IJBPAS, April, 2015, 4(4):1858-1867

ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)

'A Bridge Between Laboratory and Reader'

www.ijbpas.com

PHASE ASSESSMENT OF VITAL ASSETS RISK IN OIL INDUSTRY

MOHAMMAD NEMATI GOODARZI[1], AHMAD FARMAHINI FARAHANI[2], SEYED EMAD HOSSEINI[3] AND MEHDI TAVAKOLI[4*]

1: Planning manager of institute for International Energy Studies (IIES), Tehran, Iran

2: Director of Research, Institute for International Energy Studies (IIES)

3: Research deputy of institute for International Energy Studies (IIES), Tehran, Iran

4: HSE, NIOC, National Oil Company

***Corresponding Author: E Mail: Tavakolimehdi@yahoo.com**

ABSTRACT

Chemical industry because of having a large volume of chemical materials, are always in danger of terrorism and manmade menaces. Therefore, it is too important to have a master plan in security risk management, which includes: new assessment of vital assets risk techniques in industries, specially oil and gas industries. In this research, assessment of security risks done by assets (SRFT) security risk factor table. Important factors of security risk such as: situation, possession, visibility, stock and etc, are used in this model. In this essay, by using phase logic, the security risk factor table changes its form and it reduces assets risk uncertainty assessment. The changed model, uses one 3pointed and one 4pointed phase scales, based on trapezium phase numbers. At last, the phase numbers of experts exited from phase mode and the results were expounded.

Keywords: Terrorism, Vital assets, Security vulnerability assessment, Security risk factor table, Phase logic

INTRODUCTION

Before the terrorism attack to the world trade center in New York, September 11, 2001 A.D, the emphasis is on the risks of natural and technological events and incidents analysis, at assessment of oil industry and other related industries risks. In other words, before the September 11, man made events did not count into common risks assessments. It was after the September 11 that the terrorism events were placed on the center of chemical and petroleum attention. Chemical industry such as oil industries, store and carry out a large amount of chemical materials. Therefore, potential menaces, are always dangerous because of economic, life and environmental considerable damages, which lead to explosion, poisonous materials releases, and fire. So, vital assets risk assessments results from security menaces, is nowadays an origin. Chemical industries depends on circumstances, may increase security processing and/or may content to existing circumstances, but often, chemical sites which are in danger of considerable menaces and/or are near to populated centers, do need to increase maneuvers against security and man made menaces. So, in sensitive industries such as Chemical industry, it is too important to use continued security risk management plans, containing security risk assessments techniques and execute these techniques.

It is necessary for security risk assessments to be flexible in compare with technological events and natural circumstances risk assessments, that is the main different between these two. In other words, making uncommon and unpredictable decisions, in order to surprise the menaces, is one of the most important points in security risk management. For example, change in protocol of stocking the chemical materials in stock tanks, and/or change in time of some parts of campaign. Learning suitable confronting against potential menaces, can be helpful to increase the assets resistance. In fact, most of the security and risk assessment common ways with logic changes, can be useful as confronting method.

Security risk management

Security risk management plan, as it shown at **Figure 1**, needs a systematic approach for vital assets risk analysis. It is necessary for this plan to have ability of recognizing sensible assets, & natural & unnatural considerable menaces, & also vulnerability & existed risks assessment, & stationing confronting plans. The most important part of Security risk management in each assets, is SVA (Security vulnerability assessment). SVA is not necessarily a quantitative method & almost it uses from qualitative methods, specially experts judgments. Assessment output by the experts, is useful for risk computing & then risk priority, in order to make new confronting methods, & geographical positions, campaign kind, & chemical materials kind & volume, have very important rule to optimize SVA approach.

