Computing with Words in Risk Assessment

Jun Liu¹, Luis Martínez³, Hui Wang¹, Rosa Mª Rodríguez³ and Vasily Novozhilov²

¹School of Computing and Mathematics, University of Ulster at Jordanstown,
BT37 0QB, Newtownabbey, Northern Ireland, UK
E-mail: j.liu,h.wang@ulster.ac.uk

²School of Built Environment, University of Ulster at Jordanstown,
BT37 0QB, Newtownabbey, Northern Ireland, UK
E-mail: vb.novozhilov@ulster.ac.uk

³Department of Computer Science, University of Jaén,
E-23071 Jaén, Spain
E-mail: martin,rmrodrig@ujaen.es

Received: 25-01-2010; Accepted: 25-05-2010

Abstract

This paper presents a comprehensive overview of currently known applications of computing with words (CWW) in risk assessment. It is largely grouped into the following 5 categories: (1) fuzzy number based risk assessment; (2) fuzzy rule-based risk assessment; (3) fuzzy extension of typical probabilistic risk assessment; (4) ordinal linguistic approach for risk assessment; and (5) miscellaneous applications. In addition, the role of CWW within the broad area of risk assessment is briefly characterized.

Keywords: risk assessment, linguistic information, fuzzy logic, computing with words

1.- Introduction

Risk management is an inherent value in finance, health, engineering and other decision support environments and a central part of any organization’s strategic management. It is the process of assessing risks and taking steps to either eliminate or to reduce them (as far as is reasonably practicable) by introducing control measures. The general purpose of a risk management is to ensure that the risks that could be a potential source of harm, damage of property and degradation of the environment, are sufficiently minimized by addressing all the relevant risk lifecycle stages including the design, implementation, operation and maintenance through to decommissioning ¹.

Risk assessment is one of the key elements of risk management. Expressions such as “risk assessment”, “risk evaluation” and “risk analysis” are used in a somewhat interchangeable way to describe a variety of techniques and processes involved in the overall management of risk ². Despite this lack of clarity, Frosdick ³ and other researchers consistently use the term “risk assessment” as a catch-all to include all those activities that are needed before appropriate risk reduction methods can be decided upon.

The goal of a risk assessment system is to identify the factors, weigh their relative influence, and provide enough information to raise awareness and prompt mitigative action. Accordingly, the general area of risk assessment is vast, with many methods and tools available to use for assessing risk of various environments.

A lot of systems are extremely complex, involving many components: human, mechanical, technological, and environmental. Consequently, the risks associated with these systems are equally complex and diverse. Handling uncertainty is one of the crucial issues in the risk assessment in complex systems with diverse environments. Uncertainty is an unavoidable component affecting the behavior of systems and more so with respect to their failure limits. Thus, uncertainties arise in the values of the parameters and in the hypotheses on the structure of the models used to represent the system failure behavior. Such
uncertainties propagate within the model used to compute the system reliability and risk, which become uncertain themselves. Notwithstanding how much dedicated effort is put into improving the understanding of systems, components and processes through the collection of representative data, the appropriate characterization, representation, propagation and interpretation of uncertainty will remain a fundamental element of the reliability and risk analyses of any complex system.

In general, uncertainty in risk assessment can be considered essentially of two different types: randomness due to inherent variability in the system (i.e., in the population of outcomes of its stochastic process of behavior) and imprecision due to lack of knowledge and information on the system. The former type of uncertainty is often referred to as objective, aleatory, stochastic whereas the latter is often referred to as subjective, epistemic, state-of-knowledge. In most risk assessment, we have to rely on such imperfect information through appropriate risk management.

Extensive research has been devoted to the analysis and management of the risks under uncertainty. Some detailed overviews of uncertainty aspects in risk and safety management can be found in Chowdhury et al. provided a detailed review of uncertainty analysis in risk management studies associated with disinfection by-products (DBPs) in drinking water and human health risk. Markowski discussed and presented the sources and types of uncertainties encountered in process safety analysis and also methods to deal with them. From the literature, many different formal techniques have been developed over the past two decades for dealing with uncertain information for risk assessment in decision making, where Bayesian probability theory, Dempster-Shafer theory of evidence, and fuzzy logic are three of the most common methods of representing and reasoning with uncertain knowledge.

In this paper, we focus on fuzzy logic application in risk assessment. Fuzzy logic, which is the collective name for “fuzzy set analysis” and “possibility theory”, allows us to use imprecise and approximate data that are typically met in risk assessment, has been regarded as one of the promising methods for reduction of the uncertainties in risk assessment. Zadeh proposed the concepts of Computing with Words (CWW), linguistic variables and fuzzy sets to model and compute with linguistic descriptions that are propositions drawn from a natural language. CWW has been intensively used and opened several new research fields and applied to various areas.

Fuzzy logic has been also widely applied to risk assessment in different areas. Unfortunately the literature on this topic is distributed and extensive. A survey and discussion of this topic would be beneficial to the research community and the public. This paper aims to address this objective. Hence the study is intended to provide a general guidance and overview of currently known applications of CWW in risk assessment. It is largely grouped into the following 5 categories: (1) fuzzy number based risk assessment; (2) fuzzy rule-based risk assessment; (3) fuzzy extension of some typical probabilistic risk assessment; (4) ordinal linguistic approach for risk assessment; and (5) miscellaneous applications. In addition, the role of CWW within the wide area of soft computing is briefly characterized.

The rest of this paper is organized as follows: Risk assessment is briefly overviewed in Section 2. The detailed review of CWW in risk assessment is provided in Section 3 including risk assessment from different categories, from the methodology point of view, and miscellaneous applications in different areas. Conclusions are drawn in Section 4.

2. Overview of Risk Assessment

Risk is regarded as the potential for realization of undesirable consequences of an event, e.g., operational risk of software is the likelihood of untoward events occurring during operations due to software failures. It can appear as personal injury or death, mission degradation, property technical damage or destruction. The risk can be a measure of harm or loss associated with the human activity.
Fig. 1 shows the different processes in risk management procedure and presents a simplified relationship between risk analysis, risk assessment and risk management. This definition of the risk management process has been adopted from the International Electrotechnical Commission (IEC). There are other relationships between the definitions of risk analysis, risk assessment and risk management, where risk assessment is part of the risk analysis. In this paper, we focus only on risk assessment issue.

The general area of risk assessment is vast, with many methods and tools available that can be used for assessing risk of various environments, such as RiskWatch, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), CORAS. A non-exhaustive list of available tools can be found at the Riskworld website. Related work to risk assessment is very difficult to categorize. A Sandia National Laboratories report attempted to classify risk assessment methods according to level of detail and approach in order to users would be able to select the most appropriate method.

Some review of risk assessment can be found for security and risk assessment in critical infrastructures and industrial automation, IT project risk assessment, risk assessment of construction projects, environmental risk assessment and so on.

As can be seen from Fig. 1, risk assessment is a key element of risk management; it can be further separated depending on how detailed are the analysis and the labour resources available in at least three levels:

- qualitative methods
- semi-quantitative methods
- quantitative methods

During risk analysis, all three levels can be used in sequence. Qualitative methods are used to determine which scenarios are relevant to continue with the quantitative risk analysis. Initially, risk assessments were qualitative because of their subjectivity. The search for greater objectivity, led to the development of quantified risk analysis techniques.

Quantitative risk analysis methods fall under the broad category of probabilistic risk assessment (PRA). A generally accepted definition of PRA is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity. PRA includes all fault/attack (FTA) tree analyses, event tree analysis (ETA), failure mode and effect analysis (FMEA) or failure mode effect and criticality analysis (FMECA), and cause/consequence analysis (CCA), equivalent annual fatality analysis, Monte Carlo Analysis, Scenario Planning, Decision Tree, Program Evaluation and Review Technique, as well as methods that use directed graphs and logic diagrams.

