Journal of Hazardous Materials 173 (2010) 258–264

Contents lists available at ScienceDirect

Journal of Hazardous Materials

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

Security risk assessment: Applying the concepts of fuzzy logic

Shailendra Bajpai[a,*], Anish Sachdeva[b], J.P. Gupta[c,d]

[a] Department of Chemical Engineering, National Institute of Technology, Jalandhar, India
[b] Department of Industrial Engineering, National Institute of Technology, Jalandhar, India
[c] Rajiv Gandhi Institute of Petroleum Technology, Noida, India
[d] Indian Institute of Technology, Kanpur, India

ARTICLE INFO

Article history:
Received 7 May 2009
Received in revised form 17 August 2009
Accepted 18 August 2009
Available online 25 August 2009

Keywords:
Terrorism
Security
Chemical facility
Risk assessment
Security Risk Factor Table
Fuzzy logic

ABSTRACT

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 an earlier work, it has been shown that security risk assessment can be done by conducting threat and vulnerability analysis or by developing Security Risk Factor Table (SRFT). HAZOP type vulnerability assessment sheets can be developed that are scenario based. In SRFT model, important security risk bearing factors such as location, ownership, visibility, inventory, etc., have been used. In this paper, the earlier developed SRFT model has been modified using the concepts of fuzzy logic. In the modified SRFT model, two linguistic fuzzy scales (three-point and four-point) are devised based on trapezoidal fuzzy numbers. Human subjectivity of different experts associated with previous SRFT model is tackled by mapping their scores to the newly devised fuzzy scale. Finally, the fuzzy score thus obtained is defuzzyfied to get the results. A test case of a refinery is used to explain the method and compared with the earlier work.

1. Introduction

1.1. A new risk paradigm

Prior to September 11, 2001 (the day terrorists struck World Trade Centre in New York), the risk assessment of chemical process industries (CPI) handling hazardous chemicals (Hazchems) was focussed on the analysis of risk related to technological accidents and natural calamities (unintentional acts). Deliberate acts by terrorists or disgruntled employees, etc., were not included in the formal risk assessment. The events of 9/11 have changed the scene dramatically [1,2].

Chemical plants such as oil refineries, fertiliser plants, etc., store and transport bulk of the Hazchems, operate processes under extreme conditions of temperature and pressure, with fast material flows and complex kinetics. Therefore, terrorists having sufficient knowledge of the chemical operations and layout of the plant may exploit extreme operating conditions, which may then lead to toxic release, fire and/or explosion further resulting in mass casualties, property damage, and economic and environmental impacts [3].

Therefore, the risks originating from deliberate acts are now considered both real and credible and must be examined to determine if the existing security measures are adequate or need enhancement. Security enhancements may be required, especially for the chemical sites that pose attractive targets due to their strategic location, closeness to the population centre, economic importance, etc. It is imperative to have comprehensive security risk management programme including effective security risk assessment techniques, implementing appropriate security countermeasures and managing emergency.

Unconventional approach is essential for dealing with intentional acts. Idea is to provide an element of surprise to the adversaries, prior to or during attacks. For example, change the protocol of storing Hazchems in storage tanks, or vary the routine being followed at the facility. Appropriate security countermeasures in place will help in hardening the target against attacks for adversaries. Limiting the consequences in case of successful terrorist attacks is a challenging task. In fact, all conventional existing safety and security measures (that are in place from years in CPI) will still work for intentional acts as well, but many of these need to be significantly modified and supplemented by new ones [2,3].

1.2. Overview of terrorism and some security incidents

Terrorism is defined as, “the unlawful use of force or violence against persons or property to intimidate or coerce a government,

* Corresponding author. Tel.: +91 181 2690301/2690036; fax: +91 181 2690932.
E-mail addresses: bajpais@nitj.ac.in (S. Bajpai), sachdevaa@nitj.ac.in (A. Sachdeva), jpg@iitk.ac.in (J.P. Gupta).

