Development of a hierarchical fuzzy model for the analysis of inherent safety focused on process simulation

M. Gentile, W.J. Rogers, and M. S. Mannan
Mary Kay O'Connor Process Safety Center
Chemical Engineering Department
Texas A&M University
College Station TX 778433122
Email: mannan@tamu.edu

ABSTRACT

Inherent safety (IS) has been recognized as a design approach useful to remove or reduce hazards at the source instead of controlling them with add-on protective barriers (as in the case of extrinsic safety). However, inherent safety is based on qualitative principles that cannot easily be evaluated and analyzed, and this is one of the major difficulties for the systematic application and quantification of inherent safety in plant design.

The model proposed here is based on a hierarchical tree that integrates the knowledge available for three main factors that contribute to process hazard: chemical properties that imply toxic hazards for humans and the environment; chemical properties that imply process hazards such as fire and explosion; and design characteristics of the plant. Because, in general this information is not only scarce but also highly uncertain and vague, the model is based on fuzzy logic. The system is composed of 35 local fuzzy inference systems based on a Mamdami model that condenses expert, heuristic, and technical knowledge by using IF-THEN rules.

The proposed hierarchical fuzzy model is based on the idea that safety can be understood as a complex system where the interaction of several factors can increase or decrease the overall inherent hazard of a chemical plant. However, because of the complexity of the problem, factor interaction is rarely taken into account. Each fuzzy inference system describes a local part of knowledge that is then integrated into the overall evaluation by the hierarchical tree, able to model factor interaction.

Because traditional approaches for extrinsic and intrinsic safety analysis are based on simple discrete scoring systems, they cannot be integrated into process simulation and optimization. However, fuzzy logic allows the evaluation of safety as a continuous function and therefore can be linked to process simulation. The prototype methodology proposed in this research relies on process information that can be obtained through simulation and cost estimation (i.e., preliminary equipment sizing) even during early stages of the development of a chemical process. Therefore process safety evaluation and hazard identification can be applied earlier and by engineers who do not need to be safety experts.

1. Introduction to process safety

The chemical industry is inherently hazardous because of the variety and quantities of potential dangerous chemicals involved and the different types of processing operation and equipment used. The accepted definition of safety is associated to low risk, where risk is understood as the multiplication of the event's likelihood and magnitude of the potential consequences. The questions that are sought to be answered are: which are the most likely incident scenarios? How frequent is the scenario? How bad are the consequences? After the potential hazards and its consequences are identified, protective barriers are designed (e.g., relief valves, control systems, emergency operating procedures) in order to reduce the likelihood of the incident and/or the magnitude of its consequences. However, because the hazard is not removed or reduced, the occurrence of the incident is still possible if the protective barriers fail.

Inherent safety is a different approach that understands safety as lack of hazards (and therefore low risk) and has the objective to remove the hazards by design eliminating the requirements of protective barriers. This is the safety approach used for the novel methodology proposed in this work. Although inherently safer design is proposed as the first and most effective approach for risk reduction, the lack of a systematic analytical approach focused on computer-based tools is a significant practical limitation.

Process safety and loss prevention in the chemical industry are concepts that have been developed during the last fifty years. In general, well-accepted methodologies for the analysis of process safety have not been adapted to be used with process simulators therefore safety analysis is understood as an activity that is performed after the basic design of the process plant has been developed. Only few attempts have been made to integrate safety analysis into process simulation and process design software [Koller et al, 2001].The approach proposed here is computer-based and process simulator-oriented with the goal of reducing the time and expertise required for the analysis. It is expected that in the future, by linking the present approach to a process simulator, process engineers can develop safety analysis during the early stages of the design in a rapid and systematic way.

This paper presents only the first step of the research and introduces the approach and methodology. Future research will focus on the connection to a process simulator, and the expected advantages are the following:

1) Automated inherent safety evaluation and cost estimation that allow a rapid analysis and generation of processing alternatives when process synthesis is carried out with a systematic generation of design that follows the economic and safety constraints.
2) Possible application to operative plants allowing the identification of processing alternatives according to the cost and environmental constraints. As in the case of optimization of a process with respect to environmental restrictions, optimization for safety is more efficient when applied during earlier stages of the life-cycle of a plant. However, as demonstrated by El-Halwagi (1997) and Sikdar and El-Halwagi (2001) it is possible to apply the same optimization principles to existing plants to obtain more environmentally friendly processes. A similar application is expected for the inherent safety principles when an inherent safety quantification methodology is available.

3) The application of process simulation presents the additional advantage of permitting analysis of the hazard level of processing areas interconnected to units or equipment modified toward an inherently safer design.

1.1 Traditional process safety approach

The modern conceptual and methodological framework for process safety is mainly based on concepts and ideas borrowed from the nuclear industry such as reliability analysis and fault tree analysis. During the 1970s and early 1980s, methods for consequence analysis, and calculation of incident likelihood and probability were adopted by the chemical industry after the nuclear industry recognized the potential magnitude of incidents [Brown, 1999; Kletz, 1999a].

Currently, only few methodologies are used and well-accepted for loss prevention analysis and they were developed during the '50s to the '80s. The accepted methods range from relatively simple tools mainly based on discrete scoring systems (e.g., Dow Fire and Explosion Index), to very complex tools often used only in simplified versions (e.g., Quantitative Risk Assessment and Fault Tree Analysis). In general, these analytical tools are not computer-based therefore they tend to be time consuming and because they have to be used as simplified version, they cannot capture the complexity of a chemical processing plant. A review of these methods is presented by Lees (1996), Kletz (1999), and Gentile (2004).

The modern technical literature includes a large number of other methodologies proposed during the '90s and in general not well-accepted by the industry. Tixier et al. (2002) reviewed 62 methods and classified them based on the type of input, type of output, data required, type of method (i.e., deterministic, probabilistic, qualitative, quantitative), relation between input and output data, and risk hierarchy. Most of the new methodologies are based on usual and traditional safety and risk concepts and attempt to address the limitation of the well-accepted methods and some of them focus on computerization.

Nevertheless, the continuous proposal of new tools for process safety highlights the fact that we are still not able to understand what safety is and how to take into consideration the high uncertainty and complexity of chemical plants. The answer to the question "How safe is a chemical plant?" has become a circular problem. The more recent methodologies have been shaped around the early and now well-accepted ideas and techniques for safety and risk assessment, hence innovation is itself bounded by the limitations of the original now well-accepted methods [Gentile, 2004].

1.2 Inherent safety

T.A. Kletz formally introduced inherent safety in the late '70s [Kletz, 1996] and since then it has been recognized as a smart approach to improve process safety. The main purpose of Inherently Safer Design is quite different in comparison with the aim of the traditional concepts of safety. While the former aims to eliminate or to reduce the hazards present in a process facility, the latter aims to control hazards and to reduce the consequences of a possible accident by using add-on barriers. Thus the hazard may still be present and "safety" depends upon the reliability of the protective barriers, which present other disadvantages such as high installation and maintenance costs. A review of the benefits and problems associated with both inherently safer design and the traditional approach are presented by Gentile (2004).

