Korean J. Chem. Eng., **27**(2), 399-408 (2010)
DOI: 10.1007/s11814-010-0094-x

Development of a risk assessment program for chemical terrorism

Younghee Lee, Jinkyung Kim, Junghwan Kim, Jiyong Kim, and Il Moon†

Department of Chemical Engineering, Yonsei University, 134 Shinchon-dong, Seodaemun-gu, Seoul 120-749, Korea
(*Received 21 July 2009 • accepted 14 September 2009*)

Abstract−The study focuses on assessing the security risk of the terrorism in the chemical industry. This research modifies conventional risk assessment methods for including terrorism and sabotage scenarios. The objective of this risk assessment is to identify security hazards, threats and vulnerabilities facing each target facility, and to find the adequate countermeasures to protect the public, workers, national interest, environment, and companies. This study results in implementing software to analyze the possibility of terrorism and sabotage. This program includes five steps: asset characterization, threat assessment, vulnerability analysis, risk assessment and new countermeasures. It is a systematic, risk-based approach in which risk is a function of the severity of consequences of an undesired event, the likelihood of adversary attack, and the likelihood of adversary success in causing the undesired event. The reliability of this method is verified by the dock zone case. This study suggests an effective approach to chemical terrorism response management.

Key words: Chemical Terrorism, Risk Assessment, Vulnerability Analysis, Countermeasures, Terrorism Response, Security Analysis

INTRODUCTION

After the 9.11 disaster in New York, we have become more aware of the catastrophic threats posed by toxic chemicals in our communities. While the 9.11 disaster was not directed toward the chemical industry, chemical facilities may pose an attractive target for terrorism, with the purpose of using the effective physical and chemical properties to cause mass casualties, property damage, and economic or environmental impacts. The concept for a "new' form of terrorism has emerged in the 21st century. The attractive targets of terrorists are moved from "hard" to "soft." As a soft target, chemical plants have traditionally remained unprotected against a possible terrorist attack. The chemical industry is faced with new demand to assess whether current security measures effectively address this new and unforeseen threat, and make enhancements as required to provide for the safety of the public, workers, and the environment. Chemical security has to be balanced with other objectives such as economy, and has to be commensurate with the threat and likelihood of occurrence. Consequently, the chemical security management process requires a systematic approach to analyzing the risk of these issues. But most of the current safety management techniques such as SVA, HAZOP, FMEA, FTA, Checklist, PHA, Accident scenario, Monitoring and SMV, deal with only the accidents or minimize the damages in case of natural and intensive events. We have conducted chemical facility terror risk assessment using an SVA methodology. As a result, a new risk assessment method is developed and it is implemented as software to analyze the possibility of terrorism and sabotage.

SECURITY VULNERABILITY ANALYSIS (SVA) METHODOLOGY

The American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) developed the security vulnerability assessment methodology (SVA) available to the petroleum and petrochemical industry in 2003. The first step in the process of managing security risk is to identify and analyze the threat and the vulnerabilities facing a facility by conducting an SVA. The SVA is a systematic process that evaluates the likelihood that a threat against a facility will be successful. The SVA process is a systematic approach that combines the multiple skills and knowledge of the various participants to provide a complete security analysis of the facility and its operations. Depending on the type and size of the facility, the SVA methodology may include individuals with knowledge of physical and cyber security, process safety, facility and process design and operations, emergency response, management and other disciplines as necessary. The objective of conducting an SVA is to identify security hazards, threats, and vulnerabilities facing a facility, and to evaluate the countermeasures to provide for the protection of the public, workers, national interests, the environment, and the company. With this information, security risks can be assessed and strategies can be formed to reduce vulnerabilities as required. SVA is a tool to assist management in making decisions on the need for countermeasures to address the threats and vulnerabilities.

1. Asset Characterization

The asset characterization includes analyzing the technical information on facilities and public utilities as required to support the analysis, identifying the potential critical assets, identifying the hazards and consequences of concern for the facility or public utility and its surroundings and supporting infrastructure, and verifying the existing layers of protection. A consideration of possible chemical terrorism threats should include internal threats, external threats, and internally assisted threats. The available threats are chosen according to reasonable local, regional, or national situation. This step results in the attractiveness of the target each asset from each adversary's perspective.

For each asset identified, the criticality of each asset must be understood. This is a function of the value of the asset, the hazards of

†To whom correspondence should be addressed.
E-mail: ilmoon@yonsei.ac.kr

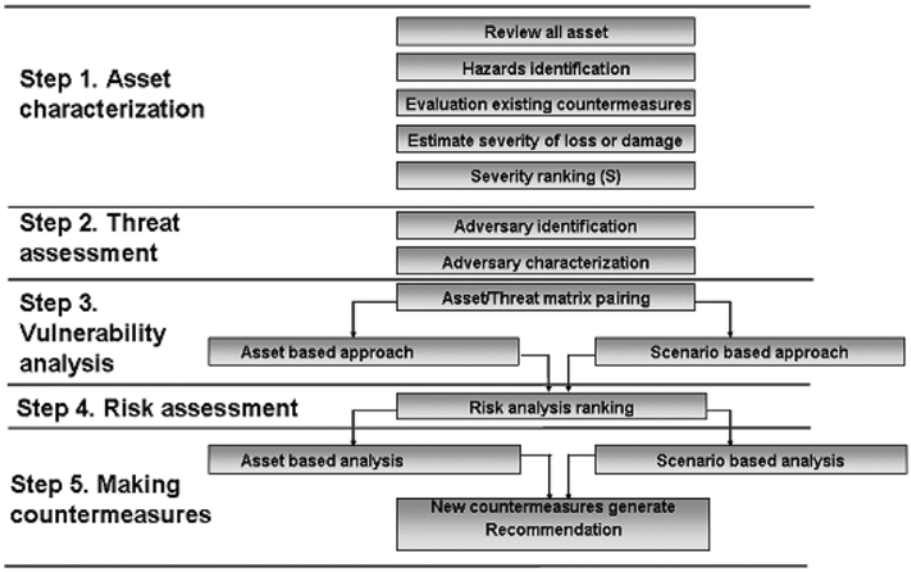

Fig. 1. Overall security vulnerability analysis methodology (API 2003).

