Received 2 May 2020
Revised 14 July 2020
20 October 2020
Accepted 9 November 2020

Security risk management: a case of Qalhat liquefied natural gas terminal

Kambiz Mokhtari
Department of Maritime, International Maritime College Oman, Sohar, Oman

Noorul Shaiful Fitri Abdul Rahman
Department of Logistics Management, International Maritime College Oman, Sohar, Oman

Hamid Reza Soltani and Salim Ahmed Al Rashdi
Department of Maritime, International Maritime College Oman, Sohar, Oman, and

Kawkab Abdul Aziz Mohammed Al Balushi
Department of Foundation, International Maritime College Oman, Sohar, Oman

Abstract

Purpose – At the substantive level, there exists a gap in knowledge about the position of security risk management (i.e. SRM) during the terminals' operations and management; particularly when there is potential for deliberate anti-security acts. Correspondingly, the purpose of this paper is a need for more practical research to find out the justification for the existence of the SRM and different techniques for its appropriate execution on these logistics infrastructures principally with due regard to the potential requirements in the near future.

Design/methodology/approach – Both qualitative and quantitative techniques are used in this study incorporating fuzzy set theory and risk assessment matrix to achieve the research objective.

Findings – A designed SRM framework tailored for Qalhat liquefied petroleum gas (LNG) terminal in Sultanate of Oman was established to manage the security threats which can be resulted from any probable terrorist attacks.

Research limitations/implications – The limited numbers of experts for the purpose of the addressed SRM are causing challenges in data collection.

Practical implications – The pressures for enhanced attention to critical infrastructure security have fostered new challenges for petrochemical seaports and terminals (PSTs). 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.

Originality/value – The development of the security risk factor table model in the case of Qalhat LNG Terminal.

Keywords Security risk management, Petrochemical seaports and terminals,
Security threat analysis, Security vulnerability analysis, Liquefied natural gas, Fuzzy set theory

Paper type Research paper

Maritime Business Review
Vol. 6 No. 4, 2021
pp. 318-338
Emerald Publishing Limited
2397-3757
DOI 10.1108/MABR-05-2020-0028

This research was partially supported by the ASYAD Group, Oman Shipping Company, Sohar Port and Oman LNG L.L.C. in the Sultanate of Oman.

1. Introduction

As a part of marine and process industries, PSTs 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 September 11 was the former paradigm-shifting occurrence for transport systems' security in common. For the maritime and logistics industries, that even, thus, motivated significant changes in the persistent perceptions on security now needed by everyone even remotely related with the operation and management of port's and terminal's security, as well as the vessels, nearby facilities or plants, multimodal transports, the public and employees concerned (Sutton, 2014).

Many of the seaports and offshore terminals are located next to petrochemical complexes such as oil and gas refineries, fertiliser 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 LNG, crude oil, liquefied petroleum gas (LPG) plus a variety of dangerous petrochemical commodities such as ammonia, chlorine, naphtha, sulphur, urea, coal and so on. Any intentional releases of such substances (i.e. due to humans' deliberate acts or intended and malicious operations) or accidental discharges (i.e. due to operator, technical or organisational failures) which can result in the release of the mentioned harmful materials will adversely affect the health and safety of employees within the PSTs and the nearby community in huge amount including damaging the environment. In addition, accidental releases can also result from happenings such as natural catastrophes (CSC, 2018).

Natural disasters are events such as tsunami, earthquake, volcanic activity, flooding, a heavy rainstorm, windstorms, revolving tropical storms all of which can have a destructive consequence on the PSTs. However, all of them addressed events whether they are as a result of intentional or accidental acts can lead to toxic releases, fires, explosions and finally can cause multiple fatalities, economic losses, property and environmental damages (Rubin and Cutter, 2019).

As PSTs 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. Researchers argue that extremists groups could find a benefit in establishing maritime activities as a means for overcoming present security measures on land. 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 happenings and losses are outside the scope of this article and they will not be discussed in this paper, they can be examined under process risk or process safety and reliability engineering but not under the title of SRM. The intentional happenings, as was addressed; i.e. only the three categories of deliberate anti-security acts will be enclosed in this paper for the PSTs. Therefore, an SRM framework will be proposed in the next part of

this paper to overcome the existing and/or potential security-related challenges within the PSTs.

