Contents lists available at GrowingScience

Management Science Letters

homepage: www.GrowingScience.com/msl

Fuzzy logic for pipelines risk assessment

Ali Alidoosti[a], **Ali Jamshidi**[b], **Siamak Haji Yakhchali**[c], **Mohammad Hossein Basiri**[d], **Ramin Azizi**[e] and **Abdolreza Yazdani-Chamzini**[f*]

[a]*MSc of Mechanical engineering, Mlek-ashtar Univesity of Technology, Tehran, Iran*
[b]*MSc of Disaster Management, University of Tehran, Tehran, Iran*
[c]*Assisstance professor of Tehran University, Department of Industrial Engineering, College of Engineering, University of Tehran, Tehran, Iran*
[d]*Assisstance professor of Tarbiat Modares University, Department of Mining Engineering, School of Engineering, University of Tarbiat Modares, Tehran, Iran*
[e]*MSc of Natural Disaster Management, Faculty of Environment, University of Tehran*
[f]*Young Researchers Club, South Tehran Branch, Islamic Azad University, Tehran, Iran*

ARTICLEINFO

Article history:
Received December 20, 2011
Received in Revised form
March, 25, 2012
Accepted 20 April 2012
Available online
April 23 2012

Keywords:
RAMCAP
Risk management
Fuzzy logic
Pipeline

ABSTRACT

Pipelines systems are identified to be the safest way of transporting oil and natural gas. One of the most important aspects in developing pipeline systems is determining the potential risks that implementers may encounter. Therefore, risk analysis can determine critical risk items to allocate the limited resources and time. Risk Analysis and Management for Critical Asset Protection (RAMCAP) is one of the best methodologies for assessing the security risks. However, the most challenging problem in this method is uncertainty. Therefore, fuzzy set theory is used to model the uncertainty. Thus, Fuzzy RAMCAP is introduced in order to risk analysis and management for pipeline systems. Finally, a notional example from pipeline systems is provided to demonstrate an application of the proposed methodology.

1. Introduction

Pipelines are the most practical and economically effective modes for transporting dangerous and flammable substances, such as natural gas while roads or rail transportation are often impractical (Papadakis et al., 1999). There are literally different methods to assess risks in pipeline systems (Jo & Ahn, 2005; Henselwood & Phillips, 2006; Dziubnski et al., 2006; Cagno et al., 2000; Yuhua et al., 2005 Sklavounos & Rigas, 2006; Bartenev, 1996; Jo & Ahn, 2001). Pipeline systems play essential role on managing the gas distribution and risk assessment can help decision maker detect the high risk components and make an appropriate decisions to reduce or limit the risk. An appropriate technique requires to assess risks more precisely and more accurately (Alidoosti et al., 2011).

* Corresponding author. Tel: +989126980426
E-mail addresses: abdalrezaych@gmail.com (A. Yazdani-Chamzini)

doi: 10.5267/j.msl.2012.04.017

For this reason, the Department of Homeland Security presented Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework, which is a function of three parameters (Cox, 2009): consequence, vulnerability and threat. RAMCAP provides a consistent and technically sound methodology for investigating consequences of attack. It also identifies security vulnerabilities and develops threat information based on both asset owner and government information (Moore et al., 2007). On the other hand, uncertainty is a part of real-world systems, which are either in crisp or Boolean logic and it is not possible to make a precise assessment. The existing uncertainty is created through two factors (Markowski et al., 2009): (1) uncertainty due to physical variability, and (2) uncertainty due to lack of knowledge.

One of the most popular and efficient ways to face with inherent uncertainty is the possibility theory emerged from the fuzzy sets developed by Zadeh (1965). In accordance with ability of fuzzy logic in modeling uncertainty, this approach is used in different fields of risk management (Chen & Sanguansat, 2011; Nieto-Morote & Ruz-Vila, 2011; Bajpai et al., 2010; Acosta et al., 2010; Rehana & Mujumdar, 2009; Markowski & Mannan, 2009; Liu et al., 2009; Flores et al., 2009; Azadeh et al, 2008; Sadiq et al., 2007; Sadiq & Husain, 2005, Fouladgar et al., 2012).

This paper presents a new methodology established based on the adaptation of RAMCAP method and fuzzy inference system to build a more secure, safe, and resilient pipeline system. As a result, the outputs obtained using the conventional methodology are compared with the proposed framework.