Most of other methods are extensions or combinations of these. Many of the tools previously mentioned incorporate these methods to varying degrees. Brandsæter summarizes the implementation and use of the Quantitative Risk Assessments (QRA) in the offshore industry and reveals that QRA has been widely accepted in the area.

Risk is generally characterized by the severity (or magnitude) of an adverse consequence that can result from an action and the likelihood of occurrence of the given adverse consequence. In probabilistic risk assessment, consequences are expressed numerically and their likelihoods of occurrence are expressed as probabilities or frequencies. Accordingly, risk is defined as the product of likelihood and severity. To determine risk via PRA, a set of scenarios or initiating events are developed to find what can go wrong, then evaluating the probability of these scenarios, and finally estimating their consequences, then to make informed decisions. Determination of needed basic event
probabilities is the most difficult task in applying this technique. Many references explain all aspects of PRA in great detail 26-28.

Risk is sometimes characterized not only by likelihood and severity, but also with some additional parameters depending on the different applications. The definitions of those parameters also vary according to different application contexts. Take FMEA approach as an example, which is a widely used engineering technique for defining, identifying and eliminating known and/or potential failures, problems, errors and so on from system, design, process, and/or service before they reach the customer 29. The so-called failure mode is defined as the manner in which a component, subsystem, system, process, etc. could potentially fail to meet the design intent. A system, design, process, or service may usually have multiple failure modes or causes and effects. In this situation, each failure mode or cause needs to be assessed and prioritized in terms of their risks so that high risk (or most dangerous) failure modes can be corrected with top priority. The traditional FMEA determines the risk priorities of failure modes through the risk priority number (RPN), which is the product of the occurrence (O), severity (S) and detection (D) of a failure. That is:

\[ \text{RPN} = O \times S \times D, \]

where O and S are the frequency and seriousness (effects) of the failure respectively, and D is the ability to detect the failure before it reaches the customer. The failure modes with higher RPNs are assumed to be more important and will be given higher priorities for correction.

Wang et al. 29 used three fundamental parameters to assess the safety level of an engineering system on a subjective basis: failure rate (FR), consequence severity (CS) and failure consequence probability (FCP). FR describes failure frequencies in a certain period, which directly represents the number of failures anticipated during the design life span of a particular system or an item. CS describes the magnitude of possible consequences, which is ranked according to the severity of failure effects. FCP defines the probability that consequences happen given the occurrence of the event.

In addition, four risk parameters, considered to be sufficiently generic to deal with a wide range of applications, have been combined to risk assessment as well 1. These parameters are: consequence (C), frequency and exposure time (F), possibility of avoiding hazard (P), and probability of the unwanted occurrence (W). All parameter aspects imply a quantitative or qualitative valuation of undesired events or harmful events effects. Table 1 shows an example of a risk graph as used in the UKOOA guidelines and quantitative definitions of risk parameters 30, 31.

Recently, Baybutt 32 has developed an improved risk assessment with the following four parameters: initiating cause frequency, enabling events/conditions, safeguards failure probability and consequences of the hazardous event.

Because the nature of risk is usually affected by numerous factors including human errors, in many circumstances, it may be extremely difficult to assess the associated risks with a system due to the great uncertainty involved. The quantitative risk assessment approaches rely heavily on statistical information. Quantification of risk in scalar values is subject to uncertainties for many reasons including difficulties in defining the likelihood and consequence severity and the mathematics of combining them. Collecting sufficient data to base a statistical probability of risk is costly, and in many situations, such data are limited or unavailable due to a lack of research or the complexity of the system/process considered.

Those quantitative assessments of risk are particularly challenging in domains where undesired events are extremely rare, and the causal factors are difficult to quantify and non-linearly related, e.g., include the difficulty of determining both the probabilities of rare events (such as a nuclear accident, or only incomplete information is available during the very early phases of the system life cycle), and their severity, further, the probabilities may be dynamic, and vary with a variety of factors which are not known in advance.

Table 1 Qualitative and quantitative parameters

<table>
<thead>
<tr>
<th>Risk parameter</th>
<th>Qualitative description</th>
<th>Quantitative description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence (C)</td>
<td>Minor injury</td>
<td>No deaths per event</td>
</tr>
<tr>
<td></td>
<td>Malignant: one death or permanent injury</td>
<td>(10^{-2}) probable deaths per event</td>
</tr>
<tr>
<td></td>
<td>Critical: several deaths</td>
<td>(10^{-1}) probable deaths per event</td>
</tr>
<tr>
<td></td>
<td>Catastrophic: many deaths</td>
<td>(\geq 1) probable deaths per event</td>
</tr>
<tr>
<td>Exposure (E)</td>
<td>Rare</td>
<td>(&lt; 1%) of time</td>
</tr>
<tr>
<td></td>
<td>Frequent</td>
<td>(\geq 1%) of time</td>
</tr>
<tr>
<td>Assistance (A)</td>
<td>Possible</td>
<td>0.95 probability of avoiding hazard</td>
</tr>
<tr>
<td></td>
<td>Not likely</td>
<td>(&lt; 0.05) probability of avoiding hazard</td>
</tr>
<tr>
<td>Demand rate (D)</td>
<td>Very low</td>
<td>(&lt; 1 \text{ in } 3,000\text{, or } 0.03 \text{ per year} )</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>([1, 10] \text{ or } [0.01, 0.03] \text{ per year} )</td>
</tr>
<tr>
<td></td>
<td>Relatively high</td>
<td>([0.1, 1 \text{ or } [0.01, 0.1] \text{ per year} )</td>
</tr>
</tbody>
</table>

Published by Atlantis Press
Copyright: the authors
To overcome the above drawbacks, many approaches have been proposed, where fuzzy logic has been widely applied in risk assessment to different areas and has been regarded as one of the promising methods for the reduction of uncertainties in risk assessment. This will be reviewed in the next section.

3. Computing with Words for Risk Assessment

A normal practice to overcome the risk quantification under uncertainty is the use of expert opinions (i.e., expert knowledge and experience or engineering judgment), which can be exploited to estimate risk qualitatively, and is commonly used as a data source and support for system analysis, evaluation and decision-making processes in a wide range of fields.

There are however, factors associated with expert’s opinion such as under specificity and vagueness that can considerably increase the uncertainty present in such approaches. In order to reduce this uncertainty and make expert data useful, it is necessary to consider three main aspects in the risk assessment process: (i) the knowledge of experts, (ii) the elicitation method, and (iii) when several experts are considered, the averaging technique.

In this case, risk assessment is an “assessment” of something hypothetical defined as “risk”, which can naturally be interpreted as linguistic terms, such as “high”, “low”, or “tolerable”, which are more expressive and natural in risk assessment. A linguistic variable differs from a numerical one in that its values are not precise numbers, but words or sentences in a natural or artificial language. The concept of a linguistic variable serves the purpose of providing a means of approximated characterization of phenomena, which are too complex, or too ill-defined to be amenable to their description in conventional quantitative terms.

This fact has led to many authors to apply fuzzy sets theory as a natural extension to PRA which involves the use of fuzzy concepts. Fuzzy logic provides a powerful tool to deal with imprecise information, especially linguistic information. It provides a systematic technique that can accommodate the above three considerations, therefore, can be viewed as complementary to traditional methods for dealing with risk-based processes that rely on expert opinions, i.e., experts model qualitatively the risk prediction because it allows them to evaluate the risk with linguistic terms. A fuzzy risk methodology has been described as a contribution to the modeling of uncertainties involved in a risk assessment process.