Inherent safety is based on four principles that can be extended to 14 when the “friendly plant” ideas are included [Kletz, 1998]. The principles for inherently safer plants are:

- INTENSIFICATION: Reduction of the inventories of hazardous materials.
- SUBSTITUTION: Replacement of the chemical substances by less hazardous chemicals.
- ATTENUATION: Reduction of the quantity of hazardous materials required in the process. Design processes working at less dangerous processing conditions by reducing temperature, pressure, flow, or other relevant variables.
- LIMITATION of EFFECTS: The facilities must be designed in order to minimize the effects of the release of hazardous chemicals or energies.

The lack of a measurement methodology has been recognized as one of the reasons for the slow implementation of the inherently safer design approach. The methodologies proposed for the evaluation of inherent safety are summarized and analyzed by Gentile et al. (2003) and Gentile (2004). Because ISD requires the modification of the chemical process and the design of the plant, it is recognized that it is more efficient to apply it during the early stages of design. Therefore the analytical methods reported by the specialized literature tend to be simplistic and based on manual computations; furthermore they require limited information and are unable to describe the interaction of the relevant variables and the complexity of a chemical plant.

1.3 Design and simulation

The application of inherently safer design requires a holistic approach and a complete understanding of the implications of the changes within the whole plant. When the design of equipment is modified towards an inherently safer option, the achieved local hazard reduction may cause more hazardous conditions in other parts of the plant. When inherent safety is applied only to one single element (e.g., distillation column by reducing liquid space volume) while the other aspects are not improved accordingly (e.g., control system strategy) the expected results probably will not increase the overall safety level (e.g., increased control instability). This example highlights the fact that not only it is required to analyze variable interactions within the same equipment but also among interrelated units.

The whole plant must be analyzed not only from the processing viewpoint but also from the capital and operating cost, to understand where and how the hazards have been removed (or created) and the economic impact of the proposed changes. Process hazard migration, capital cost, and operation cost, change due to plant modification toward inherent safety. In order to facilitate the application of the proposed methodology during engineering design and being able to analyze the effects of hazard migration and the interaction of the variables, it is necessary to link the procedure to a process simulator. Process simulation is useful for evaluating the processing alternatives from the processing requirements. When process simulation is linked to cost estimation software, the capital and operating costs can be evaluated, and the results of the analysis can be used by process synthesis to generate better processing alternatives based on the technical, environmental, and economic constraints.

A limitation for the application of traditional safety methodologies to process simulation is the discrete nature of the scoring systems and interval-based variables, commonly used in process safety analysis. The development of an overall inherent safety index based on continuous functions will facilitate the application of inherent safety to process simulation and process synthesis. As noted by Mansfield (1991) in order to measure inherent safety it is necessary to develop an index capable of measuring a “degree” of “inherent safetiness.” In other words, the question that should be asked is “How inherently safer is the plant?” rather than “Is the plant inherently safer?” The difference implicit in these two questions is more evident when the concept “inherent safety” is recognized as an uncertain idea without defined boundaries rather than a concept limited by crisp limits [Gentile, 2004].

2. Approach: Inherent safety as a fuzzy system

Safety, as many other concepts used in chemical engineering, is a fuzzy idea that cannot be limited to only two possible states, safe/unsafe. In other words a piece of equipment, a processing unit or a chemical plant cannot be classified as safe or unsafe because of the complex nature of these systems and the many factors (objective and subjective) that are to be taken into consideration. However, when safety is evaluated by using a Boolean approach, an element can only be classified into the two categories, and this dichotomy establishes another problem related to how to set the limit between the two states. Analytical methods for loss prevention based on scores assigned to predefined subintervals of a variable follow the Boolean approach. On the other hand, fuzzy logic allows a gradual transition between the two extremes (safe/unsafe) and the degree of safety can be related to the value of the membership function into the “Inherently Safer” fuzzy set [Gentile et al., 2001]. An extended discussion on the approach is presented by Gentile (2004).

Fuzziness originates from the imprecise nature of abstract concepts and thoughts rather than from the random properties of an event. As indicated by Almond (1995), fuzzy logic allows working with imprecision and real-world, vague engineering problems that would otherwise be rejected by the traditional statistical methodologies. Fuzzy set theory and fuzzy logic offer an alternative mathematical framework where vague and imprecise concepts and phenomena can be rigorously modeled and analyzed by allowing an element to belong simultaneously to more than one category or set.

3. Introduction to fuzzy logic and fuzzy system

This section provides a brief introduction to the most important concepts of fuzzy logic necessary for understanding the methodology proposed. The following references may be consulted for additional information and examples on fuzzy logic, fuzzy measure, and possibility theory: Berkan and Trubatch (1997); Klir and Folger (1988); Klir and Yuan (1995); Lootsma (1997); Jang et al. (1997); Yen and Langari (1999); Tanaka (1996); Zimmermann (1996).

3.1 Elements of fuzzy logic

Fuzzy logic is based on the concept of partial membership into a set described by the membership function ($\mu_{\hat{A}}$). In the case of a Boolean set, when the element x belongs totally to the set A then $\mu_{\hat{A}}$ = 1, while if the element x does not belong to the set $\mu_{\hat{A}}$ = 0. In fuzzy logic, partial membership in the fuzzy set Â is allowed and it is described by real values $0 \le \mu_{\hat{A}} \le 1$. The partial membership permissible by fuzzy logic allows modeling vague concepts (e.g., warm temperature, very comfortable, unsafe) therefore it is a useful tool to model the concept of “degree of inherent safety” bounded by the limits safe/unsafe [Gentile et al., 2001].

A fuzzy variable is known as linguistic variable and it is divided into fuzzy sets defined by the membership function, which indicates the degree of membership into that set (Figure 1). The temperature of 70 ^{O}F belongs to the fuzzy set “moderate” with a membership degree of $\mu_{moderate}$ = 0.4 and to the fuzzy set “low” with a membership degree of μ_{low} = 0.1.

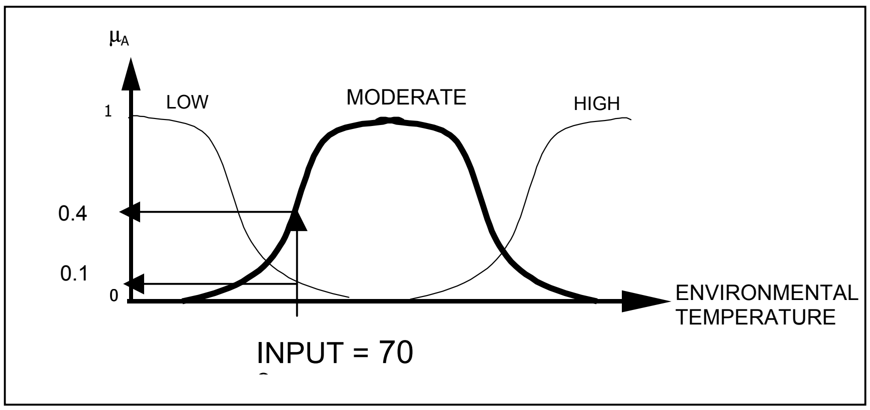

Figure 1: Example of linguistic variable (ENVIRONMENTAL TEMPERATURE), fuzzy sets (HIGH, MEDIUM, LOW) [Gentile, 2004].