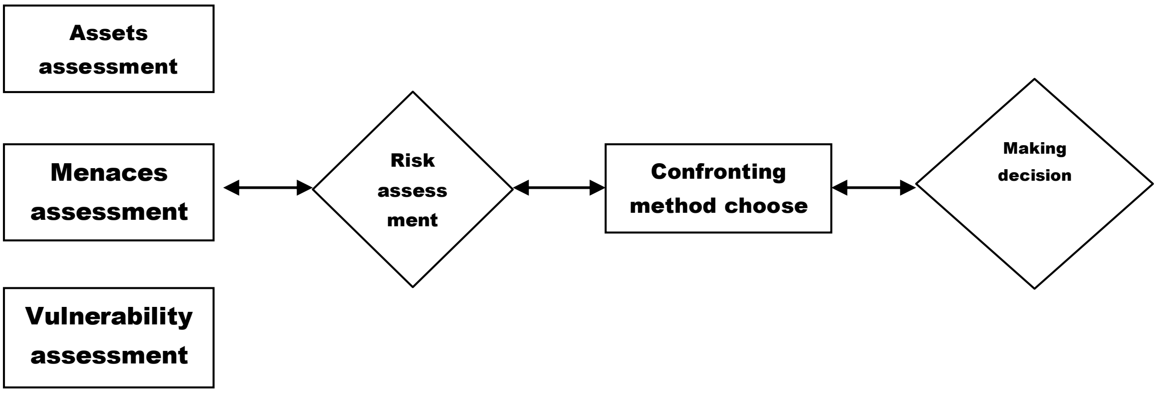

Figure 1: SVA (Security vulnerability assessment)

SVA at chemical industries vital assets concludes below steps:

Assets specifications: the purpose of this step is to recognize sensitive assets. Sensitive assets are those assets which need more security resistance against potential menaces.

Menace Assessment: in this step, recognizing & distinguishing potential menaces, & assets assessment according to their attraction volume & also probable consequence evaluation in case of menaces to be successful.

Vulnerability assessment: is to recognize potential security vulnerability which menaces the vital assets.

Security risk assessment: this step, is for determining the risk of each menace according to their correctness & their consequences. After determining the risk of each menace, the risks classified & if the volume of the computed risk is high, some recommendations will present in order to reduce it.

Suggestions: after compute & classify the risk, in order to recognize & evaluate methods of reducing risks effects, present options will adopt. Also if it is needed, the confronting methods reconsidered.

In this essay, as it shown at **Table 1**, we use SRF (security risk factor table) as a tool for security risk assessment in chemical industries.

This model uses from security risk factors such as: situation, visibility, possession, & so on. Also, effort is to reducing human errors scoring to this factor, using with phase logic. In the way that, we have got a phase mark to each risk factor, in form of two verbal scales (3 pointed & 4 pointed) with a domain from zero to five, & then total achieved phase mark, will exited from phase mode in order to evaluate the situation of risk site with more attention.

As a conclusion, as it shown at **Table 2**, total achieved risk mark, is shown the situation of assets security vulnerability.

Table 1: SRF (security risk factor table)

Risk factors	Risk marks domain				Real marks
Position	Rural 1	Urban 2,3,4,	High density 5		1
Visibility	Sight disability 0	Low 1,2	Middle 3,4	High 5	1
Extant	Low 1	Middle 2	High 3,4	Very high 5	1
Possession	Private 1	Public 2,3	Governmental 4,5		5
Terrorism background in region	Non-existent 0	Rarely 1,2,3	Much 4,5		5
Exist security actions	High	Ordinary	Weak		3
Availability control	1	2,3	4,5		2
Environmental support	1	2,3	4,5		2
Reduce the risks effects	1	2,3	4,5		2

Table 2: Security risk ranking

Exit security risk situation	Achieve risk mark
Low	< 15
Middle	16 – 30
High	31 – 45
Very high	45 >

Phase system theory

In making decision process of security management & security risk, always there is a degree of uncertainty in available data. Also, establishing quantitative data base is challenging, because of many reasons such as: lack of frequency in security events risk, human errors & economic circumstances. Even if the data is available, has considerable errors & uncertainty. So, establishing a suitable data base is impossible in this situation. Therefore, in such a situation, phase logic theory is useful & helpful to reduce uncertainty of the data. This theory was discussed by Mr. Lotfizade for the first time, which is so helpful to solve complicated issues & useful in industries. But to increase security risk assessment exactness, using with phase logic, many attempts is done.

