Journal of Integrated Security Science
©Delft University of Technology

JOURNAL OF
INTEGRATED
SECURITY
SCIENCE

Editors-in-Chief
Nima Khakzad
Genserik Reniers
Pieter van Gelder

ISSN: 2468-4546

TUDelft

Vulnerability and Security Risk Assessment of a Thermal Power Plant Using SVA Technique

Abbas Sadeghi[1], Mousa Jabbari[1,*], Ali Alidoosti[2], Mohsen Rezaeian[3]

1. Department of Industrial Safety Engineering, School of Health, Safety and Environment, Shahid Beheshti University of Medical Sciences, Tehran, Iran, Sadeghi_osh@yahoo.com

2. Crisis Management Research Center, Malek-e-Ashtar University of Technology, Tehran, Iran, a_alidoost@yahoo.com

3. Department of Mechanical Engineering, School of Mechanical Engineering, Amir kabir University of Technology, Tehran, Iran, Rezaeian@aut.ac.ir

Received 30 September 2016
Accepted 1 February 2017

In the present study, vulnerability and security risk of a combined cycle power plant using Security Vulnerability Assessment (SVA) technique in a computer aided software has been estimated. In general, 17 assets were identified in the under study facility of which 13 assets with high and extreme risk priority through Security Risk Factor Table (SRFT) were determined. These 13 assets for further analysis on vulnerability and possible threats were entered into the software Joshan-Pro. Subject matter experts used to score threat, consequence and vulnerability for each asset, qualitatively. For each asset, associated checklists within the software helped the participant experts with safety, security, process, management, IT, maintenance, etc. experience and knowledge to determine vulnerability and other security risk factors. Therefore, security risk for each asset by multiplying threat, consequence and vulnerability scores was calculated and to reduce the risks and vulnerabilities, countermeasures were proposed.

Keywords: Security risk; Security Vulnerability Assessment; Power plant

1. Introduction

The philosophy behind the creation of every organization or facility is bound up with the objectives for each it has been created. There are always factors threatening the continuation of the organization’s activities or even its existence. Some of these factors involve common threats in the field of security and deliberate incidents. Unfortunately, war, terrorism, theft and vandalism are the bitter realities of human life and today world. Prior to 11 September 2001 attack in USA, the risk assessment in the industries was based on assessment and evaluation of unintentional incidents due to human errors, technical failures or natural disasters while the human intelligence to occurring deliberate sabotages was ignored. The 9/11 terrorist attack, mainly has changed this perspective (Bajpai and Gupta, 2007; Reniers et al., 2008, 2013; van Staalduinen et al., 2016).

Infrastructures and critical facilities such as governmental organizations, airports, military bases, power plants and oil & gas industries due to their importance and significant roles which playing in many aspects of country’s consistency such as economy, politics, psychology, health and

[*] Corresponding author.
Email address: Jabbarim@sbmu.ac.ir

DOI: 10.18757/jiss.2017.1.1390
ISSN: 2468-4546

welfare are the attractive targets to terrorists, criminals and saboteurs. Therefore, it is imperative that these undesired threats through a systematic security risk management process should be identified, their associated risks should be assessed and appropriate security countermeasures and emergency response must be devoted to reduce the risks and vulnerabilities (Akgun et al., 2010; Bajpai et al., 2007 & 2010). Many studies have been conducted with regards to the security and vulnerability analysis in infrastructures and critical facilities. Among them, Moore (2004), explained a new pattern of security risk management for chemical industries which investigates the differences in the interpretation of the security risk against the risk of process accidents and the challenges ahead. Bajpai and Gupta (2005) argue that from methodology point of view, security risk assessment is necessary for process industries, including the threat assessment, vulnerability assessment, security measures and emergency response in emergency situations. The study revealed that the most serious terrorist threats are directed towards chemical transportation system (road, rail, ships, pipelines, etc.). Reniers et al. (2008) a theoretical approach to manage intentionally induced domino effects in a complex industrial cluster have introduced. Srivastava and Gupta (2010) presented a new model for evaluating security risk in the oil and gas and other process industries that includes both the idea of a Security Risk Factor Table (SRFT) and a Stepped Matrix Procedure (SMP). Researchers also highlighted the need for announcing the news and information related to terrorist threats. Using a Delphi technique, Esmaeeli Shahrokht and Taghvayee (2011) presented a method for assessment of city vulnerability and influencing security issues. Yazdani et al. (2012) introduced a developed framework to overcome the limitations of traditional methods of security risk assessment for vital facilities. The introduced framework develops the RAMCAP through the introduction of new parameters that affect the rate of the risk. In another study, Jamshidi et al. (2012) introduced the software Joshan-Pro to assess the security vulnerability caused by man-made incidents in southern oil islands in the Middle East. Van Staalduinen et al. (2016) a security vulnerability assessment, prevention and prediction (SVAPP) model proposed. The authors adapted safety barriers approach to security facet and a probabilistic security attack barrier approach through Bayesian updating technique to reduce the uncertainty in the proposed model.