Based on the concept of linguistic variables and fuzzy sets, Zadeh also proposed a concept of Computing with Words (CWW) to model and compute with linguistic descriptions that are propositions drawn from a natural language emphasizing that the core conceptions in CWW are linguistic variables and fuzzy logic (or approximate reasoning). The use of linguistic variables implies processes of CWW such as their fusion, aggregation, and comparison. Different computational approaches in the literature addressed those processes.

Actually, fuzzy approaches have been applied successfully in a wide range of industrial processes. In recent years, many researchers have seen CWW as a very interesting methodology to be applied in decision making. As it allows to model perceptions and preferences in a more human style and it can provide computers some of the needed tools, if not to fully simulate human decision making, to develop complex decision support systems to ease the decision makers to reach a solution. Herrera et al. provided an overview about CWW in decision making including foundations, trends, and prospects.

In general, it is mostly accepted that fuzzy logic provides useful tool to processing vaguely defined variables, and variables whose relationships cannot be defined by mathematical relationships. It takes into account the vagueness and uncertainty inherent in risk and provides a good assessment based upon experts judgment. Actually the rising scientific interest in fuzzy logic and their potential applications has triggered an explosive progress in the field of risk management and fundamental research. Studies focusing on the risk and safety analysis are available to a large extent. Since early nineties fuzzy logic has been widely applied for risk issues. Through a quick Google search we may find 3,740,000 for keywords fuzzy +risk; about 2,810,000 results for the keyword fuzzy +safety. From Science Direct: 4,295 articles are found for: pub-date > 1979 and pub-date < 2001 for fuzzy and risk; 11,351 articles found for: pub-date > 1999 for fuzzy and risk; 4979 records in Compendex & Inspec for 1990-2010.

The rapid increasing research activity is reflected in the exponentially growing number of publications.
per year since 1992 (see Fig. 2). From the above quick search, there is an abundance of literature that discusses risk assessment by using fuzzy logic. In the following sections a general discussion of application of CWW in risk assessment in different categories is presented by giving some papers in detail to have a better picture of the inside model, others are listed and cited. For further detailed information of each category, the reader is referred to the references cited in.

3.1 Overview of Fuzzy Logic Application in Risk Assessment

3.1.1 Generic view and insightful technical framework for risk assessment using fuzzy logic

In the literature there is not a general review for fuzzy logic application in risk assessment but rather some context dependent and problem specific review, for example, in some specific area. Quelch and Cameron investigated uncertainty representation and propagation in quantified risk assessment using fuzzy sets. Ru and Eloff discussed in a general way about risk analysis modeling with the use of fuzzy logic, although the case studies were given on risk analysis related to computer security. Cai provided an introductory overview about system failure engineering and fuzzy methodology. Cho et al., presented a risk assessment methodology for incorporating uncertainties using fuzzy concepts. Zolotukhin and Gudmestad gave an overview of application of fuzzy sets theory in qualitative and quantitative risk assessment. Pokorádi provided a short overview of risk management and assessment and illustrated the possibility of using the fuzzy set theory to assess the risk. Gentile et al. discussed about development of an inherent safety index based on fuzzy logic. Elishakov and Ferracuti presented fuzzy sets based interpretation of the safety factor. Tay and Lim provided a detailed analysis on the use of fuzzy inference techniques in assessment models including theoretical properties and industrial applications. Chowdhury et al. provided a detailed review of uncertainty characterization approaches for risk assessment of DBPs in drinking water. Ebrahimnejad et al. provided a detailed overview and review of risk identification and assessment for Infrastructure project (build–operate–transfer projects) risk assessment. Bajpai et al. presented a general view of applying the concepts of fuzzy logic in security risk assessment. Jablonowski reviewed the impacts of fuzziness, i.e., knowledge imperfection, on high-stakes risk management, including its implementation via computationally intelligent decision aids.

Existing risk assessment methods are largely based on checklists and analysis of a risk matrix. A risk matrix is a mechanism to characterize and rank risks that are typically identified through one or more multifunctional reviews (e.g., process hazard analysis, audits, or incident investigation). Risk matrix is a very useful tool for semi-quantitative risk assessment as well as a selection of risk control measures. In the analysis of a risk matrix, risk factors such as likelihoods of occurrence and severity, are scored according to their influence on the potential risk. These scores are then arithmetically aggregated into an overall risk score. The essential ideas of fuzzy risk analysis are to use fuzzy scales to assess risk parameters in order to deal with uncertainties that arise in each phase of the risk assessment process. Linguistic terms defined on numerical universes and supported by fuzzy sets, provide a rather natural tool for numeric/symbolic interfaces and would be a very adequate alternative when available information is imprecise, incomplete and/or uncertain.

Based on the literature review, a generic and
insightful framework for risk assessment using fuzzy logic approach starts from creating a hierarchical risk breakdown structure representation used to develop a formal model for qualitative risk assessment, then a common language will be presented for describing risks, including terms for quantifying likelihoods and impacts so as to achieve consistent quantification using linguistic terms characterized by fuzzy membership functions, which is regarded as knowledge acquisition and representation for risk modeling, and consists of the following steps:

1) Identification of causes/factors: In this step, all anticipated causes/factors to failures of a system are identified. This can be done by a panel of experts during a brainstorming session at the early conceptual design stages of the system.

2) Identify and characterize fuzzy input and output variables: Some fundamental parameters used to assess the risk level of system on a subjective basis (using linguistic variables instead of ultimate numbers in probabilistic terms) need to be defined, such as failure rate (FR), consequence severity (CS) and failure consequence probability (FCP), are more appropriate for analysis using these three parameters as they are always associated with uncertainty, especially for a novel system with high level of innovation. These linguistic assessments can become the criteria for measuring risk/safety levels.

For example, to estimate FR, one may choose to use such linguistic terms as “very low (VL)”, “low (Lo)”, “reasonably low (RLo)”, “average (A)”, “reasonably frequent (RF)”, “frequent (F)”, and “highly frequent (HF)”. The possible range of the frequencies of failure occurrence and definition of the linguistic terms of FR are provided, such ranges and definitions may vary with different engineering systems.

3) Selection of the types of fuzzy membership functions: They will be used to delineate each input variable, and provide interpretation for each fuzzy set of each variable. It is possible to have some flexibility in the definition of membership functions to suit different situations. Fuzzy membership functions are generated using linguistic categories identified in knowledge acquisition and consist of a set of overlapping curves. The application of categorical judgments has been quite positive in several practical situations. It is also common and convenient for safety analysts to use categories to articulate safety information. They are the triangular membership function and trapezoidal membership function. Both of these membership functions are commonly used to describe risk in safety assessment.  

The definitions and identifications of those parameters differ from different applications according to different requirements in codes and standards (e.g., safety/risk guidelines, regulations, laws etc.) and different aspects of engineering systems such as fire, explosions, structure, safety system, etc., for example, different definitions can be found in references.

Safety estimate or risk estimation is normally the only output fuzzy variable used to produce safety evaluation. This variable is also described linguistically, which is described and determined by the above parameters. It is common to express a safety level by degrees to which it belongs to such linguistic variables as “Poor”, “Fair”, “Average”, and “Good” referred to as safety expressions.