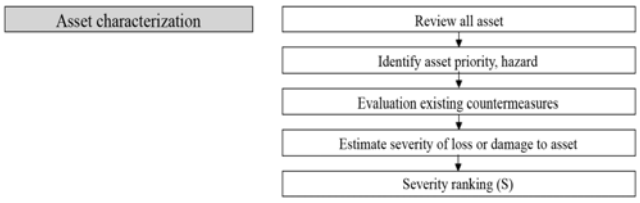

Fig. 2. Asset characterization process.

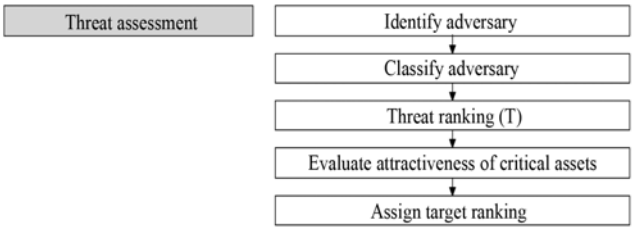

Fig. 3. Threat assessment process.

the asset, and the consequences if the asset was damaged, stolen, or misused. For hazardous chemicals, consideration includes toxic exposure to workers or the community, or potential for the misuse of the chemical to produce a weapon or the physical properties of the chemical to contaminate a public resource. This methodology uses ranking systems that are based on a scale of 1-5 where 1 is the lowest value and 5 is the highest value. Based on the consequence ranking and critical of the asset, the asset is tentatively designated a candidate critical target asset. The attractiveness of the asset is used for screening important assets.

2. Threat Assessment

This step is to identify specific classes of adversaries that may be responsible for the security-related events. It identifies specific classes of adversaries that may be responsible for the security-related events. Depending on the threat, we can determine the types of potential attacks and, if specific information is available on potential targets and the likelihood of an attack, specific countermeasures may be taken.

The threat assessment evaluates the likelihood of adversary activity against a given asset or group of assets. It is a decision support that helps to establish and prioritize the security-ranking system. The threat assessment identifies and evaluates each threat on the basis of various factors, including capability, intention, and impact of an attack.

Types of target are defined as follows:

· Usefulness of the process material as a weapon
· Proximity to national asset or landmark
· Ease of access (soft target)
· High company reputation and brand exposure
· Symbolic target
· Chemical weapons precursor chemical
· Reorganizations of the target

Types of effect are defined as follows:

· Potential for causing casualties
· Potential for causing damage and loss to the facility and company
· Potential for causing damage and loss to the geographic region
· Potential for causing damage and loss to the national infrastructure

Attractiveness factors ranking definitions are:

1-Very Low: Adversary would have no level of interest in the asset
2-Low: Adversary would have some degree of interest in the asset
3-Medium: Adversary would have a moderate degree of interest in the asset
4-High: Adversary would have a high degree of interest in the asset
5-Very High: Adversary would have a very high degree of interest in the asset

3. Vulnerability Analysis

The vulnerability analysis includes the relative pairing of each target asset and threat to identify potential vulnerabilities related to pro-

cess security events. This involves the identification of existing countermeasures and their level of effectiveness in reducing those vulnerabilities.

When we determine how an event can be induced, it should determine how an adversary could make it occur. There are two kinds of methodologies: the accident scenario-based approach and the asset-based approach. Both approaches are identical in the beginning, but different in the degree of the detailed analysis of threats scenarios and specific countermeasures applied to a given scenario. The first is to define accident scenarios and evaluate specific consequences by using scenario and the asset-based analysis to document the adversary's potential actions against an asset. The existing risk response measure is identified to protect the critical assets, and we estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary. The degree of vulnerability of each valued asset and threat pairing is finally evaluated by the formulation of security-related scenarios and by the asset protection basis. When certain criteria are met, such as higher consequence and attractiveness ranking values, it is useful to apply an accident scenario-based approach to conduct the vulnerability analysis. It covers the assignment of risk rankings to the security-related scenarios. When the asset-based approach is used, the determination of the asset's consequences and attractiveness is enough to assign a target ranking value and protection via a standard protection set for the target level. In this case, scenarios may not be developed further than the general thought that an adversary is interested in damaging or stealing an asset.

4. Risk Assessment

The next step is to determine the level of risk of the adversary exploiting the asset according to the existing security countermeasures. The risk assessment determines the relative degree of risk for the facility and the public utility in terms of the expected effect on each critical asset as a function of consequence and probability of occurrence. Using the assets identified during the asset characterization, the risks are prioritized based on the likelihood of a successful terrorism. Likelihood is determined after considering the attractiveness of the target assets, the degree of threats and vulnerability.

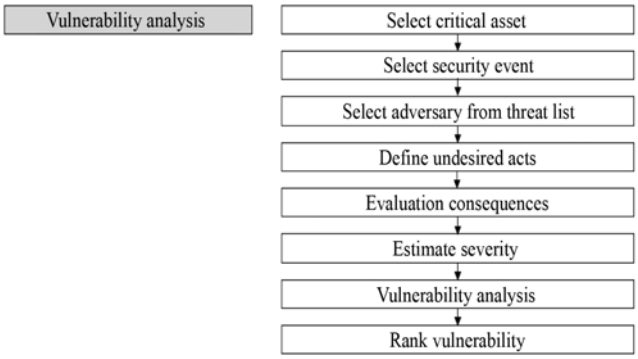

Fig. 4. Vulnerability analysis process.

Risk matrix		Severity				
		1	2	3	4	5
Frequency	1	R1	R2	R3	R4	R5
	2	R2	R4	R6	R7	R8
	3	R3	R6	R7	R8	R9
	4	R4	R7	R8	R9	R10
	5	R5	R8	R9	R10	R10

Fig. 6. Risk ranking matrix.