0304-3894/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2009.08.078

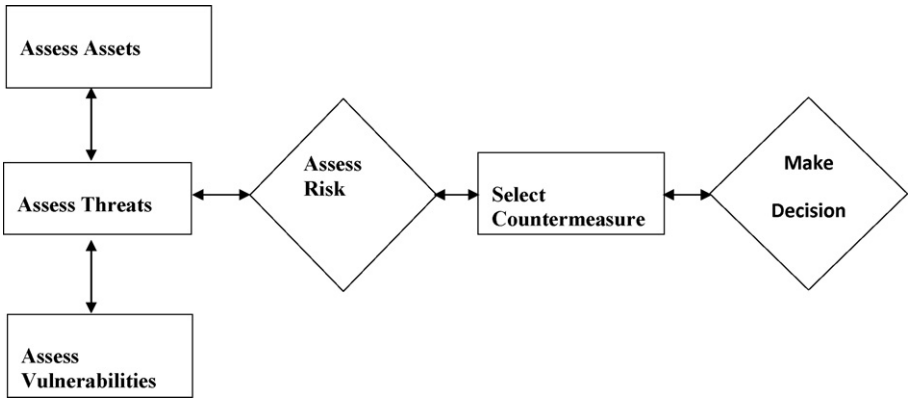

Fig. 1. Security risk management process [8].

the civilian population, or any segment thereof, in furtherance of political or social objectives [4]." It has become abundantly clear that various organizations and individuals are determined to use new means and forces to cause maximum damage and harm to governments, businesses, the environment, and the public.

There have been several terrorist activities directed towards the CPI or their transportation systems thus far. Some of them are briefly discussed below:

- In 1997, four Ku Klux Klan members plotted to place an improvised explosive device on a hydrogen sulfide tank at refinery near Dallas, USA as a diversion for an armored car robbery on the other side of the town [5].
- Anhydrous ammonia is a key ingredient in the illegal production of methamphetamine drugs. There have been numerous incidents worldwide where thieves, looking for ammonia for manufacturing illegal drugs, have broken into refrigerated warehouses, or ice manufacturing facilities, frequently leaving valves open. In some cases, the thieves have been overcome by the ammonia and needed to be rescued; in other cases, the community has been evacuated, and there have been injuries to the general public and to law enforcement personnel from exposures to the released ammonia [6].
- In 2001, the Trans Alaska pipeline in USA was closed for three days after it was hit by a bullet in the event described as drunken mischief. Over 6000 barrel of oil was released [7].
- A cyber attack on a computerized waste-treatment system in Queensland, Australia, sent millions of gallons of raw sewage spilling into local parks and rivers. A 49-year old man, who worked for the supplier that installed the sewage system, angry over a job application rejection by the city, was found guilty of attacking the computerized system 46 times, and sent to prison for two years [5].

It is important to mention here that several other incidents have happened worldwide, however no major successful terrorist attack has happened in CPI thus far.

2. Security risk management

Security risk management programme requires a systematic approach to analyze security risks [8]. The process involves identifying critical assets to be protected, identifying credible threats from various adversaries, assessing vulnerabilities and risks, and evaluating the adequacy of countermeasures (Fig. 1). The analytical part of this process is called security vulnerability assessment (SVA). SVAs are not necessarily a quantitative risk assessment, but are usually performed qualitatively using the best judgement of the SVA Team. The expected outcome is a qualitative determination of risk to provide a sound basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures. Different organizations have developed their own SVAs that are best suited for them [4,9,10].

Differences in geographic location, type of operations, and on-site quantities of Hazchems all play an important role in determining the approach taken for SVA. Independent of the SVA method used, all techniques include the following activities [4,9]:

- Asset characterization: Characterize the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure.
- Threat assessment: Identify and characterize threats against assets and evaluate the assets in terms of attractiveness of the targets to each adversary and the consequences if they are damaged or stolen.
- Vulnerability assessment: Identify potential security vulnerabilities that threaten the asset's service.
- Assessment of security risks: Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur. Rank the risk of the event occurring and, if high risk, make recommendations for lowering the risk.
- Recommendations: Identify and evaluate risk mitigation options (both net risk reduction and cost/benefit analyses) and re-assess risk to ensure adequate countermeasures are being applied.

The present work focuses on risk assessment part. In the earlier work [2,3], it has been shown that security risk assessment can be done by conducting threat and vulnerability analysis or by developing Security Risk Factor Table (SRFT). HAZOP type vulnerability assessment sheets can be developed that are scenario based. In the SRFT model, important security risk bearing factors such as location, visibility, inventory, etc. (Table 1), have been used. In this paper, the fuzzy logic approach has been incorporated in the SRFT model. The modified SRFT will reduce the human subjectivity associated with the previous SRFT. In the modified SRFT model, each risk factor is given fuzzy scores (in place of actual scores) in two linguistic scales (three-point and four-point scale) in the range of 0–5. Finally, the total score obtained is defuzzyfied to determine the security risk status of a given facility. The brief overview of fuzzy set theory is presented in Section 3:

3. Fuzzy set theory

In safety and security decision making situations, high degree of uncertainty is involved in the available data set. It is difficult to

Table 1
Security Risk Factor Table [2,26].

