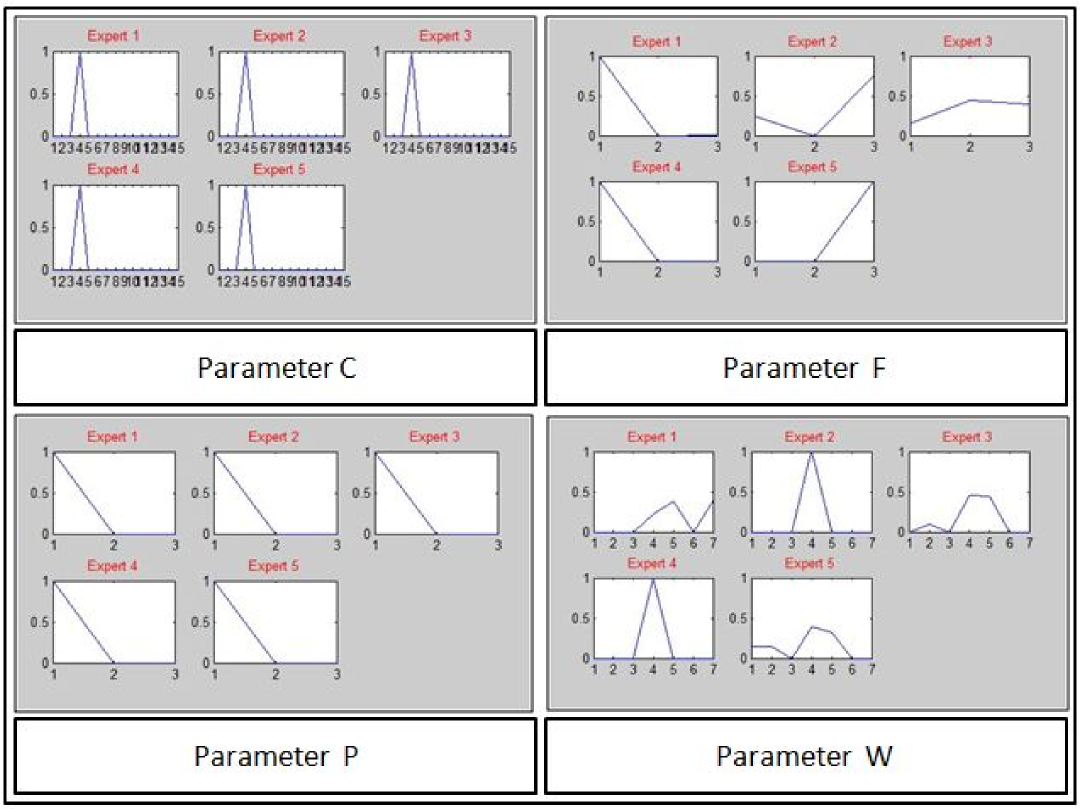

Figure 4.6: Graphical representation of expert opinions

Table 4.9: The result of the conjunctive combination

Parameters	**Clusters**	**Focal elements**
F	Cluster1	$m(\{H_F\}) = 1$
	Cluster2	$m(\{H_F\}) = 0.24$ $m(\{H_F \cup M_F\}) = 0.76$
	Cluster3	$m(\{H_F\}) = 0.16$ $m(\{M_F\}) = 0.44$ $m(\{H_F \cup M_F\}) = 0.4$
W	Cluster1	$m(\{\emptyset\}) = 0.3$ $m(\{H_W\}) = 0.05$ $m(\{L_W\}) = 0.54$ $m(\{H_W \cup L_W\}) = 0.11$
	Cluster2	$m(\{L_W\}) = 1$

Aggregation of expert opinions

Once the groups of experts are generated, then we can aggregate the different opinions using the hierarchical method explained in chapter 3.

- Conjunctive combination
  The information provided by experts belonging to the same group are combined using the cautious conjunctive rule (Denœux, 2008).

  In this use case, all experts assert that parameters C and P are certain. So, the $bba's$ of these parameters do not change from a step to another.
  The result of the conjunctive combination within each group of experts for parameters F and W is summarized in table 4.9.

- Disjunctive combination
  After aggregating data within each cluster, it is necessary now to combine the different results of the previous step in order to have a unique and useful information for each parameter.

Table 4.10: The result of the collecting data process

Parameters	**Focal elements**
C	$m(\{M_C\}) = 1$
F	$m(\{H_F\}) = 0.04$ $m(\{H_F \cup M_F\}) = 0.96$
P	$m(\{H_P\}) = 1$
W	$m(\{L_W\}) = 0.84$ $m(\{L_W \cup H_W\}) = 0.16$

The result of this step will be the result of the collecting data process. It is summarized in table 4.10.

4.4.3 Evidential risk graph

These results are the input of the evidential risk graph. As mentioned previously, the inference in the evidential risk graph is similar to the classification process in the belief decision trees.