RAMCAP framework

RAMCAP process was first developed to facilitate the analysis and management of risk and resilience of critical facilities and infrastructures. It is based on a primary definition that risk is the expected value of the consequences of specific terrorist attacks and natural events, weighted by the likelihood of the event and the conditional likelihood accomplished by the estimated consequences. So, risk (R) is determined by the intersection of consequences of the attack (C), the threats of the attack (T) and vulnerabilities to the attack (V) (ASME, 2009):

Risk = (Threat) × (Vulnerability) × (Consequence) or R = T × V × C

where:

Vulnerability:

Vulnerability is an important element of a security risk assessment and it is an instrument to determine existing and residual risk (Douglas, 2006). Any weakness in an asset or infrastructure’s design, implementation or operation exploited by an adversary contributes to functional failure in a natural disaster. In risk analysis, vulnerabilities are usually summarized as the conditional probability that, *given* an attack or natural event, the estimated consequences will ensue, i.e., the attack will succeed or the natural event will cause the estimated damage. Vulnerability of an infrastructure element is a function of its intrinsic design, protection systems (physical or other) and changes over time (Baker et al., 2002).

Consequence:

The outcome of an event includes different things including immediate, short and long-term, direct and indirect losses and effects (ASME, 2009). Loss may include human fatalities and injuries, financial and economic damages and environmental impacts, which can generally be estimated in quantitative terms. Consequences may also include less tangible and less quantifiable factors, including political ramifications, decreased morale, reductions in operational effectiveness or military readiness or other impacts. The concept of consequence is defined as the effect of an event or incident.

Threat:

The concept of threat is defined as an event with an undesired impact. Cox (2009) defined threat as any indication, circumstance or event with the potential to cause the loss of, or damage to, an asset or population. In the case of terrorism risk in pipeline systems, threat is based on the analysis of the intention and capability of an adversary to undertake actions detrimental to a section of pipeline or population and the attractiveness of the asset or population relative to alternative assets or populations.

2. Fuzzy logic

2.1. Fuzzy set

A fuzzy set is a collection of elements in a universe of information where the boundary of the set contained in the universe is ambiguous, vague and otherwise fuzzy. Each fuzzy set is specified by a membership function, which assigns to each element in the universe of discourse a value within the unit interval [0, 1] (Wang & Elhag, 2007). Unlike crisp (or ordinary) sets, fuzzy sets have no sharp or precise boundaries (Aydin, 2004). The concept of a fuzzy set provides mathematical formulations that can characterize the uncertain parameters involved in particular risk analysis method.

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. So, even the most sophisticated, precise, and well constructed quantitative model may give misleading results if uncertainties are not treated at some level. Uncertainty in risk analysis can range from modeling uncertainties, to incomplete and unreliable information. Data uncertainties are a major source. Any system under study has dominant risk contributors in addition to the dependent failures usually studied (Vesely, 1983). Fig. 1 shows the different case of a secure set.

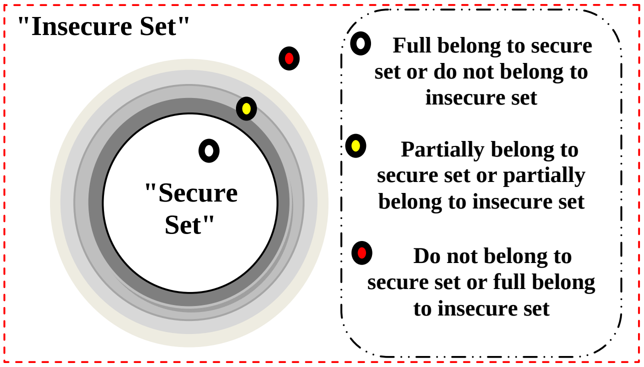

"Insecure Set"
"Secure Set"
Full belong to secure set or do not belong to insecure set
Partially belong to secure set or partially belong to insecure set
Do not belong to secure set or full belong to insecure set

Fig. 1. Fuzzy and crisp states

There are different states in a secure set depicted in Fig. and it shows smooth change from secure to insecure state in fuzzy set under consideration. Vice versa, Boolean logic only takes into account two values 0, 1, where 1 addresses full membership for set under consideration and 0 addresses element do not belong to the set (Alidoosti et al., 2011).

2.2. Fuzzy inference systems

Fuzzy inference is the process of mapping from a given input set to an output set using fuzzy logic. Membership functions, fuzzy logic operators and if-then rules are used in this process. (Elsayed, 2009). The basic idea of a fuzzy inference system is to use fuzzy logic to define an output as a function of measured inputs (Horgby, 1998). The basic advantage of such system is its tolerability to linguistic/imprecise data. The structure of a typical FIS is depicted in Fig 2.