Therefore, 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 PSTs. Moreover, this work consists of the following sections. In Section 2, 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 PSTs. Section 5 is a case study conducted to validate the proposed methodology. Section 6 will explain conclusions and suggestions.

2. Security risk management

As per Borodzicz (2005), the ancient philosophers of Egypt, Greece and China were not only between affiliates of early civilisations to have been concerned about security, several forms of security must have been the origin for these early civilisations 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). From a PST risk point of view, security can be viewed logically as just another dangerous exposure. Although SRM may be viewed as expenditure against the operation, it also stands for a significant threat if not managed thoughtfully. Therefore, managing PSTs' security risk factors as a loss prevention activity can assist a broader appraisal of PSTs' exposure (HS, 2012). As discussed earlier, this could acknowledge terrorists' threats, but also tolerate for broader security agenda. Such losses could be the result of both external and internal terrorists' crimes, but they could also begin from a natural disaster or an accident with no connection to criminal activities. Terrorist attacks such as what they did in New York (9/11), 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 happen again in any place at any time even in PSTs. A terrorist attack on a marine port, particularly if several such attacks take place at the same time, can also disturb the countries' economy. Marine ports tend to be extensive and significant, so it is not likely that any attack would demolish a marine port's infrastructure. However, 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 (CNN, 2019) and (Mokhtari, 2020). However, in the case of petrochemical plants and process facilities if they are located close or within the terminals' or ports' bounders, the overall view similar to the one discussed before 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 (OCIMF, 2012). 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 (e.g. the position of dangerous chemicals, tank farms, pipelines, bypass valves, essential safety and warning systems, emergency stops/shutdown devices or buttons, sites (e.g. terminal) and timetables for leaving and entering many types of ships such as crude oil carriers, LPG, LNG, Chemical tanker, product tanker, bulk carriers handling hazardous goods in bulk, the position of the terminals in which the discharging and loading take place, the amount, duration and type of goods, related cargo manifests, category of the chemical operations and other sensitive information) may make use of them to cause contaminated releases, fires and explosions.

This can lead to a severe impact on health and safety of people, economy, environmental damages and pollutions, as well as fatalities (CSC, 2018; Matteini, *et al.*, 2018 and Morenoa *et al.*, 2018) in "on-site and/or off-site" seaports' areas.

Nevertheless, the theoretical approach towards a generic SRM for PSTs 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 taking proper countermeasures against the identified and assessed threats. For this reason, a generic SRM framework for PSTs can be illustrated in Figure 1.

In overall security threats such as terrorists' deliberate acts on a processing facility like a PST can be avoided if the security triangle (i.e. asset, vulnerability and threat) in a processing facility can be broken down. 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). Security triangle signifies that if any of its three associated elements within the addressed chain reaction is adequately halted or mitigated the risk of a security incident by terrorists can be avoided. This can be fulfilled whether by accurately knowing which types of assets in a PST 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. The statements mentioned 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, resulted from vagueness. Therefore, a significant 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