1. Generation of the global frame of discernment Ω_G :

$$\begin{aligned}
&\Omega_G = \{(L_C, L_F, L_P, L_W); (L_C, L_F, L_P, M_W); (L_C, L_F, L_P, H_W);\\
&(L_C, L_F, M_P, L_W); (L_C, L_F, M_P, M_W); (L_C, L_F, M_P, H_W);\\
&(L_C, M_F, L_P, L_W); (L_C, M_F, L_P, M_W); (L_C, M_F, L_P, H_W);\\
&(L_C, M_F, M_P, L_W); (L_C, M_F, M_P, M_W); (L_C, M_F, M_P, H_W);\\
&(M_C, L_F, L_P, L_W); (M_C, L_F, L_P, M_W); (M_C, L_F, L_P, H_W);\\
&(M_C, L_F, M_P, L_W); (M_C, L_F, M_P, M_W); (M_C, L_F, M_P, H_W);\\
&(M_C, M_F, L_P, L_W); (M_C, M_F, L_P, M_W); (M_C, M_F, L_P, H_W);\\
&(M_C, M_F, M_P, L_W); (M_C, M_F, M_P, M_W); (M_C, M_F, M_P, H_W);\\
&(H_C, L_F, L_P, L_W); (H_C, L_F, L_P, M_W); (H_C, L_F, L_P, H_W);\\
&(H_C, L_F, M_P, L_W); (H_C, L_F, M_P, M_W); (H_C, L_F, M_P, H_W);\\
&(H_C, M_F, L_P, L_W); (H_C, M_F, L_P, M_W); (H_C, M_F, L_P, H_W);\\
&(H_C, M_F, M_P, L_W); (H_C, M_F, M_P, M_W); (H_C, M_F, M_P, H_W);
\end{aligned}$$

$(VH_C, L_F, L_P, L_W); (VH_C, L_F, L_P, M_W); (VH_C, L_F, L_P, H_W);$
$(VH_C, L_F, M_P, L_W); (VH_C, L_F, M_P, M_W); (VH_C, L_F, M_P, H_W);$
$(VH_C, M_F, L_P, L_W); (VH_C, M_F, L_P, M_W); (VH_C, M_F, L_P, H_W);$
$(VH_C, M_F, M_P, L_W); (VH_C, M_F, M_P, M_W); (VH_C, M_F, M_P, H_W)\}$

2. Extension of $bba's$ to the global frame of discernment for each parameter:

   - Parameter C:

     - $m_{C\uparrow G}(\{M_C\} \times \Omega_F \times \Omega_P \times \Omega_W) =$
       $m_{C\uparrow G}(\{(M_C, L_F, L_P, L_W) \cup (M_C, L_F, L_P, M_W) \cup (M_C, L_F, L_P, H_W) \cup$
       $(M_C, L_F, M_P, L_W) \cup (M_C, L_F, M_P, M_W) \cup (M_C, L_F, M_P, H_W) \cup$
       $(M_C, M_F, L_P, L_W) \cup (M_C, M_F, L_P, M_W) \cup (M_C, M_F, L_P, H_W) \cup$
       $(M_C, M_F, M_P, L_W) \cup (M_C, M_F, M_P, M_W) \cup (M_C, M_F, M_P, H_W)\}) = 1$

   - Parameter F:

     - $m_{F\uparrow G}(\{H_F\} \times \Omega_C \times \Omega_P \times \Omega_W) = 0.04$
     - $m_{F\uparrow G}(\{H_F \cup M_F\} \times \Omega_C \times \Omega_P \times \Omega_W) = 0.96$

   - Parameter P:

     - $m_{P\uparrow G}(\{H_P\} \times \Omega_C \times \Omega_F \times \Omega_W) = 1$

   - Parameter W:

     - $m_{W\uparrow G}(\{L_W\} \times \Omega_C \times \Omega_P \times \Omega_F) = 0.84$
     - $m_{W\uparrow G}(\{L_W \cup H_W\} \times \Omega_C \times \Omega_P \times \Omega_F) = 0.16$

3. Combination of the extended $bba's$:

   - $m_G(\{(M_C, M_F, H_P, L_W) \cup (M_C, H_F, H_P, L_W)\}) = 0.8064$
   - $m_G(\{(M_C, M_F, H_P, L_W) \cup (M_C, H_F, H_P, L_W) \cup (M_C, M_F, H_P, H_W) \cup (M_C, H_F, H_P, H_W)\}) =$ 0.1536
   - $m_G(\{(M_C, H_F, H_P, L_W)\}) = 0.0336$
   - $m_G(\{(M_C, H_F, H_P, L_W) \cup (M_C, H_F, H_P, H_W)\}) = 0.0064$

4. Computation of beliefs on levels:
   Let $\Omega_{SIL} = \{No; SIL1; SIL2; SIL3; a; b\}$ be the frame of discernment containing

the safety levels generated by the evidential risk graph. Figure 4.7 shows the decision tree that corresponds to this problem. Leaves of this tree are numbered in order to characterize each road generated by this tree.

