Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):1448-1454

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

The concept of vulnerability in security assessment of chemical plants

Dongfeng Zhao[1], Su Hu[2], Yifei Meng[1], Cong An[2] and Shuang Chen[2]

[1]Department of Environmental and Safety Engineering, China University of Petroleum (East China), Qingdao, PR China
[2]Department of Safety Technology and Engineering, China University of Petroleum (East China), Qingdao, PR China

ABSTRACT

Security assessment with vulnerability is based on American Petroleum Institute (API) Standard 780 Security Risk Assessment (SRA) Methodology which gives fixed steps combining with vulnerability, As Low As Reasonably Practicable, Swiss Cheese Model and cost-effectiveness theory. Vulnerability of different periods were analyzed emphatically, such as vulnerability before accidents, vulnerability in accidents and vulnerability after accidents. As Low As Reasonably Practicable can allow managers to know clearly that which assets should be protected deeply. Swiss Cheese Model helps analyzers understand detailed reasons of attacks and avoid adversaries' attacks. Through cost-effectiveness theory, benefits of the security investments can be maximized. Overall, this article can make managers know more about the risk level in multiple dimensions and enlighten analyzers to assess the risk level of chemical plants.

Key words: Vulnerability, security assessment, chemical plants, countermeasures

INTRODUCTION

The scope of terrorist attacks is broader and the impact is greater since 9/11 [1], so terrorist attacks have been a global issue which is paid wide attention by community of nations. The appearance of terrorism is due to two main requests that one is to obtain supporters' support and trust and the other is to threaten others. Most acts of terrorism always try to reach the two requests [2]. Terrorists make others suffer violence or sabotage non-combat goals (sometimes iconic targets) to get up panic and fear. Because of chemical plants' characteristics of process flow, materials, facilities, once they are damaged, there will be serious consequences, which may arise much more attacks later.

The refinery in Kingdom of Saudi Arabia was attacked by militants in February 2006. Attackers drove several cars with suicide bombers to rush into the refinery and were killed by security department near the refinery. Moreover, projecting campsites of China Petroleum & Chemical Corporation in the southeast of Ethiopia were attacked by more than 200 attackers which resulted in theft of minibuses, buses and cars, all facilities were destroyed, 9 people were killed, 7 people were kidnapped on April 24, 2007. Oil and gas field in Algeria was attacked by armed forces and many people from different countries were kidnapped on January 16, 2012. Terrorist activities, kidnapping and other events of the same kind have become a serious threat to people's life and property.

Risk evaluation methods at present mainly apply to process safety, while those methods apply a little to social security assessment. American petroleum institute published a risk guideline for security vulnerability assessment (SVA) [3]. This guideline was an outline of SVA, and it introduced the concept of SVA and main steps. DHS and ASME improved the criterion of RAMCAP (Risk Analysis and Management for Critical Asset Protection) [4]. Dennis P. Nolan compared HAZOP, PHA, What-IF with SVA, applied the idea of PHA to SVA and emphasized the staff composition of SVA team [5].

This article is based on the concept of vulnerability in security assessment of chemical plants, focusing on the role of vulnerability in different phases of security assessment. Risk of terrorist attacks on chemical plants is established on four dimensions: the frequency of attacks, the frequency of successful attacks, the vulnerability of assets and the consequence of attacks.

THE CONCEPT OF VULNERABILITY

Vulnerability came from the study of natural disasters initially [6]. With the extension of the study, vulnerability has been widely used in climate change, sustainable development, ecology, human health, economics and other fields[7]. General concept of vulnerability points the possibility of systems being damaged and the extent of the damage. Vulnerability is the description and measure of the degree of exposure, susceptibility and resilience [8]. It can determine different risk factors and levels according to different environment and people, so it is more suitable for public security risk assessment.

Vulnerability of chemical plants refers to that chemical plants can sustain the influence of accidents and protect its function under the action of accidents of certain intensity. The chemical plant's vulnerability includes the external and the internal vulnerability, the external means the exposure while the internal means the sensibility, coping ability, resilience (Fig. 1).