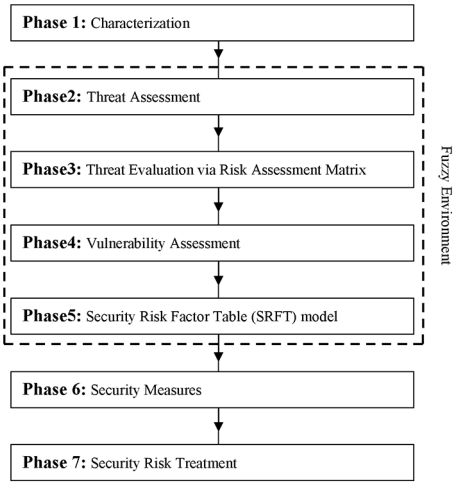


Figure 1.
A generic SRM framework for PST

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 whatsoever, while fuzzy sets permit partial membership. It is possible to use different fuzzy numbers depending on circumstances and in practice, triangular and trapezoidal fuzzy numbers are used (Marco, 2018). Amongst the commonly used fuzzy numbers, triangular and trapezoidal fuzzy numbers are likely to be the adoptive ones due to their ease in modelling easy interpretations. Ross (2017) explains it is known that for engineering applications, to reduce the computational complexity, fuzzy sets with triangular or trapezoidal forms are most commonly used. Both triangular and trapezoidal fuzzy numbers are applicable to the present study. For this reason, fuzzy triangular or fuzzy trapezoidal numbers can be used to deal with threat matrix for the evaluation of the potential security risk factors threatening a PST and to prioritise the threats if it is needed. As the Author has used fuzzy triangular numbers in his previous works (Mokhtari, 2020) then for the purpose of this study trapezoidal fuzzy numbers will be used in SRFT (See Phase 5) for obtaining the overall security score of a PST. 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 $\tilde{M}_1 = (l_1, m_1, u_1)$ and $\tilde{M}_2 = (l_2, m_2, u_2)$ 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.$\otimes$ can be defined as follows (Yang and Hung, 2007):

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

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 is 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 the 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 Bajpai and Gupta (2005); further explanations can be found in their work. However,

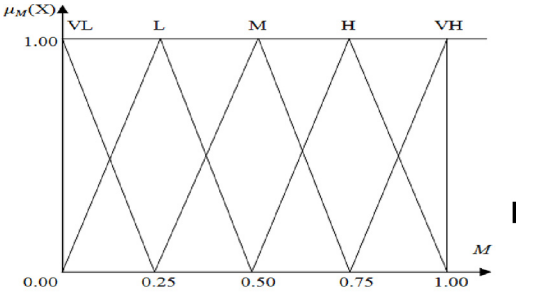


Figure 2.
Fuzzy triangular membership functions

Source: Modified from Yang and Hung (2007)

in this paper, after its application, a different defuzzification method and the process will be used to obtain the final result.

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

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

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

For a trapezoidal fuzzy number of $\tilde{M} = (l, m, n, u)$; i.e.:

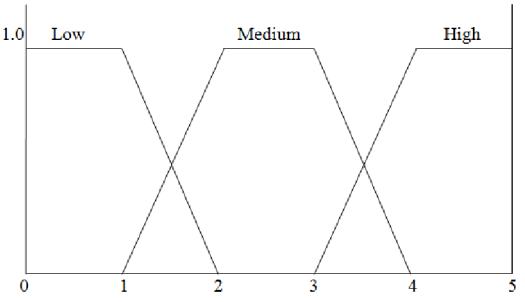
$$\mathrm{M} = \frac{1}{3} \times \frac{(u + n)^2 - (u \times n) - (l + m)^2 + (l \times m)}{(u + n - m - l)} \tag{3}$$

4. Methodology

A suitable methodology, including seven steps, is illustrated in Figure 1. The depicted steps can be easily applied to different petrochemical seaports' and terminals' facilities and their operations at varying degrees of the feature as needed.

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

In the case of the PSTs apart from visiting ships, critical assets are mainly export and import terminals where ships will be made fast alongside the specialised jetties, port control tower or vessel traffic service/management, sound or fog signals, lights, warehouses, breakwaters, firefighting, policing, security, emergency, health and patrol units, office buildings, tugs, pilot boats, dredgers, loading/discharging arms and platforms, power generators, area lightings, CCTVs, fences, gates, emergency shutdown valves, cargo



Source: Bajpai and Gupta (2005)

Figure 3.
Fuzzy trapezoidal membership functions

transfer equipment, safety and security equipment, alarms, gas detection systems and any other equipment and devices related or connected to the adjusting processing plants or units (OCIMF, 2012).

Phase 2 – Threat assessment: Identify and characterise 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, 2014 and Landucci *et al.*, 2017).

As Kamien (2012) describes a threat assessment can be based on categories or sources of threats. In the case of PSTs and as per the sources of threats, whether they are based on external or internal sources, Table 1 illustrates examples of these sources of threats.

The below-mentioned threat categories are possible types of security risk factors in PSTs due to deliberate acts caused by terrorists as per ISPS (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;
- Robbery of harmful substances 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;

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

Source: Modified and based on Sutton (2014)

Table 1.
Examples of sources of threats in PSTs

- 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 for instance 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' probability. The probabilities of the potential security risk factors' occurrences can be assessed 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 the security risk factors (threats) of a PST. Moreover, in a PST, the depicted various theorists' acts can be planned in such a manner to be carried out even by travelled pirates from remote places, asylums or stowaways.