This step consists on computing the beliefs on levels defined on Ω_{SIL} by taking into account roads generated by each focal element found in the previous step according to the tree in figure 4.7. Thus, we get:

- $bel^{\Omega_{SIL}}[\{(M_C, M_F, H_P, L_W) \cup (M_C, H_F, H_P, L_W)\}] = bel_7 \ \textcircled{\cup} \ bel_{13}$
  where bel_7 and bel_{13} are beliefs that correspond to leaves 7 and 13.
- $bel^{\Omega_{SIL}}[\{(M_C, M_F, H_P, L_W) \cup (M_C, H_F, H_P, L_W) \cup (M_C, M_F, H_P, H_W) \cup (M_C, H_F, H_P, H_W)\}] = bel_7 \ \textcircled{\cup} \ bel_9 \ \textcircled{\cup} \ bel_{13} \ \textcircled{\cup} \ bel_{15}$
- $bel^{\Omega_{SIL}}[\{(M_C, H_F, H_P, L_W)\}] = bel_{13}$
- $bel^{\Omega_{SIL}}[\{(M_C, H_F, H_P, L_W) \cup (M_C, H_F, H_P, H_W)\}] = bel_{13} \ \textcircled{\cup} \ bel_{15}$

5. Aggregation of beliefs defined on Ω_{SIL}:
   This step consists on computing the belief of each level using equation (4.3). These beliefs are transformed into $bba's$ as follows:

   - $m^{\Omega_{SIL}}[m_G](\{SIL1\}) = 0.0336$
   - $m^{\Omega_{SIL}}[m_G](\{SIL1 \cup a\}) = 0.8064$
   - $m^{\Omega_{SIL}}[m_G](\{SIL1 \cup SIL3\}) = 0.0064$
   - $m^{\Omega_{SIL}}[m_G](\{SIL1 \cup SIL2 \cup SIL3 \cup a\}) = 0.1536$

6. Decision making:
   In order to make a decision and know the risk reduction level needed for this system, it is necessary to transform the beliefs computed for each level into probabilities using the pignistic transformation. The pignistic probabilities are shown in table 4.11.

Thus, the risk reduction level needed for the studied system is SIL1.

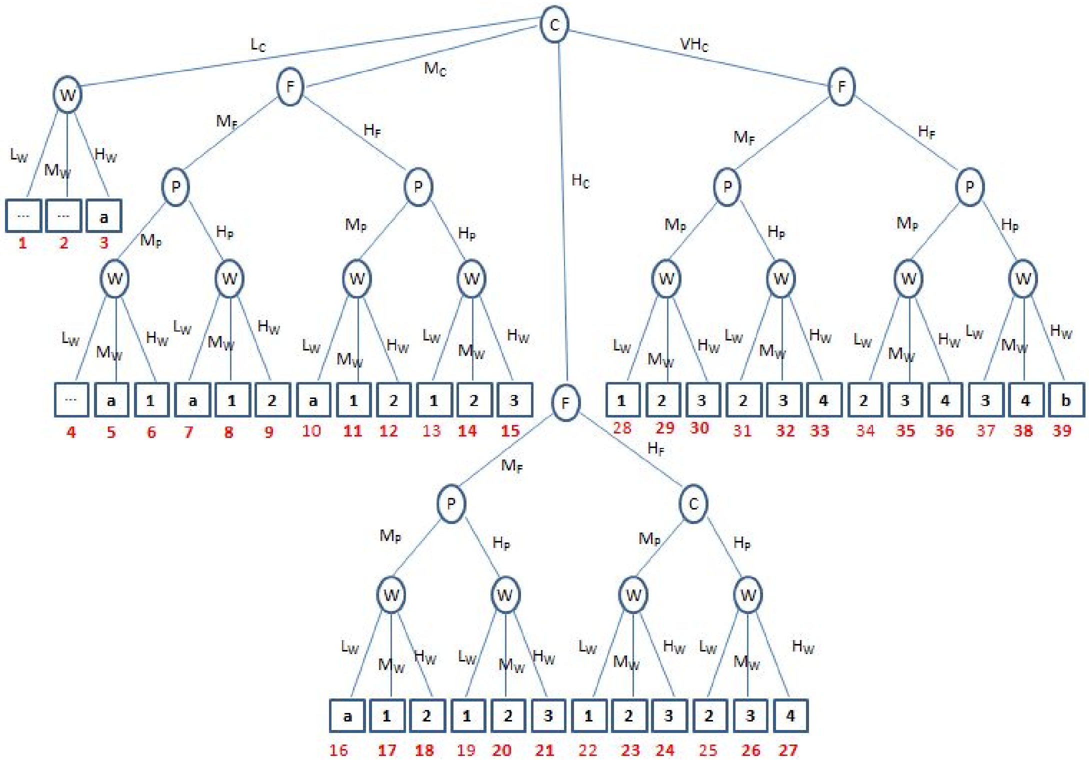

Figure 4.7: The decision tree corresponding to the risk graph of the vessel problem

Table 4.11: The results of the evidential risk graph

Level	*BetP*
b	0
a	0.4416
SIL4	0
SIL3	0.0416
SIL2	0.0384
SIL1	0.4784
No	0

4.5 Conclusion

In this chapter, we have presented the evidential risk graph: a generalized risk graph for dealing with imperfect data using the belief function theory.

We have also presented the global approach used for determining safety integrity level which includes the elicitation of expert opinions, the division of these opinions, the aggregation process and the performing of the evidential risk graph.