Phase concepts

Orisp sets, in fact are usual & common sets. Making difference by adding adjective orisp, easily helps us to use a vital & innovative concepts in phase logic named membership function. Orisp sets model, membership function can just get two amounts: yes or No (1 & zero) these two are those possible in classic 2valued logic. So, phase set defines based on membership function which contains an all embracing set of (1 to zero). In other word, each member has a different membership. Phase set is established with generalize classic sets theory. In classic sets theory, membership of a set member is based on the Binary system, which shows a member is, or is not a member of a set. While in phase theory, proportional degree of a set member is permitted. Members evaluation with marking them by functions, shows the degree of their membership.

If membership degree of an element in a set is zero, that member exited from the set & if it is equal 1, that member is completely entered in the set. As a conclusion, we can say classic set is a mode or a subset of phase set. If membership degree of a member is btw 1 & zero, this mark shows gradually membership degree. So, according relation 1 we have:

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

Which in this relationship, $M_a(X)$, is element feature function (x) at (A) as an orisp set. Also, membership function for phase set (A) is as relation (2) as below:

$M_A : U \rightarrow [\,0\,,1]$ (2)

Which in this, M_a, is membership degree of (x) at phase set (A).

Membership functions

In phase logic, uses different kinds of functions (MF) such as triangular, trapezium, Gamma, & rectangular. One phase number include a phase set, which is a set of real numbers with different membership degree btw zero to 1. Towards, triangular & trapezium membership functions (TFN) because of simplicity & understandability, is used widespread in order to compute & interpret data.

Although, using complicated relations such as Gaus relation, gives us more meticulous description.

But these relations are so time-consuming, & in compare with other methods in this essay their additional complication, without presenting any considerable concession, reduce their validity.

A trapezium membership functions, which is used in this research, shows with A:(a,b,c,d) & members of this function define as relation 3 as below:

$$\begin{cases} \dfrac{x-u}{b-a} & \\ \text{MA} = \dfrac{x-u}{b-a} & A \le x \le b, \quad b \le x \le c, \ b \le x \le c \\ 0 \text{ Otherwise} & \end{cases}$$

So, according to numbers domain used in SRFT, using trapezium membership function is the best phase method.

Verbal variable

A verbal variable shows as (X,T,U,M) from, which is in it:

X: is verbal variable

T: verbal volumes set which (X) is able to a chive them, as a model we have:(T-) very high, high, middle, low..

U: real domain which (X) variable is able to achieve it.

M:is a semantic law based on, each verbal volume at (T) is related with a phase set in U. for example, (M) determine "middle" & "high" volume, shown in (T), as a certain membership function from.

(X) with (0/3) membership volume, may assess middle, & with (0/7) membership volume, may assess high.

Phase exit

Phase exit, is a situation within, numbers exited from phase mode. There are many different methods n order to phase exiting, but common methods in this field are Yager & Chen. This research uses from average phase exit method, which compute parameters average volumes as relation (4).

Phase exit volume: $$\frac{\int MB'(y)\,\text{ydy}}{\int MB'(y)\,\text{dy}} \quad (4)$$

B`: is phase set output & MB` is membership function.

Security risk phase factor table

(SRFT) can be used as a pre measurement tool in SVA model in other to security situations assessment in each site. In SRFT model, important parameters such as situation, visibility, possession and etc, rated by zero to 5 scale, which zero is "lowest risk" & **5** is "highest risk". Rating the parameters is based on experts, quantitative & experimental. Adding up the achieved scores, as it shown at table number 3, can be helpful for vital assets security situation assessment. If different experts help to score, because of human errors, answers uncertainty will increase. So, in order to reduce this uncertainty phase theory is used. First, all of the parameters allocated scores, will be phase, and then will be phase exited. Achieved add up from security risk phase factor table, have better conclusion in compare with un-phase mode.

In this essay, uses from 2 verbal scales, scale number 1 has 3 limits **(Figure 2)** & scale number 2 has 4 limits **(Figure 3)** as below.