Phase 3 – Threat evaluation via risk assessment matrix: There are many assessment means and tools to assist security risk management experts to calculate the different threats' levels within the particular facilities. By the way, 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 source are subjective and estimated by experts' judgements. The particular technique for its application mainly depends on whether the essential risk mitigation is specified in a statistical or qualitative approach. 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 valuation tools because of its simplicity. The security threat matrix handles the frequency (likelihood) and consequence (impact or severity) of the security threats qualitatively, based on a categorisation 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 plan the condition under thought in the illustration. 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 segregate the threat impacts or severities into catastrophic, major, moderate, minor and insignificant as per the level of threat's impact or

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

Source: MCS (2019)

Figure 4.
A classic risk evaluation matrix designed for threat assessments in PST

severity. The likelihood types are also segregated into almost certain, likely, possible, unlikely and rare. The addressed categories can be chosen either qualitatively, using experts' judgements as described above and exposed in Figure 4. However, quantitative methods (e.g. See fuzzy sets in Section 3) can besides be used by experts to make it helpful for assessing 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 (2003) argues a regular risk assessment and presentation technique is basically to multiply the likelihood (L) of each unwanted happening by each severity (S) or impact and after that add these products together for all cases considered in the estimation. As a result, for the mentioned explanations, risk levels can be determined by the use of the depicted parameters and via using the below-mentioned equation:

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

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

$$\tilde{R} = \tilde{L} \otimes \tilde{S} \tag{5}$$

where $\otimes$ is a symbol of multiplication under fuzzy environments.

As Baybutt (2017) describes a security risk (threat) matrix can be used to determine each one of the security risk factors related to and/or contained by a facility with no 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 assessing 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 mixture use of both discussed quantitative and qualitative methods, security risk factors (threats) could be prioritised for further use and reasons. As per Figure 2, proper fuzzy linguistic scales beside their membership functions have been demonstrated for the happening likelihoods. The same fuzzy numbers and scales can be used 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 per Figure 3 if a security risk factor (threat) as per 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 our capability to discover it, time and duration of the warning, the organisation's reaction and the capability of the aggressor to defeat the reaction. 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, as per 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 maintain a vulnerability assessment must be thoroughly recognised with the engineering or business-related processes under inspection, e.g. highly skilled and 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 fertiliser plant. 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, intelligence services regulators.

As per Nolan (2014), Argenti *et al.* (2017); Baybutt (2017) and Yazdi (2018) three types of persons are required to carry a vulnerability assessment: a team leader, a recorder/scribe and the experts. The experts are usually:

- The project manager or engineer who has planned and designed the addressed plant/facility;
- An individual well-known with how the plant will be operated, e.g. a safety and/or process engineer; and
- An individual was 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; nevertheless, there will be more important to relate its review to highly visible, expensive and vital operations, plants and/or facilities.

As a vulnerability assessment is a qualitative shape of evaluation, the subsequent processes must be conducted by vulnerability assessment experts to accomplish a victorious investigation within a PST:

- Divide the PST 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.
- Recognise 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 in-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 the 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 PST 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 PST are demonstrated. Following scoring the security risk factors planned within the addressed SRFT by specialists or security auditors, using the three points trapezoidal fuzzy numbers depicted in Figure 3, the total score acquired from SRFT will cause to assess the present status of the security risk within a PST.

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 has 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.

After 9/11 happenings as International Ship and Port Facility Security (ISPS) Code ratified, it has been incorporated in Chapter 11 of the Safety of Life at Sea Convention (SOLAS) 1974 of the International Maritime Organisation (IMO). Because of this fact, the 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. Consequently, after 9/11, the vulnerability of an attack on countries using port facilities and ships has been more understood. In this respect, 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 on 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.