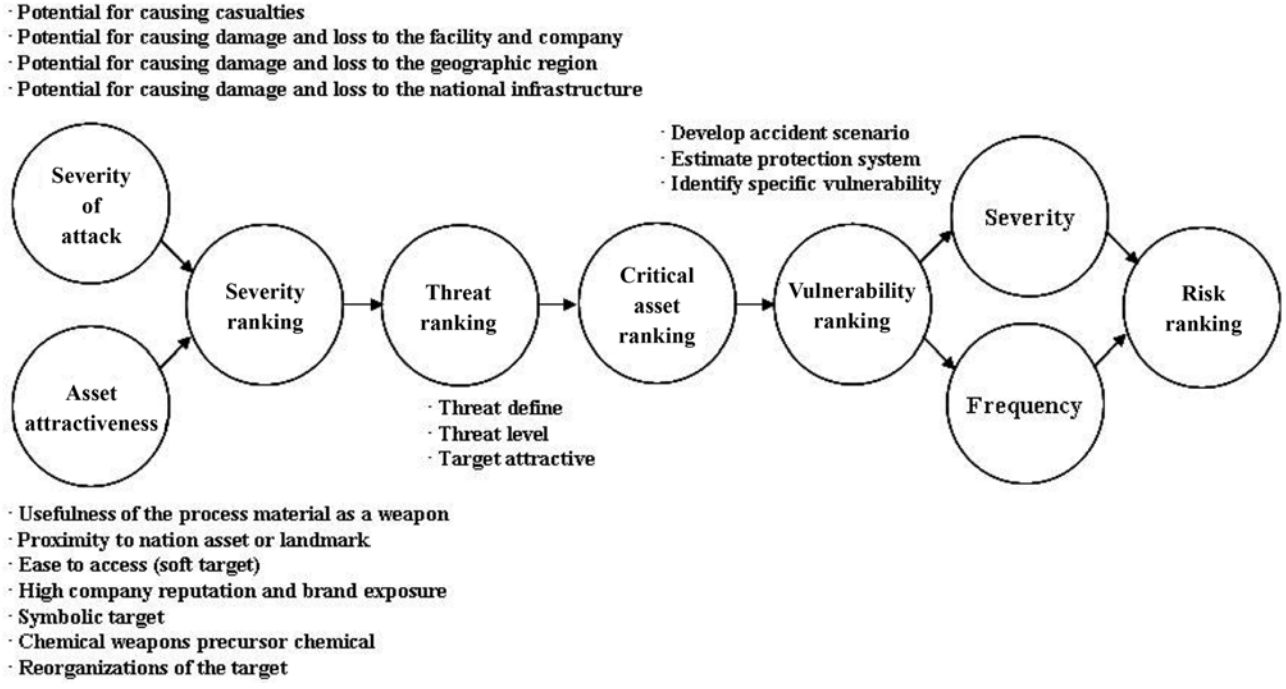

Fig. 5. Overall risk ranking.

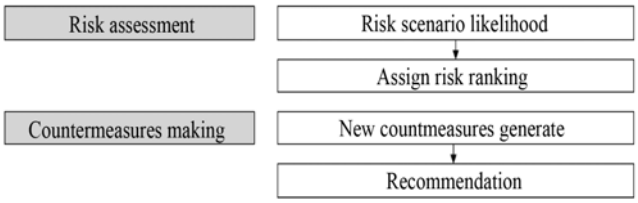

Fig. 7. Risk assessment and countermeasures building process.

COUNTERMEASURES MAKING

The countermeasures analysis identifies shortfalls between the existing security and the desirable security where additional recommendations are justified to reduced risk. An appropriate enhanced countermeasure option is identified to further reduce vulnerability at the facility. The improved countermeasures present the following index: the process security doctrines of deter, detect, delay, response, mitigate and possibly prevent.

The factors in this step to be considered are;
· Reduced probability of successful attack
· Degree of risk reduction by the options
· Reliability and the maintainability of the options
· Capabilities and the effectiveness of mitigation options
· Costs of mitigation options
· Feasibility of the options

The countermeasure options are re-ranked to evaluate effectiveness, and prioritized to assist management decision making.

IMPLEMENTATION

This system is implemented in commercial software. The fields in the program are completed as follows:

a. Asset: The asset under consideration is documented. User selects form the targeted list of assets and considers the scenarios for each asset in turn based on priority.

b. Security Event Type: This column is used to describe the general type of malicious act under consideration.

c. Threat Category: The category of adversary including terrorist and disgruntled employee.

d. Undesired Act: A description of the sequence of events that would have to occur to branch the existing security measures is described in this column.

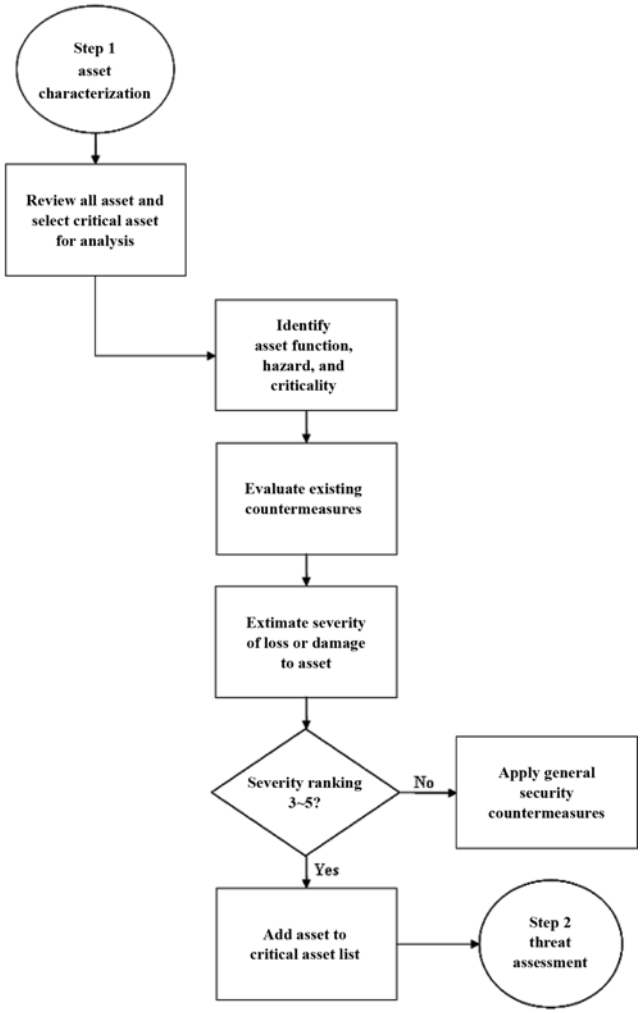

Fig. 8. Terror risk assessment algorithms I.