Table 3: SRFT (Security risk phase factor table)

Risk factors	Risk marks domain				Experts scores	Phase exited scores
Position	Rural (0,0,1,2)	Urban (1,2,3,4)	High density 5		1.5	1.5
Visibility	Sight disability (0,0,1,2)	Low (0.5,1.5,2.5, 3.5)	Middle (2,3,4,5)	High (3.5,4.5,5,5)	2	2
Extant	Low (0,0,1,2)	Middle (0.5,1.5,2.5, 3.5)	High (2,3,4,5)	Very high (3.5,4.5,5,5)	4.5	4/33
Possession	Private (0,0,1,2)	Public (1,2,3,4)		Governmental (3,4,5,5)	5	4.5
Terrorism background in region	Non-existent (0,0,1,2)	Rarely (1,2,3,4)		Much (3,4,5,5)	2	2.5
Exist security actions	High	Ordinary		Weak		
Availability control	(0,0,1,2)	(1,2,3,4)		(3,4,5,5)	2.5	2.5
Environmental support	(0,0,1,2)	(1,2,3,4)		(3,4,5,5)	2	2.5
Reduce the risks effects	(0,0,1,2)	(1,2,3,4)		(3,4,5,5)	1.5	1.5

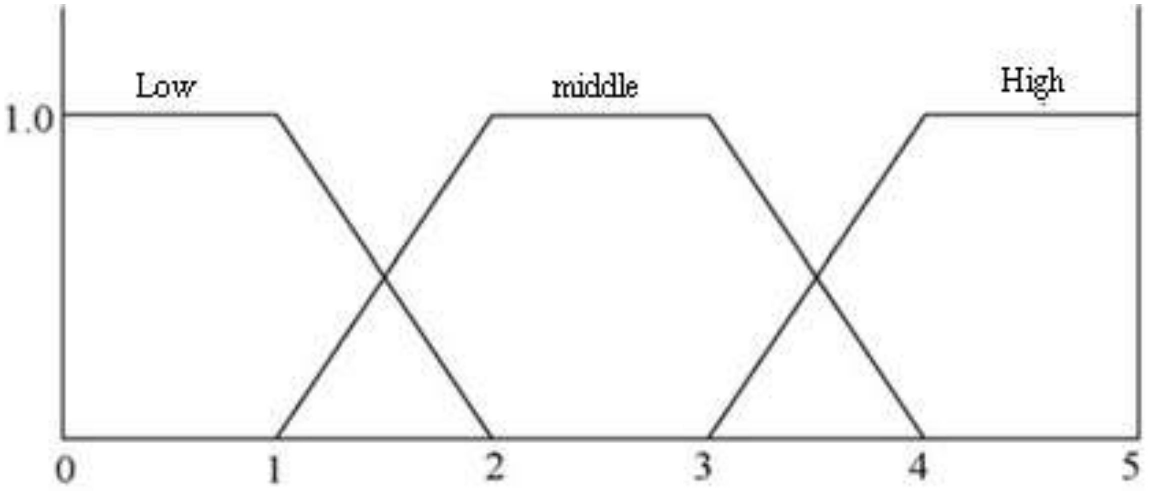

Figure 2: 3-pointed scale

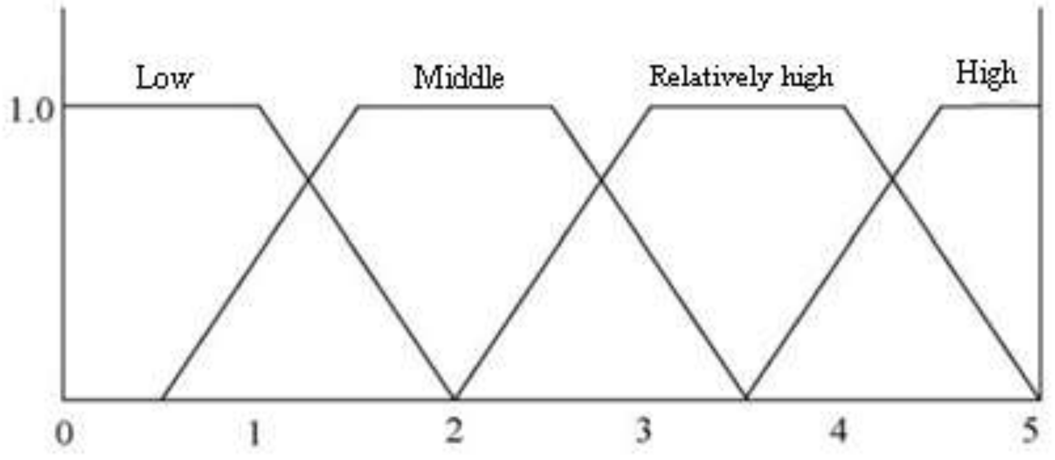

Figure 3: 4-pointed scale

Trapezium phase numbers used in 3-pointed scale are: low(0,0,1,2), middle (1,2,3,4), & high (3,4,5,5) & for 4-pointed scale are : low(0,0,1,2), middle (0/5,1/5,2/5,3/5), & quite high (2,3,4,5) & high (3/5,4/5,5/5). SRFT is shown at **Table 3**.