After the previous knowledge acquisition and representation procedures, different methodologies have been proposed to model the relationships between risk factors and risk level in order to provide fuzzy estimates of the risk components at the bottom level of a hierarchical system (e.g., each cause to technical failure). For example, to assess the safety associated with an event, it is required to synthesize the associated occurrence likelihood, consequence severity and failure probability. The way of “synthesis” of risk factors into risk estimation can be represented in different ways based on cause and effect relationship. As an extension and enhancement of classical risk matrix approaches, fuzzy arithmetic on fuzzy numbers and fuzzy rule-based systems have emerged over the last years as two major and appropriate tools in modeling the relationship in order to dealing with uncertainty and non-linear relationship in risk and safety analysis, which will be reviewed in the subsequent section.

Finally, some aggregation approaches are used in the later stage of the framework to deal with safety/risk synthesis at higher levels of the engineering system with complexity involving multi-experts, or multi-attributes, or a combination of both (this is to integrate all the possible causes to a specific technical failure, or estimates made by a panel of experts). The ranking and interpretation of the final safety/risk synthesis of a system is given.

3.1.2 Fuzzy risk analysis based on fuzzy numbers and fuzzy arithmetic
Fuzzy numbers and fuzzy arithmetic have been used to represent and manage uncertainty in various risk analysis applications in the past 10-20 years.

The early work of fuzzy risk analysis based on fuzzy number was proposed by Schmucker, where the evaluating values are represented by fuzzy numbers. Fuzzy logic and fuzzy set operations enable characterization of fuzzy sets of likelihood and consequence severity and the mathematics to combine them to determine risk. A basic structure of fuzzy risk analysis is provided and still widely used in the current fuzzy risk analysis. Schmucker, in assumes that there are \( n \) components \( A_1, A_2, \ldots, A_n \), where \( n \) manufactories \( C_1, C_2, \ldots, C_n \), respectively. Each component \( A_i \) consists of \( p \) sub-components \( A_{ik}, A_{i(2)}, \ldots, A_{ip} \), and \( A_{in} \), where 1 \( \leq i \leq n \). Two evaluating items \( R_{ik} \) and \( W_{ik} \) are then used to evaluate each sub-component \( A_{ik} \), where \( R_{ik} \) denotes the probability of failure of the sub-component \( A_{ik} \), \( W_{ik} \) denotes the severity of loss of the sub-component, 1 \( \leq k \leq p \), and 1 \( \leq i \leq n \). Furthermore, linguistic terms characterized by fuzzy numbers are used to evaluate the probability of failure and the severity of loss of each sub-component \( A_{ik} \). The fuzzy aggregation method based on fuzzy number arithmetic operations are then used to integrate the factors of each sub-component \( A_{ik} \) to obtain the probability of failure \( R_i \) of each component \( A_i \) made by manufactary \( C_i \). Then the ranking method is used to calculate the ranking indexes \( R(R_i), 1 \leq i \leq n \). The larger the value of \( R(R_i) \), the higher the risk of the manufactory. It improves upon existing qualitative methods and allows the ranking of risk alternatives based on a unified fuzzy risk index measure.

The main ideas behind Schmucker’s early work have been applied extensively in the later work, which can be briefly summarized as follows: the linguistic terms are used to represent the risk factor variables where fuzzy numbers are used to characterize those linguistic terms (e.g., define the basic event data into a fuzzy probability set) and then fuzzy set operations (aggregation operations) used to combine the risk factors, such as severity of consequences and likelihood of occurrence, to calculate risk. Finally, the value is defuzzified to obtain a precise top event probability.

In this type of fuzzy risk analysis, the number of risk factors with the corresponding definitions, fuzzy number/fuzzy membership function representation, the fuzzy aggregation techniques, as well as the ranking of fuzzy number play important roles. Extensive work varies according to the difference of those aspects and different improvements. The existing work shows that the improvement of approaches in each aspect affects the fuzzy risk analysis.

There is a huge body of literature on this type of fuzzy risk analysis available for the interested reader. For example, in Schmucker, the fuzzy weighted mean method based on fuzzy arithmetic operations is used for fuzzy risk analysis. Ferson & Kuhn used fuzzy numbers to propagate uncertainty in ecological risk analysis. Lee built a hierarchical structure model of aggregative risk in software development and rated aggregative risk in a fuzzy environment by fuzzy set theory. In succeeding studies, Lee and his associates proposed improved algorithms to find the aggregative risk in software development within a group decision making settings. Lin and Wang combined fuzzy set theories with expert elicitation to evaluate failure probability of basic events of a robot drilling system based on triangular and trapezoidal fuzzy numbers.

Shyi-Ming Chen et al. presented fuzzy risk analysis method based on the similarity measure of fuzzy numbers and generalized fuzzy numbers to overcome the drawbacks of the methods presented in Kangari and Riggs, and Schmucker. Xu et al. also presented a fuzzy risk analysis method based on the similarity measure of fuzzy numbers. Similar work based on different types of fuzzy numbers can be also found which presented a fuzzy risk analysis based on ranking fuzzy numbers using \( \alpha \)-cuts, belief features and signal/noise ratios.

Tah and Carr provided a very insightful use of fuzzy logic in a very complex project, full of risk. Schemel et al. used fuzzy numbers to represent uncertainty in failure probabilities in fault trees regarding the reliability of foam suppression systems. Abrahamsson et al. made use of fuzzy numbers to represent uncertainty in probabilities in a decision-making situation regarding which level of fire protection to use in an industrial facility. The semi-quantitative approach is taken into account and risk matrix is used for the risk evaluation and assessment provided results on the application of the fuzzy logic in the classical Process Safety Analyses, such as fault and event tree which can be further used in the so called bow-tie approach for accident scenario.
risk assessment. Hadjimichael 78 has presented a methodology by which the safety knowledge inherent in an organization such as an airline can be elicited, represented, and used for operational risk analysis. Buyukozkan and Ruan 79 proposed an integrated framework to assess software development projects in terms of the associated risks. This evaluation framework was based on the Choquet integral based aggregation method, which enabled us to consider dependencies among identified risk factors. Davidson et al. 80 presented a Fuzzy Risk Assessment Tool (FRAT) for early-stage risk assessment of microbial hazards in food systems. The user defines parameters to describe initial hazard level, potential changes during processing and consumer preparation as well as factors related to consumption and health impact. The inputs are defined in linguistic terms or semi-quantitative levels which are converted to fuzzy numbers. Some other work can be found, such as, applying fuzzy set theory to ecological risk analysis using interval and fuzzy arithmetic 81; fuzzy risk assessment of urban natural hazards 82; evaluate risk in software development 82, 83; use of fuzzy numbers in project risk (criticality) assessment 84; investment risk appraisal 85; quantitative microbial risk assessment 86; risk assessment for industrial installations 87; trade credit risks 88; fundamental fuzzy relation concepts for the estimation of natural disasters' risk using trapezoidal membership function 89; fuzzy portfolio selection method using possibilistic approach.90.

Risk is usually assessed against multiple criteria (or risk factors) and by a group of decision makers (DMs) and is therefore a typical group decision making problem. Within fuzzy number based approaches, fuzzy multiple attribute decision making (MADM) approaches have been also one typical approaches applied into risk assessment. For example, Wang and Elhag 91 presented a fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment, also a fuzzy group decision making approach for bridge risk assessment in 92. Similarly a fuzzy extension of TOPSIS and another MADM method called LINMAP in risk assessment work can be also found in 93-96. Other examples of fuzzy MADM in risk assessment can be found, such as, fuzzy group decision making for evaluating the rate of aggregative risk in software development 82; group decision making using fuzzy sets theory for risk assessment in software development 60-62; multi-attribute analysis of investments risk alternatives in construction 97; intelligent multi-criteria fuzzy group decision-making for situation assessments 98, 99 presented an integrated AHP–DEA methodology for bridge risk assessment.