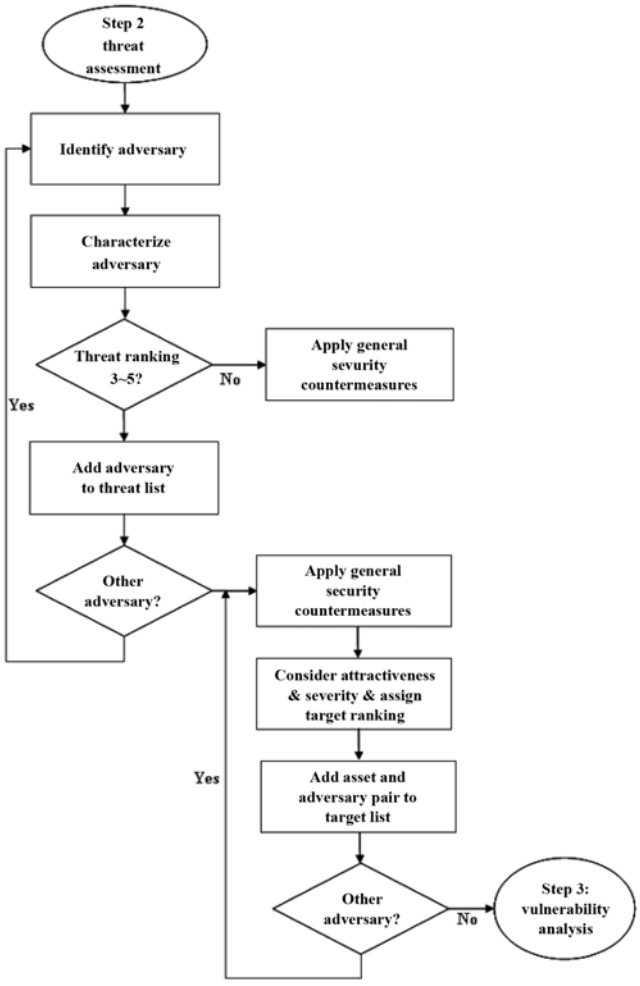

Fig. 8. Terror risk assessment algorithms II.

e. Consequences: Consequences of the event are analyzed and entered into the consequence column of the worksheet. The consequences should be conservatively estimated given that the intent of the adversary is to maximize their gain. Users are encouraged to understand the expected consequence of a successful attack or security breach by this column.

f. Existing Countermeasures: The existing security countermeasures that relate to detecting, delaying, or deterring the adversaries from exploiting the vulnerabilities are listed in this column.

g. Vulnerability: The specific countermeasures that would need to be circumvented or failed should be identified.

h. Vulnerabilities Level: The degree of vulnerability to the scenario rated on a scale of 1-5.

i. Risk Ranking: The severity and likelihood rankings are combined in a relational manner to yield a risk ranking.

j. New Countermeasures: The recommendations for improved countermeasures that are developed are recorded in the recommendation column.

CASE STUDY

The case is a dock zone including a storage farm, a manufacturing plant, an electrical supply utility, a hydrotreater unit, many containers, and an administration building. It is an attractive target because of environmental release, combustible liquids fire and explosion hazard, easy access, many toxic hazard chemicals, possibility to shutdown if electrical supply unit were damaged, public impact, business interruption, etc.