For example, experts using with scale 1 gave score 5 to "possession" parameter. Governmental possession gets the highest risk with membership volume 1. The achieved volume of possession risk parameter for phase exit, compute using with average method according to relation 5.

$$y' = \frac{4/5 \times 1}{1} = 4/5 \quad (5)$$

By phase scale 2 also, we can phase other parts of parameters. For instance, "stock" parameter gets 4/5 score. This amount, suggests high stock volume with 0/5, & very high with membership volume 1, on phase scale, also, phase exit campaign shows the same as "possession" parameter, present in relation 6.

$$y' = \frac{4/75 \times 1 + 3/5 \times 0.5}{1 + 0.5} = 4/33 \quad (6)$$

All of these computes shown in **Table 3**.

This is essential to say that, if several experts get their judgments for risk assessment, different scores will achieve in a parameter. The average of scores as the score of each parameter will determine & other parts of process will be unchangeable.

CONCLUSION

Increase of recent terrorism attacks all over the world, makes it necessary to review the principles of security risk at vital assets. To store & to carry a huge amount of chemical materials, which some of them are very dangerous for human being, lead to increase security potential menaces at industries assets. So, in order to strengthen the plans of security risk management it is very important to improve risk assessment techniques having suitable, useful & with confronting method economic justify.

In this essay, we used security risk factor phase table, design with 2 phase scales (3-pointed & 4-pointed) based on trapezium phase numbers. Also, considering phase logic can reduce the human errors resulting from several expert judgments as much as possible.

At last, the conclusions will extract by phase exit computes. This research shows that it is necessary to review the security & safety management standards before the September 11, 2001 A.D.

The most important aspect of this metamorphosis, is flexibility of security risk management facing with unpredictable purpose of security menaces such as terrorism attacks. In other words, security risk proficiency assessment of a chemical-industrial site, is possible when we consider all of the risk parameters. After considering the situation of vital assets security at chemical industry, we bear in mind the confronting methods against menaces according to computed risks at model in the shape of security system stationing into & around the site. The (SRFT) model is efficient when we consider all of the possible scenarios. The best situation in this model, is to improve models of "reducing the affects of menaces", compare with "making decisions based on new security systems establishing".

Economic consideration is one of the efficient principle models of risk assessment. So, security risk management at chemical industry is vital, & SVA model is considered as a tool to compute exist security risk at vital assets more than SRFT model at these assets.

REFERENCES

[1] S. Bajpai, J.P. Gupta, Securing oil and gas infrastructure, J. Pet. Sci. Eng. 55 (2007)174 186.

[2] M. Gentile, W.J. Rogers, M. Sam Mannan, Development of an inherent safetyindex based on fuzzy logic, AIChE J. 49 (4)(2004)

[3] S. Bajpai, J.P. Gupta, Protecting chemical plants from terrorist attacks, Chem. Weekly L34 (2005)

[4] S. Bajpai, J.P. Gupta, Site security for chemical process industries, J. Loss Prev.Process. Ind. 18 (2005)

[5] American Petroleum Institute (API), Security Guidelines for the Petroleum Industry, Washington, DC, 2003, available at: http://new.api.org/policy/otherissues/upload/Security.pdf.

[6] P. Baybutt, Process security management: set up your plant s program, Chem.Eng. 110 (1) (2003)

[7] K.Y. Cai, System failure engineering and fuzzy methodology: an introductory overview, Fuzzy Sets Syst. 83 (1996) 113-133.

[8] S.H. Chen, Ranking fuzzy numbers with maximizing and minimizing set, FuzzySets Syst. 17 (2) (1985) 113 129.

[9] P Baybutt, Process security management: set up your plant s program, Chem.Eng. 110 (1) (2003) 48.