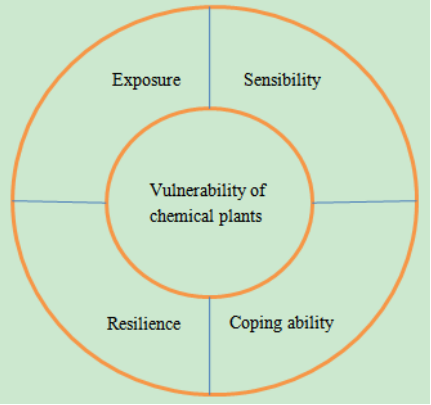


Fig. 1 Chemical plants' vulnerability concept

1.1. Exposure

Exposure means the assets of chemical plants which are exposed to the accidents, such as people, materials, facilities and environment. Exposure is the critical factor of accidents. Only assets are exposed to the environment, can accidents happen. The amount of people, materials, facilities and environment which are exposed to the danger decide the consequence directly. The distance and location between the assets and the accident places also decide the consequence.

1.2. Sensibility

Sensibility means the possibility of being damaged after a certain attack. For example, hospitals and schools around the danger belong to high sensibility. The sensibility depends on the structure of the assets. If toxic substances spill, people will easily be affected by toxic substance, while facilities are hard to be damaged which is the difference between different assets.

1.3. Coping ability

Coping ability means the regulation ability that assets can adjust and avoid accidents [9]. It is also the regulation ability when the system changes abruptly. It is a kind of inherent attribute of system.

1.4. Resilience

Resilience mainly means the ability of people, materials, facilities, environment and other factors that can reduce the loss, as well as recover to normal conditions through self-regulation after being attacked. It specifically means the overall system's ability of adjusting & recovering. Resilience includes people's resilience, facility's resilience, natural resilience, social resilience and economic resilience. The speed of recovery and the condition after recovery can represent the resilience. We need to find out the weakness of recovery and adopt effective measures to strengthen the resilience of chemical plants.

OVERVIEW OF SECURITY ASSESSMENT

The security assessment in this article is mainly based on scenarios and assets of chemical plants. It needs to assess incidental accident's or frequent accident's risk level on the basis of people, property, reputation which are hurt by accidents. Events include terrorism, mass incidents, armed conflicts, political upheaval, religious problems, public safety affairs and other serious affected social events.

Security assessment needs to identify the likelihood of attacks, the vulnerability of assets, the effectiveness of safeguards and the severity of consequences to calculate the risk level so as to compare with standard, if the risk level is below standard, then chemical plants need to maintain the safeguards, while the risk level is above standard, chemical plants need to strengthen the safeguards according to the risk level.

To conduct security assessment, we need to understand the aims of terrorist's attacks, and then follow fixed steps to get the risk level (Fig. 2).

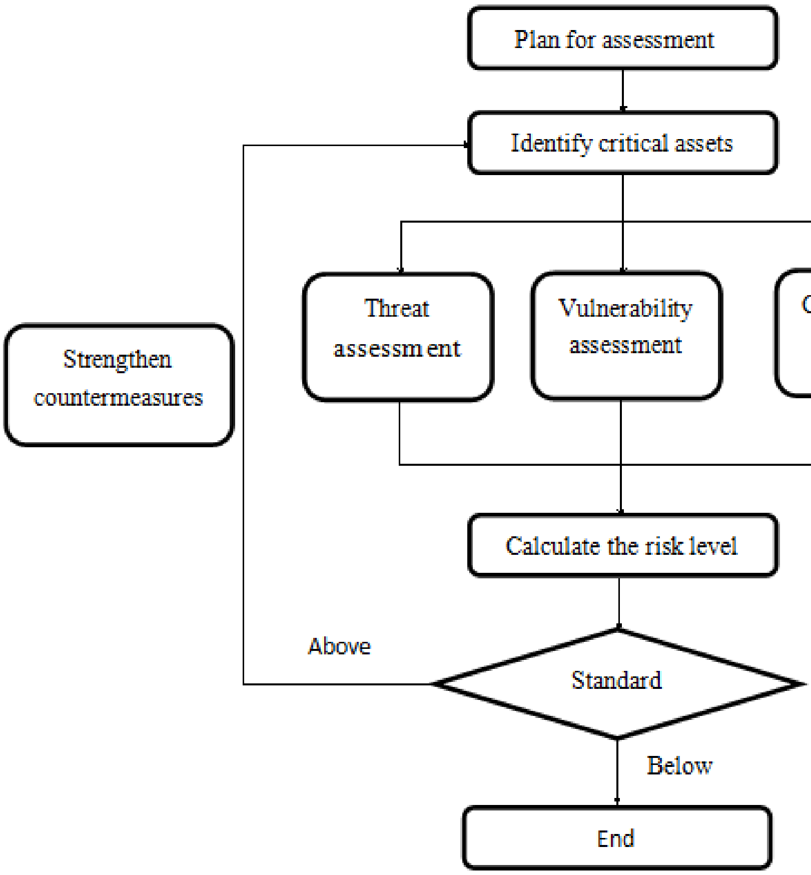


Fig. 2 Steps of security assessment

PLAN FOR ASSESSMENT

To conduct security assessment, we first need to get the favor of management. Then it needs to form a team about security assessment. The team includes a chairman who is professional in security assessment, a secretary, a security manager, a politician, a HSE representative, a security consultant, a project manager who designed the facility and a knowledgeable operator who knows how the facility will be operated.