The current study conducted in a combined cycle thermal power plant. Power plants producing electrical energy considered as infrastructures in every country; so that it is required to be evaluated in terms of security issues and adverse man-made events. Appropriate measures also must be taken into account to reduce the vulnerabilities and security risks in such these facilities. SVA technique was used to estimate vulnerability and security risk of the critical assets in the under study facility. Section 2 describes the security risk management, its definition and process. Furthermore available security risk assessment techniques, as well as theirs pros and cons mentioned. Section 3, explores SVA technique and its process and steps. Section 4, represents software Joshan-Pro and its application to accomplish SVA. Section 5 has been devoted to initial screening of the identified assets. Section 6 expresses types of threats in a thermal power plants. The results being discussed in Section 7. Conclusions are provided in Section 8.

2. Security risk assessment

A security risk is defined as ‘‘the likelihood that a defined threat will exploit a specific vulnerability of a particular attractive target or combination of targets to cause a given set of consequences’’ (CCPS, 2010; Reniers et al., 2008).
Indeed, American Petroleum Institute (API) defines security risk as “a function of consequences of a successful attack against an asset and likelihood of a successful attack against that asset”. It also, expresses “Likelihood is a function of the attractiveness to the adversary of the asset, the degree threat of posed by the adversary and the degree of vulnerability of the asset” .Thus, to determine security risk for every asset in the facilities, the likelihood, consequence, attractiveness, threat and vulnerability of each asset in case of security issues should be determined (API/NPRA, 2003).
Several security risk analysis techniques/tools have been developed. Some most important of which are security vulnerability assessment (SVA) (API/NPRA, 2003; API, 2005), Risk Analysis Methodology for Critical Asset Protection (RAMCAP) (Al Mannai, 2008; Moore, 2007; Nickell, 2004), Critical Accessibility Recoverability Vulnerability Espy ability Redundancy (CARVER) (Al Mannai, 2008), Maritime Security Risk Assessment Methodology(MSRAM) (Al Mannai, 2008; Downs, 2007), Transit Risk Assessment Methodology (TRAM) (Al Mannai, 2008) and Model-Based Risk Assessment (MBRA) (Al Mannai, 2008; Lewis et al., 2006). Each tool has its respective strengths and weaknesses. (Al Mannai, 2008) has described capabilities and disabilities of every each of outlined tools which is listed in Table 1.

Table 1. Comparison of security risk analysis techniques (Al Mannai, 2008)

Factors	Tools				
	RAMCAP	CARVER	MSRAM	TRAM	MBRA
Generality	All sectors	All sectors	Ports	Transportation	All sectors
Network model	Asset level	Asset level	Asset level	Asset level	Network
Risk calculation	No	No	Yes	Yes	Yes
Resource allocation	No	No	No, asset level	No, asset level	Yes, network level
Repeatable	No	No	No	No	Yes

Based on Al Mannai key factors of the mentioned tools having explained as following:

- Generality refers to the tool’s ability to assess infrastructure in any of the sectors, not just one or two specific ones.
- Network model refers to the tool’s ability to consider the network attributes of a sector.
- Risk calculation refers to whether or not the tool calculates risk using the approved security risk equation.
- Resource allocation refers to whether or not the tool is able to directly inform the allocation of resources to the assets.
- Repeatable refers to whether or not two analysts using the same descriptive data will come up with the same result (Al Mannai, 2008).