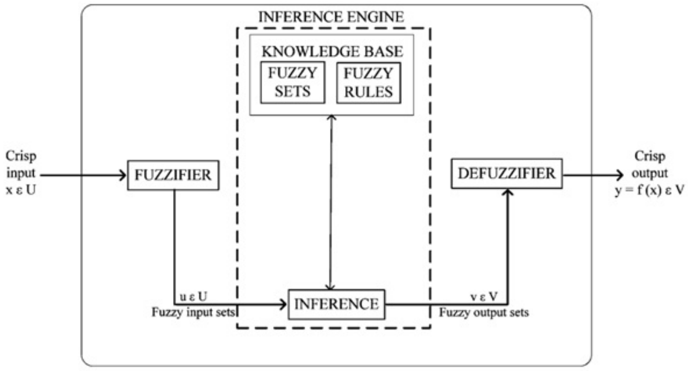


Fig. 2. The structure of a typical FIS (Markowski, 2008)

In general, a fuzzy inference system consists of four steps. First, the inputs have to be modified to linguistic values. Following steps are necessary for successful application of modeling through a general fuzzy system. These are:

(i) Fuzzification of the input and output variables by considering appropriate linguistic subsets such as high, medium, low, heavy, light, hot, warm, big, small.

(ii) Construction of rules based on expert knowledge and/or the basis of available literature. The rules relate the combined linguistic subsets of input variables to the convenient linguistic output subset. Any fuzzy rule includes statements of ‘‘IF . . . THEN. . .” with two parts. The first part that starts with IF and ends before the THEN is referred to as the predicate (premise, antecedent) which combines in a harmonious manner the subsets of input variables. Consequent part comes after ‘‘THEN” which includes the convenient fuzzy subset of the output based on the premise part. This implies that there is a set of rules, which is valid for a specific portion of the inputs variation domain. The input subsets within the premise part are combined most often with the logical ‘‘and” conjunction whereas the rules are combined with logical ‘‘or”.

(iii) The implication part of a fuzzy system is defined as the shaping of the consequent part based on the premise (antecedent) part and the inputs are fuzzy subsets.

(iv) The result appears as a fuzzy subset and therefore, it is necessary to defuzzify the output for obtaining a crisp value that would be required by the administrators or engineers (Ross, 1995).
Defuzzification procedure is frequently achieved through centroid method as applied in this paper.

3. Fuzzy RAMCAP

3.1. Fuzzification

Consequences, Threats, and Vulnerabilities as the inputs should be divided based on their field in a number of fuzzy sets. RAMCAP provides data for the number of sets. The details of fuzzy sets applied in the first step of fuzzy inference system are presented in Table 1. The structure of fuzzy inference system constructed in the paper is depicted as Fig. 3. In this paper, the generalized bell type of membership function (gbell MF) was employed. It’s the most widely applied membership function, which is described by the three parameters, a, b, and c (Eq. 1) (Buyukbingol et al., 2007）.

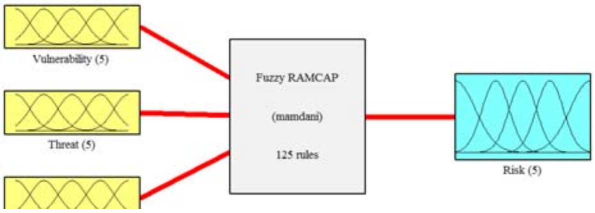


Fig. 3. The architecture of the fuzzy inference system

$$Bell\ (x; a, b, c) = \frac{1}{1 + \left|\frac{x-c}{a}\right|^{2b}} \tag{1}$$

Fig. 4. represents the membership functions for vulnerability (V), consequence (C) and threat (T).