Since the team is formed, the team members should decide the assessment objective and scope so as to assess specifically. Team members need to collect relevant information and go to chemical plants to have field research. Information can include people, facilities, materials, buildings, support systems, transportation interface, cyber systems and information technology, surroundings, historical attacks, state of the country and other information which may affect the assessment.

IDENTIFY CRITICAL ASSETS

During the process of assets, not all assets need to be analyzed and critical assets should be screened which need a further assessment. Most important of all, we must consider critical assets from the point of adversaries. Adversaries may attack assets from stealing assets, damaging assets, taking revenge from society by demonstrating their capabilities. Different assets can take different protection measures. Assets of chemical plants include people (staff, contractors, vendors, visitors, customers, outsiders), physical assets (facilities, vehicles, materials, infrastructure, buildings, fixtures, electronic products), proprietary information (data, operation record, development program, files), business, business reputation, environment (natural environment, social environment).

RISK ASSESSMENT

Threat assessment

In the analysis of risk, threat is based on the analysis of the intention and the capability of the adversaries going to take actions. Anyone who may attack the assets should be analyzed. Political instability and historic attacks are of great importance. Adversaries may include terrorists, vandals, gangs, thieves, computer hackers, paramilitary, disgruntled employee and contractors, suicides, psychopaths. Since we have got the types of adversaries, then we need to analyze every type of adversary, the frequency of attack and the frequency of successful attack. If an attack happens, would it lead to a successful attack? If a successful attack happens, can it result in consequence? So the frequency of adversaries' attack (F) is determined by two aspects, the first one is the frequency of attack (F1), the second one is the frequency of successful attack (F2), Eq. 1.

$$F=F1\times F2 \quad (1)$$

Swiss cheese model can be used in this methodology. If we prevent the appearance of adversaries, then accidents won't happen. The adversaries appear, but we hold back their intentions then accidents won't happen either. Adversaries take action but we have rigorous protection measures then there will be less loss. So we should take every step into consideration to reduce the effect of adversaries.

Vulnerability assessment

Vulnerability can simply be represented by any weakness in an asset or facility's design. Vulnerability assessment is based on the analysis of scenario or the vulnerability of every asset. Vulnerability assessment also includes the assessment of system's effectiveness that concentrates on physical protection systems (prevention, detection, delay, response, resilience). Facilities such as vehicle barriers, fences, barbed wire, doors, windows, walls, terrain-following, locks and other physical protection systems are equipped primarily to prevent the occurrence of adversary's attacks. If adversaries take action to attack assets of chemical plants, security forces must be able to detect an attack soon enough so as to react to adversaries. Continuous video monitoring of an area, fixed cameras, pan-tilt-zoom (PTZ) cameras, sensors, line detection, physical detection and CCTV all can be used in the process of detection. Also, a sufficiently potent response force to arrive and interrupt the attack is needed before the attack succeeds in stealing, releasing, destroying or otherwise compromising the facilities' critical assets. Since the attacks really happen and give rise to consequences, emergency relief workers must react to the accidents as soon as possible. Public relations officials and media professionals need to take action according to the situation in case of false reports.

The vulnerability of accidents can be separated into three phases according to the process (Fig. 3).