Risk factors	Range of security points				Actual points
Location	Rural (1)	Urban (2,3,4)		High density (5)	1
Visibility	Not visible (0)	Low (1,2)	Medium (3,4)	High (5)	1
Inventory	Low (1)	Medium (2)	Large (3,4)	Very large (5)	5
Ownership	Private (1)	Public/co-operative(2,3)		Government(4,5)	5
Presence of chemicals which can be used as precursors for WMD	Absence (0)			Presence (5)	0
Worst case impact on-site	Negligible (0)	Low (1)	Moderate(2,3,4)	Severe (5)	5
Worst case impact off-site	Negligible (0)	Low (1)	Moderate(2,3,4)	Severe (5)	3
History of security incidents	Nil (0)	Few (1,2,3)		Frequent (4,5)	3
Presence of terrorist groups in region	Absence (0)	Few (1,2,3)		Large no. (4,5)	3
Existing security measures	High level	Ordinary		Poor/none	
• Access control	1	2,3		4,5	2
• Perimeter protection	1	2,3		4,5	2
• Mitigation potential	1	2,3		4,5	2
• Proper lighting (all over)	1	2,3		4,5	3
• Use of metal detector/X-ray/CCTV (at entrance and at all critical locations)	1	2,3		4,5	3
Personal preparedness and training	Well prepared(1)	Average (2,3)		Poor (4,5)	2
				Total score	40

obtain the quantitative data due to numerous constraints such as rare occurrence of the events, human subjectivity and economic considerations. Even if the data is available, it is often inaccurate or subject to uncertainty. Thus, it is difficult to establish rational database for safety and security considerations. Fuzzy set theory can provide a framework for handling such subjectivity and uncertainty associated with the data. Zadeh [11] initiated the fuzzy set theory. Bellman and Zadeh [12] presented some applications of fuzzy theories to the various decision making processes of fuzzy environment. Fuzzy logic has been applied to solve many real world problems where fuzziness exists. The potential of using fuzzy sets theory in treating different sources of uncertainty has been acknowledged in the literature [13–15]. Several authors make use of fuzzy set theory to tackle uncertainties in risk and security decision making. Pelaez and Bowles [16], Bowles and Pelaez [17], Cai [18], Moss and Woodhouse [19], Braglia et al. [20], and Sharma et al. [21] suggested the use of fuzzy logic theory for the risk criticality analysis and risk priority number (RPN) evaluation. The basic fuzzy concepts are outlined briefly in later section.

3.1. Fuzzy Concepts

3.1.1. Fuzzy sets

Crisp (classical) sets contain objects that satisfy precise properties of membership functions. Only two possibilities whether an element belongs to, or does not belong to a set exist. A crisp set 'A' can be represented by a characteristic function $M_A(x) = \{0, 1\}$.

$$M_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

where U: universe of discourse; X: element of U; A: crisp set, and M: characteristic function.

On the other hand fuzzy sets contain objects that satisfy imprecise properties of membership functions, i.e. membership of an object in a fuzzy set can be partial. Contrary to classical sets, fuzzy sets accommodate various degrees of membership on continuous interval [0,1], where '0' conforms to no membership and '1' conforms to full membership. Mathematically, the membership function for a fuzzy set $\tilde{A}$ is defined as:

$$\mu_{\tilde{A}}(x) : U \rightarrow [0, 1]$$

where $\mu_{\tilde{A}}(x)$: degree of membership of element x in fuzzy set $\tilde{A}$.

3.1.2. Membership functions

Various types of membership functions (MF) such as triangular, trapezoidal, gamma and rectangular can be used for analysis. A fuzzy number is a convex fuzzy set, characterized by a given interval of real numbers, each with a grade of membership between 0 and 1. However, triangular membership functions and trapezoidal membership functions (TFN) are widely used for calculating and interpreting reliability data because of their simplicity and understandability [22]. Though using more complex numbers, like Gaussian ones, allows a more precise description of the problem under analysis. However, they cause greater computational complexity without giving significant advantage [23].