5

Implementation and Simulation

5.1 Introduction

In the previous chapter we have presented our approach for determining the safety integrity level (SIL). In order to use and test this approach, an implementation phase is very important.

The chemical companies present high risk especially for persons and environment. Therefore, they need to evaluate this risk and reduce it. Many methods can be applied in this field such as the risk matrix (ISO14121-2, 2005) and the HAZard OPerability (HAZOP) analysis (61882, 2003).

For the simulation phase, we have applied the evidential risk graph for a chemical system studied in (Summers, 1998). The provided results by will be compared by those given by the risk matrix and the HAZOP analysis.

This chapter is composed of two sections. In the first section, we present the most important variables and procedures used for the implementation of our approach. The second section is dedicated to the simulation task.

5.2 Implementation

In order to ensure the implementation of our approach, we have developed our programs in Matlab V7.4.

5.2.1 Main variables

Many variables are used in our programs to implement the evidential risk graph process. In the following we present the most important ones.

- PC: a binary matrix containing all the propositions in 2^{Ω_C} of the parameter C. Each row in this matrix represents a proposition.
- PF: a binary matrix containing all the propositions in 2^{Ω_F} of the parameter F. Each row in this matrix represents a proposition.
- PP: a binary matrix containing all the propositions in 2^{Ω_P} of the parameter P. Each row in this matrix represents a proposition.
- PW: a binary matrix containing all the propositions in 2^{Ω_W} of the parameter W. Each row in this matrix represents a proposition.
- $rank\_c$, $rank\_f$, $rank\_p$, $rank\_w$: matrices containing the rank given by each expert to each focal element for the parameters C, F, P and W. Each column in this matrix represents the opinion of an expert and each row represents a proposition according to the matrix PC, PF, PP or PW. If a proposition is not a focal element, its rank is 0.
- m_c, m_f, m_p, m_w: matrices containing the *bba* of each proposition in 2^{Ω_C}, 2^{Ω_F}, 2^{Ω_P} and 2^{Ω_W} corresponding to the opinion of each expert. Each row in this matrix represents the opinion of an expert and each column represents a proposition according to the matrix PC, PF, PP or PW.
- M_c, M_f, M_p, M_w: matrices containing the *bba* of each proposition in 2^{Ω_C}, 2^{Ω_F}, 2^{Ω_P} and 2^{Ω_W}. These matrices have one column that corresponds to the opinion of all experts.
- k_c, k_f, k_p, k_w: the number of clusters (groups of experts) for parameters C, F, P and W.
- $Group\_c$, $Group\_f$, $Group\_p$, $Group\_w$: matrices containing the different groups of experts after the clustering step. Columns in these matrices represent the groups of experts and rows include experts within group.
- $BetP$: a matrix containing the pignistic probability of each SIL level.
- SIL: The risk integrity level resulting at the end of the risk evaluation process.

5.2.2 Main procedures

In the following, we present the main procedures developed to ensure the construction of our approach. These procedures are structured as follows:

> **Algorithm** *SIL_allocation*
>
> 1. For each parameter C, F, P and W do:
>   - Elicitation
>   - K-means
>   - Aggregation
> 2. Evid_Risk_Graph

Elicitation **procedure**

- *Input:* this procedure has as an input:
  - A matrix containing all the propositions in the frame of discernment (this can be for example PC, PF, PP or PW).
  - A matrix containing the rank given by each expert (this can be for example $rank\_c$, $rank\_f$, $rank\_p$ or $rank$).
- *Output:* the output of this procedure is a matrix containing the *bba* generated for each focal element. Each column represents the opinion of an expert and each row represents a proposition (m_c, m_f, m_p or m_w).
- *Feature:* the elicitation procedure is used to generate the belief masses from the preferences of experts.

K-means **procedure**

- *Input:* this procedure has as an input, the following variables:
  - A matrix containing all the propositions in the frame of discernment (PC, PF, PP or PW).

  - A matrix containing the different $bba's$ (m_c, m_f, m_p or m_w).
  - The number of clusters (k_c, k_f, k_p, k_w).

- *Output:* a matrix including the different groups of experts ($Group\_c$, $Group\_f$, $Group\_p$ or $Group\_w$).
- *Feature:* this procedure is used to divide the opinions of experts according to the k-means algorithm detailed in section (3.4).

This procedure uses the ***dist_jousselme*** procedure which computes the distance between two belief masses according to Jousselme's distance.

Aggregation procedure

- *Input:* this procedure has as an input, the following variables:
  - A matrix containing all the propositions in the frame of discernment (PC, PF, PP or PW).
  - A matrix containing the different $bba's$ (m_c, m_f, m_p or m_w).
- *Output:* a matrix including the final belief masses(M_c, M_f, M_p or M_w).
- *Feature:* this procedure is used to aggregate the different $bba's$ as detailed in section (3.3.2).

In the following, some procedures used in the ***Aggregation*** procedure:

- ***discount***: computes the *bba* after the discounting operation.
- ***cautious_conjunctive_rule***: combines two $bba's$ using the cautious conjunctive rule of combination.
- ***disjunctive_rule***: combines two $bba's$ using the disjunctive rule of combination.