3. Security vulnerability assessment (SVA)

Security vulnerability is defined as any weakness or deficiency that can be exploited by terrorists or criminals to damage to the assets. Vulnerabilities not only included the building characteristics or equipment properties which are known as assets generally but also comprises personnel behavior, locations of people or operational and personnel activities (CCPS, 2010). On the other hand, (Reniers et al. 2015) categorizes assets as: people, property and infrastructure, reputation and information. Thus, asset refers to the vast range of resources in an organization/facility which has to be protected against undesired deliberate incidents. However, security vulnerability assessment of infrastructures is a challenging issue because such facilities are complex in terms of topology and function (Akgun, 2010). Nevertheless, SVA is considered as the significant and preliminary step versus deliberate acts in the security risk management process (API/NPRA, 2003; Garrick et al., 2004; Sarewitz et al., 2003).

SVA is a systematic and integrated approach to identify deliberate man-made threats, assess vulnerabilities of the assets and determine the likelihood and consequences of these types of adverse events (API, 2005; Reniers et al. 2015). It is not necessarily a quantitative method but qualitative methods such as subject matter experts who provide estimates on the attributes for each asset to rank vulnerabilities can be used (API/NPRA, 2003; Bajpai et al., 2005 & 2010). Depending on the type and size of the facility, the SVA team may include experts with knowledge, experience and expertise of physical and cyber security, process safety, process design and operations, emergency response, management and etc. in understanding how and where the security risks may appear and what are the countermeasure to combat them (API/NPRA, 2003; CCPS, 2010). The SVA methodology used in the present study has been adapted from (API/NPRA, 2003) having shown in Fig. 1.

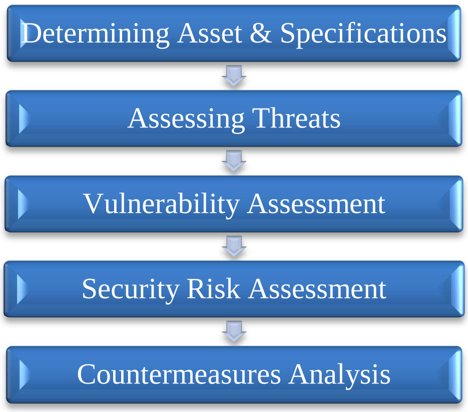

Fig. 1: API/NPRA Security Vulnerability Assessment (API/NPRA, 2003; CCPS, 2010)

A SVA process consists of main steps which are described briefly as following:

3.1. Asset characterization

At the first step, all assets in terms of security and deliberate concerns should be identified and characterized. SVA team do this. These assets include process, equipment, operations, personnel, information, process control systems and support utilities (API/NPRA, 2003; Bajpai et al., 2010; Moore, 2004). Indeed value and importance of every asset, as well as, the relevance and interdependency of these assets to the public, suppliers, customers and other stakeholders has to be characterized and based on the worst possible incident, intentional adversaries and malicious security events on assets should be determined (CCPS, 2010).

3.2. Threat assessment

Threat assessment is an important part of the security management process and is used to evaluate the likelihood of malicious actions, threat capabilities, adversary strength, motives, weapons and tactics against a given asset or group of assets (API/NPRA, 2003; Reniers et al. 2013). In this part, both internal and external threats against assets and attractiveness of each asset in terms of security issues are identified and characterized (API/NPRA, 2003; Reniers et al. 2013 & 2015). Moreover, type of threats including physical, financial, cyber or psychological threats which might impose damages and result in casualties to the assets should be analyzed. Adversary characterization involves adversary’s history, capabilities and intention (API/NPRA, 2003).

3.3. Vulnerability assessment

In this step, potential security vulnerabilities that threaten the assets are identified and evaluated. This part consists of three following subparts:

3.3.1. *Define scenarios and evaluate specific consequences*

After that SVA team determined how an adverse security event can be induced, it should determine how adversary could accomplish that undesired action and what is the consequences and damages of a successful adverse action (API/NPRA, 2003).