A trapezoidal membership function, which has been used in this study, is represented by $\tilde{A} = (a, b, c, d)$ and its membership function is defined as:

$$\mu_{\tilde{A}}(x) = \begin{cases} \dfrac{x-a}{b-a}, & a \le x \le b, \\ 1, & b \le x \le c, \\ \dfrac{d-x}{d-b}, & b \le x \le d, \\ 0, & \text{otherwise.} \end{cases}$$

The nature of data points in the modified SRFT model is best represented by the trapezoidal function. The other type of membership function, e.g., triangular fuzzy number, if used, will provide full membership value (i.e., '1') at only single point. However, in case of trapezoidal fuzzy number, the full membership value is obtained for a particular range, which is more suitable for the modified SRFT model.

3.1.3. Linguistic variables

Normally when human experts are asked to evaluate a variable, they feel more comfortable in giving the answer in words. Fuzzy logic allows formulating vague description in natural languages in precise mathematical terms. Fuzzy linguistic variables are extensions of numeric variables in the sense that they are able to represent the condition of an attribute at a given interval by taking fuzzy set as their values. The values obtained in a development of fuzzy linguistic variable are considered as fuzzy measures. These values then become the criteria for measuring attributes of objects.

A linguistic variable is characterized by (X, T, U, M) where:

X	The linguistic variable, for example, X is the fuzzy linguistic of an item.
T	The set of linguistic values that X can take, for example, T = {low, medium, high, fairly high}.
U	The actual physical domain in which the linguistic variable X takes its quantitative (crisp) values, for example, $U = [F_{\text{medium}}; F_{\text{high}}]$.
M	Semantic rule that relates each linguistic value in T with a fuzzy set in U, for example, M relates "medium" and "high" with the specific MF, i.e. X may have 'medium' with a membership value of 0.3 and 'high' with membership value of 0.7 in fuzzy set U.

3.1.4. Defuzzification

The defuzzifier is defined as a mapping from fuzzy set A' in V to a crisp point. Conceptually, the task of defuzzifier is to satisfy a point in V that best represents fuzzy set B'. For defuzzification various techniques are available in the literature [13,14], but most commonly used are Chen's ranking [24] and Yager's centroidal [25]. In the present study, the centre average defuzzifier for defuzzification is used as it gives mean value of the parameters. It is mathematically represented as: Defuzzified value $= \dfrac{\int_y \mu_{B'}(y)y\,dy}{\int_y \mu_{B'}(y)dy}$ where, B' is the output fuzzy set, and μ'_{Bi} is the membership function.

In the paper, the fuzzy scales represent the set B in V and the experts score for the various factors represents the set A in U. After obtaining the response from the experts, these are mapped onto the fuzzy scales and defuzzied value as discussed above is obtained for further analysis.

4. Modified Security Risk Factor Table

In earlier work [2,3], a Security Risk Factor Table model was developed that helps in assessing the current security risk status of a facility and can be used as a pre-screening tool before initiating detailed and time consuming SVAs. In SRFT model, important risk bearing parameters such as location, visibility, ownership, etc. (Table 1) are considered and rated on a scale from 0 to 5, with 0 being the "lowest risk" and 5 the "extreme" [26]. The rating can be done by the experts qualitatively who, based on their experience, can assign the score to a given risk parameter. The total score obtained from SRFT helps in assessing the current security risk status of the facility (Table 2). In the previous model, the experts used to give a crisp integer score to all risk parameters. The actual scores thus obtained were prone to human subjectivity involved in making the right decision. In other words, the score assigned to a risk parameter may vary from one expert to the other. Therefore, in order to reduce this subjectivity, fuzzy set theory has been used. In this paper, fuzzy scores have been assigned in place of crisp integer scores in previous SRFT model. All the risk elements of previous SRFT model are first fuzzified and later defuzzyfied to get the results. The total score thus obtained in modified SRFT, after defuzzification, will give better security risk status of a given facility.

In modified SRFT model, two linguistic scales are used, scale 1 for three ranges (Fig. 2) and scale 2 for four ranges (Fig. 3). The trapezoidal fuzzy numbers used for three-point scale were: low (0,0,1,2), medium (1,2,3,4) and high (3,4,5,5). Those for four-point scale were: low (0,0,1,2), medium (0.5,1.5,2.5,3.5), moderately high (2,3,4,5) and high (3.5,4.5,5,5). The modified SRFT is shown in Table 3. The evaluation for the actual security score for each risk parameter as given by the experts is performed as follows for the two scales mentioned above:

For scale 1 consider the risk parameter 'ownership', the expert gives the score '5' for this factor. This value suggests government ownership (i.e., high risk) with membership value of 1. The corresponding defuzzyfied value using centre average method is obtained as follows:

$$y'(\text{ownership}) = \frac{(4.5 \times 1)}{1} = 4.5$$

Similar calculations were performed for other factors of scale 1 as given in Table 3.