Evid_risk_graph procedure

- *Input:* this procedure has as an input, the following variables:
  - PC, PF, PP and PW.
  - M_c, M_f, M_p and M_w.

- *Output:* $BetP$ and SIL.
- *Feature:* determines the safety integrity level as detailed in section (4.2.3).

In the following, some procedures used in the ***Evid_risk_graph*** procedure:

- ***global_frame***: generates the global frame of discernment .
- ***extension***: extends the different $bba's$ to the global frame of discernment.
- ***conjunctive_rule***: combines two $bba's$ using the conjunctive rule of combination.
- ***bel_sil***: computes the belief functions of the SIL levels.
- ***bel_to_m***: transforms a belief function to a bba.
- ***pign_transformation***: calculates the pignistic probability of a belief mass.
- ***security_level***: determines the safety integrity level.

5.3 Simulation

The implementation of our approach will be used in the simulation task in order to test our evidential risk graph. Thus, we will apply three methods of risk evaluation for determining the safety integrity level of chemical system. The risk matrix and the modified HAZard and OPerability analysis which are generally used in the chemical and petrochemical companies and the evidential risk graph.

5.3.1 Problem's description

Let us consider the reactor shown in figure 5.1. This system is used for the production of chemical C. Chemicals A and B are reacted together to produce chemical C. Chemicals A, B, and C are flammable and, under certain conditions, explosive.

The reaction is exothermic, so the reactor temperature must be controlled using cooling water. The flow rates of chemical A and chemical B are controlled, because the rate of reactant addition and the ratio of the reactant addition influence the reaction path.

A process hazards analysis has documented that, if the flow rates of either chemical A or chemical B exceed certain levels, the reaction will runaway. In addition, the process hazards analysis has shown that if the reaction temperature is not controlled, the reaction path can shift, resulting in a runaway reaction.

Both runaway reactions result in volatilization of the reactants and overpressure of the vessel. Consequence analysis was performed for the various reaction scenarios. It was shown that ignition of the released contents of the vessel would create a pressure wave that would damage a large portion of the facility including the control room (Summers, 1998).

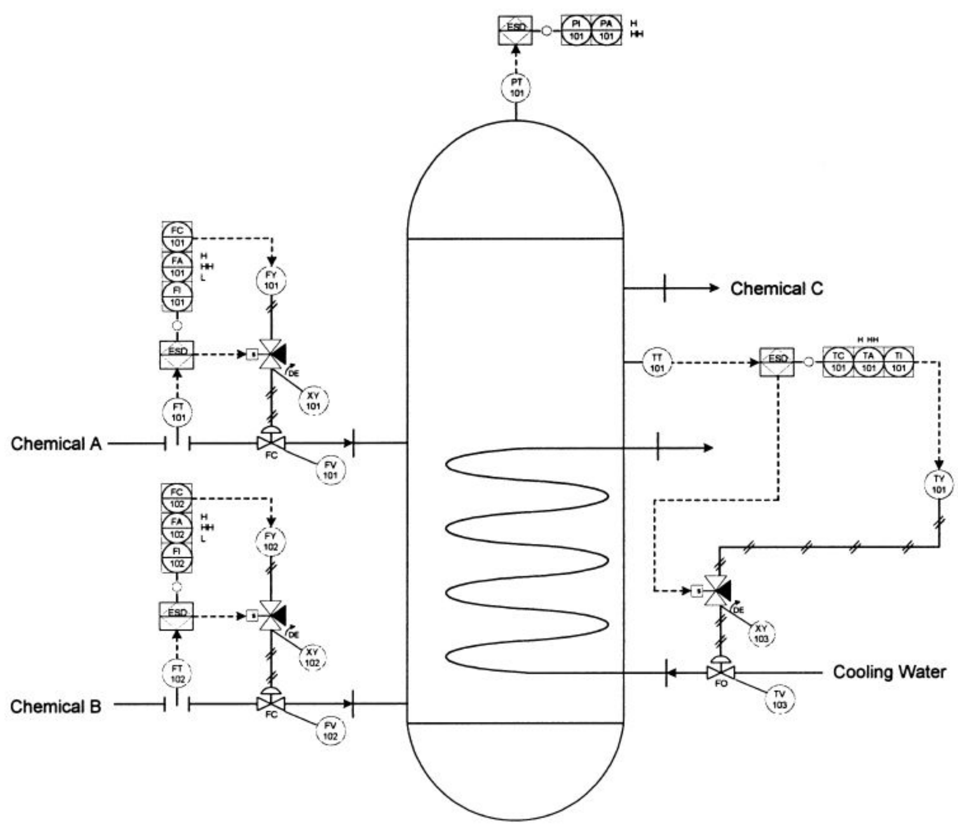

Figure 5.1: Exothermic reactor

5.3.2 Problem's results

The problem described above has been studied by Summer (Summers, 1998) by means of different methods for risk evaluation. We are interested on the results of the risk matrix and the HAZOP methods as they are included in semi-quantitative and qualitative methods and generally used for this type of problems. The results of these methods will be compared with those found by applying the evidential risk graph.

Risk matrix's results

Several information have been developed during the hazard analysis for determining the risk matrix parameters.

