Vulnerability assessment of offshore terminals in the Sultanate of Oman: The case of a security audit for SPM Terminal of Mina al Fahal

Kambiz Mokhtari
Mehrdad Behforouzi
Kais Ali Hassan
SDS Dadwal
Arife Tugsan Colak
Maritime Department
International Maritime College Oman (IMCO), Sohar, Sultanate of Oman

Keywords
Fuzzy Set Theory; Petrochemical Seaports and Offshore Terminals; Security Risk Management; Security Threat Analysis; Security Vulnerability Analysis; Sultanate of Oman.

Abstract

Nowadays, the pressure for enhanced attention to critical infrastructure security and the focused concern on threats emanating from both domestic and foreign terrorist groups have fostered new challenges for Petrochemical Seaports and Offshore Terminals (PSOTs). These tendencies dictate to maintain comprehensive security regimens that can be integrated with national and international strategies to support the country's security against terrorism. Therefore, the need for a Security Risk Management (SRM) programme will be an essential part of the business of running a seaport particularly if the addressed port or terminal is handling hazardous chemicals produced from a nearby plant or refinery for export purposes. As a result, by the use of a case study in this paper, the identified security risk factors for an offshore Single Point Mooring (SPM) terminal located inshore side of the seaport of Mina al Fahal in Sultanate of Oman will be assessed by introducing its designated Security Risk Factor Table (SRFT) in order to examine the vulnerability of the addressed terminal. Consequently, the proposed framework can be used by intelligence analysts or port security and risk managers for the protection of these critical infrastructures. Suitable mitigation measures and further treatments for lessening the impact of a successful terrorist attack or potential likelihood of other threats in PSOTs facilities will be studied carefully.

Corresponding author: Kambiz Mokhtari
Email address for corresponding author: kambiz@imco.edu.om
First submission received: 15th April 2020
Revised submission received: 20th July 2020
Accepted: 18th September 2020

1. Introduction

PSOT security is an issue and there is legally mandatory framework for all PSOTs to follow (i.e. maritime related conventions). In addition, as a part of marine and process industries, PSOTs are critical infrastructures for the operation of all nations' economies, which can influence their financial structures and competitiveness on the international level. These logistics essentials can afford primary support to oil and gas, power, transport, agriculture, and manufacturing industries in any country. Nevertheless, these essential components of international transport in the past have not been so far subjected to an inclusive governmental regulatory due diligence and/or security supervision. In this view, the terrorist attack of 9/11, 2001 was the former paradigm-shifting occurrence for transport systems' security in common. For the maritime industry, that event has prompted remarkable shifts in the focused perspectives on security now required by anyone even remotely associated with the operation and management of ports and terminals security, as well as the ships, adjacent facilities or plants, multimodal transports, the people and employees involved (Sutton, 2014).

Furthermore, after 9/11 the International Ship and Port Facility Security (ISPS) Code was ratified and incorporated into Chapter Eleven of the Safety of Life at Sea Convention (SOLAS) 1974 of the International Maritime Organisation (IMO). Because of this fact, the ISPS Code has been imposed internationally by the IMO since July 2006, and all the member states had to act per the addressed Code. The execution of the Code since July 2006 assists port facilities to supervise their security levels.

Many of the seaports and offshore terminals are located next to petrochemical complexes such as oil and gas refineries, fertilizer production and different chemical plants or even power generators. Otherwise several of them are in the form of complexes particularly for exporting or/and importing of Liquefied Natural Gas (LNG), crude oil, Liquefied Petroleum Gas (LPG) plus a variety of dangerous petrochemical commodities such as ammonia, naphtha and so on. Even some of these terminals are in the form of a fixed installation or floating offshore terminal positioned in the middle of the sea used for similar reasons. Any intentional or accidental discharge or awful event of such release of harmful materials can massively jeopardize the health and safety of employees, the community and it can cause serious damage to the environment. Accidental releases can result from the potential mistakes within the facilities or even as a result of natural catastrophes. Accidents happen when employees make a mistake or due to equipment failures (Chemical Safety.Com (CSC), 2018).

Natural disasters are events such as tsunami, earthquake, volcanic activity, flooding, a heavy rainstorm, windstorms, revolving tropical storms etc. all of which can have a destructive consequence on the PSOTs. Alternatively, intentional releases can result from intended and malicious operations. However, all of the addressed events (i.e. above mentioned probable accidents in PSOTs and/or natural disasters) whether they are as a result of accidental or intentional acts can lead to toxic releases, fires, explosions and finally can cause in multiple fatalities, economic losses, property and environmental damages (Rubin and Cutter, 2019).

As PSOTs handle dangerous goods and products regularly, they can simply become possible targets for intentional attacks under the main three categories, i.e. terrorism, sabotage and those by members of the community living in the region near the port facility. Terrorism is perhaps the form of attack that the public mainly fears, not least for the reason that terrorists globally would like to create such panic. In addition, terrorists often have much larger destructive means than other malicious individuals, thus giving them the potential to cause lots of harm, to plan and commit acts of terrorism over a long period of time. In the case of sabotage, the aggressor can cause a very hostile condition, but still, it is supposed to be indented for a worse case. For the case of the community members' security violations such as theft; the addressed members may desire to cause harm and would not generally like to cause a disaster (Mokhtari, 2020).

Accidental events are outside the scope of this paper, and they will not be discussed here. They can be examined under process safety, process risk or reliability engineering but not under the heading of SRM. The intentional events discussed above i.e. only the three categories of deliberate anti-security acts will be discussed in this paper for the purpose of the PSOTs. Therefore, a SRM framework will be introduced in the next section to overcome the security challenges within the PSOTs.

The main aim of this paper is to propose a generic SRM framework to assess and prioritise the identified security risk factors (threats) within the PSOTs. Moreover, this work consists of the following sections. In the next section, brief literature related to the SRM will be reviewed. In Section 3, the fuzzy set theory to be used in this paper will be explained. Section 4 proposes a generic framework and methodology for the SRM of PSOTs. Section 5 is a case study conducted to validate the proposed methodology. Lastly, Section 6 will discuss the conclusions and suggestions.

2. Security risk management

As per Borodzicz (2005) the ancient philosophers of Egypt, Greece and China were certainly not only between members of early civilizations to have been concerned about security, but several forms of security must also have been the origin for these early civilizations to exist. Furthermore, "the relationship between risk and security is perhaps more than simply a linguistic turn. Indeed, security can be seen as an element of risk management in a holistic sense; Borodzicz (2005); page: 23". From a PSOT risk perspective, security threat can be viewed reasonably as just another hazardous exposure. Although SRM may be viewed as expenditure against the operation, it also stands for a significant threat if not managed thoughtfully. Therefore, managing PSOTs' security risk factors as a loss prevention activity can assist a broader appraisal of PSOTs' exposure. As discussed earlier, this could acknowledge terrorists' threats, but it could also lead to more security issues. Such losses could be the result of both external and internal terrorists' crime, but they could also initiate from an accident with no connection to criminal activities.

Terrorist attacks such as those which occurred in New York (2001), Bali (2002), Madrid (2004), Mumbai (2008), Paris (2015), London (2017), U.A.E (2019), Gulf of Oman (2019) and so on are examples that can reoccur again in any place at any time even in PSOTs. A terrorist attack on a marine port, particularly if several such attacks take place at the same time, can also disturb the countries' economies. Marine ports tend to be extensive and large, so it is not likely that any attack would demolish a marine port's infrastructure. Nevertheless, an attack could interrupt a transportation system for a significant period and would most likely lead to a postponement of all activities at ports until security measures were reassessed and improved. Though, in the case of petrochemical and process facilities if they are situated nearby or within the terminals' or ports' boundaries, the overall view on security from the point of view of the PSOT will be changed.