For scale 2 consider the risk parameter 'inventory', the expert gives the score '4.5' for this factor. This value suggests large inventory with membership value of 0.5 and very large inventory with membership value of 1 on scale 2. The corresponding defuzzyfied value using centre average method is obtained as follows:

$$y'(\text{inventory}) = \frac{(4.75 \times 1) + (3.5 \times 0.5)}{1 + 0.5} = 4.33$$

Similar calculations were performed for other factors of scale 2 as given in Table 3. It is important to mention here that if more than one expert is involved for the risk assessment, the different experts may assign a different score to a same risk parameter. In such a case, the average of different scores will be chosen as the score of expert in the modified SRFT and the remaining process will be the same as discussed above. Therefore, the modified SRFT model will work for one as well as multiple experts.

5. Test case

In this section, a refinery (X) is considered as a possible target for terrorist attacks. The modified SRFT has to be made for this refinery to know current security risk status of this facility.

5.1. Facility description

Refinery X is government owned (high risk involved in 'ownership' parameter of SRFT), involved in producing all major petroleum products in large quantities (high risk due to large 'inventory'). Crude oil comes to the refinery via pipeline and final products are sent out through pipelines as well as by road tankers and rail wagons to the marketing terminals. Important site information, vital for risk assessment, is as follows [3] (Fig. 4):

- It is situated in a remote location and the nearest city is 20 km away. There are a few small villages that surround the site and

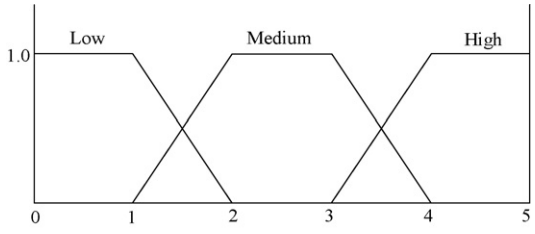

Fig. 2. Fuzzy linguistic scales (three points).

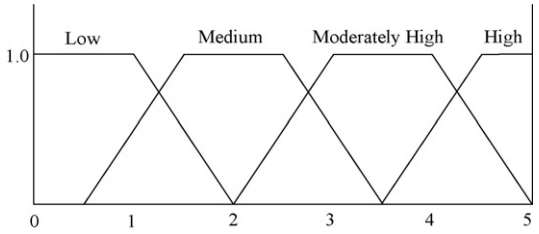

Fig. 3. Fuzzy linguistic scales (four points).

Table 2
Security risk rankings [2,26] (based on score obtained from SRFT).

Current security risk status	Actual points obtained	Recommendations
Low	<15	Maintain security awareness without excessive concern.
Moderate	16–30	Review and update existing security procedures in light of possible threats.
High	31–45	Identify risk-drivers that can be reduced with reasonable controls. Conduct threat and vulnerability analysis and work with law enforcement agencies to enhance security.
Extreme	>45	Initiate aggressive risk-reduction activity, in conjunction with consultation with law enforcement agencies. Conduct threat and vulnerability analysis.

the refinery township is 1 km away from the refinery (low risks involved due to 'location' and 'off site consequences').
- The processing area is not visible from the main highway, but the storage tanks and other taller units can be seen from some parts of the road that surround the perimeter (low risk due to 'visibility').
- It has a good safety record and is well prepared for dealing with any technical emergency (average personal preparedness and training).
- Several units of paramilitary forces are deployed for maintaining the security. The use of security equipment such as CCTV, explosive and metal detectors is limited, and access control procedures followed are average (average security measure followed).
- There have been a few unsuccessful attempts of blowing up the pipeline in the past in this region. A few cases of theft and violence have been reported in and around the facility (this suggests that there have been few security incidents and the presence of limited extremist groups in this region).

5.2. Modified SRFT for refinery X

Based on the above facts, SRFT was completed for this refinery in the earlier work [4] and the total score obtained was '40'. In the present work, previous SRFT model has been modified by assigning the fuzzy scores to all risk parameters of SRFT instead of crisp integer score. The modified SRFT using fuzzy logic has been prepared for this refinery (Table 3). The final score thus obtained, i.e. 38.08, suggests it is a high risk facility in terms of Table 2 and therefore demands serious security attention. The refinery X should go through detailed security and vulnerability assessment and initiate aggressive risk reduction exercise in coordination with the local law enforcement agencies.