The relations between the fuzzy sets of the linguistic variables for the inputs are related to the fuzzy sets of the variables of the outputs by IF-THEN rules that condense the knowledge about the behavior of the system. The evaluation process is called fuzzy inference and the system is designed according to a Mamdami model defined by a simple structure of max and min operations. Mamdami’s method uses rules such as:

$$\text{IF } x \text{ is } \hat{A}_i \text{ AND } y \text{ is } \hat{E}_j \text{ THEN } z \text{ is } \hat{C}_k$$

where Â, Ê, and Ĉ are fuzzy sets and x, y, and z are linguistic variables divided respectively into i, j, and k fuzzy sets, whose relation is described by the rule.

The Mamdani fuzzy inference algorithm is based on a model that uses groups of r rules such as [Yen and Langari, 1999]:

Rule 1: $\text{IF } x \text{ is } \hat{A}_{i1} \text{ AND } y \text{ is } \hat{C}_{j1} \text{ THEN } z \text{ is } \hat{E}_{k1}$

Rule 2: $\text{IF } x \text{ is } \hat{A}_{i2} \text{ AND } y \text{ is } \hat{C}_{j2} \text{ THEN } z \text{ is } \hat{E}_{k2}$

. . .

Rule r: $\text{IF } x \text{ is } \hat{A}_{ir} \text{ AND } y \text{ is } \hat{C}_{jr} \text{ THEN } z \text{ is } \hat{E}_{kr}$

where Â and Ĉ are input fuzzy sets and Ê represents the output fuzzy sets; r is the number of rules (r = 1… r). The connectors AND and OR are evaluated respectively by the standard operations of fuzzy intersection ($\mu_{\hat{A} \text{ and } \hat{E}}(x) = \mu_{\hat{A} \cup \hat{E}}(x) = \mu_{\hat{C}}$) and fuzzy union ($\mu_{\hat{A} \text{ or } \hat{E}}(x) = \mu_{\hat{A} \cap \hat{E}}(x) = \mu_{\hat{C}}$) [Klir and Yuan, 1995]. In the rules the connector AND can be replaced by OR depending on the requirements of the physical model. The linguistic variables x, and y are the input variables, while the linguistic variable z is the output. The linguistic variables x is divided into i fuzzy sets while the variables y and z are divided into j and k fuzzy sets, respectively.

After the rules have been evaluated, the output fuzzy sets $\hat{E}_r$ for each rule must be aggregated by using $\hat{E} = \bigcup_{r=1}^{n} \hat{E}_r$ where r is the number of rules. The obtained fuzzy set Ê is the fuzzy output of the inference system and must be defuzzified to obtain a crisp result. The defuzzification methodology used is the center of mass (although there are several possible methods) of the resultant fuzzy set Ê, because it takes into account the strength of the fuzzy set $\mu_{\hat{E}}(x)$ and its support, where $\mu_{\hat{E}}(x)>0$ [Runkler, 1997, Berkan and Trubatch, 1997, Yen and Langari, 1999, Zimmermann, 1996]. A simplified example of inference system applied to process safety is presented by Gentile et al., (2003), and Gentile (2004).

3.2 Computing with words

In order to understand the methodology of this work it is helpful to establish an analogy between traditional mathematical and statistical modeling procedures with similar methodology for fuzzy systems. A traditional model is constituted of a set of mathematical equations that describe the behavior and interaction of its independent variables. When the equation is solved, the dependent variables are assigned numbers, which are the solution of the equation. If the model is built from physical principles, a mathematical equation or set of equations is obtained, which are then tested against real experimental data. In fuzzy logic, the equivalent of the traditional independent variables, are fuzzy sets defined for specific linguistic variables. Each fuzzy set is combined to the fuzzy sets of the other variables by IF-THEN rules that describe the relation existing between the sets. Procedures for fuzzy modeling can be classified in a similar way as for traditional models.

As indicated by Zadeh (1996) fuzzy logic is a methodology that allows computing with words and no other modeling method offers such flexibility. The basic concept upon which "computing with words" is based is the "granule" that groups points that have similar features; in other words a granule is a fuzzy set. A granule can be atomic (e.g., safe) or composite (e.g., very safe) and is represented by a word which is a fuzzy constraint on the variable. For example, for the proposition "Mary is young" the word "young" represents a granule that groups certain ranges of ages and act as a fuzzy constraint (i.e., fuzzy set) on the linguistic variable "age".

When there are several propositions expressed in terms of IF-THEN rules, as for example:

IF X is small THEN Y is small
IF X is medium THEN Y is large
IF X is large THEN Y is small

the rules describe a function *f*: U →∈V, X ∈U, Y∈V. The function *f* is approximated by the fuzzy graph f^*:

$$f^* = \text{small x small + medium x large + large x small}$$

where the symbols x and + indicate disjunction and Cartesian product [Gentile, 2004]. For example, if A and B are two words, then the expression AxB represents a Cartesian granule (shown as gray rectangles in Figure 2), therefore the fuzzy graph f^* can be understood as a disjunction of Cartesian granules. In other words, a fuzzy graph f^* is an approximation of a function or relation *f* as shown in Figure 2.

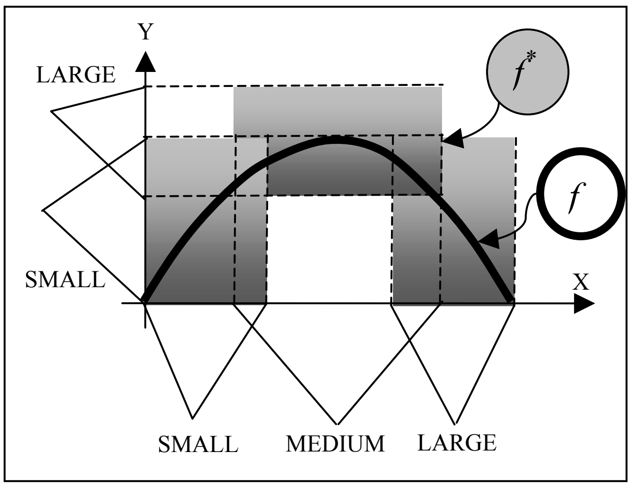

Figure 2: Unknown function *f* approximated by a fuzzy graph f^* built from the linguistic granules of the linguistic variables X and Y [Gentile, 2004].

Computing with words is defined by Zadeh (1996) as "…a necessity when the available information is too imprecise to justify the use of numbers, and when there is a tolerance for imprecision which can be exploited to achieve tractability, robustness, low solution cost, and better rapport with reality..." When the concepts of "computing with words" are applied to the problem of inherent safety quantification, several advantages become evident.

In inherent safety quantification function *f* is unknown, but heuristic and empirical knowledge is available. The inherent safety principles are an example of the type of knowledge that can be modeled through the "computing with words" methodology in order to approximate the unknown "safety function" f_s through a fuzzy graph f_s^*. The procedure for the selection of the variables, definition of the granules, and definition of the rules is described in the following section. The application to the specific problem of inherent safety is described Gentile (2004).

3.2 Elements of hierarchical fuzzy systems

The application of fuzzy logic to complicated process control problems with a large number of inputs highlighted the problem of rule-explosion. If a system requires n input variables each partitioned into m membership functions, the total number of rules required to model the system by using one single fuzzy inference system is m^n. As the complexity of the problem increases, the number of required inputs increases too, requiring an exponentially larger number of rules.