These types of marine ports and terminals will be considered as petrochemical plants rather than being explained like an ordinary transportation hub. In this case, approximately the same security threats, vulnerabilities, and hazards (i.e. risk factors) relevant to process industries with slight changes will be applied to these critical infrastructures. Additionally, there is a potential security risk due to the harmful nature and quantity of products and goods being transported by vessels, marine ports and terminals, intense processing conditions of pressure and temperature, and value of the produced goods to the country. Terrorists have sufficient information such as the position of dangerous chemicals, tank farms, pipelines, bypass valves, important safety and warning systems, emergency stops/shutdown devices etc, that they may make use of them to cause contaminated releases, fires and explosions. This can lead to severe impacts on the health and safety of people, the economy, environmental damages and pollution as well as fatalities in on-site and/or off-site seaports' areas (CSC, 2018; Matteini, *et al*. 2018 and Morenoa, *et al.* 2018).

Nevertheless, the theoretical approach towards a generic SRM for PSOTs in this paper aims to identify the threats resulting from terrorism. The proposed framework also establishes suitable security procedures like for assets characterisation, assessing the security risk factors (threats), security threat assessment, vulnerability assessment and to take proper countermeasures against the identified and assessed threats. For this reason, a generic SRM framework for PSOTs can be illustrated in Figure 1as follows:

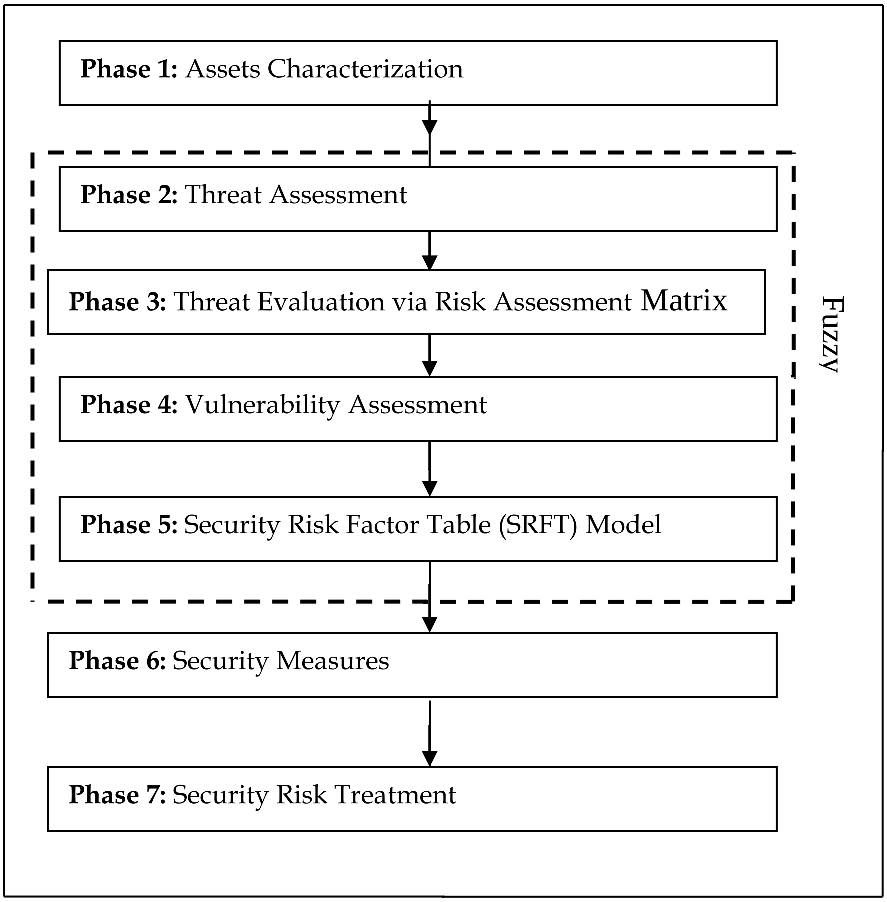

Phase 1: Assets Characterization
Phase 2: Threat Assessment
Phase 3: Threat Evaluation via Risk Assessment Matrix
Phase 4: Vulnerability Assessment
Phase 5: Security Risk Factor Table (SRFT) Model
Phase 6: Security Measures
Phase 7: Security Risk Treatment
Fuzzy

Figure 1: A generic SRM framework for PSOT

In overall security threats such as terrorists' deliberate acts on a processing facility like a PSOT can be avoided or reduced if the security related determinant factors such as asset, vulnerability and threat in a processing facility can be carefully classified and assessed in advance. This can be reached by a deliberate and well-planned programme (e.g. SRM) as a security procedure which can be designed to stop or decrease the development of a terrorist attack (i.e. security incident). The addressed security determinant factors signify that if any of these associated elements are adequately halted or mitigated the risk of a security incident by terrorists can be avoided or reduced. This can be fulfilled whether by accurately knowing which types of assets in a PSOT are critical ones or by undertaking a proper vulnerability assessment and/or threat assessment to stop and decrease the level of the vulnerabilities or security threats. For the purpose of the addressed security related determinant factors as illustrated in Figure 1, i.e. Phases of 1, 2 and 4 which are used for assets characterisation, threat assessment and vulnerability assessment correspondingly, will be dealt with individually in Section 4.

3. Fuzzy set theory

Primarily fuzzy set theory was initiated by Zadeh (1965) to handle imprecision of data and human judgement, which was oriented to the consistency of uncertainty, resulting from vagueness. Therefore, a major contribution of fuzzy set theory is its capability of representing vague data. Moreover, the fuzzy set is a class of objects with a continuum of grades of membership. Such a set is characterised by a membership (characteristic) function, which allocates to every object a grade of membership. The theory furthermore allows mathematical operators and programming to apply to the fuzzy domain. Moreover, a fuzzy set is an extension of a crisp set. Crisp sets only permit full membership or non-membership, while fuzzy sets permit partial membership. It is possible to utilize different fuzzy numbers depending on circumstances, and in practice, triangular and trapezoidal fuzzy numbers are used (Marco, 2018). In this paper, fuzzy triangular numbers are utilised to deal with the threat matrix for the evaluation of the potential security risk factors threatening a PSOT and to prioritise the threats. Then trapezoidal fuzzy numbers will be used in SRFT for obtaining the overall security score of a PSOT. This will validate the applicability of the fuzzy numbers in different situations.

There are various operations on fuzzy numbers. If two positive triangular fuzzy numbers of $\widetilde{M}_1$= (l_1, m_1, u_1) and $\widetilde{M}_2$ =(l_2, m_2, u_2) in which$l_1, m_1, u_1, l_2, m_2, and\ u_2$are real numbers subsequently under fuzzy environments their basic operations such as their multiplication, i.e. ⊗ can be defined as follows (Yang and Hung, 2007):

$$\widetilde{M}_1 \otimes \widetilde{M}_2 = (l_1,m_1,u_1) \otimes (l_2,m_2,u_2) = (l_1 \otimes l_2, m_1 \otimes m_2, u_1 \otimes u_2) \qquad (1)$$

Other algebraic operations, further details about fuzzy sets, their membership functions and linguistic variables can be found in Ross (2017).