Since the high flow rate scenario is caused by a simple loss of process control, the likelihood of this event is high.

The runaway reaction would result in an overpressure of the vessel, resulting in the potential for severe damage if the released contents are ignited. So, the severity would be rated as extensive.

No acceptable layers of protection were identified during the hazard analysis. So, the Independent Protection Layer (IPL) is low.

Using the two dimensional matrix shown in figure 5.2, the SIL level is $SIL3$. If a three dimensional matrix is used by taking into account the IPL level, the SIL level according to the matrix shown in figure 5.3 is $SIL3$.

Modified HAZOP's results

The hazard and operability (HAZOP) (61882, 2003) is a structured and systematic technique for examining a defined system. This technique aims to identify and evaluate problems that may represent risks to personnel or equipment, or prevent efficient operation.

The modified HAZOP is an extension of the HAZOP technique for determining the safety integrity level. This method is based on the team's qualitative understanding of

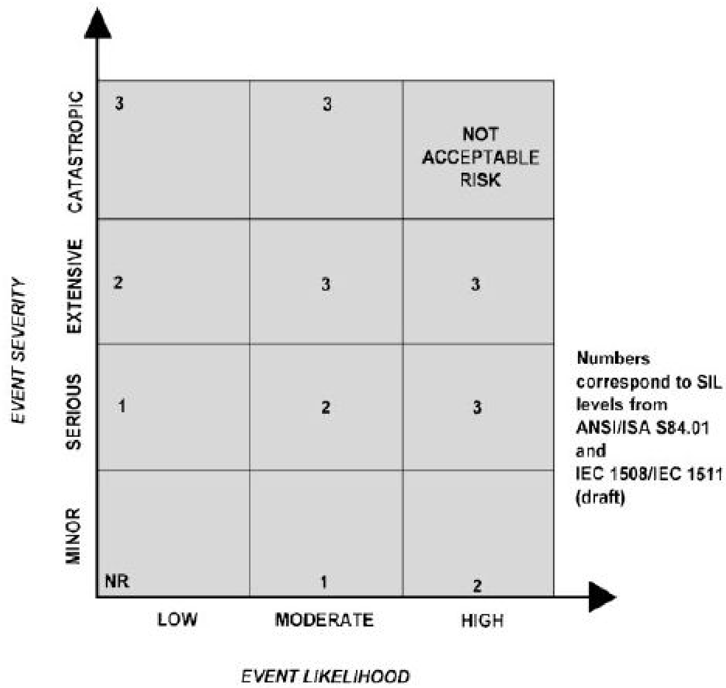

Figure 5.2: Two dimensional risk matrix

the incident severity and likelihood.

According to (Summers, 1998), the application of this technique for the studied system gives $SIL3$ as a safety level. An example of the documentation that might be created by applying the modified HAZOP is shown in table 5.1

Evidential risk graph's results

According to (Summers, 1998), the hazards analysis indicated that:

- There is multiple injuries and fatalities (C=C_C)
- The frequency of exposure is high (F=F_B)
- There is no possibility of avoidance (P=P_B)

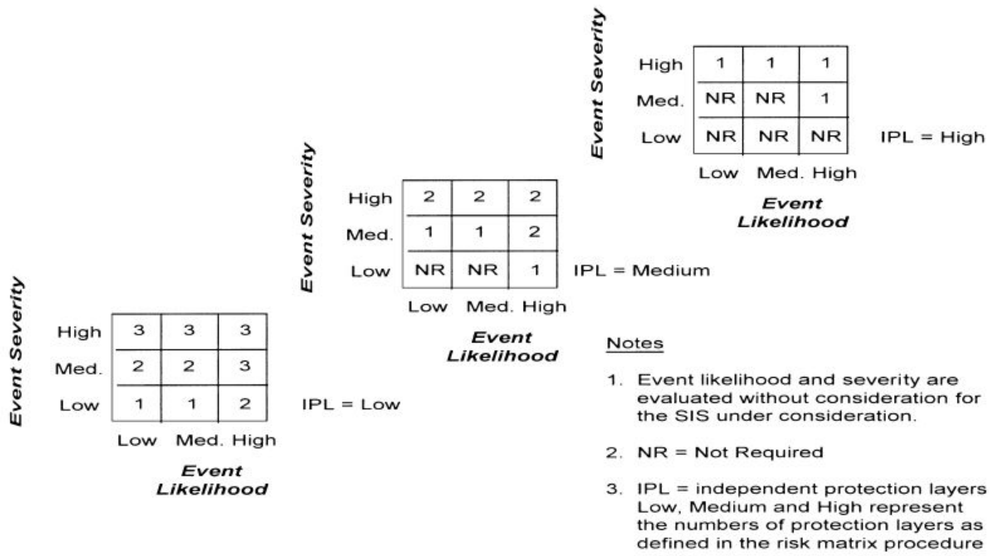

Figure 5.3: Three dimensional risk matrix

-- The likelihood is high (W=W_3)

The results of applying the evidential risk graph to the parameters above are shown in table 5.2. According to this table the required SIL is $SIL4$.