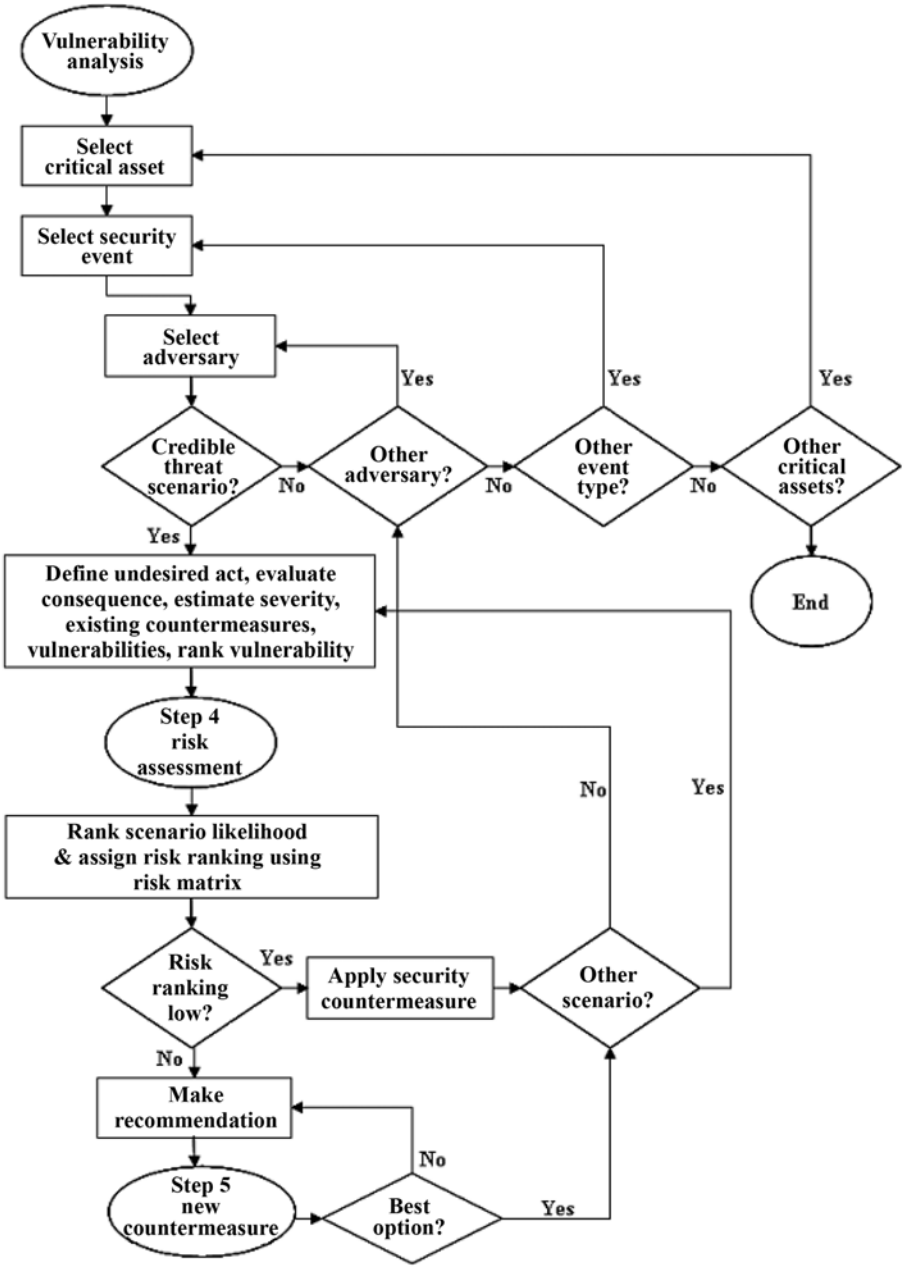

Fig. 8. Terror risk assessment algorithms III.

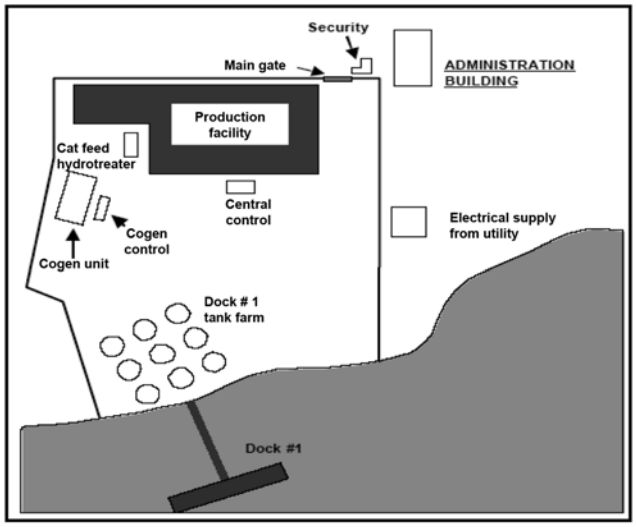

Fig. 9. Case study (dock zone facility).

We considered these vulnerabilities of each facilities and the overall zone.

1. Asset Characterization

This step determines the criticality and hazard of major facilities. The first, existing countermeasures of facility identify. And similar assets within a facility with similar location on the property, vulnerabilities and common consequences can be grouped for efficiency and to consider the value of an entire hazard function. The second, hazard, criticality of major assets is described and risk and consequences that would be realized if the asset was damaged, destruction, or stolen. Finally, rank estimating of the overall severity of the loss of asset.

■ Administration Building - Administrative offices including management offices and large number of employees, HR Manager; ordinary office building hazards; personnel exposure to approximately 100 persons; possible loss of personnel and/or critical documents in storage (business sensitive information).

■ Central Control Room - Critical security communications and monitoring; Cat, Coker 1, Alkylation, Treating Plant; Crude Units; loss of control function and long time to repair if damaged.

■ Cogen Unit and Control Room - Critical steam production and supplemental electrical power generation.

■ Dock 1 - Loss of logistics for feedstock and products; environmental release; fire and explosion; possible to shutdown channel; Coker feed, fuel oil, benzene, toluene, molten sulfur in storage; Coker feed is most critical feedstock.

■ Dock 1 Tank Farm-storage in atmospheric tanks north of Dock 1 - Flammable and combustible liquid fire and explosion hazard; possible spill to ship channel; critical to operation of marine terminal.

■ Cat Feed Hydrotreater Unit - Significant fire and explosion hazard onsite; possible public impacts from explosion; significant business interruption.

■ Electrical supply from Utility to Refinery - Utility supplied; Cat Feed HT, H2 plant, and Units 29-5; backup supply from other substations.

■ Units 29-35 cooling tower/chlorine containers - Important to operation of units 29-35; chlorine toxic hazards may have public impact if damaged.

2. Threat Assessment

Threat information is important data to allow the employers to understand the adversaries interested in the assets of the facilities, their operating history, methods, capacities, and why they are motivated.

Include consideration in this step

1. The source of the attack (external, internal)
2. General types of adversaries (terrorism, sabotage, disgruntled employee etc.)