The subjective linguistic variables, as explained in Steps 3 and 5 of Section 4, are used for assessment of the security risk factors (threats) can be defined in terms of membership functions. A membership function is a curve that defines how every one of objects or points (i.e. security risk factors), e.g. high, medium, and low in the input space is mapped to a membership value. For example, a membership value between 0 and 1 for triangular numbers to define fuzzy linguistic scales (five points) of very high, high, medium, low and very low are illustrated in Figure 2. Furthermore, the mapped membership value between 0 and 5 in case of the trapezoidal numbers for defining the fuzzy linguistic scales (three points) of high, medium, and low are shown in Figure 3. Figure 3 was formerly used in the work of the Bajpai and Gupta (2005); further explanations can be found in their work. However, in this paper, after its application, a different defuzzification method and the process will be used to obtain the final result.

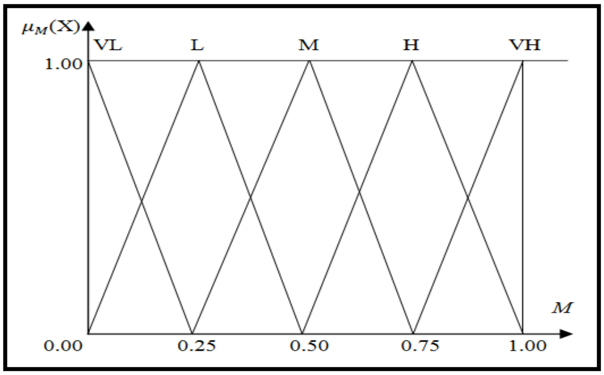


Figure 2: Fuzzy triangular membership functions
Source: Modified from Yang and Hung (2007)

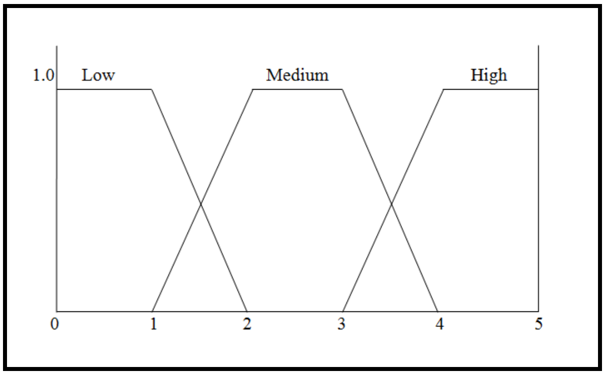


Figure 3: Fuzzy trapezoidal membership functions
Source: Bajpaiand Gupta (2005)

Subsequently, as the results of the estimates carried out for this work are all in the form of fuzzy numbers, an additional a defuzzification process must be carried out in order to change them into crisp numbers. The centre of area defuzzification technique is chosen to be used for this purpose hereafter. This method was developed in 1985 (Sugeno, 1999). It is the most frequently used method and is precise. This technique can be utilized for triangular and trapezoidal fuzzy numbers as per the following formulas:

Triangular fuzzy number $\widetilde{M}$= (l, m, u) can be defuzzified to a crisp number of M by, i.e.

$$M = \frac{(l+m+u)}{3} \qquad (2)$$

For a trapezoidal fuzzy number of $\widetilde{M}$= (l, m, n, u); i.e. $M = \frac{1}{3} \times \frac{(u+n)^2-(u\times n)-(l+m)^2+(l\times m)}{(u+n-m-l)}$ (3)

4. Methodology to carry out the proposed SRM in PSOT

A suitable methodology, including seven steps, is illustrated in Figure 1. The depicted steps can be easily applied to different PSOTs and their operations at varying degree of the feature as needed. Therefore, SRM can be used as a tool to easily implement the requirements of ISPS, in a standardized way across all PSOTs as follows:

Phase 1 – Characterisation: Characterize the facility or operation to understand what critical assets need to be secured, their importance, and their infrastructure dependencies and interdependencies. Therefore, it is required to divide the PSOTs into zones or areas and to characterise them in order to know which critical assets needed to be secured, what are their importance and interdependencies and supporting infrastructure (API, 2005; API, 2013 and Nolan, 2014).

For PSOTs apart from entering vessels, important properties like stored cargoes are principally imported. Additionally, in export terminals where vessels work quickly alongside quays, there are many specialised units and equipment such as port control tower or vessel traffic service/management, sound or fog signals, lights, warehouses, breakwaters, dredgers or any other equipment and devices connected or linked to the neighbouring processing plants or units, etc (OCIMF, 2012).

Phase 2 – Threat Assessment: Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each threat and the consequences if they are damaged, compromised, or stolen. Hence it is required to undertake a threat assessment by classifying sources, categories and determining the possibility of threats and to evaluate every possible threat within the process zone (Nolan, 2014and Landucci, *et al*. 2017).

As Kamien (2012) describes, a threat assessment can be based on categories or sources of threats. In this regard, the United States' Office of Domestic Preparedness (ODP) focuses on the type of weapon that terrorists can use explosive, biological, chemical, radiological, and nuclear. Another option is to focus on the sources of threat on any business and/or organization with the capability, motivation, and opportunity to initiate a successful attack on their systems. Thus, it is essential to develop a variety of scenarios that can be matched with probable types of attacks. In addition, each scenario should have weapons, assets, and mode of delivery Kamien (2012). Table 1 illustrates examples of these sources of threats whether they are based on external or internal sources.

Table 1: Examples of sources of threats in PSOTs

Internal	External
Port and terminal employees	International terrorists
Stevedores	Domestic terrorists
Contractors/operators	Saboteurs
Shippers/receivers/cargo owners	Vandals
Agents/ship-owners	Thieves
Customers/vendors	Activists
Visitors	
Ship's crew and officers	
Pilots	

Source: based on Sutton (2014)

The below-mentioned threat categories are possible types of security risk factors in PSOTs due to deliberate acts caused by terrorists as per IMO (2011) and Baybutt (2017):

- Release of hazardous cargo from ship and/or subsea pipelines inter-connections and causing toxic gas release, fire, and explosion.
- Stealing of classified documents and information from an offshore facility.
- Destruction of offshore terminals' and marine ports' physical assets, e.g. subsea pipelines, and tank farms.
- Causing interference on discharging and loading activities in ports and terminals by altering control settings.
- Making dangerous circumstances by creating interference using valves, or adding pollutants, poisons.
- Disturbing offshore terminal, port operators and guards.
- Robbery of harmful substances in order to use it somewhere else.
- Damaging of onshore cargo control rooms in ports and terminals and related gears.
- Halting safety and security units and systems.
- Halting port control and vessel traffic services/management centres.
- Stopping ships.
- Potential of explosives' threats through an entered ship, terminal worker and third party entered to port from outside.
- Cybersecurity attack threats.
- An attack to be carried out from vessel to terminal via using ship's goods, i.e. to use a ship as a mode of delivery.
- Along-range type of attack from air to port, e.g. via drones' strikes, long-range missiles.
- An attack from seaside to port, e.g. via pirates or speed boats.
- An attack from the underwater surface to terminal facilities, jetties, and ships by subsea devices; and
- A terrorist attack upon a ship from the shore side.

Factors like categories and quantity of goods handled or stored in port, weather conditions, varieties mode of accesses to the port facility, terminal working hours etc. are amongst the factors which can influence the threats' likelihood. The likelihoods of the probable threats' can be estimated by experts while using the pre-defined triangular fuzzy numbers. Through a threat matrix described in Phase 3, the calculated probabilities will be used for assessing and ranking of the security risk factors (threats) of a PSOT. Moreover, in a PSOT the mentioned different terrorists' acts can be organised in such a manner to be carried out even by pirates who have travelled from remote places, asylums, or stowaways.

Phase 3 – Threat Evaluation via Risk Assessment Matrix: There are many assessments means and tools to assist security risk management experts to calculate the different threats' levels within the particular facilities. Both quantitative and qualitative techniques are found helpful. Quantitative techniques explain the risk by estimates, and a statistical target rate is compared with the result. On the other hand, in qualitative techniques, the parameters used as opinion sources are subjective and estimated by experts' judgments. Selected method for the purpose of its application primarily depends on whether the necessary risk reduction is specified in a numerical or a qualitative manner. The extent and degree of the investigation would also be an influencing reason (Marszal and Scharpf, 2002).