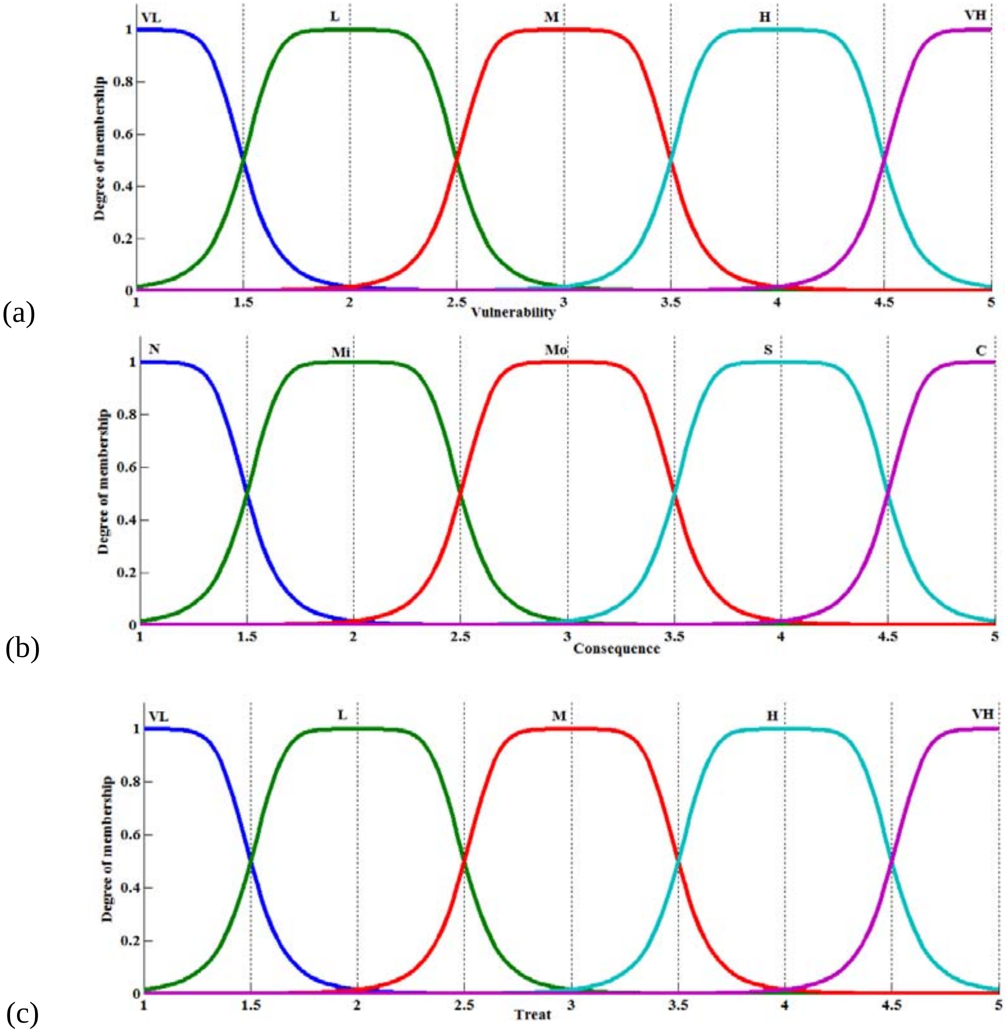


Fig. 4. The membership functions for inputs: (a) vulnerability, (b) consequence, and (c) threat

Table 1 shows the numerical ranges which fuzzy sets are selected based on them. The membership functions for risk also are depicted in a scale of 1 to 5 in Fig. 5.