In order to deal with the problem rule-explosion, the development of hierarchical fuzzy systems has been proposed. In hierarchical systems, the number of rules increases linearly with the number of inputs rather than exponentially [Lee et al., 2003]. For hierarchical fuzzy systems, the outputs from certain fuzzy inference systems (i.e., FIS or rule sets) are used as inputs for the following FIS, which are difficult to design when the intermediate outputs do not have physical meaning.

In the case of the proposed hierarchical model for inherent safety evaluation, sources of hazard represented by physical factors are combined by fuzzy rules and their aggregated outputs represent a measure of the inherent hazard. These measures of hazards are then used as inputs for the next layers of the hierarchical model; however, since the measure of hazard is related to the potential physical consequences, they keep a physical significance [Gentile, 2004].

4. Description of the hierarchical fuzzy-model

The basic assumption upon which the methodology is based is that every piece of equipment and pipeline acts as a vessel with a double objective:

- Accomplish a specific processing task (i.e., unit operation)
- Keep the chemical substances confined avoiding releases to the environment

For example, the task of a storage tank is to accumulate a certain volume of chemicals, while the task of a pump is to increase the pressure of a specific stream. For a process vessel, the task could be mixing to obtain a homogeneous chemical mixture or to ensure homogenous heat transfer. The loss of the mixing action (due to malfunction or other upsets) may imply the appearance of hazards due to heterogeneous properties such as hot spots or points with concentrations different from specifications. In the case of reactive chemicals, the heterogeneity can result in a runaway reaction. Hence there are hazards inherent to the specific task of the equipment [Gentile, 2004].

Regardless of the specific task, every equipment and pipeline has a common purpose related to avoidance of releases of chemicals. Based on this assumption a general model for the evaluation of hazards and their interactions can be developed. The general hazards analyzed by the proposed model are:

- Explosion due to continuous release of flammable chemicals
- Toxic dispersion and environmental impact due to continuous release of toxic substances

The prototype model proposed can analyze these hazards for pure chemicals, released from vessels such as storage tanks and process drums. The application to towers, heat exchangers, and pipelines is possible by modifying the basic model. For instance, heat exchangers can be modeled as two vessels; however, the hazard derived from mixing the two streams is not accounted for. Distillation towers can be modeled by assuming that the normal liquid level is the one present for the reboiler. The following aspects are not considered:

- Internal explosions
- Sudden release of chemicals (i.e., puff dispersion model)
- Domino effect
- Stability of process control related to volume intensification
- Mixtures of chemicals (unless the required mixture properties are calculated by using accepted methodologies)
- Reactivity with air or incompatible chemical contaminants
- Toxicity of combustion products
- Toxicity of reaction products due to environmental degradation
- Reaction due to mixture of incompatible chemicals
- External corrosion due to specific environments
- Corrosion under insulation

However, in the future, specific models for each type of hazard and each type of equipment can be developed by adding the required design parameters and developing the fuzzy IF-THEN rules [Gentile, 2004].

4.1 Input variables

The used fuzzy model is the Mamdami algorithm because it works with IF-THEN rules whose antecedents and consequents are based on linguistic variables defined in terms of fuzzy sets. The overall system is formed by 35 fuzzy inference systems (FIS) arranged in a hierarchical tree where the output from the lower levels are used as inputs for the lower levels. The user is required to provide 25 input values for the chemical substance, operating conditions, and vessel design. Other 11 parameters are required for the design of adaptive membership functions for the evaluation of dispersion hazard, corrosion potential, and vessel operating conditions. The list of required inputs is reported in tables 1 and 2 [Gentile, 2004].

Table 1: list of required input parameters (linguistic variables)

HUMAN TOXICITY	UNITS
ACUTE ORAL TOXICITY	MG/KG
ACUTE DERMAL TOXICITY	MG/KG
ACUTE RESPIRATORY TOXICITY (VAPOR)	PPM
ACUTE RESPIRATORY TOXICITY (GAS)	MG/L
ACUTE RESPIRATORY TOXICITY (DUST/MIST)	MG/L
HUMAN CANCER EVIDENCE	%
ANIMAL CANCER EVIDENCE	%

Table 1 (Continuation): list of required input parameters (linguistic variables)

ENVIRONMENTAL IMPACT	UNITS
CHEMICAL WATER TOXICITY	LD_{50}
HALF-TIME CHEMICAL LIFE	DAYS
BIOACCUMULATION FACTOR	-
TROPOSPHERE HALF-TIME CHEMICAL LIFE	DAYS
DATA QUALITY: TROPOSPHERE HALF-TIME	%
FIRE AND EXPLOSION	**UNITS**
NORMAL BOILING TEMPERATURE	°C
FLASH TEMPERATURE	°C
MAXIMUM POTENTIAL DENSITY	W/ML
WATER HEAT OF MIXING	CAL/GR.
UNIT AVERAGE OBSTRUCTION FRACTION	%
UNIT AVERAGE CONGESTION FRACTION	%
FLAME BURNING VELOCITY	CM/S
DISPERSION	**UNITS**
VESSEL OPERATION TEMPERATURE	°C
VESSEL OPERATION PRESSURE	°C
BOILING TEMP. AT VESSEL CONDITIONS	°C
DESIGN	**UNITS**
VOLUME OF VESSEL	GAL
NOZZLE DIAMETER	IN
NOZZLE LEVEL	%

Table 2: list of required input parameters for adaptive membership design

DISPERSION	UNITS
NORMAL BOILING TEMPERATURE	°C
FLASH TEMPERATURE	°C
ATMOSPHERIC TEMPERATURE	°C
CORROSION	**UNITS**
TEMP. FOR EXCELLENT RESISTANCE (METAL)	°C
TEMP. FOR GOOD RESISTANCE (METAL)	°C
TEMP. FOR SATISFACTORY RES. (METAL)	°C
TEMP. FOR UNSATISFACTORY RES. (METAL)	°C
TEMP. FOR UNSATISFACTORY RES. (PLASTIC)	°C
NOZZLES	**UNITS**
MAXIMUM OPERATION LEVEL	%
NORMAL OPERATION LEVEL	%
LOW NORMAL OPERATION LEVEL	%
MINIMUM OPERATION LEVEL	%
DRAIN LEVEL	%

The linguistic variables are combined by IF-THEN rules that are not modified by weights; therefore it is implicitly assumed that all the linguistic variables (i.e., inputs) have the same importance. In some cases, synergetic effects among input variables have been assumed, and the rule set takes care of it. The logic operators (i.e., AND, OR) are based on the standard max and min operators. The choice of the operators for intersection and union (minimum (min) for intersection and maximum (max) for union) is not unique. The operators selected here (min and max) are the classical operators in fuzzy logic and they are analogous to the logical operators AND (Boolean conjunction) and OR (Boolean disjunction). In the case of the classical fuzzy intersection or min operator, the lowest degree of membership involved in the intersection dictates the result of the operation [Gentile, 2004].