It is observed that for the present test case similar results have been obtained by completing both (crisp integer score based and fuzzy score based) types of SRFT. This could be due to the fact that the defuzzyfied score has uniformly increased or decreased for some risk parameters, e.g., for the risk parameter 'ownership', the score reduced from 5 to 4.5, while for the risk parameter 'pres-

Table 3
Modified Security Risk Factor Table for refinery X.

Risk factors	Range of security points				Expert score	Defuzzyfied score
Location	Rural (0,0,1,2)	Urban (1,2,3,4)		High density (3,4,5,5)	1.5	1.5
Visibility	Not visible (0,0,1,2)	Low (0.5,1.5,2.5,3.5)	Medium (2,3,4,5)	High (3.5, 4.5,5,5)	2	2
Inventory	Low (0,0,1,2)	Medium (0.5,1.5,2.5,3.5)	Large (2,3,4,5)	Very large (3.5, 4.5, 5,5)	4.5	4.33
Ownership	Private (0,0,1,2)	Public/co-operative (1,2,3,4)		Government (3,4,5,5)	5	4.5
Presence of chemicals that can be used for inflicting heavy casualties	Low quantity (0,0,1,2)	Medium quantity (1,2,3,4)		Large quantity (3,4,5,5)	0	0.5
Worst case impact on-site	Negligible (0,0,1,2)	Low (0.5,1.5,2.5,3.5)	Moderate (2,3,4,5)	Severe (3.5, 4.5,5,5)	5	4.75
Worst case impact off-site	Negligible (0,0,1,2)	Low (0.5,1.5,2.5,3.5)	Moderate (2,3,4,5)	Severe (3.5, 4.5,5,5)	3	3
History of security incidents	Nil (0,0,1,2)	Few (1,2,3,4)		Frequent (3,4,5,5)	3	2.5
Presence of terrorist groups in region	Absence (0,0,1,2)	Few (1,2,3,4)		Large no. (3,4,5,5)	2	2.5
Existing security measures:	High level	Ordinary		Poor/none		
• Access control	(0,0,1,2)	(1,2,3,4)		(3,4,5,5)	2.5	2.5
• Perimeter protection	(0,0,1,2)	(1,2,3,4)		(3,4,5,5)	2	2.5
• Mitigation potential	(0,0,1,2)	(1,2,3,4)		(3,4,5,5)	1.5	1.5
• Proper lighting (all over)	(0,0,1,2)	(1,2,3,4)		(3,4,5,5)	1	1
• Use of metal detector/X-ray/CCTV (at entrance and at all critical locations)	(0,0,1,2)	(1,2,3,4)		(3,4,5,5)	3	2.5
Personal preparedness and training	Well prepared (0,0,1,2)	Average (1,2,3,4)		Poor (3,4,5,5)	2.5	2.5
					Total score	38.08