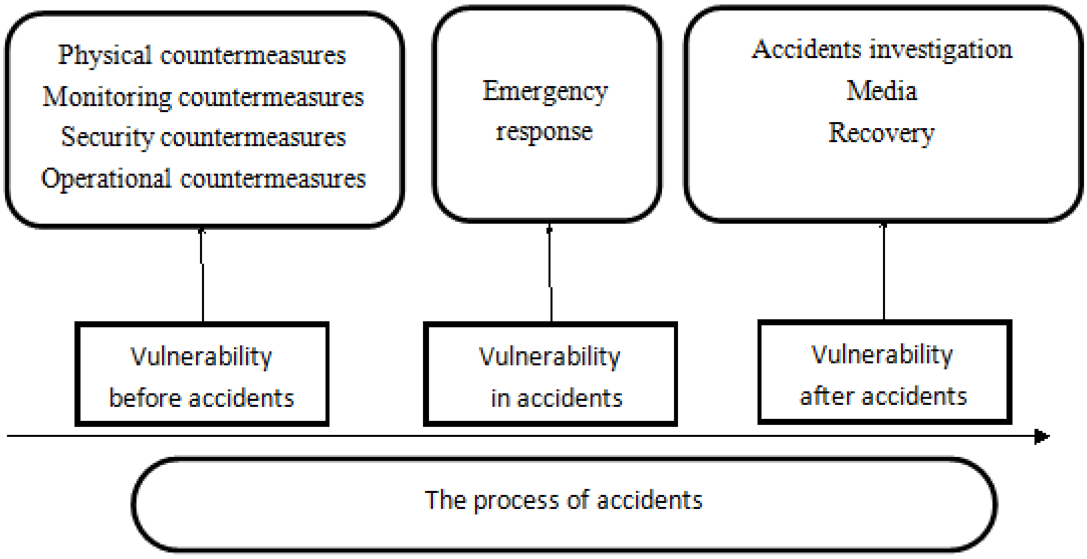

Physical countermeasures
Monitoring countermeasures
Security countermeasures
Operational countermeasures
Emergency response
Accidents investigation
Media
Recovery
Vulnerability before accidents
Vulnerability in accidents
Vulnerability after accidents
The process of accidents

Fig. 3 Vulnerability of different phases

From Fig. 3 we can find that vulnerability before accidents can be expressed by security forces, security of facilities and campsites, information security, access control, personal security & supply chain security. The point is the exposure and sensibility of assets. Vulnerability in accidents mainly considers coping ability of assets and security forces. Vulnerability after accidents needs to consider the resilience of different assets.

Consequence assessment
Human casualties, property Damage, environmental effect, interruption of service, reputation damage, political effect and short or long term situations are the consequences of accidents. Obvious and unconspicuous situations are needed to be taken into consideration. Analyzers need to consider the worst situations of successful attack.

CALCULATE THE RISK LEVEL

After the assessment of threat, vulnerability & consequence, we can give a score to every aspect. The score can be from 1 to 5 according to the extent. For example, if the vulnerability is very high, we can give a score of 5, while the vulnerability is very low, we can give a score of 1. Because all assets have the vulnerability, the score of 0 is nonexistent. In this case, we can define that the score of threat (frequency of attacks, frequency of successful attacks), vulnerability & consequence is from 1 to 5.Then the risk level can be the function of Eq. 2.

$$R=F\ (F1,\ F2,\ V,\ C) \qquad (2)$$

R represents the risk level;
F1 represents the frequency of attacks;
F2 represents the frequency of successful attacks;
V represents vulnerability;
C represents consequence;
All scores are from 1 to 5.
We can simplify the function by multiplying variables, Eq. 3. The highest score is 625, and the lowest score is 1.

$$R= F1\cdot F2\cdot\ V\cdot\ C \qquad (3)$$

Three-dimensional diagram is shown in Fig. 4 in order to express vividly.