It is assumed that each piece of equipment contributes an inherent degree of hazard due to the interaction and combination of factors (e.g., chemical hazard, operating conditions, and mechanical characteristics). The combination of all these contributions should be used, instead of only the worst hazards, to identify phenomena such as hazard migration. Chemicals, equipment, and operating conditions can be hazardous by themselves; however the hazards inherent in a chemical plant are derived from the interaction of hazardous factors [Gentile, 2004].

4.2 Description of the basic hierarchical model for vessel i in unit j

This section presents an overview of the model and examples of the rules used. Further details are provided by Gentile (2004).

The basic event taken into account by the model is the release of chemical substances and the possible consequences in terms of fire and explosion, toxic effects on humans and the environment as well as long-term effects on the atmosphere. Problems associated to the loss of production due to process upsets that reduce the quality of the final product are not considered. The model takes into account the interaction of several parameters, by using 35 sets of IF-THEN rules arranged in a hierarchical tree-like structure that describes the potential hazard due to combinations of specific conditions such as chemical properties, operating conditions, and equipment design parameters. Figure 3 presents the top of the tree where the mechanical and chemical hazards are combined [Gentile, 2004].

The first layer of the tree (i.e., Layer 1 in Figure 3) describes the inherent safety level (ISL) as a fuzzy index ($FISI_{ij}$) of the equipment i located in unit j as a function inversely proportional to the amount of hazard inherent to the chemical properties of the substances (which are also affected by specific operating conditions) and the characteristics of the design of the equipment including volume. The description of the interaction between the two main sources of hazards is obtained by the first set of IF-THEN rules of the form:

IF (“chemical hazard” is ____) AND (“mechanical hazard” is ____) THEN (ISL is ____)

This rule expresses the principles of “intensification”, “moderation”, and “substitution”, by indicating that “chemical hazard” can be reduced either by selecting a less hazardous chemical and/or less hazardous processing conditions (evaluated in Layer 2.1) while the potential consequences of “mechanical hazard” can be reduced by using smaller volumes and/or more benign operating conditions (evaluated in Layer 2.2) as shown in Figure 3. However, in order to assign each a high degree of inherent safety (i.e., low inherent hazard, $FISI_{ij}$ <0.5) both conditions, “chemical hazard” and “mechanical hazard”, must be low. The outputs from Layer 2.1 and Layer 2.2 are used as the inputs for Layer 1, and they are calculated by evaluating respectively the fuzzy inference systems for “chemical and design hazards” (ISICHEM), and “mechanical and design hazards” (ISIMECH) [Gentile, 2004].

The combination of hazards posed by the chemical substances present in the equipment i being analyzed is evaluated by the FIS called “Hazard due to chemical and design factors” (ISICHEM) whose IF-THEN rules combine the results of the inference systems that evaluate toxic chemical hazard (for humans and environmental) and hazards due to flammability and reactivity behavior. The IF-THEN rules evaluated for ISICHEM have the following general structure:

IF (“fire/explosion/reactivity hazard” is ____) AND (“toxicity/environmental impact” is ____) THEN (ISL is ____)

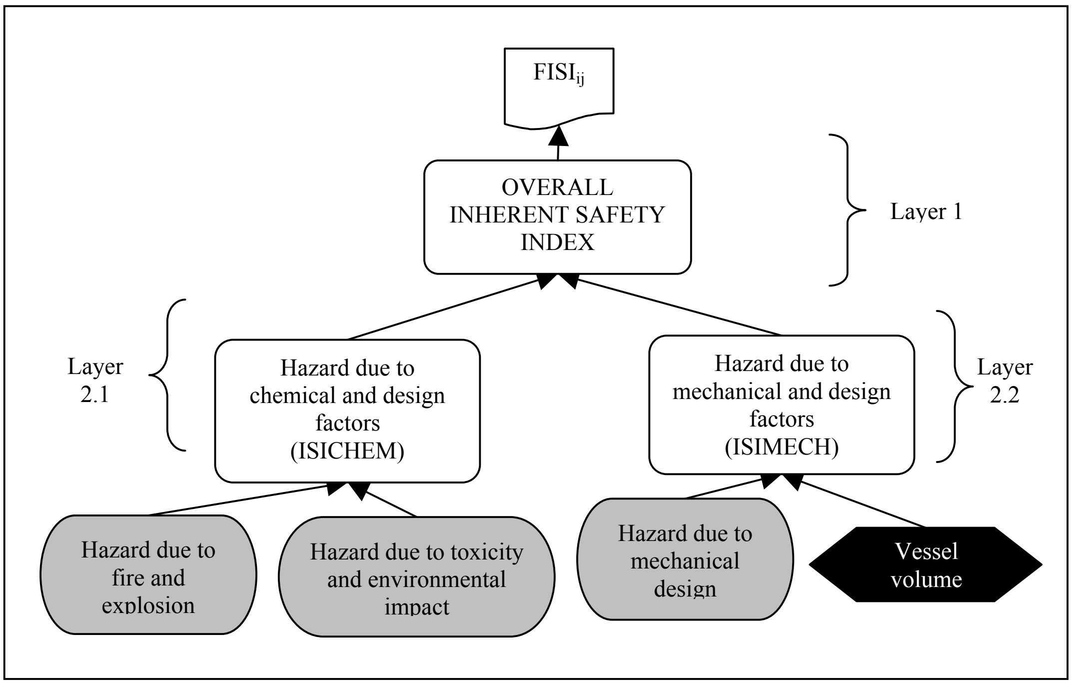

Figure 3: Hierarchical tree for Layer 1 and Layers 2.1 and 2.2 [Gentile, 2004]

The objective of this set of rules is the identification of conflicts between process safety requirements and environmental requirements. In order to be considered inherently safer a chemical must show low toxicity, be environmental friendly, and have low flammability and reactivity. If any of these properties is high then the inherent hazard posed by the substance in equipment i will increase. It is important to clarify that design factors, such as operating conditions, are able to modify the inherent hazard due to chemical properties of the substances; however, this is taken into account by the next layer as explained below. The inherent safety principle evaluated is “substitution” [Gentile, 2004].

As shown in Figure 3, the hazards due to the interaction of mechanical and design factors is evaluated by the FIS called ISIMECH which describes principles such as "minimization", "moderation" and "simplification". The general objective of this set of rules is to capture the possibility of release occurrence due to vessel failure caused by internal corrosion, or chemical release due to failure of vessel connections such as nozzles and other penetrations of the wall of the tank. The set of IF-THEN rules evaluated for ISIMECH has the following general form:

IF ("hazard due to mechanical design" is ___) AND ("volume" is ___) THEN (ISL is ___)

An important factor used as input for this FIS is the volume of the vessel. For this FIS the effect of the volume plays a double role since it affects the amount of chemical substance contained, but also is an indication of the area of plastic or metal surface exposed to the chemical and subject to corrosion or other forms of mechanical failure. If the potential for failure is high but volume is small, then the overall hazard obtained by the interaction of the two factors is reduced [Gentile, 2004].

By including the variable "volume" at this point it is possible to capture the importance of this variable for inherent safety, as recognized by several authors and also often misunderstood, when volume reduction is seen as the sole approach for reaching an inherently safer design. The value of volume has the power to minimize or magnify the hazard posed by chemical properties, operating conditions, or mechanical design. If the potential for mechanical failure is low but the volume is large then the overall hazard due to the interaction is high but must be combined with the chemical hazard; if chemical hazard is low then the overall hazard will be low to giving then a high degree of inherent safety, but if the chemical substance presents a high degree of hazard (which is obtained by combining chemical properties and operating conditions) then the overall hazard level will be higher yielding a lower inherent safety level [Gentile, 2004].