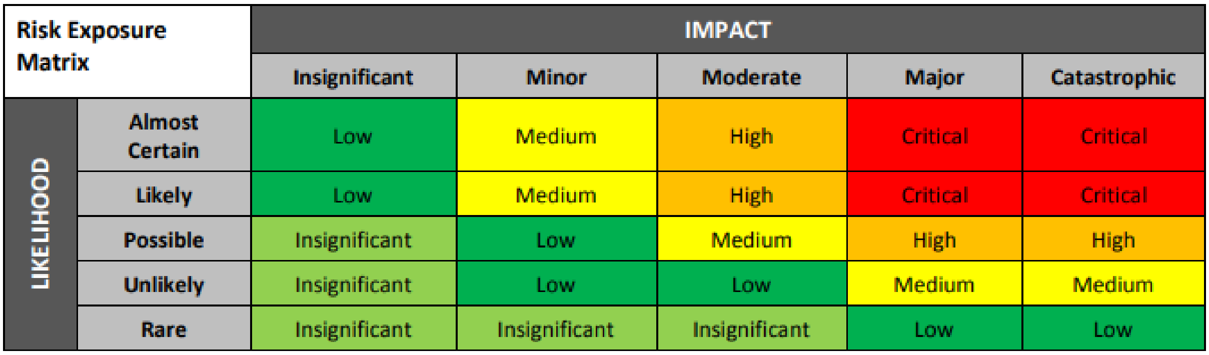
The hazard or risk factor matrix, which for this paper will be called a security threat matrix, is one of the most traditional risk evaluation tools because of its simplicity. The security threat matrix handles frequency (likelihood) and consequence (impact or severity) of the security threats qualitatively, based on a categorization of the security-related threat parameters. Figure 4 illustrates a classic threat matrix sketch which is tailored for security risks assessment purposes. The likelihood and impact of security threats make one axis each, enables the user to plot the situation under consideration in the diagram. If each box in the drawing has an attached reduced security risk level (such as insignificant), the determination procedure is straightforward. The consequence or impact categories may be expressed in the form of human (individual's safety), financial (loss or profit), or environmental damage. The risk types also divided the threat impacts or severities into catastrophic, major, moderate, minor, and insignificant as per the level of threat's impact or severity. The likelihood categories are also divided into rare, unlikely, possible, likely, and almost certain. The addressed categories can be chosen either qualitatively, using experts' judgments as described above and shown in Figure 4. However, quantitative methods (e.g. See fuzzy sets in Section 3) can be used by experts to assess the security threat levels. In Figure 4, a range of threat levels is illustrated. For instance, interception of the moderate impact and possible likelihood will lead to medium-security risk (threat). That means the assessed security risk is considered tolerable. Significant impact and possible likelihood will result in a high-security risk, while interception of the catastrophic impact and almost certain likelihood will result in critical threat exposure.

As ABS (i.e. American Bureau Shipping) (2003) argues, a regular risk assessment and presentation technique is simply used to multiply the likelihood (L) of each undesirable event by each severity (S) or impact, and then sum these products for all cases considered in the evaluation. As a result, with respect to the mentioned explanations, risk levels can be determined by use of the depicted parameters and via using the below-mentioned Equation:

$$R = L \times \mathrm{S} \tag{4}$$

Additionally, this definition demonstrates that if L and/or S, i.e. security risk parameters are used in the form fuzzy numbers, then R will also be a fuzzy number (Anoop *et al*., 2006), which means:

$$\tilde{\boldsymbol{R}} = \tilde{\boldsymbol{L}} \otimes \tilde{\boldsymbol{S}}, \text{ where } \otimes \text{ is a symbol of multiplication under fuzzy environments} \tag{5}$$



Risk Exposure Matrix		IMPACT				
		Insignificant	Minor	Moderate	Major	Catastrophic
LIKELIHOOD	Almost Certain	Low	Medium	High	Critical	Critical
	Likely	Low	Medium	High	Critical	Critical
	Possible	Insignificant	Low	Medium	High	High
	Unlikely	Insignificant	Low	Low	Medium	Medium
	Rare	Insignificant	Insignificant	Insignificant	Low	Low

Figure 4: A classic risk evaluation matrix designed for threat assessments in PSOT
Source: MCS (2019)

As Buybott (2007) describes, a security risk (threat) matrix can be utilised to determine each one of the security risk factors related to and/or contained by a facility without having a noticeable background of different avoidance countermeasures that may be part of a specific security threat scenario. In this case, the assessed threat levels can be used as an initial stage to assess the degree of a vulnerability assessment that should be executed, as well as the levels of security countermeasures and safeguards that must be maintained or to be employed at a preliminary stage. Accordingly, by a mix of both quantitative and qualitative methods, security risk factors (threats) could be prioritised for further use and reasons. As shown in Figure 2, appropriate fuzzy linguistic scales along with their membership functions have been illustrated for the occurrence likelihoods. The same fuzzy numbers and scales can be employed for the related occurrence impacts. That means a fuzzy triangular number of (0.50, 0.75, 1.00) as depicted in Figure 2 can be used for both of the occurrence impacts of catastrophic and likelihood of very high.

For instance, as shown in Figure 3 if a security risk factor (threat) as per security expert's choice has occurrence likelihood $(\tilde{L})$ of (0.00, 0.25, 0.50) i.e. possible and occurrence impact $(\tilde{S})$ of (0.50, 0.75, 1.00) i.e. major, the $(\tilde{R})$ as per Equations 1 and 5 will be (0.00, 0.1875, 0.50). Nevertheless, as a result is a triangular number, it can be defuzzified to acquire a crisp number based on Equation 2 which is equal to 0.23. The same operation in this step must be carried out for all of the security-related threats on a case by case basis to get a crisp number for everyone. Afterwards, they can be assessed and ranked based on their weights' (crisp numbers) importance. Subsequently, based on their priorities, a comprehensive vulnerability assessment can be designed and accomplished to maintain the projected SRM structure.

Phase 4 – Vulnerability Assessment: Classify possible security vulnerabilities that increase the prospect that the threat will successfully carry out the act. Therefore, it is necessary to classify vulnerabilities against each security risk factor (threat) by the use of brainstorming and using checklist methods (API, 2013 and Sutton, 2014).

As Kamien (2012) explained, a vulnerability assessment is used to estimate the vulnerability of the critical infrastructures in the circumstances, i.e. with a provided weapon and a provided target, the chance that an attack will be victorious depends on the capability to discover it, the warning time, the system's response, and the ability of the attacker to overcome the response. During the evaluation of the addressed security factors, it is essential to take into account, for each one of the targets, some existing countermeasures, appropriate physical plans, geographical arrangements etc. That may avoid admission to the addressed target, capacity to become aware of an attack in progress, or support in overcoming an identified attack. In this regard according to Sutton (2014), many organisations and plants perform a vulnerability assessment to classify and identify areas where they are mainly vulnerable, and to choose how to recover.

The team that carries out and maintains a vulnerability assessment must be thoroughly familiar with the engineering or business-related processes under inspection, e.g. highly skilled experts from maintenance, production, administration, security divisions and/or risk management departments. For instance, marine ports and terminals operator should not be selected to maintain and reassess a fertilizer plant located inside of PSOTs. The typical security review and auditor panel should also have a reasonable quantity of professionals from various organisations, for example, corporation employees, experts, equipment designers and manufacturers and intelligence services regulators.