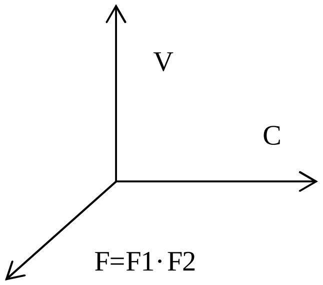


Fig. 4 Three-dimensional diagram of risk

STANDARD

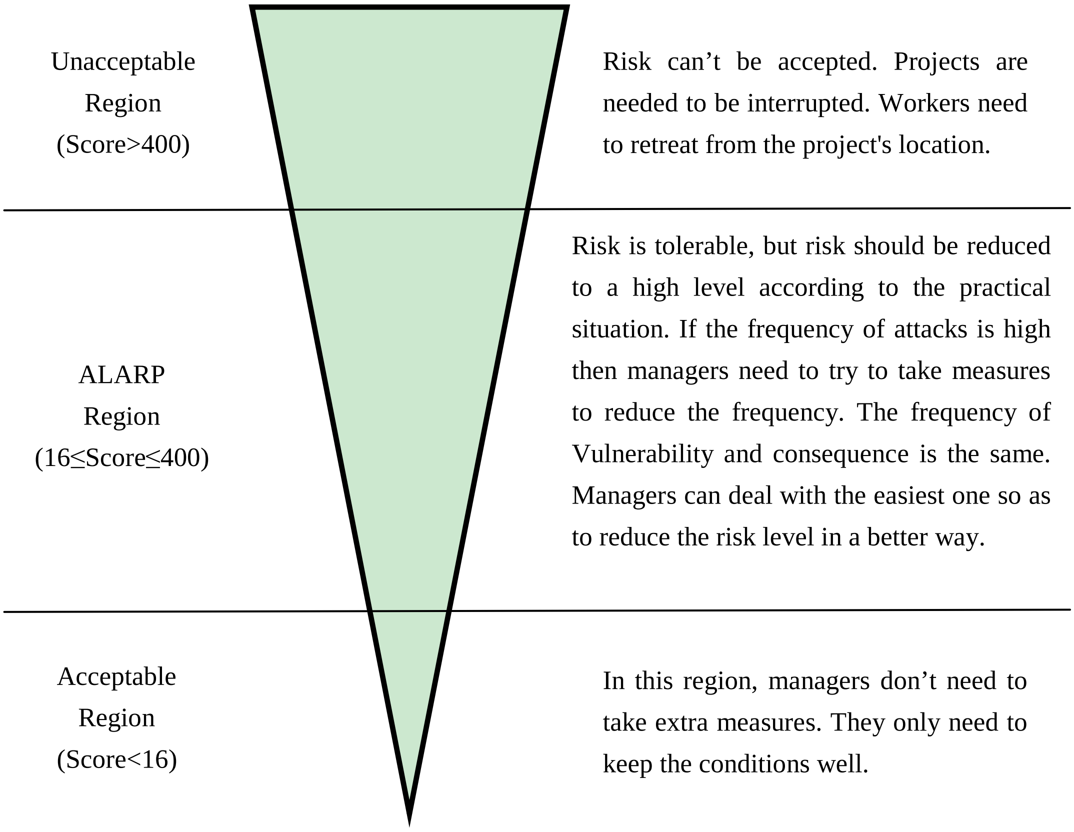
Analyzers have got the score of risk, and they are required to compare with standards. Different countries and different companies own different standards, so we assume that unacceptable risk is the score higher than 400 while acceptable risk is the score lower than 16. In this article, we apply the theory of “As Low As Reasonably Practicable” to help us make judgments (Fig. 5).

Projects lying in unacceptable region i.e high level risk, must be interrupted. Projects that lie in the acceptable region i.e low level risk are required to be maintained with present condition and then the security assessment is completed. The risk levels of most projects are in ALARP region, and managers need to try to reduce the level of risk. So the process of strengthening countermeasures is needed.

STRENGTHEN COUNTERMEASURES

To reduce the risk level and strengthen countermeasures, the following aspects can be focused on. Primarily, we can add more physical safeguards according to the assessment of threat, vulnerability and consequence. Handling methods need to do the following aspects to respond to the attacks of adversaries.

Preparing for the possible attacks in advance.
Preventing the attacks as far as possible, e.g. through the method of deterrence.
Detecting the situation as far as possible if the attacks happen.
Delaying the attacks to wait for the support.
Adopting the countermeasures to react to the attacks.
Recovering from the attack situation as far as possible.



Risk can’t be accepted. Projects are needed to be interrupted. Workers need to retreat from the project's location.

Risk is tolerable, but risk should be reduced to a high level according to the practical situation. If the frequency of attacks is high then managers need to try to take measures to reduce the frequency. The frequency of Vulnerability and consequence is the same. Managers can deal with the easiest one so as to reduce the risk level in a better way.

In this region, managers don’t need to take extra measures. They only need to keep the conditions well.

Fig. 5 ALARP description

The guiding principle of risk disposition is As Low As Reasonably Practicable to make sure that the risk level is under control (Tab. 1).

Tab. 1 Risk disposition methods

Means	Function	Approaches
Risk prevention	Reduce the risk possibility	Control & plan Security and protection system Check and audit Training and education
Risk reduction	Reduce the severity of consequences	Contingency plan Medical and emergency procedures Response plans Firefighting
Risk transfer	Share or transfer the legal responsibility	Dangerous business subcontracts Exclusion clause Outsourcing business Insurance
Risk aversion	Reduce the possibility of loss	Discontinue operation Close devices Sell business

For facilities, materials & personnel, we can take elimination, substitution, reduction, isolation, individual protection, rescue and other measures into consideration (Tab. 2). Also, the idea of reducing the system’s threat, vulnerability and consequence is needed.