The inherent chemical hazard due to toxicity combines two factors, hazards due to human toxicity and due to environmental impact, with the dispersion potential in case of release. The hierarchical tree is shown in Figure 4. The fuzzy inference system called "Hazard due to toxicity, environmental impact, and potential dispersion" (AGCHM) is formed by a set of IF-THEN rules of the type:

IF ("human/environmental chemical hazard" is ____) AND
("hazard due to toxic dispersion" is ____) THEN (ISL is ____)

The rules evaluate the interaction between the toxicity potential with the possibility of releasing the substance in a physical form capable of dispersing into the environment. The analyzed inherent safety principles are "substitution" and "moderation". If the chemical is not toxic or the operating conditions are able to reduce the dispersion potential, then the hazard posed by the vessel is reduced. However, if the chemical is toxic for humans and/or the environment and is managed at conditions such as high pressure and/or high temperature, then the potential for releasing large quantities able to vaporize and disperse increases, reducing the inherent safety level of the equipment (expressed as high hazard level).

The “hazard due to toxic dispersion” (DISPTX) requires inputs from the user in order to evaluate the rules but also to define the parameters of the membership functions, which for this fuzzy inference system are adaptive. The information required for the design of the membership functions, as shown in Figure 4, is:

- Normal boiling temperature
- Boiling temperature at vessel pressure
- Atmospheric temperature

The input parameters for the FIS are:

- Operation temperature of the vessel
- Operating pressure of the vessel

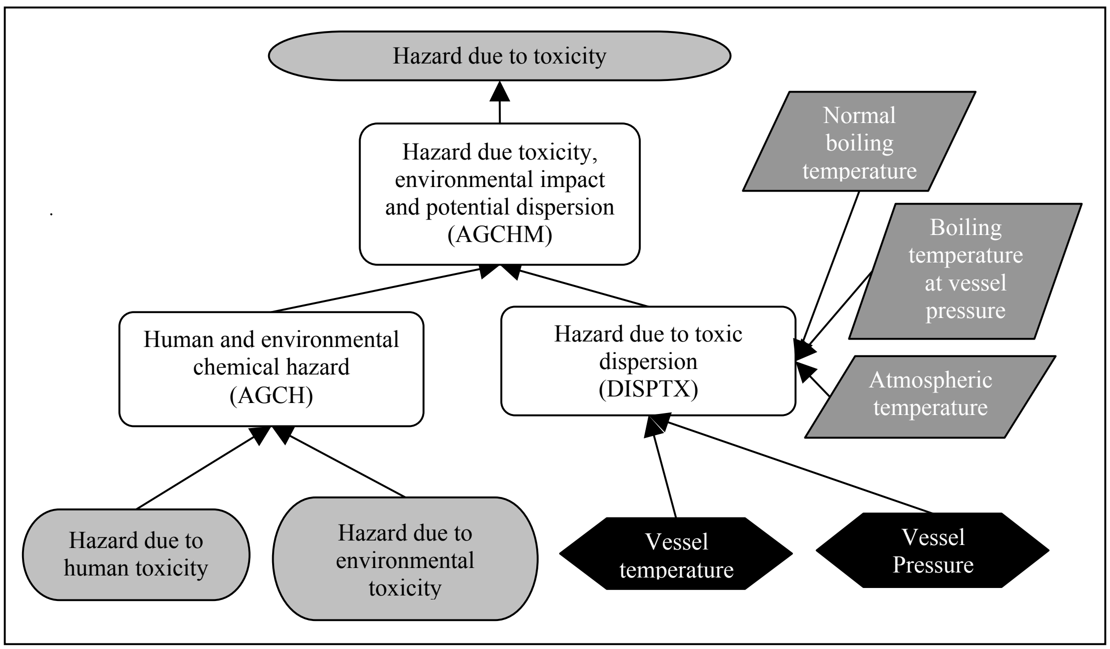

Figure 4: Hierarchical tree for the evaluation of hazards due to chemical properties [Gentile, 2004].

The values for these inputs can be provided as crisp numbers (e.g., operation temperature = 45 °C and pressure = 4 atm) or they can be given as fuzzy numbers representing the expected variation in the vessel temperature and pressure (e.g., maximum operation temperature = 55 °C, normal operation temperature = 45 °C, minimum operation temperature = 35 °C). The use of a range of temperature and pressure increases the uncertainty of the analysis, (i.e., more rules are fired) but increases the flexibility of the methodology because rather than exploring one single operation point, the whole region where the equipment is likely to operate is analyzed [Gentile, 2004].

The objective of the IF-THEN rules for this FIS is the detection of operating points near the saturation curves. In this region, when the chemicals are released in the liquid phase (e.g., operating temperature lower than saturation temperature at the vessel pressure) the released mass flow is higher compared to a vapor release (e.g., operating temperature higher than saturation temperature at the vessel pressure). However, if the released chemical is in the liquid phase and the vessel operates at a temperature higher than the normal boiling point, then the liquid will totally or partially vaporize producing a vapor cloud that will be dispersed. If the pressure of the vessel is higher than the atmospheric pressure, then the released flow rate increases but also increases the possibility of aerosol formation that increases the evaporation rate [Gentile, 2004]. The fuzzy IF-THEN rules used for DISPTX have the following general form:

IF (“vessel temperature” is ____) AND (“vessel temperature” is ____) AND (“vessel pressure” is ____) THEN (ISL is ____)

The input “vessel temperature” is used by two linguistic variables and the logic behind this requirement is explained in Chapter VII. The traditional approach for dispersion modeling requires weather and wind parameters (e.g., atmospheric stability, wind velocity) however in this case it is assumed that in order to be dispersed a chemical has to be released. If the mass of the released chemical is small then the hazard is reduced regardless of weather conditions. However, if the released mass is large and has the potential to quickly evaporate and form a toxic cloud, then the toxic hazard will be large. A similar approach is followed by Carrithers et al. (2003) to demonstrate the effect of phase type on the total mass of released chlorine from a pipeline of liquid chlorine and another of gas chlorine. The weather and wind parameters change the shape (e.g., length, width, height) of the cloud in predictable ways and, and unless the wind is strong enough to quickly dilute the cloud, the dispersion hazard remains. The rest of the system is described by Gentile (2004).

5. Case study

The case selected as example for this methodology is one unit of the process of hydrodealkylation of toluene for the production of benzene. This information used is reported by Turton et al. (1998). Only the storage tank TK-101 is analyzed here. Additional examples and results are presented by Gentile (2004). Figure 5 shows the location of the vessel and Figure 6 reports some of the parameters used.