Table 1

Fuzzy and crisp ratings

Risk items	Linguistic term	interpretation	Crisp rating	Fuzzy ratings	Universe of discourse (X)
Vulnerability (V)	Very High (VH)	Indicates that there are no effective protective measures currently in place to Deter, Detect, Delay, and Respond to the threat and so an adversary would easily be capable of exploiting the critical asset.	5	[0.5,3,5]	X_V€(1,5)
	High (H)	Indicates there are some protective measures to Deter, Detect, Delay, or Respond to the asset but not a complete or effective application of these security strategies and so it would be relatively easy for the adversary to successfully attack the asset.	4	[0.5,3,4]	
	Medium (M)	Indicates that although there are some effective protective measures in place to Deter, Detect, Delay, and Respond, there isn't a complete and effective application of these security strategies and so the asset or the existing countermeasures could likely be compromised.	3	[0.5,3,3]	
	Low (L)	Indicates that there are effective protective measures in place to Deter, Detect, Delay, and Respond, however, at least one weakness exists that an adversary would be capable of exploiting with some effort to evade or defeat the countermeasure given substantial resources.	2	[0.5,3,2]	
	Very Low (VL)	Indicates that multiple layers of effective protective measures to Deter, Detect, Delay, and Respond to the threat exist and the chance that the adversary would be able to exploit the asset is very low.	1	[0.5,3,1]	
Threat (T)	Very High (VH)	Indicates that a credible threat exists against the asset and that the adversary demonstrates the capability and intent to launch an attack, and that the subject or similar assets are targeted on a frequently recurring basis.	5	[0.5,3,5]	X_T€(1,5)
	High (H)	Indicates that a credible threat exists against the asset based on knowledge of the adversary's capability and intent to attack the asset or similar assets.	4	[0.5,3,5]	
	Medium (M)	Indicates that there is a possible threat to the asset based on the adversary's desire to compromise similar assets.	3	[0.5,3,3]	
	Low (L)	Indicates that there is a low threat against the asset or similar assets and that few known adversaries would pose a threat to the assets.	2	[0.5,3,2]	
	Very Low (VL)	Indicates no credible evidence of capability or intent and no history of actual or planned threats against the asset or similar assets.	1	[0.5,3,1]	
Consequence (C)	Critical (C)	very highly impact	5	[0.5,3,5]	X_C€(1,5)
	Serious (S)	highly impact	4	[0.5,3,4]	
	Moderate (Mo)	moderate impact	3	[0.5,3,3]	
	Minor (Mi)	only small impact	2	[0.5,3,2]	
	Negligible (N)	no substantive impact	1	[0.5,3,1]	
Risk category (R)	Very high (VH)	The need to immediately reduce risk	5 (81-125)*	[0.625,3,5]	$X_{R(fuzzy)}$€(0,5), $X_{R(crisp)}$€(1,5),
	High (H)	The need to reduce risk	4 (43-80)*	[0.625,3,3.75]	
	Medium (M)	Not acceptable without review by management	3 (15-42)*	[0.625 3 2.5]	
	Low (L)	Acceptable with review by management	2 (5-14)*	[0.625 3 1.25]	
	Very low (VL)	Acceptable without review	1 (1-4)*	[0.625 3 0]	

* Risk value based on Eq. (1)

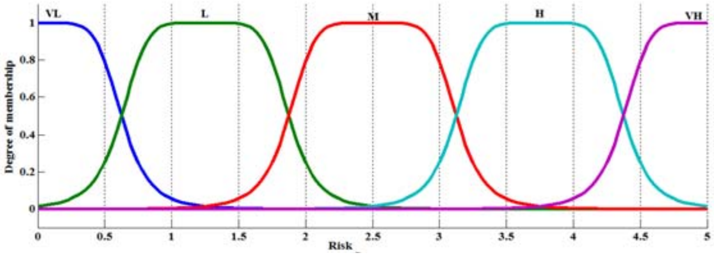


Fig. 5. The membership function of risk

3.2. Rules

There are many fuzzy inference methods. This paper uses the Min–Max fuzzy inference method proposed by Mamdani. The Mamdani fuzzy logic system has many attractive features. First, it is suitable for engineering systems because its inputs and outputs are real-valued variables. Second, it provides a natural framework to incorporate fuzzy IF–THEN rules from human experts. Third, there is much freedom in the choices of fuzzifier, fuzzy inference engine, and defuzzifier, so that we may obtain the most suitable fuzzy logic system for a particular problem. (Wang, 1994)

This paper uses 125 if-then rules to supply a data base by mapping between three input parameters (V, T, and C) and risk value

3.3. Inference engine

The inference engine maps input fuzzy sets (Vulnerability, Threat and Consequence) into fuzzy output set (Risk). Fig. 5. Shows number of if-then rules in order to provide a more comprehending of proposed FIS framework.