There is also the most unpleasant case results impact on a marine port due to any terrorist attacks. They can be assessed as per the expansion of scenarios of the outcomes of a terrorist event at a marine port. As per API (2013) and Sutton (2014), there exist other issues in a PST that should be taken into consideration when making an SRFT. Finally, consistency and importance of readiness of the emergency brigades referring to security, environment, safety and health issues of PSTs 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 (i.e. a perfectly secure and reliable port facility is the one where there are no disruptive security events that could undermine the scheduled work within the port and as per the following formula it should be equal to 1. This formula can be used by experts for rating and scoring the mentioned security risk factor within an SRFT) can be defined as follows:

$$\text{Port security reliability ratio} = \frac{\text{Number of effective days a port worked without security interruptions}}{\text{Number of scheduled working days}} \tag{6}$$

Phase 6 – Security measures: To introduce security countermeasures against security risk factors' (threats') scenarios and to assess them to check if the available protecting safeguards and/or countermeasures are sufficient. As during many of the risk mitigation phases used in most of the industry-related applications, rings of protection were needed, therefore; throughout SRM of marine ports, a similar technique can also be an appropriate one. For this purpose, the US Homeland Security (HS, 2012) describes that security tends to underline "rings of protection", which 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 PST, 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 that to reach the control room, a terrorist would have to go through and pass numerous rings of protection, for instance, a fence at the PST borders, an elevator with key-controlled floor buttons, an alert receptionist, a locked external door and a locked door to the control room. The latter verifies if the rings of protection are well-organised, 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 (2011) 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). In this stage, the explained security levels are incorporated in Table 2. The addressed thresholds for the obtained points to four levels of security risk status shown in Table 2 were originally adapted from CSC (2010) who are experts in site survey and to carry out detailed audits for onshore and offshore petrochemical and process facilities and to conduct strong risk assessments and evaluations of potential workplace hazards; recommendations for corrective actions.

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: Modified from CSC (2010)

Table 2. Countermeasures and recommendations tailored for the final score to be obtained while using an SRFT

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 furthermore, to find out if the treatments are appropriate.

Table 2 demonstrates additional procedures and/or guidelines to be adhered to in different security surroundings, depending on which level of security a terminal or port facility is kept. Subsequently, after ranking the security risk factors by use of the abovementioned steps such as using a threat matrix or an SRFT, the required procedures and/or guidelines can be tailored and implemented on a PST for this step.

5. Case study at Qalhat liquefied natural gas terminal

A marine port shown in Figure 5 is the petrochemical seaport of Qalhat in Sultanate of Oman (i.e. Geographical Position: 22°39′40″N 59°24′19″E), including the following different zones:

- *Zone A:* includes a natural gas processing plant including a single train liquefaction plant with different storage tanks, sweetening and liquefaction units and also related gas processing facility for the handling of the extracted natural gas with the ability to produce LNG and natural gas liquids (NGL), i.e. Condensate cargoes for export.
- *Zone B:* including two T-jetty type terminals for exporting produced LNG via LNG tanker ships and for exporting Condensate cargoes through product tanker ships.
- *Zone C:* includes a combined gas and steam turbine type power plant.
- *Zone D:* includes a fertiliser plant with the capability to produce ammonia and urea.

With taking into consideration of the proposed SRM methodology (i.e. See Phase 1 in Section 4) in this article petrochemical seaport of Qalhat in the Sultanate of Oman have been separated into four different areas as shown in Figure 5 and/or depicted in Table 3. For this paper, it has been decided to use only one of the T-jetties' (i.e. LNG Terminal located in

Figure 5.
Qalhat area: adopted from Google map and modified by the authors

Zone A (Liquefaction plant)	Zone B (T-jetty terminals)	Zone C (Power plant)	Zone D (Fertiliser plant)
1 Purification unit for removing CO_2, water and mercury from the feed gas	**1** T-Jetty to accommodate product tankers: Displacement 13,000 M/Ts, LOA 140 m, Draft 7.7 m (condensate export terminal)	**1** Five units of gas turbines	**1** Two ammonia production plants
2 Distillation unit to remove condensates via fractional distillation of feed gas after its treatment	**2** T-Jetty to accommodate LNG tankers: Displacement 143,400 M/Ts, LOA 315 m, Draft 12.1 m (LNG export terminal)	**2** Five triple pressure heat recovery steam generators	**2** Two urea production plants
3 Liquefaction unit to liquefy the remaining gases	**3** Port control and pilots	**3** Three steam turbines	**3** Fuel storage tanks
4 NGL storage tanks	**4** Tugs and mooring boats	**4** Diesel generators	**4** Diesel generators
5 LNG storage tanks	**5** Port's machinery parking area	**5** Pipelines and pumps	**5** Gate
6 Pipelines and pumps	**6** Port state control	**6** Guardroom	**6** Guardroom
7 Gate	**7** Blocks for Stevedores	**7** Blocks for employees	**7** Blocks for employees
8 Guardroom	**8** Onshore LNG pumping station	**8** Fire brigades	**8** Fire brigades
9 Blocks for employees	**9** Onshore NGL pumping station	**9** Car parking area	**9** Car parking area
10 Fire brigades	**10** LNG emergency shutdown unit	**10** Gate	**10** Ammonia storage tanks
11 Car parking area	**11** NGL emergency shutdown unit	**11** Fuel storage tanks	**11** Urea storage units
12 Administrative building	**12** Administrative building	**12** Administrative building	**12** Administrative building