As per Nolan (2014); Argenti, *et al*. (2017); Baybutt (2017) and Yazdi (2018) three types of persons are required to carry out a vulnerability assessment: (1) a team leader, (2) a recorder/scribe, and (3) the experts. The experts are usually (1) the project manager or engineer who has planned and designed the addressed plant/facility, (2) an individual who is knowledgeable with how the plant will be operated, e.g. a safety and/or process engineer and (3) an individual familiar with loss prevention aspects or security-related issues to the addressed plant. Vulnerability assessments will, in general, apply to all plants and/or facilities situated within PSOTs. Nevertheless, there will be more concern to apply its review to highly visible, expensive, and vital operations, plants and/or facilities.

As a vulnerability assessment is a qualitative form of evaluation, the subsequent processes must be conducted by vulnerability assessment experts to accomplish a successful investigation within a PSOT:

Divide the PSOT areas into zones of diverse security levels, e.g. low-risk, moderate-risk, high-risk and critical-risk zones. The main plan is to identify the significant locations in the terminals, refineries and plants that can be possible targets, e.g. Ammonium production unit, product tanker vessels and tank farms.

Discover the security risk factors from prospective terrorists in each zone.

Recognize the vulnerabilities within each zone. Develop various scenarios in which the realistic threats identified through threat assessment could be understood.

Declare the most unpleasant potential severities on-site/off-site in case of a successful terrorist attack to find out severity (S).

Inspect the effectiveness of the existing countermeasures for any specific security risk factor.

Propose additional security countermeasures to decrease likelihood (L) and severity (S) of a terrorist attack if it was conducted effectively.

Phase 5 – Security Risk Factor Table (SRFT): The state of security in a plant and/or facility similar to PSOT can be illustrated basically by the creation of an SRFT (Bajpai and Gupta, 2005 and CSC, 2018). In SRFT, quite a few security-related risk factors that can shape the whole security of a PSOT are demonstrated. After scoring the security risk factors listed in SRFT by experts or security auditors, using the three points trapezoidal fuzzy numbers shown in Figure 3, the total score obtained from SRFT will cause to make out and estimate the existing security risk level of a PSOT.

As per CSC (2018) SRFT can be used as a security risk evaluation device and based on Bajpai and Gupta (2005) in the form of a pre-screening means to find out whether any more comprehensive threat and vulnerability investigation is essential. The individual or panel making any SRFT have to be also practically well-known with the facility and/or plant in question. Furthermore, the subsequent descriptions are found important regarding the security risk factors being used in any SRFT.

Typically, terrorists and related groups focus on targets that can affect more extensive groups of people. Therefore, a plant or facility located in countryside places is much less attractive than a place similar to a PSOT situated close to a metropolitan area. Thus, being near to highly populated residents' areas enhances the attractiveness of a plant or facility as a target. A facility like a port neighbouring a major petrochemical tank farm is inherently at higher risk than any other. As large product carriers from various destinations enter these marine ports, terrorists can map in advance their different methods to make use of the addressed floating explosives as a delivery tool just to destroy the plants, refinery, terminals and to harm nearby residents. Moreover, terrorist groups mainly attempt to create fear by targeting larger, known corporations, such as larger, important organisations. A small and intermediate-sized business/activity or private company in a country is less expected to be targeted than a plant or facility classified under the ownership of a rich government (Kamien, 2012).

Visibility of security controls and countermeasures in a PSOT decreases its attractiveness as a target. A terminal facility on its shore-side which has very rigid perimeter control with all entrance points protected, having additional screening tools, e.g. video surveillance (i.e. CCTVs), sensors, guards and patrols a is much more complicated target than a PSOT with no or less controlled during hours of daylight. In coastal side, if a PSOT is not controlled and watched by its coast guard patrols is more prone to a terrorist attack than a PSOT with having 24 hours security watch (e.g. attack to ships in port of Fujairah in UAE on 2019). Based on the ISPS Code, there are three critical areas of concern (ICS, 2015):

- The employment of a vessel as a delivery device for conducting a terrorist attack in a terminal.
- A terrorist attack to a ship in marine ports' terminals areas and/or port limits.
- Goods to be used as a mode of delivery for targets outside of the marine ports and terminals areas.

Based on regulations declared in the ISPS Code, pre-arrival security paperwork and verifications on tanker vessels as well as ships' physical security inspections carried out by security officers in ports before cargo operations start will decrease the likelihood of a probable attack to the port facility or visiting vessel by terrorists.

Availability and existence of the weapons that terrorist groups possibly will utilize with having biological, radiological, chemical, explosive, and radioactive properties to perform terrorist attacks in any seaport will increase the security risk of the addressed facility. As the quantity of a specific target rises in terms of size and area, the security risk will be enhanced, respectively. That means in a PSOT if the capacity of target recognition by terrorists raises the security risks will rise also. Therefore, the availability of the named weapons as targets in a PSOT will raise the security risk of the port facility. There is a range of chemicals of fear, including Chemical Weapon (CW) agents such as hydrogen cyanide, chlorine, mustard gas, and ammonia. Smallpox and anthrax are the most critical biological killers. Other organisms are also of concern; they consist of bacteria such as anthrax or viruses such as yellow fever. Also, agents having uranium properties might be employed in a "dirty bomb". Whereas the risk of significant radiological harm from a dirty bomb is much less than the risk of harm from the explosion, the psychological shock of such an incidence on the impacted people will be significant. In this regard, health, and safety professionals in PSOT's should teach their workforce concerning the real magnitude of a probable terrorist attack with the described character (HS, 2012). In this regard training of port labours and workforces should be a part of the port facility's risk management agenda. Indeed, more practical exercises and drills will decrease the probabilities for a port facility to be selected as a target by terrorists (OCIMF, 2012).

There is also worse case outcomes impact on a marine port and its nearby district due to any terrorist attacks. Port facilities can be assessed as per the expansion of scenarios of the outcomes of a terrorist event. To estimate the worst-case scenario and to assess the impact of the consequence on a marine port and on its nearby places specialized experts are needed to rate these factors with awareness to get rational results.

As per API (2013) and Sutton (2014), there exist other issues in a PSOT that should be taken into consideration when making a SRFT such as visibility status of the ships o storage tanks used for storage of the imported crude oil or LNG or storage of the processed highly dangerous substances for export and internal use within the host country. If they are incredibly detectable and visible from nearby port vicinities, this will enhance the perspective of an attack. Aside from visibility the capacity, volume, number, and dimensions of the tank farms and visiting vessels also will have a significant role for an attack to occur. Presence of terrorists in the area or neighbourhood of a PSOT, security conditions or history of the PSOT with respect to the number of security occurrences taken place, etc play vital roles in investigating a security level of a port facility. Finally, consistency and importance of readiness of the emergency brigades referring to security, environment, safety, and health issues of PSOTs will have a vital role after, throughout and before a successful terrorist attack. In this regard, the security reliability ratio for a secure and reliable port facility can be defined as follows. A perfectly secure and reliable port facility where there are no disruptive security events that could undermine the scheduled work within the port and as per following formula, it should be equal to 1. This formula can be used by security experts for rating and scoring the mentioned security risk factor within an SRFT.

$$\text{Port Security Reliability Ratio} = \frac{\text{Number of effective days a port worked without security interruptions}}{\text{Number of scheduled working days}} \qquad (6)$$

Phase 6 – Security measures: To list security safeguards against threats scenarios and to evaluate them to see if the protective measures are adequate. Since many risk mitigation phases are used in most of the industry-related applications, rings of protection were needed. Therefore, throughout the SRM of marine ports, a similar technique can also be an appropriate one. For this purpose, the US Department of Homeland Security (HS, 2012) describes that security tends to underline “rings of protection,” means to, if possible, the most significant or most expensive assets should be located in the middle of concentric levels of ever more severe security countermeasures. For instance, where it is practical, in a PSOT, electronic control rooms of the processing plants should not be located beside the building’s reception area. Instead, it should be placed deeper within the building to reach the control room, a terrorist would have to go through and pass numerous rings of protection, for instance, a fence at the PSOT borders, an elevator with key-controlled floor buttons, an alert receptionist, a locked external door and a locked door to the control room. To verify if the rings of protection are well-organized, security plans must frequently be assessed using preparation tests and security drills in which the port facility has to have persons who can take part in the role of the invader to make out if the barriers work as normal. The addressed drills are applicable on vessels entering into ports and terminals, e.g. to carry out the addressed drills in ports controls, export/import terminals etc.