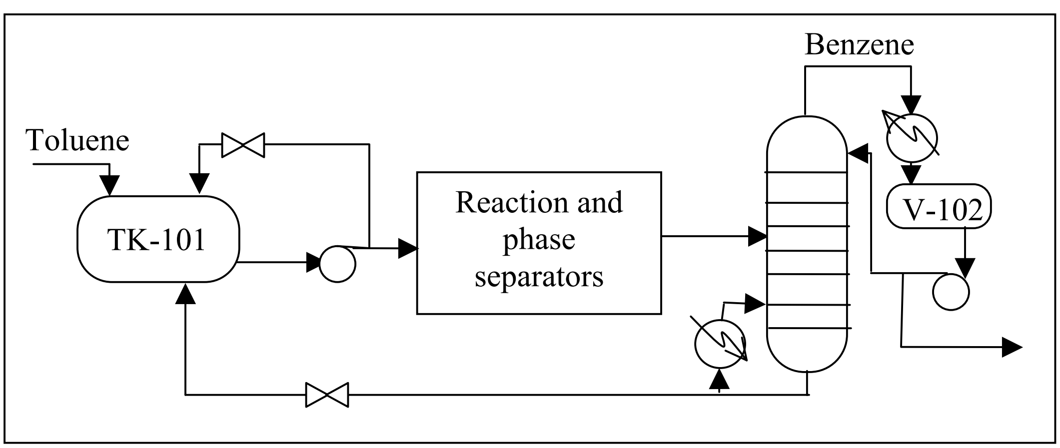

Figure 5: Diagram of the hydrodealkylation unit

Additional information for the vessel TK-101 is the following:

- Operation temperature: 59 °C
- Operation Pressure: 2.0 atm
- Operation levels: normal high = 60%, normal = 50%, normal low = 40%
- Material of construction: carbon steel
- Volume = 4,426 gal
- Unit where it is located is assumed to be obstructed 90% on three sides, while one is 50% obstructed and the other is totally open. Therefore the fraction of confinement is 84%. It is assumed that the overall volume blockage fraction (i.e., volume of equipment/volume of unit) is around 60%.
- Carbon steel has an excellent corrosion resistance for toluene up to 350 °F
- The wall penetrations for instrumentation and sampling are not taken into consideration.

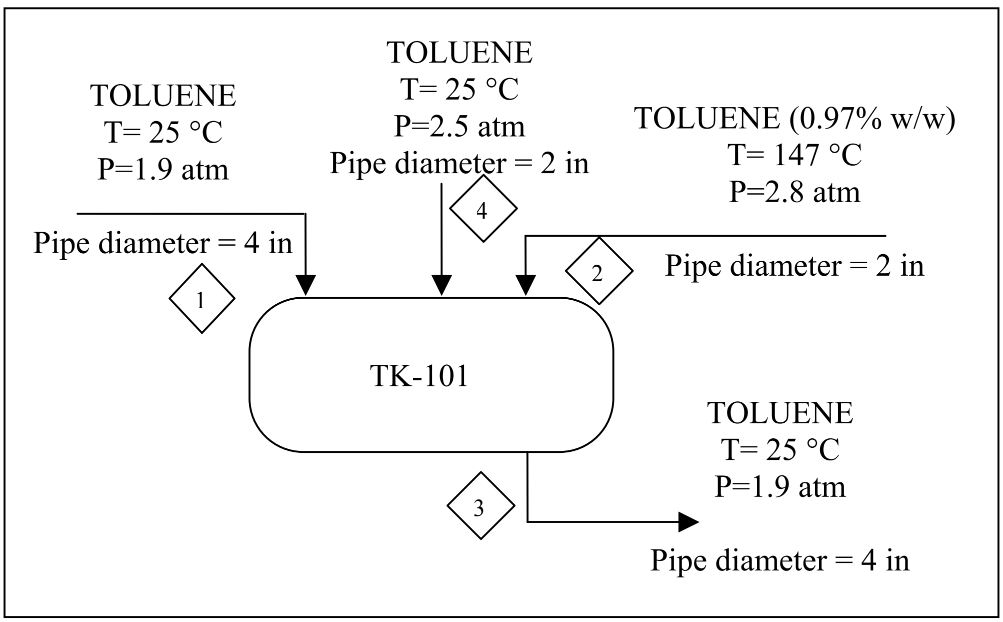

Figure 6: Diagram of the storage tank TK-101

Storage tank TK-101 is assumed to be equipment 2 of unit 1 therefore its overall fuzzy hazard index is $FISI_{12}$. If more equipment and pipelines were evaluated they would be equipment i of unit 1, where i = 0…n. Therefore, in order to obtain the overall index for unit j = 1, all the $FISI_{ij}$ should be added by using fuzzy addition [Gentile, 2004].

The storage tank TK-101 works at relatively reduced hazardous conditions since the operating temperature is not close to the normal boiling temperature. However, the pressure is relatively high and it is assumed that in case of failure of a pressure regulator on line 2, it can be pressurized. For Case 2, TK-101 is reevaluated by reducing the overall fraction of confinement but the operating pressure is not changed. For Case 3, TK-101 is evaluated with low operating pressure and low degree of confinement.

The obtained results are plotted indicating the possible range of variability of the hazard degree and the value that is given by defuzzification and therefore is the crisp solution. The plots have been developed according to the advice given by Kletz (2003). The figures show the values of $FISI_{12}$ and the two overall evaluations for the chemical hazard (ISICHEM) and the mechanical hazard (ISIMECH). The vertical axis of the plot represents the scale of hazard, which is on the real interval [0 1] and the value of 0.5 indicates the threshold between conditions that represent relevant hazards and therefore cannot be considered inherently safer. Values lower than 0.5 represent conditions associated with low hazard degrees that should not require complex layers of protection to control them and therefore are assumed to be conditions within the "inherently safer" region. The lower part of the figures presents arrows that show which indices are aggregated to obtain the index indicated by the arrow.

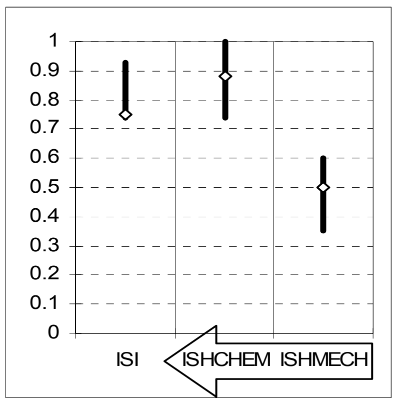

Figure 6: Main overall hazard indices for storage tank TK-101, Case 1.

From Figure 6 it is possible to detect that the major hazard contribution to the overall hazard for the storage tank TK-101, Case 1, is given by the overall chemical hazard (i.e., ISICHEM) while the mechanical contribution is not important (i.e., ISIMECH). For Case 2, the degree of obstruction and confinement are reduced to 20% in order to analyze the potential hazard reduction effects due to a less congested unit design. The overall hazard index $FISI_{12}$ is lowered due to the reduction of the chemical hazard while, as expected, the mechanical hazard does not change. The hazard due to dispersion does not change because it depends only on the operating conditions, but the overall explosion hazard AGEXPL is reduced because of the reduction of the congestion degree. Figure 7 show the new indices [Gentile, 2004].

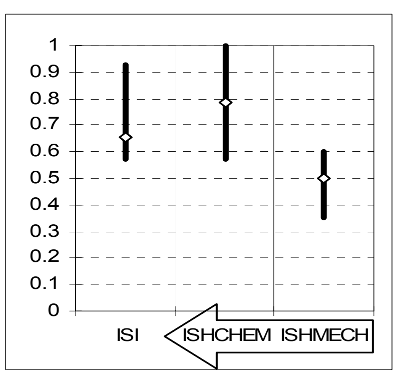

Figure 7: Main overall hazard indices for storage tank TK-101 for Case 2.