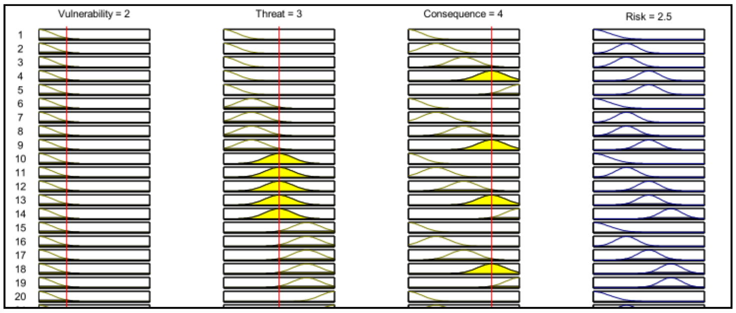
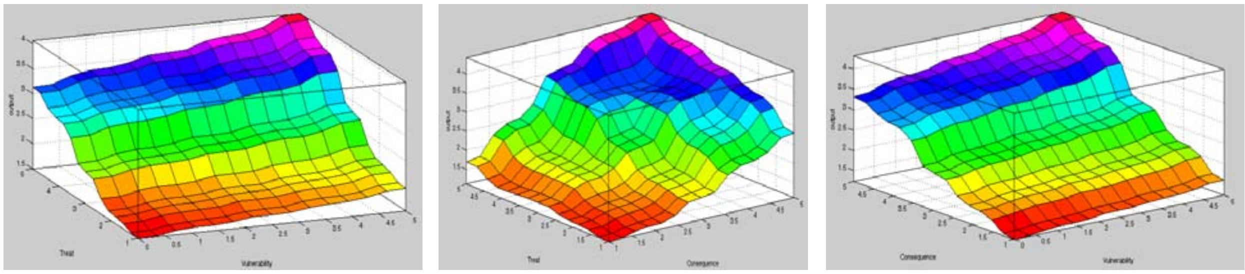


Fig. 5. Sample of rules

The relationship between the fuzzy inputs (V, T, and C) and Fuzzy output (R) can be illustrated by three-dimensional plot that represents the mapping from two inputs (Vulnerability, Threat, and Consequence) to one output (risk). (Fig. 6.)



(a) (b) (c)

Fig. 6. Three-dimensional plot of the FIS framework: (a) vulnerability and threat, (b) threat and consequence, and (c) vulnerability and consequence

3.4. Defuzzification

Defuzzification is used to convert the fuzzy result of risk value into a matching numerical value.
The Center of Gravity (COG) method is employed for defuzzification. (Eq. 2.)

$$y' = \frac{\int_{y} y\mu'(y)}{\mu'(y)} \tag{2}$$

4. Case study

A case study is used to demonstrate the proposed approach for liquids pipeline system. The case study is adapted from API & NPRA (2004) as depicted in Fig. 7. The major assets of the pipeline system are determined: Main Line (ML), ABC Branch (ABC), DEF Branch and inter-modal terminal (DEF), Endpoint storage facility (ESF), River Span Block Valve (RSBV), River Span Pipeline (RSP), and Inter-modal Terminal (IMT).

A team including eleven evaluators with high degree of knowledge in the field of risk analysis prioritizes assets in terms of V, T, and C, so that; experts agree to assess outputs in fuzzy RAMCAP by linguistic terms and then those are compared with RAMCAP outputs. So, a comparison using the fuzzy RAMCAP with RAMCAP is depicted in Table 2. A disadvantage of the RAMCAP is that different sets of V, T, and C may generate an exactly alike value of risk. For example, two assets marine terminal and control room have values of 3, 2, 4 and 2, 4, 3 for V, T and C respectively. Both these assets will have a risk value of 12; however, the risk connotation of these two assets can be entirely different. The other disadvantage of the RAMCAP method is that it does not consider as well the relative importance among inputs. It's clear this may not be precise in real world problems. Hence, fuzzy RAMCAP can result a more accurate risk analysis for protection of critical assets in pipeline systems.

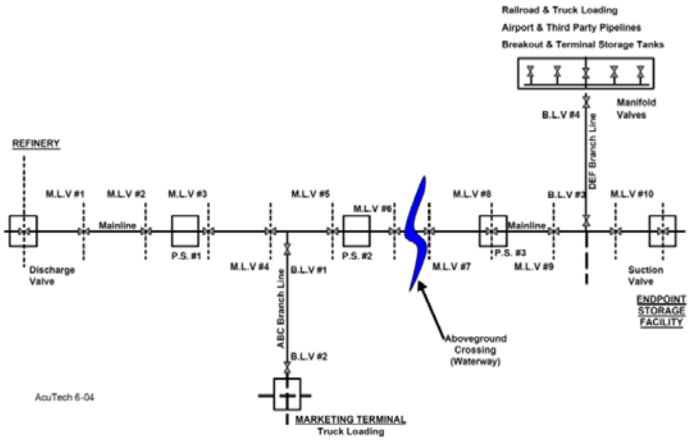


Fig. 7. Pipeline example system (API & NPRA, 2004)