Table 3. Portrayal of the petrochemical seaport of Qalhat

Zone B) for the addressed case study in this section. Now for calculating the total security score of the LNG Terminal located at Zone B of Qalhat petrochemical seaport, there is a need to modify a new SRFT for this LNG terminal. The newly designed SRFT (i.e. to modify the new SRFT; Phase 2, Phase 3 and Phase 4 in Section 4 have been used by the addressed experts in this section so as to integrate the procedures mentioned within the addressed phases to generate Phase 5 in the form of new SRFT) including the classified security risk factors (threats) are shown as follows (Table 4).

For the purpose of this case study and to fulfil the proposed SRM methodology during the course of threat assessment (i.e. see Phase 2 in Section 4) it has been decided to use deliberate acts of international terrorists as a source of threats. Moreover, during the evaluation of the security risk factors mentioned within the newly designed SRFT, the addressed experts have been taken into their consideration to use the risk assessment matrix (i.e. See Phase 3 in Section 4) to rate these risk factors. Consequently, the addressed experts in this paper have used and followed procedures mentioned within the proposed SRM methodology (i.e. See Phase 4 in Section 4) to achieve a successful analysis of the newly designed SRFT (i.e. See Phase 5 in Section 4).

Table 4.
Specified security risk factor table (SRFT) for Qalhat LNG export terminal (i.e. Zone B)

Security risk factors	Range of security points			Security experts' ratings	Defuzzyfied scores
LNG terminal's location	Rural (0,0,1,2)	Urban (1,2,3,4)	High density (3,4,5,5)	Urban	2.5
The visibility status of the LNG terminal	Not visible (0,0,1,2)	Less visible (1,2,3,4)	Highly visible (3,4,5,5)	Highly visible	4.22
Size of the nominated T-jetty	Medium (0,0,1,2)	Large (1,2,3,4)	Very large (3,4,5,5)	Very large	4.22
Size of the LNG ships	Medium (0,0,1,2)	Large (1,2,3,4)	Very large (3,4,5,5)	Very large	4.22
Tanker ships traffic	Low (0,0,1,2)	Medium (1,2,3,4)	High (3,4,5,5)	Medium	2.5
Port's ownership	Private (0,0,1,2)	Public/private (1,2,3,4)	Government (3,4,5,5)	Public/private	2.5
Presence of terrorists 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/port facility	Low (0,0,1,2)	Moderate (1,2,3,4)	Severe (3,4,5,5)	Severe	4.22
Worst impact off-site/port facility	Low (0,0,1,2)	Moderate (1,2,3,4)	Severe (3,4,5,5)	Moderate	2.5
History of security incidents in port	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		
Chemical weapon (CW) 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		0.78
Access control from land	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	High level	0.78
Access control from sea	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	High level	0.78
Perimeter protection	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	High level	0.78
Mitigation potential	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	High level	0.78

(*continued*)

Security risk factors		Range of security points		Security experts' ratings	Defuzzyfied scores
Proper lighting (All over the port)	(0,0,1,2)	(1,2,3,4)	(3,4,5,5)	High level	0.78
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)	High level	0.78
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 pieces of training	Well prepared (0,0,1,2)	Average (1,2,3,4)	Poor (3,4,5,5)	Well prepared	0.78
Reliability and status of readiness of emergency units e.g. health, safety, environment, security	Well prepared (0,0,1,2)	Average (1,2,3,4)	Poor (3,4,5,5)	Well prepared Total score	0.78 41.86

Table 4.