For Case 3 the operation pressure is reduced to atmospheric and the degree of congestion is low, as in Case 2. The overall hazard indices are reduced and are located around the inherent safety threshold by the combined effect of operating pressure reduction and lower congestion. The hazard due to the chemical properties cannot be removed by design, unless the chemicals are substituted. Figure 8 shows the indices for Case 3 [Gentile, 2004].

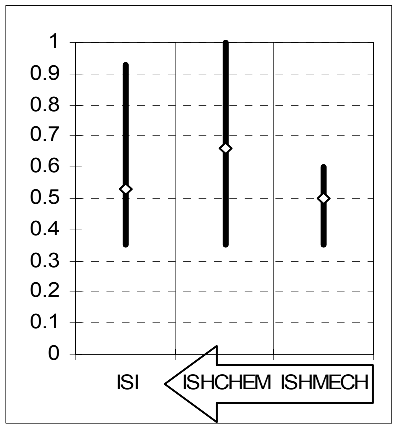

Figure 8: Main overall hazard indices for storage tank TK-101 for Case 3

6. Conclusions

The results presented for the case study show how the model is applied and its sensitivity to design changes. The results are encouraging and show the potential modeling power of the proposed hierarchical fuzzy-based approach. However, this research represents only the first step, and due to underlying complexity can be expanded and improved. As future work, it is suggested to revise the fuzzy inference systems in order to incorporate more linguistic variables and improve the modeling capacity of the system. The designed inference system should be revised by experts and optimized according to their assessments; additionally, the system should be tested on real cases and tuned when discrepancies with reality are found. The model proposed here is mainly for vessels and must be adapted to other equipment such as pumps, pipes, towers, and reactors [Gentile, 2004].

Future work is required in order to expand the model including other factors, as explained previously, and to adapt the basic model for vessels to other equipment. Because the software relies on information that is available in equipment datasheets it will be useful to develop a Visual Basic version able to run in Excel and facilitate the application during the plant design stage. On the other hand, by linking the proposed methodology to process simulation and cost estimation, it will be possible to create a powerful engineering tool able to evaluate processing units or plants from often conflicting criteria such as technical requirements, cost limitations, environmental, and safety aspects [Gentile, 2004].

7. References

Almond R., 1995, Discussion: fuzzy logic: better science? Or better engineering?, *Technometrics*, 37(3): 267-270.

Berkan R. C. and Trubatch S.L., 1997, *Fuzzy Ssystems Design Principles: Building Fuzzy IF-THEN Rule Bases* (Wiley-IEEE Press, New York, NY, USA).

Brown M, 1999, Editorial: the case for safety, *Trans. IchemE, Pt. B., Process Safety and Environmental Progress,* 77: 107-108

Carrithers G.W. Hendershot D.C., and Dowell A.M. and 2003, It's never too late for inherent safety.
Available at: http://home.att.net/~d.c.hendershot/papers/vev2late/inhersaf.htm.

El-Halwagi, M. M., 1997, *Pollution Prevention through Process Integration: Systematic Design Tools* (Academic Press, San Diego, CA, USA).

Gentile M., Williams J.R., Mannan S., "Development of an Inherent Safety Index Based on Fuzzy Logic", *Proceedings Process Safety Symposium 2001*, Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, TX, USA.

Gentile M., Williams J.R., Mannan S., 2003, Development of a fuzzy logic-based Inherent Safety Index, *Trans IChemE, Part B, Process Safety and Environmental protection* Vol. 81, Part B. Copyright 2003.

Gentile M., 2004, "Development of a Hierarchical Fuzzy Model for the Evaluation of Inherent Safety", Ph.D. Dissertation, Texas A&M University, College Station, TX, USA.

Available at: http://psc.tamu.edu/publications/thesis/Michela_dessertationS.pdf

Jang J.-S. R., Sun C.-T. and Mizutani E., 1997, *Neuro-Fuzzy and Soft Computing, a Computational Approach to Learning and Machine Intelligence*, Matlab Curriculum Series (Prentice Hall, Upper Saddle River, NJ, USA).

Kletz, T.A., 1996, Inherently safer design: the growth of an idea, *Process Safety Progress*, 15(1): 5-8.

Kletz, T.A., 1998, *Process Plants: A Handbook for Inherently Safer Design* (Taylor and Francis, Philadelphia, PA, USA).

Kletz T.A., 1999, The origins and history of loss prevention, *Trans. IchemE, Pt. B., Process Safety and Environmental Progress,* 77: 109-116.

Kletz T.A., 2003, Personal communication, Loughborough University, Leicestershire, UK.

Klir G.J. and Yuan B., 1995, *Fuzzy Sets and Fuzzy Logic, Theory and Applications* (Prentice Hall, Upper Saddle River, NJ, USA).

Koller G., Fisher U. and Hungerbuhler K., 2001, Comparison of methods suitable for assessing the hazard potential of chemical processes during early design phases *Trans. IchemE, Pt. B., Process Safety and Environmental Progress,* 79: 157-166.

Lee M.L., Chung H.Y. and Yu F.M., 2003, Modeling of hierarchical fuzzy systems, *Fuzzy Sets and Systems*, 138: 343-361.

Lees F.P., 1996, *Loss Prevention in the Process Industries, Hazard Identification, Assesment and Control*, Vols. 1 and 2, 2nd edition, (Butterworth, Heinemann, Oxford, UK).

Lootsma F.A., 1997, *Fuzzy Logic for Planning and Decision-Making* (Kluwer Academic, Boston, MA, USA).

Mansfield D., 2001, The INSIDE project – Inherent SHE in Design,

Available at: http://www.aeat-safety-and-risk.com/html/inset.html INSET 2001

Runkler T.A., 1997, Selection of appropriate defuzzification methods using application specific properties, *Fuzzy Systems, IEEE Transactions,* 5(1): 72-79.

Sikdar S. and El-Halwagi M. M., 2001, *Process Design Tools for the Environment* (Taylor and Francis, New York, NY, USA).

Tanaka K., 1996, *An Introduction to Fuzzy Logic for Practical Applications* (Springer, New York, NY, USA).

Tixier J., Dusserre G., Salvi O. and Gaston D., 2002, Review of 62 risk analysis methodologies of industrial plants, *Journal of Loss Prevention in the Process Industry*, 15: 291-303.

Turton R., Bailie R.C., Whiting W.B. and Shaeiwitz J.A., 1998, *Analysis, Synthesis, and Design of Chemical Processes* (Prentice Hall International, Upper Saddle River, NJ, USA).

Yen J. and Langari R., 1999, *Fuzzy Logic: Intelligence, Control and Information* (Prentice Hall, Upper Saddle River, NJ, USA)

Zadeh L.,1996, Fuzzy logic = computing with words, *Fuzzy Systems, IEEE Transactions,* 4(2):103-111.

Zimmermann, H.-J, 1996, *Fuzzy Set Theory and its Applications*, 2^{nd} edition (Kluwer Academic Publishing, Boston, MA, USA).