Tab. 2 Factors of countermeasures

Factor	Description
Elimination	Eliminate toxic materials, critical assets, projects and so on
Substitution	Substitute manual operation by automated operation, toxic materials by nontoxic materials and so on.
Reduction	Reduce the exposure of personnel, facilities, materials, the reserves of materials and so on.
Isolation	Isolate critical assets with fences, walls, doors, ditches and so on.
Individual protection	Individuals are equipped with PPE, necessary arms & security forces.

As we all know that, the security level is in proportion to safety investment. How to invest costs in security is a problem. Safety investment covers project investment, labor protection and health care investment, emergency rescue investment, safety education investment, daily safety management investment, insurance investment, accident management investment and other related investment. As we all know that, the more investment on safety, the enterprise will be safer. Meanwhile, it may give rise to the waste of resources and cut into the profits (Fig. 6), so the limited investment should be put into the critical aspects. Based on the result of risk assessment, limited investment can be used in carrying out the countermeasures.

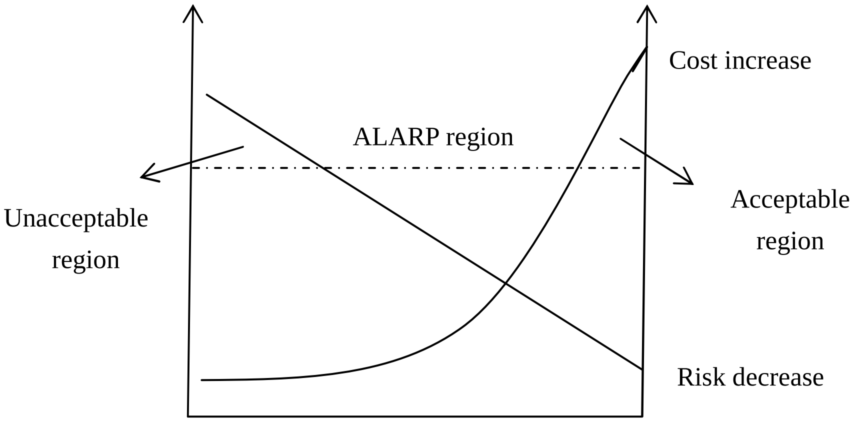


Fig.6 Cost-effectiveness principle

CONCLUSION

The ANSI/API SRA and other publications have done a lot to assess the security in making structured decisions. Owing to all assets with vulnerability, this article combines different periods of vulnerability in the process of security assessment so as to understand all aspects of assets. Swiss cheese model is used in this article to prevent the attacks from adversaries. ALARP theory and cost-effectiveness analysis can help analyzers find out better countermeasures in reducing risk level. Security assessment with the concept of vulnerability can rank the assets and optimize countermeasures according to the risk level to determine which assets need extra protection. Group companies may be in different locations, so a uniform criterion with fixed steps can help to manage, comprehend the risk level obviously and save a lot of time. Also, security assessment can bring confidence to the employees of chemical plants. Managers can adopt the theory of cost-effectiveness to make necessary countermeasures to critical assets in high risk.

Acknowledgments
The authors wish to thank the post-graduate innovation projects of China University of Petroleum (East China) for contract YCX2014043, under which the present work was possible.

REFERENCES

[1] Hoffman B. *Studies in Conflict and Terrorism*, **2002**, 25(5): 303-316.
[2] Pape R A. *American political science review*, **2003**, 97(3): 343-361.
[3] American Petroleum Institute，NPRA. Security vulnerability assessment methodology for the petroleum and petrochemical industries[M].2nd edition. Washington DC：API Publishing Services，**2004**.
[4] Moore D A, Fuller B, Hazzan M, et al. *Journal of hazardous materials,* **2007**, 142(3): 689-694.
[5] Nolan D P. Safety and Security Review for the Process Industries: Application of HAZOP, PHA, What-IF and SVA Reviews[M]. William Andrew, **2011**.
[6] Janssen MA, Schoon ML, Ke WM et al. *Global Environmental Change*, **2006**, 16(3): 240-252.
[7] Adger W N. *Global environmental change*, **2006**, 16(3): 268-281.
[8] Stewart M G. *Journal of Performance of Constructed Facilities*, **2008**, 22(2): 115-120.
[9] Turner B L, Kasperson R E, Matson P A, et al. *Proceedings of the national academy of sciences*, **2003**, 100(14): 8074-8079.