By applying the two previous methods we get the safety integrity level $SIL3$. The evidential risk graph gives as a result $SIL4$. It requires a risk reduction level higher than the other methods.

The evidential risk graph can give a precise result more than the other techniques. It takes into account more variables than the risk matrix and it does not depends on a subjective discussion like the HAZOP method.

We can notice that the result provided by the evidential risk graph is the same given by the standard one as all the parameters are certain. The application of the evidential risk graph on real problems with uncertain data can be the object of future works.

Table 5.1: Modified HAZOP's results

Deviation	Cause	Consequence	Safeguards	Action item	SIL
More flow	FV-101 fails open	Potential for runaway reaction. Potential to overpressure the reactor with release of flammable/explosive contents. Potential for multiple on-site injuries or fatalities	High flow and high pressure initiate SIS		3
High temperature	TV-103 fails closed or loss of cooling water supply	Same as above	Reactor high temperature and high pressure initiate SIS	Consider providing redundant reactor temperature transmitters	3

Table 5.2: Evidential risk graph's results

Level	*BetP*
b	0
a	0
SIL4	1
SIL3	0
SIL2	0
SIL1	0
No	0

5.3.3 Advantages of the evidential risk graph

The evidential risk graph has many advantages:

- It is a clear and simple way to determine the safety integrity level as it maintain the same graphical structure of a standard risk graph.
- It can be considered as a qualitative or a semi quantitative method.
- It is based on the belief functions theory. Thus, it can be used with perfect data as well as imperfect data.
- It can be applied with different types of systems in different fields.

5.4 Conclusion

In this chapter, we have detailed the major variables and the main programs that we have used in order to implement our approach.

Then, we have presented the results of applying the risk matrix, the HAZOP analysis and the evidential risk graph methods to a chemical system. We have noticed that the evidential risk graph requires a risk reduction level higher than the two other methods.

Conclusion

Risk evaluation is very important for reducing or eliminating the risk presented by industrial facilities. Several methods can be used for risk evaluation. Risk graph is one of the most popular methods used in industry problems.

The risk graph is based on several number of parameters, these parameters are usually incoherent, imprecise and/or uncertain. In order to deal with this type of data we propose in this work a generalized risk graph method for determining safety integrity level based on the belief functions theory.

Generally the source of data needed in the evidential risk graph are expert opinions. In this work, the process of collecting data from expert judgements is based on: eliciting expert opinions and aggregating them in order to get unique and relevant information. For the fusion of expert opinions we used a hierarchical method which divides these opinions before aggregating them. To make this process faster and easier, we proposed to automate it by means of a clustering algorithm.

Nevertheless, the proposed work is still subject to improvement. As future work, we will tend to investigate different horizons in order to improve this work:

- We will deal with uncertainty of levels in the evidential risk graph. Thus, not only parameters in the risk graph can be imperfect, the safety integrity level given by the risk graph according to some input data can be also imperfect. So, it will be interesting to deal with this type of risk graph.

- We will apply the evidential risk graph for real problems where the risk parameters can be perfect as well as imperfect.

Bibliography

61882, I. (2003). Hazard and operability studies (HAZOP studies) application guide. *International Electrotechnical Commission(IEC).*

Ben Yaghlane, A., Denoeux, T., and Mellouli, K. (2006a). Constructing belief functions from qualitative expert opinions. In *Information and communication Technologies. ICTTA'06*, volume 1, pages 1363–1368.

Ben Yaghlane, A., Denoeux, T., and Mellouli, K. (2006b). Elicitation of expert opinions for constructing belief functions. In *Proceedings of IPMU'2006*, volume 1, pages 403–411, Paris, France.

Bryson, N. and Mobolurin, A. (1999). A process for generating quantitative belief functions. *European Journal of Operational Research, EJOR*, 115:624–633.

Dempster, A. P. (1967). Upper and Lower probabilities induced by a multivalued mapping. *Annals of Mathematical Statistics*, 38:325–339.

Denœux, T. (2008). Conjunctive and disjunctive combination of belief functions induced by nondistinct bodies of evidence. *Artificial Intelligence*, 172:234–264.

Elouedi, Z., Mellouli, K., and Smets, P. (2001). Belief decision trees: theoretical foundations. *International Journal of Approximate Reasoning, IJAR*, 28:91–124.

Etherton, J. R. (2007). Industrial machine systems risk assessment: A critical review of concepts and methods. *Risk Analysis*, 27:71 – 82.

Farmer, F. (1967). Siting criteria : a new approach. *Atom*, 128:152–166.

Gouriveau, R. (2003). *Analyse de risques, formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision*. PhD thesis, Institut National Polytechnique de Toulouse.

Ha-Duong, M. (2008). Hierarchical fusion of expert opinions in the transferable belief model, application to climate sensitivity. *International Journal of Approximate Reasoning*, 49:555–574.

IEC61508 (2002). Functional safety of electrical/ electronic/programmable electronic (E/E/PE) safety related systems. *International Electrotechnical Commission(IEC)*.

Industries, M. (2009). *Safety Instrumented Systems: The "Logic" of Single Loop Logic Solvers*.