The above work shows that the improvement of fuzzy approaches affects the fuzzy risk analysis too. It was also proved that the success of these methods depends on quality of failure data collection of process components as well as on the cooperation with experts 77. Applications of possibility theory are mainly within the spectrum of fuzzy set applications. Fuzzy probability based risk assessment and possibility theory based risk assessment are closely relevant to fuzzy number based approach.

Fuzzy probability is regarded as the generic name after Zadeh 100. However, this generic term has been interpreted and mathematically formalized in various ways. One of the most attractive interpretations of fuzzy probability is where probability of a crisp event, due to the imprecision of background knowledge or sparsity of data sample. The imprecise probability value of a basic event may be defined as “about 0.5” or “around 0.5”. For estimating such vague quantities or linguistic ideas on probability estimation, fuzzy probability is appropriate. Fuzzy probability is a fuzzy number, which is expressed by a fuzzy set and characterized by its membership function.

Some earlier work on fault tree analysis using fuzzy probability can be found in 101-103. Later on, Chanda and Bhattacharjee 104 considered uncertain nature of failure rate of the components, and introduced fuzzy failure probability of the components and applied in a transmission expansion planning. Sasikumar and Majumdar 105 presented fuzzy probability approaches for the water quality management of a river. A joint density function using fuzzy membership functions and probability density functions was developed following Zadeh 100, 106. To apply fuzzy probability, some input parameters must follow probability density functions, while the others need to be characterized using fuzzy membership functions.

A hybrid fuzzy-stochastic modeling approach for assessing environmental risks at contaminated groundwater systems has been proposed in 107. Karimi and Hüllermeier 108 presented an earthquake risk assessment method based on fuzzy probability, where it explained that why a framework capable of considering imprecise probability, and in particular fuzzy
probability, is essential for assessing the likelihood of natural hazards in a reliable manner. Karimi and Hullermieier investigated about risk management of natural disasters using fuzzy-probabilistic approach.

To evaluate reliability of chemical process industries efficiently, Khan and Abbasi developed computer automated tool software, by using trapezoidal representation for the probability of a basic event and eventually the fuzzy probability could be transferred to normal probability by using the average function. Huang and Moraga introduced the interior-outer-set model for calculating a fuzzy risk represented by a possibility-probability distribution. Darby summarizes techniques that use possibility theory to estimate the risk of terrorist acts. Other work on risk analysis under variability and partial ignorance using possibility-probability approach has been developed in 113-115.

The main argument for using fuzzy numbers and fuzzy arithmetic over the more classical probabilistic approach in risk analysis is that it is claimed to “make fewer assumptions” than probability theory, principally because it is based on weaker axioms. Obviously, no one can argue against probability theory possibly proving more powerful in situations where all of its axioms are satisfied but, it is claimed that risk analysis is often performed in situations where, for example, access to data is severely limited. The many advantages of fuzzy arithmetic suggest it can be very useful for risk assessments where data are perennially in short supply 116. Fuzzy arithmetic is still considered controversial by a “nonnegligible” part of the risk analysis and decision theory community; see for instance 117.

3.1.3 Fuzzy rule-based approach for risk assessment

An important contribution of fuzzy system theory is that it provides a systematic procedure, i.e., fuzzy rule base approach, for capture the uncertainty and the non-linear relationships among the system input and output parameters. Fuzzy rule-based system is constructed using human knowledge in the form of fuzzy IF-THEN rules. In risk assessment risk factors are inputs, and risk estimation is the output. The relationship between risk factors and risk is described by IF-Then Rules. For example, the following is a fuzzy IF-THEN rule for safety analysis 118:

IF FR of a hazard is frequent AND CS is catastrophic AND FCP is likely, THEN safety estimate is Poor or risk estimate is good.

A generic framework for risk assessment modeling using fuzzy rule-based reasoning approach is depicted in Fig. 3.

Fig.3 A Fuzzy Rule-Based Risk Assessment Framework

The process of reasoning in fuzzy modeling proceeds. Apart from fuzzy number based approaches to extend the classical risk matrix approach, fuzzy rule-based inference system has been used as an alternative approach to qualitative risk matrix techniques currently used in many industries. The approach is based on the use of fuzzy sets, a rule base and a fuzzy inference engine. Traditional input probabilities and consequences used in risk assessment are represented by fuzzy sets modeling uncertainties associated with the assignment of their values. The fuzzification of risk factors, e.g., frequency and severity of the consequences of the incident scenario, are basic inputs for fuzzy risk matrix. Subsequently fuzzy rules are established enabling the development of fuzzy risk matrices. The output risk values can be presented as crisp values or fuzzy sets with associated degree of membership.

The inference engine of the fuzzy logic maps fuzzy sets onto fuzzy sets. A large number of different inferential procedures are found in the literature. Mamdani et al. described an inference engine in terms of a fuzzy relation matrix and uses the compositional rule of inference (CRI) to arrive at the output fuzzy set for a given input fuzzy set. The output fuzzy set is subsequently defuzzified to arrive at a crisp value. CRI approach has been used in most papers and practical engineering applications. Another popular one is the Sugeno’s method of fuzzy inference, in which output risk values are constant or linear. It was shown that the
Mamdani method is intuitive and well suited to human input, the Sugeno’s method is computationally more efficient and guarantees continuity of the final risk output surface. In addition, the computed risk values using a fuzzy risk index measure are consistent with those obtained using a qualitative risk matrix approach 121.

Over the years, various fuzzy logic-based risk assessment models have been introduced into different application areas. Bowles and Peláez 122 demonstrated two methods of the fuzzy logic-based assessments of criticality; Levy and Yoon 123 investigated modeling global market entry decision by fuzzy logic with an application to country risk assessment; Ohasbi and internet users in Taiwan by risk assessment. Ozbek and Pinder 130 presented a risk perception. Ozbek and Pinder 130 presented a fuzzy logic application to estimate the inherent safety of a plant or a processing unit, e.g., the estimate of a plant or a processing unit, e.g., the

Over the years, various fuzzy logic-based risk assessment models have been introduced into different application areas. Bowles and Peláez 122 demonstrated two methods of the fuzzy logic-based assessments of criticality; Levy and Yoon 123 investigated modeling global market entry decision by fuzzy logic with an application to country risk assessment; Ohasbi and internet users in Taiwan by risk assessment. Ozbek and Pinder 130 presented a risk perception. Ozbek and Pinder 130 presented a fuzzy logic application to estimate the inherent safety of a plant or a processing unit, e.g., the estimate of a plant or a processing unit, e.g., the

Strengths and limitations of the proposed methodology are also presented.

Wang et al. 95 investigated optimal decision fusion when priori probabilities and risk functions are fuzzy; Kangas and Kangas 138 discussed probability, possibility and evidence approaches to consider risk and uncertainty in forestry decision analysis; Uricchio et al. 139 provided a fuzzy knowledge-based decision support system for groundwater pollution risk evaluation; Marsili-Libelli 140 presented fuzzy prediction of the algal blooms in the Orbetello lagoon. Gallego et al. 141 examined lightning risk assessment using fuzzy logic.

Ngai and Wat 142 developed and implemented a Web-based DSS that used a model based on fuzzy set theory to perform risk analysis for e-commerce development. Fiordaliso and Kunsch 143 established a decision support system based on the combination of fuzzy expert estimates to assess the financial risks in high-level radioactive waste projects; Prassl et al. 144 provided a process-knowledge management approach for assessment and mitigation of drilling risks; Iliadis 145 established a decision support system applying an integrated fuzzy model for long-term forest fire risk estimation; Iliadis and Spartalis 89 discussed fundamental fuzzy relation concepts of a DSS for the estimation of natural disasters’ risk; Ren et al. 146 presented a preliminary safety assessment of FPSO using approximate reasoning and evidential reasoning approaches. Shakhawat et al. 147 presented a fuzzy rule-based modeling for human health risk from naturally occurring radioactive materials in produced water. Reyna and Lloyd 148 investigated physician decision making and cardiac risk using fuzzy rule-based approach.