Based on IMO and under ISPS Code, security-related countermeasures in the form of rings of protection for visiting vessels and port facilities are adapted by Security Level 1 (i.e. the level for which minimum suitable protective security countermeasures shall always be preserved). Security Level 2 (i.e. the level for which suitable extra protective security countermeasures shall be preserved for a while due to heightened risk of a security event). Besides Security Level 3 (i.e. the level for which additional detailed protective security countermeasures shall be preserved for a restricted period when a security event is apparent or imminent, while it might not be likely to spot the exact target). Table 2 is the approach which will be incorporated in the proposed method in this paper.

Table 2: Countermeasures and recommendations tailored for the final score while using an SRFT

Security risk status	Actual points obtained	ISPS security countermeasures	Security Risk Treatment (Recommendations)
Low	< 25	Level 1	The security risk is low. Maintain awareness without excessive concern.
Moderate	25 - 48	Level 2	A moderate security risk is present. Review and upgrade existing procedures. Maintain awareness without excessive concern.
High	49 - 72	Level 3	Identify risk-drivers that can be reduced with reasonable controls. Work with law enforcement agencies to enhance security.
Extreme	>72	Level 3 + State of high alert	Initiate aggressive risk-reduction activity, in conjunction with consultation with law enforcement agencies.

Source: Adapted from IMO (2011), API (2013) and CSC (2018)

Phase 7 – Security Risk Treatment: To identify and evaluate security risk mitigation options and reassess the situation to ensure adequate countermeasures (See Table 2 in Phase 6) are being applied. Evaluate the appropriate response capabilities for security events and the ability of the operation or facility to adjust its operations to meet its goals in recovering from the incident and to find out if the treatments are appropriate.

Table 2 presents additional procedures and/or guidelines to be adhered to different security surroundings, depending on which level of security a terminal or port facility is kept. Apart from taking into consideration the issues e.g. health, safety, environmental factors, the incorporated guidelines must be consistent with the elements for enhancing the security of a PSOT. For example, initiatives such as port facility security plan (i.e. a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from risks of a security incident), emergency response plan and emergency preparedness plan apart from being used as mitigation methods but necessary recommendations along with the essential countermeasures for the purpose of key concepts such as how to detect, delay and response to a terrorist attack are also included. Subsequently, after ranking the security risk factors by use of abovementioned steps such as using a threat matrix or an SRFT, the required procedures and/or guidelines can be tailored and implemented on a PSOT for this step.

5. Case study

The area shown in Figure 5 is an oil refinery and Mina al Fahal offshore terminal in Sultanate of Oman, including the following zones:

Zone A: including Mina al Fahal refinery where crude oil is processed to make fuel products (e.g. LPG, gas oil or diesel, gasoline, fuel oil and jet fuel); a tank farm consisting of 10 crude oil storage tanks with a total storage capacity of 5 million barrels; power plants; metering facilities etc.

Zone B: including three Single Buoy Moorings (SBM) for offshore export of crude oil, two Coastal Buoy Moorings (CBM) for export/import of refined petroleum products and a purpose-built harbour for accommodating three tugs, a maintenance barge and pilot boat.

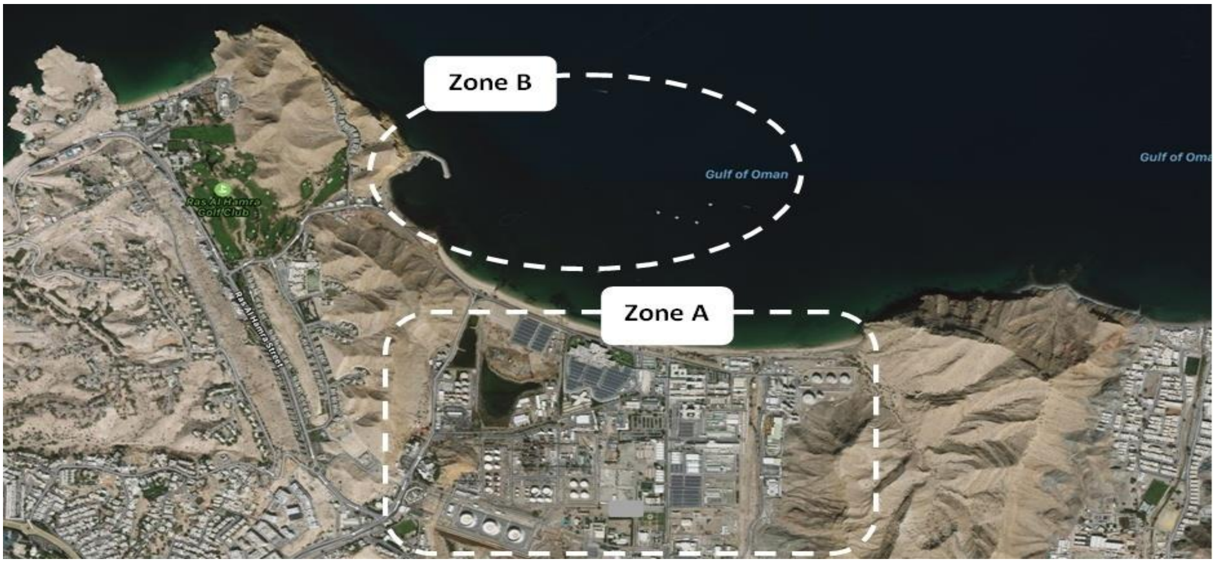


Figure 5: Google map of Mina al Fahal area

Table 3: Portrayal of Port of Mina al Fahal

Zone A (Refinery)	Zone B (Offshore Terminal)
1Main Refinery units	1 Three SBMs (Single Buoy Moorings)
2 Power plants and electricity substations	2 Two CBMs (Coastal Buoy Moorings)
3 Crude oil metering units and inter-connections	3 Port Control and Pilots
4 Crude Oil Storage Tanks for delivery of crude oil to tankers for export and to Oman Refinery for refining and producing products	4 Three Tugs
5 Storage Tanks for export/import products	5 One Maintenance Barge
6 Pipelines and pumps	6 One Pilot Boat
7 Gate	7 Block for Stevedores
8 Guardroom	8 A rigid inflatable fast response craft
9 Blocks for employees	9 A rigid inflatable anti-pollution boom craft
10 Fire Brigades	10 Three Subsea pipelines for export/import
11 Car parking area	11 A small size Harbour
12 Administrative Building	12 Administrative Building

Figure 6: Mina al Fahal Offshore Terminal in Zone B

Taking into consideration the proposed SRM methodology in this article Mina al Fahal port and offshore Terminal in Sultanate of Oman have been separated into two different areas as shown in Figure 5 and/or depicted in Table 3. For this paper, only one of the zones (i.e. Zone B: Offshore Terminal) has been addressed. To calculate the total security score of the addressed offshore terminal located at Zone B of Mina al Fahal, it is essential to modify a new SRFT for this offshore terminal. The newly designed SRFT (i.e. See Table 4) and the classified security risk factors (threats) are shown as follows (See Figure 4):