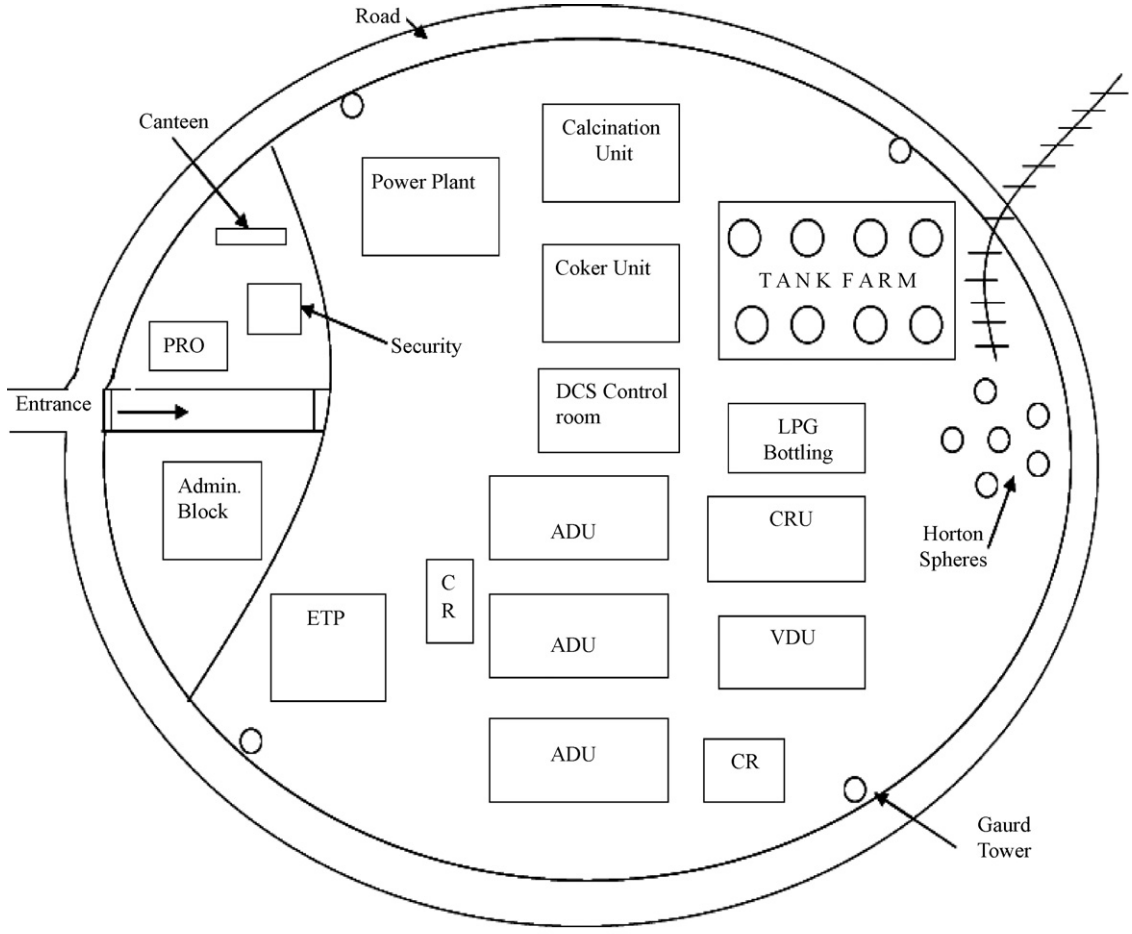

Fig. 4. Sketch of refinery X.

ence of chemicals inflicting mass casualties' the score increased from 0 to 0.5 and therefore the net result is evened out. However, if the defuzzyfied score either uniformly increases or decreases, it will result into a significantly larger variation in the two SRFT models. Incorporating fuzzy logic approach in the earlier developed SRFT model is expected to reduce the uncertainty associated with the human subjectivity of different experts in assigning the scores to a given risk parameter. Moreover, the uncertainty will increase when multiple experts are used for risk assessment. However, in the present work, observations of single expert have been used (similar to the previous work) and thereby less variation is observed in the result. That may not be the case in other examples.

6. Conclusions

The recent terrorist activities all around the globe and a few terrorist activities in and around the chemical plants have raised serious security concern for the CPI. The threat of terrorist striking CPI is now considered both real and credible as these industries handle large amount of Hazchems that can be used by the terrorist as weapons of mass destruction. In order to enforce effective security management programme, it is important to develop improved risk assessment techniques that are cost effective, useful, and suggest selective and effective security countermeasures.

In this paper, the earlier developed SRFT model has been modified using the concepts of fuzzy logic. In the modified SRFT model, two linguistic fuzzy scales (three-point and four-point) have been devised based on trapezoidal fuzzy numbers. Human subjectivity of different experts associated with previous SRFT model is tackled by mapping their scores to the newly devised fuzzy scale. Finally, the fuzzy score thus obtained is defuzzyfied to get the results. A test case of a refinery has been taken to compare the results of both the models. The total risk score obtained using previous SRFT model was '40'. The modified SRFT model gives '38.08'. The final risk score suggests it is a high risk facility and therefore demands serious security attention. The refinery X should go through detailed security and vulnerability assessment and initiate aggressive risk reduction exercise in coordination with the local law enforcement agencies. Comparing the results of both the models, minor variations are observed due to human (experts) subjectivity involved in assigning scores. However, the results may vary significantly if we take another test case.

It is concluded that conventional safety and security measures that were in place before 9/11 have to be relooked and modified with the dynamic nature of thinking adversary (terrorists). Many of the safeguards such as excess flow valves, pressure relief systems, systems to interrupt run away reactions, and other safety equipment will help in limiting the consequences during and after terrorist attacks. The terrorist may attempt to disable these safety countermeasures during the attack. The risk assessment should include all important plausible scenarios of terrorist attacks. Idea is to modify the existing safety tools and develop the new ones keeping in view the possible deliberate actions by the insiders and determined adversaries. Effective security risk assessment is vital and modified SRFT model will work as a pre-screening tool before a decision is made to carry out a detailed security vulnerability assessment.