Xu et al. 18 discussed application of fuzzy expert systems in assessing operational risk of software; Liu et al. 118 have implemented IF–THEN rules to model the risks associated to software quality and project management and in order to assess the risks they have applied fuzzy inference on the rules. Makropoulos et al. 134 presented a fuzzy logic spatial decision support system for urban water management. Sii et al. provided several fuzzy logic-based approach to safety modeling for marine systems 52, 135-137, Gentile et al. 44 reported fuzzy logic application to estimate the inherent safety estimate of a plant or a processing unit, e.g., the inherent safety evaluation of a storage tank. It shows the benefits of using fuzzy logic. Strengths and
used fuzzy risk assessment to rate cost overrun risk in international construction projects; Li et al.\textsuperscript{155} provided an integrated fuzzy-stochastic modeling approach for risk assessment of groundwater contamination; Guimarães and Lapa\textsuperscript{156} applied fuzzy inference to risk assessment on nuclear engineering systems; Markowski and Mannan\textsuperscript{157} developed a fuzzy risk matrix that may be used for emerging fuzzy logic applications in different safety analyses, Comas \textit{et al}.\textsuperscript{158} presented a risk assessment modeling of microbiology-related solids separation problems in activated sludge systems; Azadeh \textit{et al}.\textsuperscript{159} presented design and implementation of a fuzzy expert system for performance assessment of an integrated health, safety, environment (HSE) and ergonomics system: Chang \textit{et al}.\textsuperscript{160} investigated the development of audit detection risk assessment system using the fuzzy theory and audit risk model; Sun \textit{et al}.\textsuperscript{161} presented fuzzy set-based risk evaluation model for real estate projects; Liu \textit{et al}.\textsuperscript{162} presented linguistic assessment approach for hierarchical safety analysis and synthesis. Nait-Said \textit{et al}.\textsuperscript{1} presented a modified risk graph method using a fuzzy rule-based-approach. Akay \textit{et al}.\textsuperscript{163} investigated NEFCLASS based extraction of fuzzy rules and classification of risks of low back disorders.

Elsayed\textsuperscript{121} presented a multiple attribute risk assessment approach using fuzzy inference system for the risk assessment of liquefied natural gas carriers during loading/offloading at terminals in shipping operations.

Gürcanli and Müngen\textsuperscript{164} provided an occupational safety risk analysis method at construction sites using fuzzy sets; Markowski and Mannan\textsuperscript{76} investigated fuzzy logic for piping risk assessment (pLOPA); Imriyas\textsuperscript{165} established an expert system for strategic control of accidents and insurers' risks in building construction projects; Hwang \textit{et al}.\textsuperscript{166} presented a real-time warning model for teamwork performance and system safety in nuclear power plants; Berizzi \textit{et al}.\textsuperscript{167} investigated online fuzzy voltage collapse risk quantification; Lee\textsuperscript{168} presented a fuzzy supplier selection model with the consideration of benefits, opportunities, costs and risks.

Li \textit{et al}.\textsuperscript{169} presented fuzzy logic-based approach for identifying the risk importance of human error; Chen \textit{et al}.\textsuperscript{170} also investigated a rule extraction based approach in predicting derivative use for financial risk hedging by construction companies; Markowski \textit{et al}.\textsuperscript{8} provided general analysis of uncertainty aspects in process safety analysis.

Due to the nature of this review work, the fuzzy rule-based scheme in each risk assessment application is not further specified.

3.1.4 Fuzzy extensions of some typical Probabilistic Risk Analysis (PRA) approaches

Risk analysis modeling methods can be generally divided into two main approaches, namely, the inductive methods such as Event Tree Analysis (ETA), Fault ETA (FETA), etc. and the deductive methods such as Fault Tree Analysis (FTA), FFTA, and so on\textsuperscript{41} (See Section 2). A number of fuzzy logic techniques have been researched to enhance both typical PRA approaches.

This section provides a brief review of fuzzy extension of those approaches, there may be some overlaps with the previous work in the above two sections, but would be still useful for those readers interested in these two typical PRA approaches.

A. Fuzzy FETA

In the traditional fault and event tree analyses (FETA), the input variables are treated as exact values and the exact outcome data are received by an appropriate mathematical approach. In the fuzzy FETA method, all variables are replaced by fuzzy numbers in the process of fuzzification and subsequently using fuzzy arithmetic operations for “AND” gate and “OR” gate operations of a fault tree, fuzzy probability of the top event for fault tree, and fuzzy outcome probabilities for event tree are calculated. A single value for each of the outcome event result is obtained with the use of one of the defuzzification methods.

Some early work on fuzzy FETA can be found in\textsuperscript{74}, 101-104, 110, 171-177; Pillay and Wang\textsuperscript{178} used fuzzy concepts to model the occurrence likelihood and consequences of failure for the identified hazards on a fishing vessel. They used fault tree analyses (FTA) to calculate a “fuzzy” probability of the system failure. The consequences of failure for each basic event within the fault tree are considered for the four categories of negligible, marginal, critical, or catastrophic. The risk of the basic events is determined by combining the likelihood of occurrence and consequences of failure in linguistic terms via a fuzzy rule set. The output, once “defuzzified”, produces a risk ranking.

Cho \textit{et al}.\textsuperscript{41} proposed a new methodology for incorporating uncertainties using fuzzy concepts into
conventional risk assessment ETA frameworks. The detailed analysis of ETA modeling approach, how to extend it into fuzzy ETA as a fuzzy number based risk analysis approaches has been presented.

Chang et al. \textsuperscript{179} presented a fuzzy diagnosis approach using dynamic fault trees. Hauptmanns \textsuperscript{180} applied semi-quantitative fault tree analysis for process plant safety by frequency and probability ranges. Batzias and Batzias \textsuperscript{181} presented fuzzy fault tree analysis as a means for computer aided technology transfer to small/medium anodizers. Dong and Yu \textsuperscript{182} investigated estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis, where probabilities of basic events of an oil and gas transmission pipeline were treated as fuzzy number, which could be obtained by expert elicitation and theory of fuzzy set and failure probabilities of the top event (failure of the pipeline) and important analysis of the basic events were evaluated using fuzzy failure probabilities of the basic events. Ferdous \textit{et al.} \textsuperscript{183} presented a methodology for computer aided fuzzy fault tree analysis, which is a revised version of the PROFAT algorithm \textsuperscript{110}. Dokas \textit{et al.} \textsuperscript{184} presented fault tree analysis and fuzzy expert systems for early warning and emergency response of landfill operations. It showed in detail the architecture of an intelligent system providing early warning services, as well as how fuzzy fault tree analysis, possibility theory and risk analysis are integrated into one operational fuzzy expert system providing early warning services.

\textbf{B. Fuzzy FMEA}

Failure mode and effects analysis (FMEA), as another important PRA approach, has been extensively used for examining potential failures in products, processes, designs and services \textsuperscript{185, 186}.