Table 4: Security Risk Factor Table (SRFT) designated for Mina al Fahal Offshore Terminal

Security risk factors	Range of security points			Security Auditor's ratings	Defuzzyfied Scores
Offshore terminal's location	Rural (0,0,1,2)	Urban (1,2,3,4)	High Density (3,4,5,5)	Rural	0.78
Visibility status of ships and infrastructures	Not Visible (0,0,1,2)	Less Visible (1,2,3,4)	Highly Visible (3,4,5,5)	Highly Visible	4.22
Processed gas and liquid chemicals storage	Low (0,0,1,2)	Medium (1,2,3,4)	High (3,4,5,5)	Medium	2.5
Imported crude oil and natural gas storage	Low (0,0,1,2)	Medium (1,2,3,4)	High (3,4,5,5)	Medium	2.5
Range of shipping traffic	Low (0,0,1,2)	Medium (1,2,3,4)	High (3,4,5,5)	Medium	2.5
Terminal's ownership	Private (0,0,1,2)	Public/Private (1,2,3,4)	Government (3,4,5,5)	Public/Private	2.5

Presence of terrorist's groups in region	Low quantity (0,0,1,2)	Medium quantity (1,2,3,4)	Large quantity (3,4,5,5)	Medium quantity	2.5
Worst impact on-site/offshore facility	Low (0,0,1,2)	Moderate (1,2,3,4)	Severe (3,4,5,5)	Moderate	2.5
Worst impact off-site/offshore facility	Low (0,0,1,2)	Moderate (1,2,3,4)	Severe (3,4,5,5)	Low	0.78
History of security incidents in offshore terminal	Nil (0,0,1,2)	Few (1,2,3,4)	Frequent (3,4,5,5)	Nil	0.78
Meteorological conditions	Good (0,0,1,2)	Moderate (1,2,3,4)	Bad (3,4,5,5)	Good	0.78
Target identification – chemical – by terrorists:	None	Minimum	Present		
CW (Chemical Weapon) agents	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	None	0.78
Listed chemicals of concern	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	None	0.78
Chemicals of extreme toxicity	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	None	0.78
Existing security measures:	High level	Ordinary	Poor/none		
Access control from mainland	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	Ordinary	2.5
Access control from open sea	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	Ordinary	2.5
Perimeter protection	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	Ordinary	2.5
Mitigation potential	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	Ordinary	2.5
Proper lighting (All over the SBM/CBM)	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	Ordinary	2.5
Use of metal detector/X-ray/ CCTV (at entrance and at all critical locations)	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	Ordinary	2.5
Pre-arrival security control of ships	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	High level	0.78
Security inspection of ships in terminals before cargo operations begin	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	High level	0.78
Employees preparedness, awareness, and training	Well prepared (0,0,1,2)	Average (1,2,3,4)	Poor (3,4,5,5)	Well prepared	0.78
Emergency units' reliability and status of readiness, e.g. Quality, health, safety, environment, security	Well prepared (0,0,1,2)	Average (1,2,3,4)	Poor (3,4,5,5)	Well prepared	0.78
				Total Score	42.80

Based on WPS (2019) Mina al Fahal is a coastal area in the Northeast of Oman, close to Muscat. This port is operated and managed by Petroleum Development Oman LLC. The port was established near a large oil developing and petrol processing plant, Petroleum Development Oman (PDO). It was renamed from Saih al Maleh as the petroleum processing plant was developed. The cargo is loaded on to tankers off Mina Al Fahal by the use of SBMs and subsea pipelines. The offshore draft is 29.2 meters, and loading capacity is 85,000 metric tons per day. The storage capacity of the refinery is 650,000 barrels a day. Crude oil is exported by sea in tankers. The offshore oil loading and unloading facilities include three SBMs and two CBMs. The SBM-1 and SBM-2 are used for loading PDO's crude or Oman Refinery's long residue into the ships. SBM-3 and the two CBMs are used for the import/export of refined products for Shell Oman Marketing Company. There are also three tugboats and a maintenance barge. The export to ships is planned in advance. Each ship stops onshore for about 3 days to receive crude. Crude loading rate starts at a low flow rate initially for about 15 minutes and thereafter increased to normal flow rate. Offshore oil spill response and firefighting equipment are also available at the terminal. They include an 8.5 m rigid inflatable fast response craft fitted with 240 hp diesel engine and a 4.5 m rigid inflatable pollution boom craft fitted with 38 hp diesel engine.

In addition, in Port of Mina Al Fahal predominantly, there is a gusting of wind in Easterly and South-easterly directions and the addressed port is owned and shared both by the government and private sectors. Until now there has not been at all even a single report evidencing any terrorist-related incidents excluding attacks which occurred far from the port area such as multiple attacks carried out on tanker ships in Gulf the of Oman and Port of Fujairah in U.A.E on 2019 (CNN, 2019). Traffic-related circumstances, categories and quantity of hazardous cargoes are monitored by the involved bodies or persons nominated by port authorities. Port facility is executing the ISPS Code constantly. Ship to port security interface ISPS procedures and formalities are always maintained in very high intensity. After consultations with experts and available literature relevant to potential threats along with the other security risk factors which should be considered most important contributing factors affecting the addressed port are all listed in the newly designed SRFT, i.e. Table 4.

Three Ex-Master Mariners with equivalent seagoing and shore-based managerial experiences in risk management have been nominated to carry out this task with the purpose of the rating of the Mina al Fahal offshore terminal for the addressed risk factors depicted in Table 4. The nominated experts have used the fuzzy trapezoidal numbers illustrated in Figure 3 for the rating of the introduced security risk factors. The fuzzy numbers used for equivalent linguistic scales listed in Figure 3 are: high (3,4,5,5), medium (1,2,3,4) and low (0,0,1,2). After evaluation of all security risk factors employing the nominated trapezoidal numbers, as they are all fuzzy linguistic scales they need to be defuzzified to get the subsequent crisp numbers in the shape of scores before adding them all as one to get the final score. The total security score at the end will be the final score of Mina al Fahal offshore terminal, which should be taken into Table 2 for further examination. In this case study as the obtained total score for Mina al Fahal offshore terminal is 42.80, by comparing the obtained security score after rating with the real security points presented in Table 2 it will be determined that as this figure lies between the ranges of 25 to 48 its security importance will be moderate. In this case, Mina al Fahal offshore terminal should maintain security measures for level 2 as per the ISPS Code. The associated recommendations are shown in Table 2.

Furthermore, as it is shown in Table 4 identified risk factors, i.e. visibility status of the addressed offshore terminal (i.e. ships and offshore facilities) with having the maximum score of 4.22 has to be considered as an inherent risk factor of Mina al Fahal offshore terminal. Since the mentioned risk factor is unavoidable in terms of its likelihood as an inherent risk factor (i.e. it always exists in Mina al Fahal offshore terminal and its security risk cannot be decreased and/or eliminated permanently). As a result, the maximum effort to lessen the intensity of such security hazard is only to decrease its occurrences and/or severities probability (See Equation 4). In this case appropriate lookouts, surveillance and early warning system integrated with efficient proper instructions or emergency preparedness plan must be tailored by professionals and authorities such as vulnerability assessment experts to decrease the impact and/or probability of such threat which the mentioned inherent security risk factors play an important role by its contribution.