References

[1] S. Bajpai, J.P. Gupta, Protecting chemical plants from terrorist attacks, Chem. Weekly L34 (2005) 209–213.
[2] S. Bajpai, J.P. Gupta, Securing oil and gas infrastructure, J. Pet. Sci. Eng. 55 (2007) 174–186.
[3] S. Bajpai, J.P. Gupta, Site security for chemical process industries, J. Loss Prev. Process. Ind. 18 (2005) 301–309.
[4] American Petroleum Institute (API), Security Guidelines for the Petroleum Industry, Washington, DC, 2003, available at: http://new.api.org/policy/otherissues/upload/Security.pdf.
[5] P. Baybutt, Process security management: set up your plant's program, Chem. Eng. 110 (1) (2003) 48–56.
[6] http://www.chemalliance.org/_documents/SECALE-F.PDF.
[7] http://www.acusafe.com/Newsletter/Stories/1001News-MonthlyIncidents.htm.
[8] C.A. Ropar, Risk Management for Security Professionals, Butterworth Heinemann, New Delhi, 1999.
[9] United States of America Department of Justice (USDOJ), Assessment of the Increased Risk of Terrorist or Other Criminal Activity Associated with Posting Off-Site Consequence Analysis Information on the Internet (2000) 23–24.
[10] American Chemistry Council, Chlorine Institute, and Synthetic Organic Chemical Manufacturers Association, Site Security Guidelines for the US Chemical Industry, Washington DC, 2001, available at: http://www.socma.com/assets/File/socma1/PDFfiles/securityworkshop/SecurityGuideFinal10-22.pdf.
[11] L.A. Zadeh, Fuzzy sets, IEEE Inform. Control 8 (1965) 338–353.
[12] R.E. Bellman, L.A. Zadeh, Decision making in a fuzzy environment, Manage. Sci. 17 (1970) B141–B164.
[13] H. Zimmermann, Fuzzy Set Theory and its Applications, 3rd ed., Kluwer, London, 1996.
[14] T.J. Ross, Fuzzy Logic with Engineering Applications, McGraw-Hill, New York, 1995.
[15] M. Gentile, W.J. Rogers, M. Sam Mannan, Development of an inherent safety index based on fuzzy logic, AIChE J. 49 (4) (2004) 959–968.
[16] C.E. Pelaez, J.B. Bowles, Using fuzzy logic for system criticality analysis, in: Proc. IEEE Annu. Reliab. Maintainab. Symp., Anaheim, CA, 1994, pp. 449–455.
[17] J.B. Bowles, C.E. Pelaez, Fuzzy logic prioritization of failures in a system failure mode effects and criticality analysis, Reliab. Eng. Syst. Saf. 50 (1995) 203–213.
[18] K.Y. Cai, System failure engineering and fuzzy methodology: an introductory overview, Fuzzy Sets Syst. 83 (1996) 113–133.
[19] T.R. Moss, J. Woodhouse, Criticality analysis revisited, Qual. Reliab. Eng. Int. 15 (1999) 117–121.
[20] M. Braglia, M. Frosolini, R. Montanari, Fuzzy TOPSIS approach for failure mode, effects and criticality analysis, Qual. Reliab. Eng. Int. 19 (2003) 425–443.
[21] R.K. Sharma, D. Kumar, P. Kumar, Systematic failure mode and effect analysis using fuzzy linguistic modeling, Int. J. Qual. Reliab. Manage. 22 (9) (2005) 886–1004.
[22] X. Bai, S. Asgarpoor, Fuzzy based approaches to substation reliability evaluation, Electric Power Syst. Res. 69 (2004) 197–204.
[23] D. Driankov, H. Hellendoorn, M. Reinfrank, An Introduction to Fuzzy Control, Springer, Berlin, 1993.
[24] S.H. Chen, Ranking fuzzy numbers with maximizing and minimizing set, Fuzzy Sets Syst. 17 (2) (1985) 113–129.
[25] R.R. Yager, Uncertainty representation using fuzzy measures, IEEE Trans. Syst. Man Cybern. Part B. Cybern. 32 (2002) 20–28.
[26] http://chemical-safety.com/documents/pdf/SECURITY%20RAT.pdf.