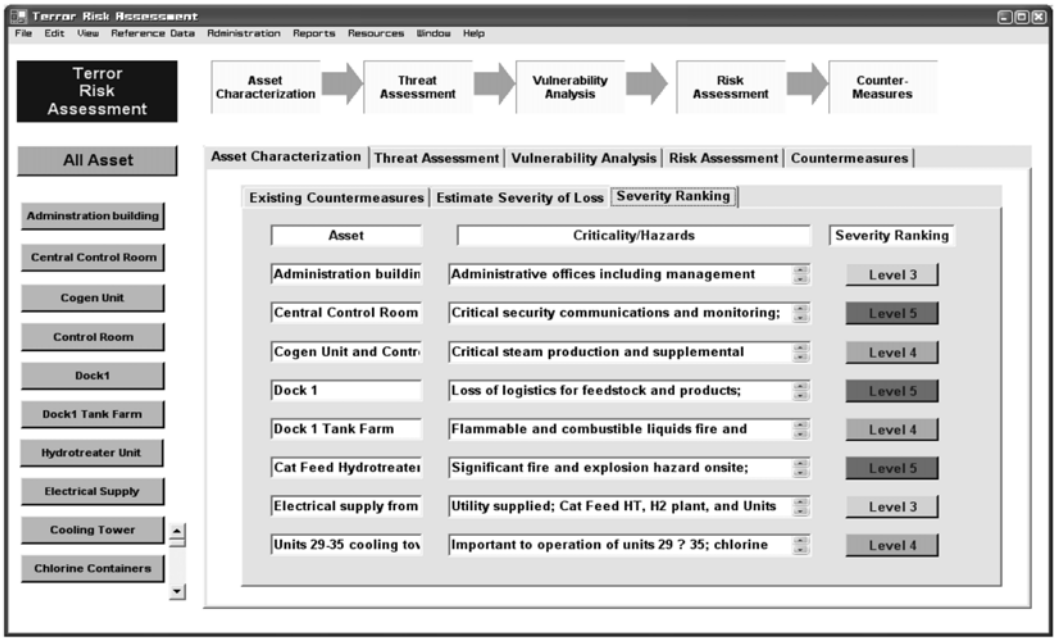

Fig. 10. Severity ranking of dock zone.

3. Evaluation of asset's attractiveness
4. Ranking assessment per the threat ranking scale or equivalent
5. The target ranking is used to judge the degree of attractiveness of the target considering all the adversaries.

■ Terrorist - Use explosives or small arms to destroy target and may be interested in theft of products of value to terrorist organizations for secondary attack. Also use of improvised explosive device possibly involving a vehicle is most likely scenario

■ Disgruntled employee or contractor - Might cause intentional overfill of tank or damage to equipment leading to release and possible for workplace violence, theft. Not likely to use weapons if sabotage but may use small arms if workplace violence

■ Activist - Possibly interested in causing public embarrassment; temporary shutdown of plant; long range goal of elimination of toxic substance in use. And highly organized; well funded to cause staged attack of multiple facility operations simultaneously (dock, rail, gate)

● Critical assets

1. Administration building - Possibly interested in seeking out management for protest but not accessible directly and business services building is more accessible.

● Central control room - Not easily accessible; does not provide opportunity for media attention and requires trespassing.

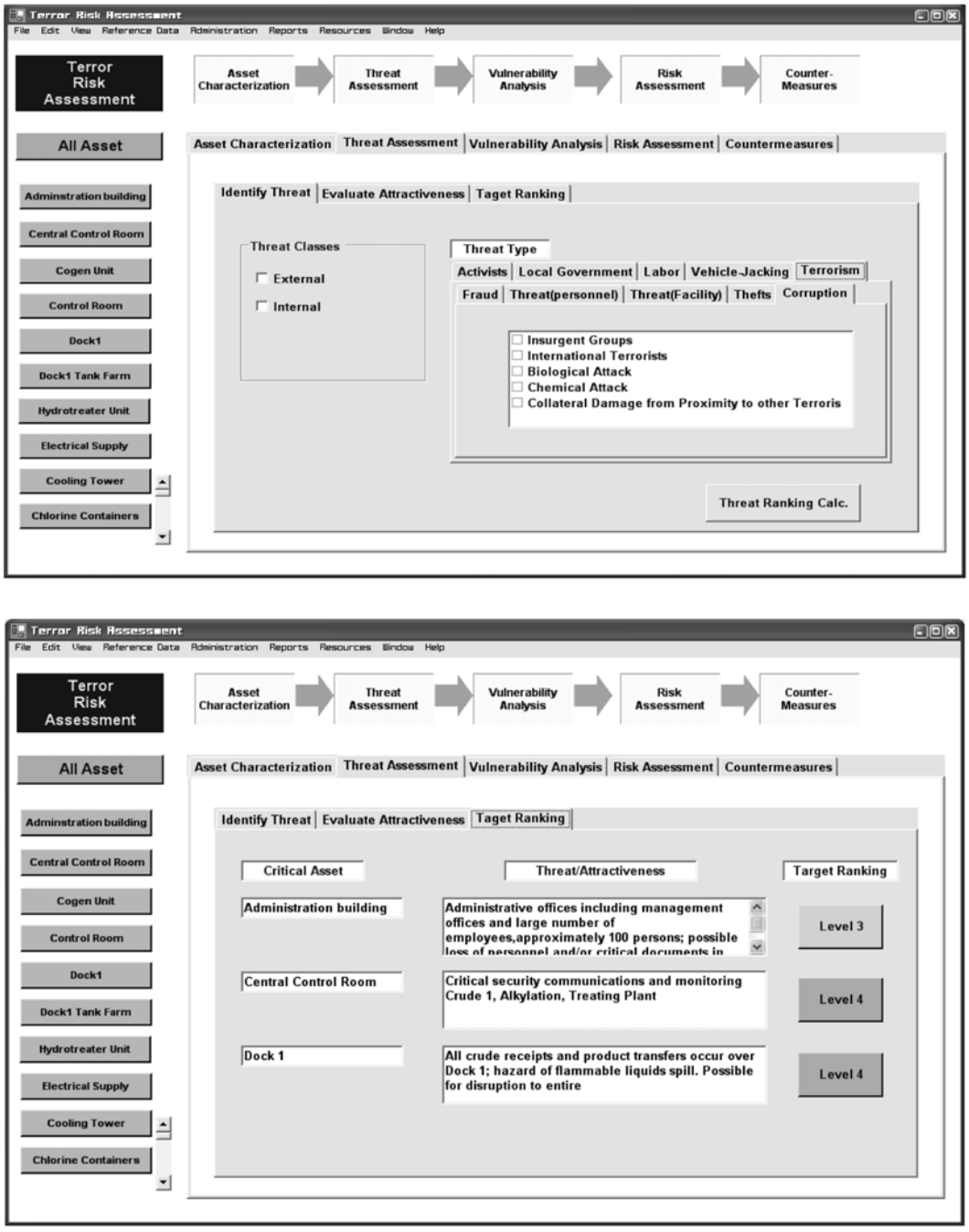

Fig. 11. Identify threat and Target ranking form.