6. Conclusions and suggestions

Security of the offshore terminal facility is a regulatory binding for any nation and counterterrorism activities are important undertakings. The security-related vulnerabilities and risk factors cannot be eliminated, but they should be decreased. A proper SRM necessitates modifications in organisational behaviour that takes time and needs knowledge if they are to be successful. The solution is to practise a methodical approach to classify critical infrastructures, evaluate security risk factors, and make accurate decisions for the supervision of the probable security threats. Consequently, it is vital to modify the SRM plans to make them compatible with probable security-related outcomes by the available resources at present. Most important outcomes of terrorism require carrying out an additional, comprehensive SRM. In the course of a resource allocation practice based on complete and thorough vulnerability assessment and/or threat analysis, efficient and effective management of the prospective security risk factors is possible. Eventually in this study, a designed SRM framework tailored for Mina al Fahal Offshore Terminal in Sultanate of Oman was established to manage the security threats which can result from any probable terrorists' attacks. The Case study in this paper illustrated how the proposed method can be applied, the results obtained and tailored risk improvement recommendations. In fact, this is a tool that can be used by all PSOTs to meet their legal requirements. For the future research, risk management experts or specialists in offshore terminals and marine ports, in particular, those working in petrochemical complexes or plants must maintain and incorporate the assessment carried out in this study with resilience, business continuity and crisis management related research works. This, in reality, will assist the offshore and marine industry to continue their operations and management even if there are permanent dangers and/or existing security threats. As a result, future work would see further validation on other case studies in theory, but also in practice through collaboration with industry.

Acknowledgements: *This research was partially supported by the Asyad Group, Oman Shipping Company and Petroleum Development Oman in the Sultanate of Oman.*

References

ABS (2003), American Bureau Shipping. A guide for risk evaluations for the classification of marine-related facilities. Available at:
https://ww2.eagle.org/content/dam/eagle/rules-and guides/current/other/117_riskevalforclassofmarinerelatedfacilities/pub117_riskeval.pdf. Accessed on: 08.01.2019.

Anoop, M. B.; Balaji, R. K. and Gopalakrishnan, S. (2006), Conversion of probabilistic information into fuzzy sets for engineering decision analysis. *Computers and Structures.* 84, pp:141–155.

API (2013), American Petroleum Institute. Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries. ANSI/API STD 780. Available At:
https://standards.globalspec.com/std/1603209/ansi-api-std-780.Accessed on: 15.12.2019.

API (2005), American Petroleum Institute. Security Guidelines for the Petroleum industry, Washington, DC, third edition, 2005. Available at:
https://www.nj.gov/dep/enforcement/security/downloads/API%20Security%20Guidance%203rd%20Edition.pdf.Accessed on: 08.01.2019.

Argenti, F.; Landucci, G.; Cozzani, V. and Reniers, G. (2017), A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. *Safety Science*.94: 181–196.

Bajpai, S. and Gupta, J.P. (2005), Site security for chemical process industries, L. Loss Prev. Process. Ind. 18, pp: 301-309.

Baybutt, P. (2017), Issues for security risk assessment in the process industries. *Journal of LossPrevention in the Process Industries*.49: 509-518.

Borodzicz, E.P. (2005), Risk, Crisis and Security Management. ISBN: 9780470867044.

CNN (2019) Cable News Network Report. Available at:

https://edition.cnn.com/2019/07/30/middleeast/yemen-market-explosion-saada-intl/index.html. Accessed on 19, October 2019.

CSC (2018, Chemical-Safety.Com Available at: www. Accessed on: 20.11.2018.

HS (2012), Homeland Security. Chemical Sector Security Awareness Guide. A Guide for Owners, Operators, and Chemical Supply Chain Professionals. Available At: https://www.dhs.gov/sites/default/files/publications/DHS-Chemical-Sector-Security-Guide-Sept-2012-508.pdf. Accessed on: 15.12.2019.

ICS (2015), Institute of Chartered Shipbrokers, UK. Port and Terminal Operations and Management. ISBN: 978-1-908833-63-1.

IMO (2011), International Maritime Organization. Measures to enhance maritime security. Maritime Security Manual – Guidance for port facilities, ports, and ships. Maritime Safety Committee. Available at: http://portalcip.org/wp-content/uploads/2017/05/Guide-to-Maritime-Security-and-the-ISPS-Code-2012.pdf. Accessed on: 15.12.2019.

Kahraman, C. (2001), Capital budgeting techniques using discounted fuzzy cash flows. In: Ruan, D.; Kacprzyk, J. and Fedrizzi, M., Editors, Soft Computing for Risk valuation and Management: Applications in Technology, Environment and Finance, Physica- Verlag, Heidelberg, pp: 375–396.

Kamien, D.G. (2012), Homeland Security Handbook. The McGraw-Hill companies. ISBN: 9780071790840.

Landucci, G.; Argenti, F.; Cozzani, V, and Reniersc, G. (2017), Assessment of attack likelihood to support security risk assessment studies for chemical facilities. *Process Safety and Environmental Protection*.110: 102–114.

Marco, E.G.V.C. (2018). The likelihood interpretation as the foundation of fuzzy set theory. *International Journal of Approximate Reasoning*. 90:333–340.

Marszal, E. and Scharpf, E. (2002), *Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis*. The Instrumentation, Systems and Society (ISA). Research Triangle Park, NC.

Matteini, A.; Argenti, F.; Salzano, E. and Cozzani, V. (2018), A comparative analysis of security risk assessment methodologies for the chemical industry. *Reliability Engineering and System Safety*, pp:1-17.

MCS (2019), Ministry of Central Services. Security risk assessment matrix. Government of Saskatchewan, Canada. Available at: https://taskroom.sp.saskatchewan.ca/Documents/Threat-Risk-Assessment-Template.pdf. Accessed on: 15.12.2019.

Mokhtari, K. (2020), RISK MANAGEMENT - A Guideline for QHSES and Risk Managers in marine ports and offshore terminals. *LAMBERT Academic Publishing in Germany;* March 2020. ISBN: 9786202515603.

Morenoa, V. C.; Reniers, G.; Salzanoa, E, and Cozzani, V. (2018), Analysis of physical and cyber security-related events in the chemical and process industry. *Process Safety and Environmental Protection*.116: 621–631.

Nolan, D.P. (2014), Safety and security review for the process industries. Application of HAZOP, PHA and What-If Reviews. 4th Edition. ISBN: 9780323322959.

OCIMF (2012), Oil Companies International Marine Forum. Marine Terminal Management and Self-Assessment (MTMSA). First Edition. Steamship international. ISBN: 9781856095501. Witherby publishing.

Ross, T. J. (2017), Fuzzy logic with engineering applications. Wiley publication. 4th Edition. ISBN: 9781119235866.

Rubin, B. and Cutter, S. L. (2019), US Emergency Management in the 21st Century: From Disaster to Catastrophe. ISBN: 978-1138354654.

Sugeno, M. (1999), Fuzzy Modelling and Control, CRC press, Florida, USA.

Sutton, I. (2014), Process risk and reliability management. Operational integrity management. 2nd Edition. Published by Elsevier Inc. ISBN: 9780128016534.

WPS (2019), World Port Source. Available at: http://www.worldportsource.com/ports/OMN_Port_of_Mina_al_Fahal_2305.php. Accessed on: 18.12.2019.

Yang, T. and Hung, C. C. (2007), Multiple-attribute decision-making methods for plant layout design problem, *Robotics and Computer-integrated manufacturing*. 23, pp: 126–137.

Yazdi, M. (2018). An extension of the fuzzy improved risk graph and fuzzy analytical hierarchy process for determination of chemical complex safety integrity levels. International Journal of Occupational Safety and Ergonomics.25(4), pp: 551-561.

Zadeh, L. A. (1965), Fuzzy sets. Information and Control. 8, pp: 338–353.