Table 2
The comparison of risk analysis results

Assets	Input						Output			
	Crisp			fuzzy						
	V	T	C	V	T	C	RAMCAP	Rank	Fuzzy RAMCAP	Rank
ML	2	2	3	2.07	2.21	3.11	2	1	1.873	3
ABC	5	3	4	4.54	3.34	3.97	4	6	3.629	6
DEF	3	2	1	2.89	2.25	1.12	2	1	1.303	1
ESF	2	3	2	1.97	2.68	2.16	2	1	1.787	2
RSBV	4	5	1	3.59	4.77	1.34	3	4	3.03	4
RSP	2	4	3	1.79	3.82	3.08	3	4	3.236	5
IMT	4	5	3	4.07	4.41	3.24	4	6	3.746	7

5. Conclusion

This paper developed an extended framework to analyze risk for critical assets in pipeline systems. The main purpose was to investigate the major security risk items in order to allocate the limited resources and time using fuzzy set theory through fuzzy RAMCAP. The proposed methodology is able to solve some inherent imperfection of the RAMCAP. In contrast with the RAMCAP, the Fuzzy RAMCAP considers the relative importance among vulnerability, threat, and consequence. Application of linguistic terms in the input and output information also can be more realistic and flexible by fuzzy RAMCAP. Fuzzy RAMCAP can result a more accurate risk analysis for protection of critical assets in pipeline systems.

Acknowledgement
The authors would like to acknowledge the financial support of University of Tehran for this research.

References

Acosta, H., Wu, D., & Forrest, B. M. (2010). Fuzzy experts on recreational vessels. a risk modelling approach for marine invasions. *Ecological Modelling, 221, 850–863.*

Alidoosti, A., Yazdani, M., & Basiri, M., (2011). Risk assessment of critical asset using fuzzy inference system. *Risk Management,* 14, 77-91.

American Petroleum Institute (API), (2004). National Petrochemical and Refiners Association (NPRA). Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries *(Second Edition). American Petroleum Institute.*

ASME Innovative Technologies Institute, (2009). *All-Hazards risk and resilience*. ASME, New York.

Aydin, A. (2004). Fuzzy set approaches to classification of rock masses. *Engineering Geology,* 74, 227–245.

Azadeh, A., Fam, I., M., Khoshnoud, M., & Nikafrouz, M. (2008). Design and implementation of a fuzzy expert system for performance assessment of an integrated health, safety, environment (HSE) and ergonomics system: The case of a gas refinery. *Information Sciences*, 178, 4280–4300.

Bajpai, Sh., Sachdeva, A., & Gupta, J. P. (2010). Security risk assessment: Applying the concepts of fuzzy logic. *Journal of Hazardous Materials,* 173, 258–264.

Baker, A. B., Eagan, R. J., Falcone, P. K., & Harris, J. M. (2002). A Scalable Systems Approach for Critical Infrastructure Security. *Sandia National Laboratories.*

Bartenev, A.M., Gelfand, B.E., Makhviladze, G.M., & Roberts, J.P. (1996). Statistical analysis of accidents on the Middle Asia-Centre gas pipelines. *Journal of Hazardous Materials*, 46, 57–69.

Buyukbingol, E., Sisman, A., Akyildiz, M., Alparslan, A., & Adejare, A. (2007). Adaptive neuro-fuzzy inference system (ANFIS): A new approach to predictive modeling in QSAR applications: A study of neuro-fuzzy modeling of PCP-based NMDA receptor antagonists. *Bioorganic & Medicinal Chemistry*, 15, 4265–4282.

Cagno, E., Caron, F., Mancini, M., & Ruggeri, F. (2000). Using AHP in determining the prior distributions on gas pipeline failures in a robust Bayesian approach. *Reliability Engineering & System Safety,* 67, 275–84.

Celikyilmaz, A., & Türksen, I. B. (2009). Modeling Uncertainty with Fuzzy Logic; With Recent Theory and Applications. *Springer-Verlag Berlin Heidelberg.*

Chen, Sh. M., & Chen, J. H. (2009). Fuzzy risk analysis based on ranking generalized fuzzy numbers with different heights and different spreads. *Expert Systems with Applications,* 36, 6833–6842.

Cox, L.A.J. (2009). Risk Analysis of Complex and Uncertain Systems. *Springer Science. Business Media, LLC.*

Douglas, J. L. (2006). The Security Risk Assessment Handbook; A Complete Guide for Performing Security Risk Assessments, *Taylor & Francis Group. LLC.*

Dziubnski, M., Fratczak, M., & Markowski, A.S. (2006). Aspects of risk analysis associated with major failures of fuel pipelines. *Journal of Loss Prevention Process Industries,*19,399–408.