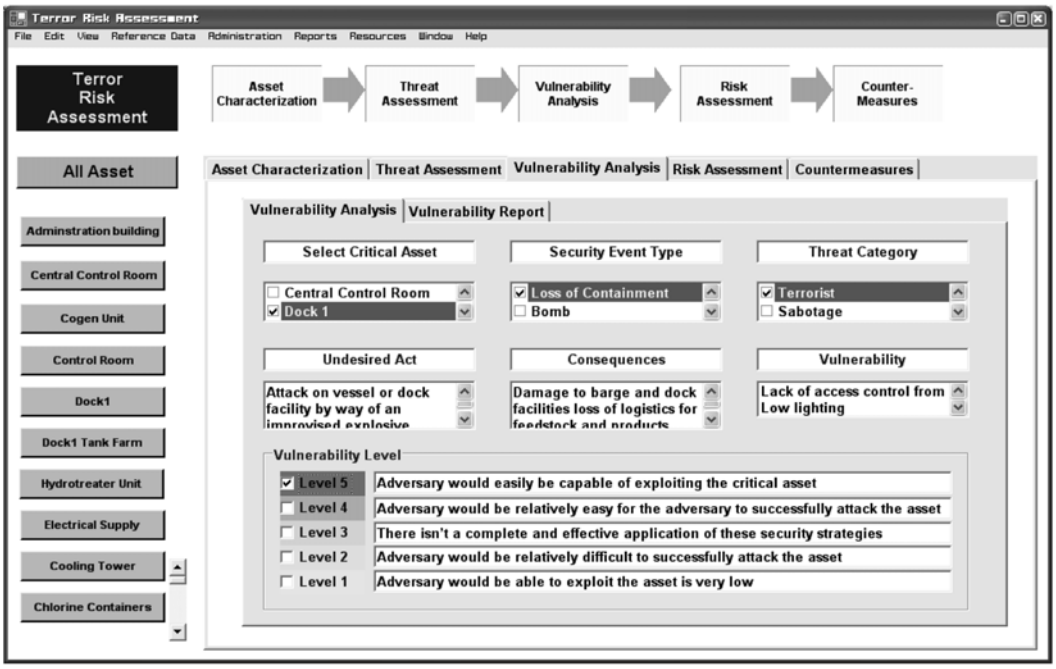

Fig. 12. Vulnerability analysis form.

Asset: Dock1

Scenario worksheet form										
Security event type	Threat category	Undesired act	Consequences	s	Existing countermeasures	Vulnerability	Vulnerability ranking	L	R	New countermeasures
Bombing	Terrorist	Attack on vessel or dock facility by way of an improvised explosive device	Damage to barge and dock facilities; Major environmental release; fire and explosion; possible to shutdown channel	S5	Boat patrols of the channel and port	1. Lack of access control from water, 2. Low lighting 3. No intrusion detection	5	L4	Very high	Consider improving lighting, access control, monitoring by CCTV, and administrative controls per requirements

Asset: Central Control Room

Scenario worksheet form										
Security event type	threat category	Undesired act	Consequences	s	Existing countermeasures	Vulnerability	Vulnerability ranking	L	R	New countermeasures
Infiltration or degradation of assets	Disgruntled employee	Reveal of insider information on process control and access	Unauthorized control of facility; Loss of critical data; Disruption to company operation	S5	CCTV ID Card	1. Lack of access network system 2.A few guards 3.Relative easy of insider crime	5	L2	Mid	1.Controlling access in-out 2.Package screening system 3.Security personnel

Asset: Administration building

Scenario worksheet form										
Security event type	threat category	Undesired act	Consequences	s	Existing countermeasures	Vulnerability	Vulnerability ranking	L	R	New countermeasures
Gas scattering	Terrorist	Toxic gas was scattered throughout an extractor fan.	About 100 person exposed toxic gas. asphyxy; hallucination; having fever;	3	ERP(emergency response plan); CCTV	Lack of chemical & bio terror response plan; Lack of emergency treatment;	4	L3	High	Chemical & bio terrorism response plan. Monitoring the security of the vulnerability site.

● Dock 1 - Could be easily accessible by watercraft; provides opportunity for media attention; activists against dock in past.

3. Vulnerability Analysis

This step involves making a vulnerability analysis report throughout selected critical asset, security event type, threat category, undesired act, consequence etc. In the case of Dock 1, there is a lack of access control from low lighting. So the adversary would easily be capable of exploiting the critical asset.

4. Risk Assessment

Severity level involves estimating the severity of loss of life, asset, environment, community and national economy. Risk ranking level is also determining the severity ranking and possibility of occurrence by matrix method. If terrorism is successful in the dock facility, the damage to the economy and environment is very high. Because ship accidents associated with terrorism occur once every 5 years, the possibility of occurrence is very high.

5. New Countermeasure

Finally, this step proposes new countermeasures against the vulnerability of a critical asset. New countermeasure options would be identified to further reduce vulnerability at the facility. These include improved countermeasures of the process security doctrines of deter, detect, delay, respond, mitigate and possibly prevent.

- Restricted area within the facility
- Handling unaccompanied baggage
- Controlling access ingress and egress
- Package screening system
- Hardening process preventing and controlling releases of hazardous materials
- Emergency response, crisis management.