3.3.2. *Evaluate effectiveness of existing security measures*

The SVA team review and assess the existing countermeasures intended to protect the facility assets in the perspective of their effectiveness, integrity, reliability and ability to deter, detect and delay malicious security attacks and reducing the vulnerabilities of each asset to each threat or adversary (API/NPRA, 2003).

3.3.3. *Identify vulnerabilities and estimate degree of vulnerability*

The SVA team estimates the vulnerabilities of each asset through the provided vulnerability assessment checklists. The SVA team should brainstorm vulnerabilities for all of the deliberate acts and threat types that are possible at a minimum (API/NPRA, 2003).

3.4. Security risk assessment

To establish an understanding of security risk, scenarios can be assessed in terms of the severity of outcomes and the likelihood of occurrence of security incidents. These are qualitative analyses based on the expert’s judgment and deliberation of knowledgeable team members. Recommendations should be justified to reduce the risks (API/NPRA, 2003).

3.5. Recommend countermeasures

Finally, risk mitigation options should be identified and evaluated cost-effectively. After implementation of countermeasures, security and vulnerability of assets should be re-assessed to be ensured adequate and effective countermeasures are being applied (API/NPRA, 2003; Bajpai et al., 2010; Moore, 2004).

4. The software Joshan-Pro

The local version of the software SVA-Pro called Joshan-Pro was used to assess vulnerability of the assets in the under study facility. In this software, the vulnerability of assets is analyzed through security considerations which have been collected from the diversified checklists. These checklists are consisted hazardous materials, process equipment, communication and electrical equipment, information technology procedures and equipment, buildings, water and wastewater facilities checklists and etc. Therefore, all risk factors that affect assets critically, are ranked from 0 (lowest) to 5 (highest) point. This ranking is based on the expert’s judgment. As a result, in order to calculate the security risk in the SVA technique, Eq. (1) is used:

$$Security\ Risk = T \times V \times C \tag{1}$$

Where; T is the rating of threats, V is the vulnerability and C is the consequence of each threat. Finally, to reduce the vulnerability and security risks in the assets, countermeasures are offered.

5. Initial screening

Prior launching a SVA, an initial screening at a system level/asset level should be done. The screening can be used to review the facility/asset to determine whether further security analysis and detailed threat and vulnerability assessment is required or not (API, 2005). Security Risk Factor Table (SRFT) used to evaluate the identified assets in terms of security risk. In SRFT, important factors affecting security risk such as location, visibility, access control, presence of chemicals, etc. are listed. Other factors are represented in Table 2.

Table 2. Security Risk Factor Table (SRFT) presented by Bajpai and Gupta (2005)

Risk factors	Range of security points			Actual points
Presence of chemicals which can be used as precursors for WMD	Absence 0		Presence 5	
Location	Rural 1	Urban 2,3,4	High density 5	
Ownership	Private 1	Public 2,3	Government 4,5	
History of security incidents	Nil 0	Few 1,2,3	Frequent 4,5	
Presence of terrorist group in region	Absence 0	Few 1,2,3	Largo no. 4,5	

Personal preparedness and training	Well prepared		Average	Poor	
	1		2,3	4,5	

Table 2. Security Risk Factor Table (SRFT) presented by Bajpai and Gupta (2005) *(Continued)*

Risk factors	Range of security points				Actual points
Existing security measure:	High level		Ordinary	Poor/None	
Access control	1		2,3	4,5	
Perimeter protection	1		2,3	4,5	
Mitigation potential	1		2,3	4,5	
Proper lighting	1		2,3	4,5	
Using metal detector /X-ray/CCTV	1		2,3	4,5	
Visibility	Not Visible	Low	Medium	High	
	0	1,2	3,4	5	
Inventory	Low	Medium	large	Very large	
	1	2	3,4	5	
Worst case impact on-site	Negligible	Low	Moderate	Severe	
	0	1	2,3,4	5	
Worst case impact off-site	Negligible	Low	Moderate	Severe	
	0	1	2,3,4	5	
	Total Actual Risk Score				

For each asset, safety and security experts estimate the security risk by scoring the asset a number from 0 (lowest risk) to 5 (highest risk). Finally, numbers related to different factors are then added into a single risk score (Bajpai and Gupta, 2005; Rivera et al., 2014). Based on the value of the risk score, the identified assets classified in low, moderate, high, extreme risk according to the Table 3.