Elsayed, T. (2009). Fuzzy inference system for the risk assessment of liquefied natural gas carriers during loading/ off loading at terminals. *Applied Ocean Research*, 31, 179_185.

Executive Order 13010. Critical Infrastructure Protection-*Federal register.* 61(138), 37347-37350.

Feng, L. H., & Luo, G.Y. (2009). Analysis on fuzzy risk of landfall typhoon in Zhejiang province of China. *Mathematics and Computers in Simulation*, 79, 3258–3266.

Flores, W. C., Mombello, E., Jardini, J. A., & Rattá, G. (2009). Fuzzy risk index for power transformer failures due to external short-circuits. *Electric Power Systems Research*, 79, 539–549.

Fouladgar, M.M., Yazdani-Chamzini, A., & Zavadskas, E.K. (2012b). Risk Evaluation of Tunneling Projects. *Archives of civil and mechanical engineering*, 12, 1-12.

Henselwood, F., & Phillips, G. (2006). A matrix-based risk assessment approach for addressing linear hazards such as pipelines. *Journal of Loss Prevention Process Industry,*19, 433–41.

Horgby, P. (1998). Risk Classification by Fuzzy Inference. *The Geneva Papers on Risk and Insurance Theory*, 23, 63–82.

Jo, Y.D., & Ahn, B.J. (2002). Analysis of hazard areas associated with high- pressure natural-gas pipelines. *Journal of Loss Prevention Process Industries*, 15, 179–88.

Jo, Y.D., & Ahn, B.J. (2005). A method of quantitative risk assessment for transmission pipeline carrying natural gas. *Journal of Hazardous Materials, 123, 1–12.*

Liu, K., Hao, J., & Pang, Y. (2009). Algorithm Research on Project Risk Fuzzy Evaluation. *The First International Workshop on Database Technology and Applications, 160-164.*

Markowski, A. S., & Mannan, M. S. (2008) Fuzzy risk matrix. *Journal of Hazardous Materials.* 159, 152–157.

Markowski, A. S., & Mannan, M. S. (2009). Fuzzy logic for piping risk assessment (pfLOPA). *Journal of Loss Prevention in the Process Industries,* 22, 921–927.

Moore, D., Fuller, B., Hazzan, M., William, J., (2007). Development of a security vulnerability assessment process for the RAMCAP chemical sector. *Journal of Hazardous Materials,* 142, 689–694.

Nieto-Morote, A., & Ruz-Vila, A. (2011). Fuzzy approach to construction project risk assessment. *International Journal of Project Management, 29(2), 220-231.*

Papadakis, GA., Porter, S., & Wettig J. EU, (1999). initiative on the control of major accident hazards arising from pipelines. *Journal of Loss Prevention in the Process Industries,*12, 85–90.

Rehana, S., & Mujumdar, P., P., (2009). An imprecise fuzzy risk approach for water quality management of a river system. *Journal of Environmental Management,* 90, 3653–3664.

Ross, J. T. (1995). *Fuzzy Logic with Engineering Applications*. McGraw-Hill Inc, New York.

Sadiq, R., & Husain, T. (2005). A fuzzy-based methodology for an aggregative environmental risk assessment: a case study of drilling waste. *Environmental Modelling & Software,* 20, 33-46.

Sadiq, R., Kleiner, Y., & Rajani, B., (2007). Risk analysis using fuzzy logic and evidential reasoning. Water quality failures in distribution networks. *Risk Analysis,* 27, 1381-1394.

Sklavounos, S., Rigas, F., (2006). Estimation of safety distances in the vicinity of fuel gas pipelines. *Journal of Loss Prevention in the Process Industries*, 19, 24–31.

Vesely, W. E. (1983). *The Façade of Probabilistic Risk Analysis: Sophisticated Computation Does Not Necessarily Imply Credibility*. Proceeding annual reliability and maintainability symposium.

Wang, X. (1994). *Adaptive Fuzzy Systems and Control – Design and Stability Analysis*. Prentice Hall.

Wang, Y. M., & Elhag, T. (2007). A fuzzy group decision making approach for bridge risk assessment. *Computers & Industrial Engineering,* 53, 137–148.

Yuhua, D., & Datao, Y. (2005). Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis. *Journal of Loss Prevention in the Process Industries,* 18, 83–88.

Zhao Y, Xihong L, & Jianbo L. (2007). Analysis on the diffusion hazards of dynamic leakage of gas pipeline. *Reliability Engineering & System Safety,* 92, 47–53.