An important issue of FMEA is the determination of risk priorities of the failure modes that have been identified. The traditional FMEA determines the risk priorities of failure modes using the so-called risk priority numbers (RPNs), which require the risk factors like the occurrence (O), severity (S) and detection (D) of each failure mode to be precisely evaluated. In the fuzzy FMEA, the risk factors O, S and D are treated as fuzzy variables and are evaluated using fuzzy linguistic terms and fuzzy ratings. As a result, fuzzy risk priority numbers (FRPNs) are proposed for prioritization of failure modes. In \textsuperscript{187}, the FRPNs are defined as fuzzy weighted geometric means of the fuzzy ratings for O, S and D, and can be computed using alpha-level sets and linear programming models. For ranking purpose, the FRPNs are defuzzified using centroid defuzzification method, in which a new centroid defuzzification formula based on alpha-level sets is derived. A detailed literature review of fuzzy FMEA has been also provided in \textsuperscript{187}. Some other examples are listed as follows: Bowles and Peláez \textsuperscript{122} and Rudiger \textit{et al.} \textsuperscript{188} presented a fuzzy rule-based technique for FEMA, similar fuzzy inference methods also appeared in \textsuperscript{142}, \textsuperscript{189-193}. Braglia \textit{et al.} \textsuperscript{194} proposed fuzzy TOPSIS approach for FMECA; Pillay and Wang \textsuperscript{195} proposed a new approach by using “fuzzy rule base” and “grey relation theory” to overcome some of the drawbacks of traditional FMEA approach. Yang \textit{et al.} \textsuperscript{196} presented a novel, efficient fuzzy rule-based Bayesian reasoning (FuRBar) approach for prioritizing failures in FMEA. The technique was specifically developed to deal with some of the drawbacks concerning the use of conventional fuzzy logic (i.e. rule-based) methods in FMEA. The applicability of the proposed approach was demonstrated by studying a maritime collision risk due to technical failures.

\textbf{3.1.5 Ordinal fuzzy linguistic approach for risk assessment}

Apart from fuzzy-set theories based CWW, there exist some alternative methods developed in last few years to model and compute with linguistic information in natural languages from a different point of view, called linguistic-valued based intelligent information process approach \textsuperscript{197}. Ordinal fuzzy linguistic approach based on the ordering of linguistic terms set is the most typical one in these types of work.

A key insight and the main focus behind linguistic-valued based approaches is that the linguistic value reflects the use of “words” as computational variables, i.e., directly represent and manipulate the available linguistic information in natural language, where the symbolic approach acts by the direct computation and reasoning on linguistic terms. These approaches are regarded as alternative methods to modify and overcome limitations of fuzzy-set theories based CWW, e.g., difficulty in determining and interpreting fuzzy set membership functions of linguistic values, computational complexity and loss of information due to linguistic approximations. Its application is beneficial because it introduces a more flexible framework for representing the information in a
more direct and suitable way when it is not possible to express it accurately. Thus, the burden of quantifying a qualitative concept is eliminated and the systems can be simplified.

There have been a number of publications on risk assessment based on ordinal fuzzy linguistic approach; the technical focuses have been given on the aggregation operators based on ordinal linguistic values.

Ordinal fuzzy linguistic approach has been also applied in risk assessment of typical hazards associated with open cast mining where the model only demands ordinal information of experts’ preferences and the importance of each individual factor. It has been stated that this model can be used by the practicing engineers who may not be having in-depth knowledge on fuzzy mathematics.

Herrera and Martinez proposed the 2-tuple fuzzy linguistic representation model, which allows one to make processes of computing with words without loss of information. This model is based on the concept of symbolic translation. It represents linguistic information by means of linguistic 2-tuples and defines a set of functions to facilitate computational processes over 2-tuples. 2-tuples model approach has been applied in different areas, in risk assessment as well. For example, Doukas et al. extended the numerical multicriteria method TOPSIS for processing linguistic data in the form of 2-tuples, so as to show how energy policy objectives towards Sustainable Development (SD) and Renewable Energy Sources (RES) are assessed using linguistic variables. Chang and Wen combined 2-tuple and the Ordered Weighted Averaging (OWA) operator for prioritization of failures in a product Design Failure Mode and Effect Analysis (DFMEA). After comparing the result that was obtained from the proposed method with the other two listed approaches, it was found that the proposed approach can effectively solve the problem of measurement scales and has not lost any expert to provide the useful information. As a result, stability of the product and process can be assured. Wang applied 2-tuple fuzzy linguistic computing approach to deal with heterogeneous information and information loss problems during the processes of subjective evaluation integration in product development performance, also for stock portfolio selection based on computing with linguistic assessment. Martinez et al. have applied 2-tuple modeling approach into safety evaluation and synthesis including some multigranular hierarchical linguistic model for design evaluation based on safety and cost analysis. Liu et al. introduced a safety model based on the concept of approximate reasoning for safety analysis. A safety estimate for possible causes of a technical failure can be obtained by the approximate reasoning approach. However, a safety synthesis based on an ordinal fuzzy linguistic approach by means of a direct computation on linguistic values instead of the approximation approach by their associated membership functions, is then applied to integrate all possible causes for a specific technical failure, or applied at the safety estimate made by a panel of experts. The use of the ordinal fuzzy linguistic approach makes the safety analysis more effective. Ruan and Liu have been working on linguistic assessment approach for managing nuclear safeguards indicator information. Augusto et al. provided a decision procedure using linguistic ordinal preference modeling approach in relation to situation assessment during disaster management monitoring.

3.2 Miscellaneous applications

As a complementary part of the above review, this section provides some miscellaneous applications of fuzzy logic approach in risk assessment.

3.2.1 Security risk assessment using fuzzy logic

The reason we set a separate section for security risk assessment because security is becoming one of the most important criteria for measuring the performance of the design, control and management of engineering systems. Over the past several years, there has been a growing international recognition that risks associated with threats (also referred to as security risks) need to be reviewed on an urgent basis. The term security may in general be defined as freedom from vulnerability which is an exposure to serious disturbances arising from threats. Whilst conventional hazard-based risk is a combination of the probability of occurrence of an undesirable event and the degree of its possible consequences, security risks are different from hazard-based risks and need to be modelled differently. As a result, security and risk assessment is a process of analysing both threats and hazards in a system and making respective decisions on suitable strategies against the potential vulnerability of the system.

Early in the studies of risk analysis related to
computer security, fuzzy modeling was used to analyze and rank risks in a computing facility 40. The authors created a set of fuzzy rules describing likely vulnerabilities such as “if the hard drive is old, then the customer database loss risk factor is increased”. These rules are combined to produce a total risk factor associated with the loss of the customer database. Similar rule sets and associated risk factors can be calculated for all computer facility assets.

Darby 112 summarized techniques that use possibility theory to estimate the risk of terrorist acts. Chang and Hung 209 considered the fuzzy number based aggregation in risk assessment by applying the fuzzy-weighted-average approach to evaluate network security systems. Van de Walle and Rutkowski 210 developed a fuzzy decision support system for IT service continuity threat assessment. Yager 211 focused on aggregation issue and investigated the OWA trees and their role in security modeling using attack trees.

Yang et al. 196 stated that the use of traditional risk assessment and decision-making approaches to deal with potential terrorism threats in a maritime security area reveals two major challenges. They are lack of capability of analyzing security in situations of high-level uncertainty and lack of capability of processing diverse data in a utility form suitable as input to a risk inference mechanism. To deal with such difficulties, Yang et al. 196 proposed a subjective security-based assessment and management framework using fuzzy evidential reasoning (ER) approaches. Consequently, the framework can be used to assemble and process subjective risk assessment information on different aspects of a maritime transport system from multiple experts in a systematic way. Outputs of this model can also provide decision makers with a transparent tool to evaluate maritime security policy options for a specific scenario in a cost-effective manner.