Table 3. Security Risk Factor Score Ranking

Security Risk Factor Score	Risk Ranking
<15	Low
16-29	Moderate
30-39	High
>40	Extreme

The minimum security risk factor score to enter each asset into Joshan-Pro for further is 30 and therefore, among 17 identified assets, 13 assets with high and extreme risk were entered Joshan-Pro. Table 4 lists identified assets, their security risk factor scores and their ranking of risks.

Table 4. Determining the analysis priority for the assets under study

Assets	Security Risk Factor Score	Risk Ranking
Land and power plant area	23	Moderate
Industrial building	33	High
Office building	38	High
Storage building	23	Moderate
4-Gas oil storage tanks	36	High
Natural gas station	30	High
Accessories	28	Moderate
230 kV Substation	33	High
Refinery unit	29	Moderate
Gas turbine transformer	33	High
Steam turbine transformer	33	High
Gas turbine control room	42	Extreme
Steam turbine control room	42	Extreme
Natural gas fueled turbine	40	Extreme
Gas oil fueled turbine	38	High
Steam turbine	34	High
Steam Boilers	32	High

6. Types of threats in thermal power plants

Some of the possible security threats for the facilities under study are as follows: Air strikes, terrorist attacks, bombing facilities with electromagnetic and graphite bombs, cyber-attacks, protests and riots by the disgruntled employees and contractors and stealing equipment, tools, materials and information of which each of these threats has at least one history record in the facilities under study or similar facilities (Garrick et al., 2004). Possible scenarios, security incidents, consequences, threats and vulnerability for each of the assets in the under study facility have been represented in Table 5.

By multiplying the threat, consequence and vulnerability scores, security risk for each of the assets is estimated. Considering the fact that the highest imaginable number for each of the threat, consequence, and vulnerability is 5, the highest possible security risk is 5×5×5=125 and the security risk for each of the assets is calculated as a fraction of 125. In Table 6, the vulnerability and security risk for each of the selected assets has been shown.

Table 5. The assessment of scenarios, security incidents, consequences and assets vulnerability of under study facility

Assets	Scenarios	Type of Security Incident	Consequences	Type of Threats	Vulnerability
Industrial building	Airstrike	Missile impact	Explosion-fire-power cut-disruption in organization management	Airstrike	1.45
Office building	Terrorist attack	Infiltration of malwares into the office server	Disruption in management and correspondence of the organization	Cyber attack	1.8
Gas oil storage tanks	Military attack or terrorist attack	Airstrike and missile attack	Explosion and fire and environmental pollution	Airstrike	2.33
Natural gas station	Terrorist attack	Planting bombs	Explosion and fire in pipelines and gas station	Terrorist attack	1.54
230 kV substation	Theft, terrorist attack or graphite bombardment	Arching, broken insulators	Nationwide power cut	Terrorist attacks, bombardment	0.96
Gas turbine transformer	Graphite bombardment	Terrorist sabotage-power cut	No electricity production	Bombardmen, disgruntled employees and contractors	1.15
Steam turbine transformer	Graphite Bombardment -terrorist attack	Terrorist sabotage-technical problems	Causing problems in the process of electricity production	Disgruntled employees and contractors	1.35
Gas turbine control room	Severe terrorist attack , Cyber attack	Planting bombs-sabotage and technical problems, Infecting control systems with malwares	Disruption in the process of control rooms operation-no production of electricity	Terrorist attack, Cyber attack	1.04
Steam turbine control room	Severe terrorist attack, Cyber attack	Planting bombs-sabotage and technical problems, Infecting control systems with malware s	Disruption in the process of control rooms operation-no production of electricity	Terrorist attack, Cyber attack	0.94
Natural gas fueled turbine	Terrorist attack	Planting bombs or causing technical problem in turbine system	Causing disruption in the process of electricity production	Terrorist attack	1.34
Gas oil fueled turbine	Terrorist attack	Planting bombs or causing technical problem in turbine system	Causing disruption in the process of electricity production	Terrorist attack	1.07

Table 5. The assessment of scenarios, security incidents, consequences and assets vulnerability of under study facility