Based on WPS (2019) LNG Terminal at the petrochemical seaport of Qalhat is situated within 20 km distance from the coastal city of Sur. The city is situated at the Southeast of the addressed port along the coastline and predominantly, there is a gusting of wind in Easterly and South-easterly directions. As it is evident from Figures 5 and 6 the addressed facility is situated in a rural area. Qalhat LNG exports 3.3 million tons per annum. All of LNG Tanker ships berthing at Qalhat LNG terminal and other units situated within the harbour or the addressed T-jetty are always highly visible from the seaside, as well as outside of the port. Port is under the ownership of the government and private sectors. Up to that time, there have not been any reports for terrorist activities except attacks that happened outside of the port area such as multiple attacks carried out on tanker ships in the Gulf 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 regularly. Ship to port ISPS related interface procedures and paperwork are at all times kept in particularly high intensity. After consultations with experts and available literature relevant potential threats along with the other security risk factors which to be considered most critical contributing factors affecting the addressed port are all listed in the newly designed SRFT, i.e. Table 4.

Three Ex-Master Mariners (i.e. all experts have BSc degrees in Nautical Studies and are also holding Class I unlimited Master Mariner Certificate of Competency) with equivalent seagoing and shore-based managerial experiences in marine operations and management have been introduced to carry out this assignment during the designing of the addressed SRFT and to rate Qalhat LNG Terminal for the security risk factors depicted in Table 4. Presently all these three captains are nautical lecturers at International Maritime College Oman. They also train all Qalhat Terminal's Pilots for their Pilotage Proficiency Training courses within the Sultanate of Oman and they are expert enough in the addressed tasks and maritime fields. The security experts have used the fuzzy linguistic scales of trapezoidal

Figure 6.
Qalhat LNG terminal

Source: Oman Daily Observer (2019)

numbers illustrated in Figure 3 to score the risk factors. The fuzzy trapezoidal numbers used to match with the linguistic scales demonstrated in Figure 3 are such as low (0,0,1,2), medium (1,2,3,4) and high (3,4,5,5). After scoring of all security risk factors using the described linguistic scales, as they are all fuzzy trapezoidal numbers, they are required to be defuzzified [i.e. Equation (3)] to get the related crisp numbers in the form of scores before adding them all together to obtain the total score. The total score will be the security score of Qalhat LNG Terminal, which need to be taken into Table 2 for further inspection. The rating for security risk factors shown in Table 4 was the same during the course of experts' judgements and the weights of the addressed experts in respect of each other were also the same. Therefore, if the same opinions are aggregated and then divided by three then the result will be the same opinion.

In this case study as the resulted final score for Qalhat LNG Terminal is 41.86 then by comparing the obtained score with the actual security points existing in Table 2 it will be confirmed that as this number lies between the ranges of 25 to 48 its security position is moderate. In addition, the reason for using only one score to present the risk level of the addressed terminal is that the chosen linguistic scales of trapezoidal numbers by experts for each one of the individual security risk factors are based on fuzzy numbers and after their defuzzifications to get their crisp values, they will only represent the weight of each one of the individual risk factors. Therefore, the sum of the total weights of all risk factors will represent the overall risk level of the addressed terminal about the studied risk factors which is specified in Table 2. That means Qalhat LNG Terminal should preserve and acquire countermeasures as per ISPS Code security level 2. The associated countermeasures can be found in Table 2 (i.e. See Phase 6 in Section 4). Furthermore, as it can be seen from Table 4 security risk factors, i.e. visibility status of the LNG Terminal, worst impact on-site/port facility, size of the T-jetty and size of the LNG Tankers with having a maximum score of 4.22 for each can be considered as inherent risk factors of Qalhat LNG Terminal. As the described risk factors are inevitable in terms of their probability as inherent risk factors that mean they are permanently present in Qalhat LNG Terminal and they cannot be decreased, avoided or controlled forever, therefore, there is a need for incorporating a security risk treatment procedure on them (i.e. See Phase 7 in Section 4). Consequently, the maximum efforts to decrease the level of such security risk factors are only to decrease their impact and/or likelihood [Equation (4)]. In this case, a proper lookout, surveillance and early warning system integrated with an efficient emergency preparedness plan. Alternatively, appropriate instructions must be modified by security professionals and experts like vulnerability assessment team members to decrease the severity and likelihood of such security risk factors which the exposed inherent security risk factors play a substantial role by their contributions.