Bajpai et al. 49 is one of the latest representative paper about security risk assessment by applying the concepts of fuzzy logic. Chemical process industries (CPI) handling hazardous chemicals in bulk can be attractive targets for deliberate adversarial actions by terrorists, criminals and disgruntled employees. It is therefore imperative to have comprehensive security risk management programme including effective security risk assessment techniques. In their paper, Bajpai et al. 49 modified the earlier developed Security Risk Factor Table (SRFT) model using the concepts of fuzzy logic with application in CPI.

Generally, from the literature review, there are no much work been done yet on the application of fuzzy logic in security risk management process. However, the existing security measures need enhancement. Security enhancements may be required, especially under uncertain conditions. So this would be an important and imperative direction for now and for the future.

3.2.2 Other applications

The use of fuzzy logic in different aspects of risk and safety analysis to tackle uncertainties has been reviewed in the previous section. In this subsection, some additional lists are provided to show the fat that fuzzy logic has been widely used to assess various risks in different areas; this section provides some additional review to reflect this diversity of application.

Some early work fuzzy logic application in various risk assessment can be found, such as in industrial safety engineering 212; system failure and criticality analysis 5, 122, 173, 213, 214; ecological risk analysis 58; fault tree analysis using fuzzy probability 101, 102; environmental risk 39; software development and operational risk 39, 59-61 risk assessment of urban natural hazards 81.

Some latest applications can be found, such as failure mode, effects and criticality analysis in 93, 195, 215; construction project risk assessment 41, 84, 217-219; software development and operational risk assessment 18, 62, 82; risk assessment for microbial hazards in food systems 80, 86; plant safety 44; risk assessment of hydrocarbon-contaminated site 220; performance evaluation of an irrigation reservoir system, agricultural water management 221; investment risk 85; forest fire risk estimation 145; risk-based decision making in water resources planning 135, 220; risk analysis in e-commerce development 142; environmental risk assessment 63, 115; bridge risk assessment 91, 96, 222; audit detection risk assessment system 160; occupational safety and risk analysis 164, 225; risk assessment of Landfall Typhoon 224; classification of risks of low back disorders in classification of industrial jobs 163.

Fuzzy logic application for occupational safety and health (OSH) was discussed just in the pioneer paper of Falconer & Hoel 225. Only in recent years, a new interest for fuzzy logic and OSH have been demonstrated by a few number of papers, including Mura et al. 226; Guldemunda et al. 227; Chang et al. 160;
Fuzzy logic systems are nowadays commonly used in fields where different levels of uncertainty are present. Most of these studies have applied traditional fuzzy sets (i.e., type-1 fuzzy sets, T1FS), however, the use of expert opinion itself is sometimes limited by its inherent vagueness, which can be an important source of uncertainty that reduces the validity and applicability of the assessment. Fuzzy logic, specifically interval type-2 fuzzy logic (IT2FS) \cite{228-230}, is able to model and propagate this type of uncertainty, and is a useful technique in risk assessment where expert opinion is relied upon. Acosta et al. \cite{33} detailed the procedure and relevant literatures of using IT2FS into risk assessment, where it describes the implementation of a NIS fuzzy expert system (FES) for assessing the risk of invasion in marine environments via recreational vessels based on IT2FS approach.

### 4. Conclusions and Prospective

From the previous detailed literature review, we could find some main characteristics of fuzzy systems that give them good performance for specific applications in risk assessment:

- A fuzzy system is well suited for risk assessment applications where evidence is itself fuzzy in nature.
- Fuzzy systems are suitable for uncertain or approximate reasoning, especially for systems where mathematical models are difficult to derive in risk assessment.
- Fuzzy logic provides an alternative way to map an input space to an output space. It is also tolerant of imprecise data and therefore provides a simple way of obtaining relationships based on experimental data.
- Fuzzy logic allows decision making with estimated values under incomplete or uncertain information; this is especially useful in risk assessment.

There are also some disadvantages of fuzzy set theory identified in the risk assessment application, such as:

1) It is not always clear how to construct reasonable membership functions. Various methods have been proposed including the use of statistical data, and the composition of simpler functions, but no completely general approach seems to exist yet. According to Zadeh, membership functions are subjective and context dependent, therefore, there is no general method to determine them either by experiment or analysis \cite{17}.

2) The choice of appropriate definitions for the operators can be problematic. As Zadeh himself has acknowledged, different definitions are needed in different situations; however it is not always clear as to what definitions should be used.

3) The inherent flexibility of fuzzy set theory can also be a disadvantage since there is little guidance as to which methods to use to solve a given risk problem.

4) There is the inherent lack of formal definitions for functional modifier rules. This can lead to inconsistencies between knowledge bases.

However, these problems have not stopped researchers from creating successful risk assessment application. It is clear that after nearly thirty years of research, fuzzy logic has proven its worth as a practical engineering and problem-solving tool, and an important tool in risk assessment. Fuzzy logic has been also widely applied in risk assessment in different areas and has been regarded as one of the promising methods for reduction of the uncertainties in risk assessment. A significant amount of fuzzy set application to risk assessment in the literature is based on hypothetical information or test cases. Applications of fuzzy systems to real risk assessment problem with real decision-makers are urgently needed to demonstrate the efficacy of the fuzzy systems approach for solving real-world problems.

Fuzzy logic is not a single method suitable for the entire spectrum of problems encountered in uncertainty analyses for risk assessment. Parameter uncertainty is a major aspect of risk assessment. Quantitative assessment of risk is particularly challenging in domains where undesired events are extremely rare, and the causal factors are difficult to quantify and non-linearly related. However, it is impossible to identify a single approach to uncertainty analysis that will prove to be the most powerful in all situations. In practice, it may occur that certain model parameters can be reasonably represented by probability distributions, because there are sufficient data available to substantiate such distributions by statistical analysis, while others are better represented by fuzzy numbers (due to data scarcity). The question then arises as to how these two modes of representation of model parameter uncertainty can be combined for the purpose of estimating the risk of exposure. Hence, it should be necessary and potentially beneficial to apply the
different kinds of uncertainty theories to safety and risk based assessment and decision-making. The selection of uncertainty handling approaches depends on the purpose of the risk assessment, the availability of failure data (quantitative and qualitative information), the indenter level of the analysis required, the degree of complexity of the interrelationships in a design, the level of innovation in the design, the causes of “uncertainty”, and languages required by the final observer 231. Indeed, the differences between the methods are substantial, and the choice of method may significantly influence the final result of the risk assessment. Some papers about uncertainty characterization approaches for risk assessment could also be interesting for the readers, such as 6, 10, 118.

Hybrid approach for addressing uncertainty in risk assessments in 115, 232, some general theoretical background can be found in 232, 233. Guyonnet et al. 115 proposes an approach (termed a hybrid approach) which combines Monte Carlo random sampling of probability distribution functions with fuzzy calculus. Also, because the hybrid approach takes advantage of the “rich” information provided by probability distributions, while retaining the conservative character of fuzzy calculus, it is believed to hold value in terms of a “reasonable” application of the precautionary principle. A hybrid approach combining fuzzy rule-based system with D-S theory for safety estimation and synthesis is also provided in 7, 115, 234, 235.

The complexity and dynamics of real-world engineering, financial and economical problems require advanced and sophisticated methods and tools to build hybrid risk assessment tools which can deal more powerfully with issues like fast-learning, uncertainty, online adaptability, knowledge capability and hierarchical solution etc.

Acknowledgments

This contribution has been partially supported by the projects TIN-2009-0828, P08-TIC-3548 and FEDER funds.

References

104. Liu, J., et al., Review of uncertainty reasoning approaches as guidance for maritime and offshore


148. Reyna, V.F. and F.J. Lloyd, *Physician decision making and cardiac risk: effects of knowledge, risk perception,