(Continued)

Steam turbine	Terrorist attack	Planting bombs or causing technical problems	Disruption in the process of electricity production	Terrorist attack	1.19
Steam boilers	Airstrike	Bombardment and missile attack on the boilers	The explosion of boilers and creating holes in them	Airstrike	0.95

Table 6. Vulnerability and security risk for each of the assets

Assets	Threat Ranking	Consequence	Vulnerability	Security risk
Industrial building	5	5	1.45	36.25
Office building	3	4	1.8	21.60
Gas oil storage tanks	4	5	2.33	46.60
Natural gas station	3	3	1.54	13.86
230 kV Substation	3	3	0.96	8.64
Gas turbine transformer	4	3	1.15	13.80
Steam turbine transformer	4	3	1.35	16.20
Gas turbine control room	4	4	1.04	16.64
Steam turbine control room	4	3	0.94	11.28
Natural gas fueled turbine	4	4	1.34	21.44
Gas oil fueled turbine	4	3	1.07	12.84
Steam turbine	4	3	1.19	14.28
Steam boilers	3	5	0.95	14.25

7. Results and discussion

In the under study facility 17 assets were identified and entered into security risk factor table (SRFT) for screening and among them, 13 assets with extreme and high security risk were determined and entered the software Joshan-Pro for further analysis. Gas oil storage tanks with the vulnerability of 2.33 out of five and security risk of 46.60 out of 125 is ranked as the highest in terms of security risk and if they stop operating, they cause the highest economic damage to the under study power plant. The reason is the high volume of hydrocarbons including gas oil fuel in 4 tanks containing 117 million liters. Next, industrial buildings (warehouse and facility holds), office building and natural gas fueled turbine are ranked in terms of security risk, respectively. The 230 KV substation with the vulnerability of 0.96 and security risk of 8.64 was identified as the asset with the lowest security risk ranking. To reduce the security vulnerability of the assets in the under study facility, defensive countermeasure such as camouflage, concealment, covering and construction of parapet and explosion-proof structures for some sensitive installations such as transformers are proposed. The cables to not be detected by criminals, should be buried. For storage tanks operating in war conditions, the camouflage painting must be used. Modern methods of cyber protection should be deployed in depth to deny access of terrorists to the key information. Access control and monitoring system for the entry and exit of people and vehicles into and out of the facility through regular and non-regular inspections must be strengthened. Lighting system in the entire facility using a CCTV should be Strengthened and improved and the total facility area must be monitored at all hours of the day. It is also essential that special attention must be paid to the cyber security and its importance in the prevention of physical injuries and calamities to the power plant equipment and facilities. Also, in response programs under emergency situations, security scenarios should be taken into account and through periodic and regular maneuvers and proving integrated training course, the personnel's preparation to encounter such conditions should be increased.

8. Conclusion

Energy section is one of the most important section that has been threated around the world in various ways. Any long interval in supplying one of the basic types of energy such as electricity, oil or natural gas can cause remarkable damage to the economy of the society and the people. In the present study, the vulnerability and security risk of critical assets in a thermal power plant using SVA technique were determined. Among 17 identified assets in the facility, 13 assets with high and extreme risk priority through Security Risk Factor Table (SRFT) were determined and for further analysis on vulnerability and possible threats were entered into the software Joshan-Pro. Subject matter experts used to score threat, consequence and vulnerability for each asset, qualitatively. For each asset, associated checklists within the software helped the participant experts with safety, security, process, management, IT, maintenance, etc. experience and knowledge to determine vulnerability and other security risk factors. Therefore, security risk for each asset by multiplying threat, consequence and vulnerability scores was calculated and to reduce the risks and vulnerabilities, countermeasures were proposed. The suggested further research can be performed on the quantitative evaluation of the vulnerabilities and security risks in the thermal and nuclear power plants as the critical facilities in perspective of both physical and cyber security issues.

Acknowledgments

Here, the authors would like to express their gratitude to the management and all the officials of the thermal power plant under study for their cooperation and assistance in this study.

References

American Petroleum Institute/National Petrochemical & Refiners Association. Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries. 2003, Washington (DC).