INERIS-DRA-2006-P46055-CL47569:Omega7 (2006). Méthode d'analyse des risques générés par une installation industrielle. Technical report, INERIS.

ISA-TR84.00.02-2002 (2002a). Safety instrumented fonctions (SIF), safety integrity level (SIL), evaluation techniques. *Instrumentation Society of America (ISA)*.

ISA-TR84.00.02-2002 (2002b). Safety instrumented fonctions (SIF), safety integrity level (SIL), evaluation techniques part 2 : Determining the SIL of a SIF via simplified equations. *Instrumentation Society of America (ISA)*.

ISA-TR84.00.02-2002 (2002c). Safety instrumented fonctions (SIF), safety integrity level (SIL), evaluation techniques part 4 : Determining the SIL of a SIF via markov analysis,. *Instrumentation Society of America (ISA)*.

ISO14121-2 (2005). Sécurité des machines- appréciation du risque; partie 2: guide pratique et exemples de mthodes. *AFNOR*.

Jain, A. (2009). Data clustering: 50 years beyond k-means. *Pattern Recognition Letters*.

J.Marsot and L.Claudon (2006). Etat de l'art des méthodes et outils utilisés pour lévaluation en conception d'un poste de travail. Technical report, INRS.

Jousselme, A.-L., Grenier, D., and Bossé, E. (2001). A new distance between two bodies of evidence. *Information Fusion*, 2:91–101.

MacQueen, J. (1967). Some methods for classification and analysis of multivariate observations. In *Fifth berkeley symposium on mathematics, statistics and probability*, pages 281–297.

Nait-Said, R., Z.-F. and Ouzraoui, N. (2008). Fuzzy risk graph model for determining safety integrity level. *International Journal of Quality, Statistics, and Reliability*.

O'Shaughnessy, W. (1992). *La faisabilité de projet, une démarche vers l'efficience et l'efficacité*. Les Editions SMG, 1992. ISBN 2-89094-051-9.

Quinlan, J. (1986). Induction of decision trees. *Machine Learning*, 1:81–106.

Sallak, M., A. J. and Simon, C. (2006). Aide à la décision dans la réduction de l'incertitude des SIL : une approche floue/possibiliste. In *Conférence Internationale Francophone d'Automatique, CIFA'2006*.

Sallak, M. (2007). *Evaluation de paramètres de sûreté de fonctionnement en présence dincertitudes et aide à la conception: Application aux Systèmes Instrumentés de sécurité*. PhD thesis, Institut National Polytechnique de Lorraine.

Sallak, M., S. C. and Aubry, J. (2005). Impact de limprécision des taux de défaillances dans les arbres de défaillances et facteurs dimportance flous. In *Journées Doctorales Modélisation, Analyse et conduite des systèmes dynamiques, JDMACS2005*, Lyon, France.

San, O., Huynh, V.-N., and Nakamori, Y. (2004). An alternative extension of the k-means algorithm for clustering categorical data. *International Journal of Applied Mathematics and Computer Science*, 14 i2:241–247.

Sandri, S.A., D. D. and Kalfsbeek, H. (1995). Elicitation, assessment, and pooling of expert judgements using possibility theory. In *IEEE Transactions on Fuzzy Systems*, volume 3, pages 313–333.

Schön, W. and Denoeux, D. (2004). Prise en compte des incertitudes dans les évaluations de risque à l'aide de fonctions de croyance. In *14ème Congrès de Maîtrise des Risques et de Sûreté de fonctionnement*, Bourge.

Shafer, G. (1976). *A mathematical theory of evidence*. Princeton University Press.

Simon, C., Sallak, M., and Aubry, J. (2006). Allocation de SIL par aggregation d'avis d'experts. In *15ème Colloque National de Maîtrise des Risques et Sûreté de Fonctionnement*, Lambda-mu 15.

Simon, C., Sallak, M., and Aubry, J. (2007). SIL allocation of SIS by aggregation of experts' opinions. In *Safety and Reliability Conference*, Stavanger: Norvege.

Smets, P. (2000). Data Fusion in the Tranferable Belief Model. In *International Conference on Information Fusion*, volume 1, pages 21–33, Paris, France.

Smets, P. and Gabbay, D. (1998). The transferable belief model for quantified belief representation. In *Handbook of Defeasible Reasoning and Uncertainty Management Systems*, volume 1. Kluwer, Doordrecht.

Smets, P. and Kennes, R. (1994). The Transferable Belief Model. *Artificial Intelligence*, 66:191–234.

Summers, A. (1998). Techniques for assigning a target safety integrity level. *ISA Transactions*, 37:95–104.

Tanzi, T. and Delmer, F. (2003). *Ingénierie du risque.* Les Editions Lavoisier.

Villemeur, A. (1988). *Sûreté de fonctionnement des systèmes industriels Fiabilité Facteurs humains Informatisation.* Collection de la Direction des Etudes et Recherches d'Electricité de France.

Wong, S. K. M. and Lingras, P. (1994). Representation of qualitative user preference by quantitative belief functions. *IEEE Transactions on Knowledge and Data Engineering*, 6:72–78.

Zadeh, L. A. (1965). Fuzzy sets. *Information Control*, 8:338–353.