CONCLUSIONS

A risk assessment is developed and it is implemented as software to analyze the possibility of terrorism and sabotage. This program is applied to a case (a dock field). The result reports the following 10 indexes: asset, security event type, threat category (terrorist and sabotage), undesired act(a description of the sequence of events that would have to occur to breach the existing security meas-

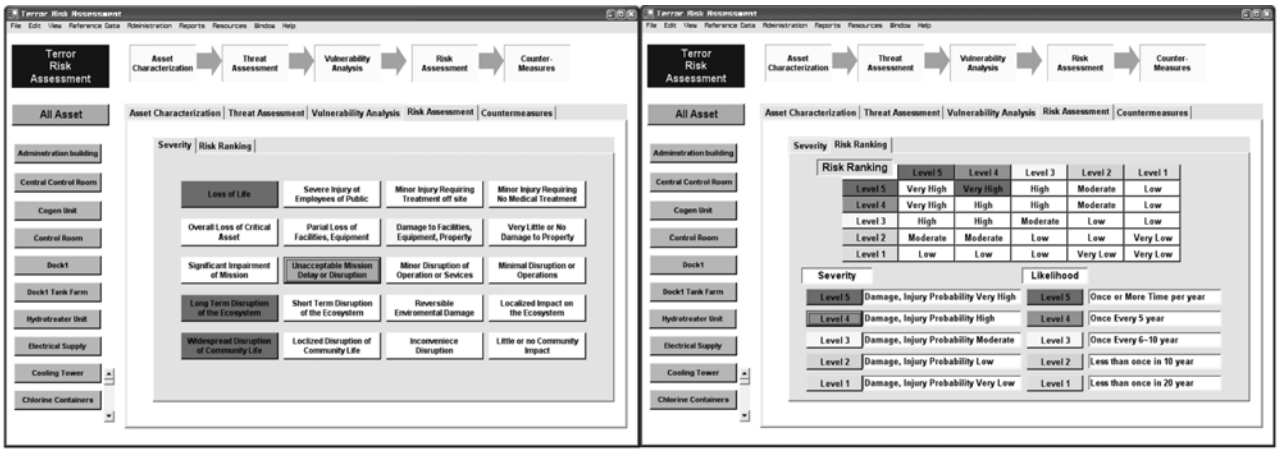

Fig. 13. Risk assessment form.

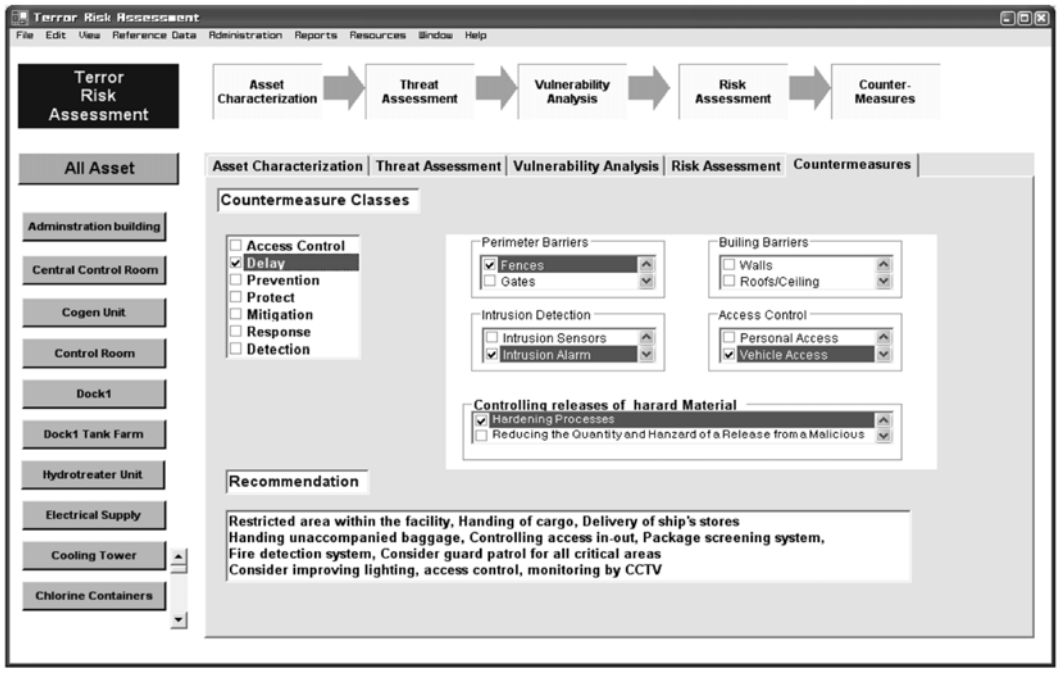

Fig. 14. New countermeasure form.

ures), consequences, existing countermeasures, vulnerability, vulnerability ranking, degree of risk (the severity and the likelihood rankings are combined in a relational manner), and new countermeasures. This paper presents a chemical terrorism response technology, a prevention plan and new countermeasure by using risk and vulnerability assessment method in the chemical industry and the public utility. This study suggests an effective approach to the chemical terrorism response management in decision making.

ACKNOWLEDGMENT

The authors acknowledge the financial support of the Ministry of Education through the second stage Brain Korea 21 Program at Yonsei University.

REFERENCES

1. D. Kim, I. Moon, Y. Lee and D. Yoon, *Journal of Loss Prevention in the Process Industries*, **16**, 121 (2003).
2. S. Bajpai and J. P. Gupta, *Journal of Loss Prevention in the Process Industries*, **18**, 301 (2005).
3. C. Jochum, *Process Safety and Environmental Protection*, **83**, 459 (2005).
4. M. Sam, *Chemical security*, Lees' loss prevention in the process industries (third edition), Butterworth-Heinemann, Burlington, 1-8 (2005).
5. V. Sutton and D. A. Bromley, *Technology in Society*, **27**, 263 (2005).
6. J. C. Laul, F. Simmons, J. E. Goss, L. M. Boada-Clista, R. D. Vrooman, R. L. Dickey, S. W. Spivey, T. Stirrup and W. Davis, *Journal of Chemical Health and Safety*, **13**, 6 (2006).
7. D. A. Moore, *Journal of Hazardous Materials*, **130**, 107 (2006).
8. S. Bajpai and J. P. Gupta, *Process Safety and Environmental Protection*, **85**, 559 (2007).
9. R. W. Phifer, *Journal of Chemical Health and Safety*, **14**, 12 (2007).
10. S. C. Patel, J. H. Graham and P. A. S. Ralston, *International Journal of Information Management*, **28**, 483 (2008).