American Petroleum Institute. Security Guidelines for the Petroleum Industry-3rd Edition. 2005: API Publishing Services.

Akgun I, Kandakoglu A, Ozok AF. Fuzzy integrated vulnerability assessment model for critical facilities in combating the terrorism. Expert Systems with Applications, 2010; 37(5): 3561-3573.

Al Mannai WI. Development of a decision support tool to inform resource allocation for critical infrastructure protection in Homeland Security. 2008. Available online at http://calhoun.nps.edu/bitstream/handle/10945/10327/08Jun_Al_Mannai_PhD.pdf?sequence=1.

Srivastava A, Gupta JP. New methodologies for security risk assessment of oil and gas industry. Process Safety and Environmental Protection, 2010; 88(6): 407-412.

Bajpai S, Gupta JP. Securing oil and gas infrastructure. Journal of Petroleum Science and Engineering, 2007; 55(1): 174-186.

Bajpai S, Sachdeva A, Gupta JP. Security risk assessment: Applying the concepts of fuzzy logic. Journal of Hazardous Materials, 2010; 173(1–3): 258-264.

Bajpai S, Gupta JP. Site security for chemical process industries. Journal of Loss Prevention in the Process Industries, 2005; 18(4–6): 301-309.

Center for Chemical Process Safety. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. 2010: Wiley.

Downs B. Balancing Resources to Risk, U.S.C. Guard, Editor. 2007: Presentation to SCOTS/NCHRP 20-59. Irvine, CA.

Downs, B., The maritime security risk analysis model. The Coast Guard Journal of Safety and Security at Sea, 2007. 64(1): 36-38.

Esmaeli Shahrokht M, Taghvayi AA. Urban Reorganization with focus on Passive defense. Urban Management, 2011; 9(28): 93-110.

Garrick, B.J., et al., Confronting the risks of terrorism: making the right decisions. Reliability Engineering & System Safety, 2004; 86(2): 129-176.

Jamshidi, A., et al., The Presentation of Security Vulnerability Assessment in oil industry Case study: Marine Oil Industry. Journal of Emergency Management, 2012; 1(1): 61-67.

Lewis T, Darken R, Mackin T. Managing Risk in critical Infrastructures using Network modeling. IEEE Spectrum, 2006.

Moore DA. The new risk paradigm for chemical process security and safety. Journal of Hazardous Materials, 2004; 115(1–3): 175-180.

Moore DA, Fuller B, Hazzan M, Jones JW. Development of a security vulnerability assessment process for the RAMCAP chemical sector. Journal of hazardous materials, 2007; 142(3) 689-694.

Nickell R, Jones J, Balkey K. RAMCAP: Risk Analysis and Management for Critical Asset Protection, overview of methodology. AMSE International Mechanical Engineering Congress and RD7D Expo, Annaheim, CA. 2004.

Reniers G, Dullaert W, Audenaert A, Ale B, Soudan K. Managing domino effect-related security of industrial areas. Journal of Loss Prevention in the Process Industries, 2008; 21(3): 336-343.

Reniers G, Herdewel D, Wybo JL. A Threat Assessment Review Planning (TARP) decision flowchart for complex industrial areas. Journal of Loss Prevention in the Process Industries, 2013; 26(6): 1662-1669.

Reniers G, van Lerberghe P, van Gulijk C. Security risk assessment and protection in the chemical and process industry. Process safety progress, 2015; 34(1): 72-83.

Rivera B, Zapata F, Kreinovich V. Security Risk Assessment: Towards a Justification for the Security Risk Factor Table Model. 2014. Departmental Technical Reports (CS), Paper 887.

Sarewitz D, Pielke R, Keykhah M. Vulnerability and risk: some thoughts from a political and policy perspective. Risk Analysis, 2003; 23(4): 805-810.

van Staalduinen MA, Khan F, Gadag V. SVAPP methodology: A predictive security vulnerability assessment modeling method. Journal of Loss Prevention in the Process Industries, 2016; 43: 397-413.

Yazdani M, Alidoosti A, Basiri M H. Risk Analysis for Critical Infrastructures Using Fuzzy TOPSIS. Journal of Management Research, 2012; 4(1): 1-19.