6. Conclusion

Security of the petrochemical seaport and the terminal facility is binding for any nations and antiterrorism are great undertakings. The security-related vulnerabilities and risk factors cannot be removed in total, but it 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 practice 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. The most important outcomes

of terrorism facilitate for 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 Qalhat LNG Terminal in Sultanate of Oman was established to manage the security threats which can be resulted from any probable terrorist attacks. For 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. In addition, the addressed zones of A, C and D can be assessed for the same reason in future 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.

References

American Bureau Shipping (ABS) (2003), "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 08 January 2019).

American Petroleum Institute (API) (2005), *Security Guidelines for the Petroleum industry*, API Washington, DC, third edition, available at: www.nj.gov/dep/enforcement/security/downloads/API%20Security%20Guidance%203rd%20Edition.pdf (accessed 08 January 2019).

American Petroleum Institute (API) (2013). "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 15 December 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*, Vol. 84 No. 3-4, pp. 141-155.

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*, Vol. 94, pp. 181-196.

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

Baybutt, P. (2017), "Issues for security risk assessment in the process industries", *Journal of Loss Prevention in the Process Industries*, Vol. 49, pp. 509-518.

Borodzicz, E.P. (2005), "Risk, crisis and security management", ISBN: 9780470867044.

Cable News Network (CNN) (2019), "Cable network news report", available at: https://edition.cnn.com/2019/07/30/middleeast/yemen-market-explosion-saada-intl/index.html (accessed 19 October 2019).

Chemical Safety Com (CSC) (2010), "Advanced chemical safety", available at: www.chemical-safety.com (accessed 20 November 2019)

Chemical Safety Com (CSC) (2018), "Advanced chemical safety", available at: www.chemical-safety.com (accessed 19 October 2019)

Homeland Security (HS) (2012), "Chemical sector security awareness guide", A Guide for Owners, Operators, and Chemical Supply Chain Professionals, available at: www.dhs.gov/sites/default/files/publications/DHS-Chemical-Sector-Security-Guide-Sept-2012-508.pdf (accessed 15 December 2019).

Institute of Chartered Shipbrokers (ICS) (2015), "Portand terminal operations and management", Institute of Chartered Shipbrokers, ISBN: 978-1-908833-63-1.

International Ship and Port Facility Security Code (ISPS) (2011), "Measures to enhance maritime security", Maritime Security Manual – Guidance for port facilities, ports and ships. Maritime Safety Committee. International Maritime Organization, available at: http://portalcip.org/wp-content/uploads/2017/05/Guide-to-Maritime-Security-and-the-ISPS-Code-2012.pdf (accessed 15 December 2019).

Kamien, D.G. (2012), *Homeland Security Handbook*, The McGraw-Hill Companies. New York, NY, 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*, Vol. 110, pp. 102-114.

Marco, E.G.V.C. (2018), "The likelihood interpretation as the foundation of fuzzy set theory", *International Journal of Approximate Reasoning*, Vol. 90, pp. 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.

Ministry of Central Services (MCS) (2019), "Security risk assessment matrix", Ministry of Central Services. Government of Saskatchewan, available at: https://taskroom.sp.saskatchewan.ca/Documents/Threat-Risk-Assessment-Template.pdf (accessed 15 December 2019).

Mokhtari, K. (2020), *Risk Management – A Guideline for QHSES and Risk Managers in Marine Ports and Offshore Terminals*, *LAMBERT Academic Publishing;* Saarbrücken ISBN: 9786202515603.

Morenoa, V.C., Reniers, G., Salzanoa, E. and Cozzani, V. (2018), "Analysis of physical and cybersecurity-related events in the chemical and process industry", *Process Safety and Environmental Protection*, Vol. 116, pp. 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.

Oil Companies' International Marine Forum (OCIMF) (2012), *Marine Terminal Management and Self-Assessment (MTMSA)*, 1st ed., Steamship international Witherby publishing. ISBN: 9781856095501. Livingston.

Oman Daily Observer (2019), "Oman LNG weighs capacity expansion", available at: www.omanobserver.om/oman-lng-weighs-capacity-expansion/ (accessed 20 October 2020).

Ross, T.J. (2017), *Fuzzy Logic with Engineering Applications*, 4th ed., Wiley publication. New York, NY 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, FL.

Sutton, I. (2014), "Process risk and reliability management", *Operational Integrity Management*, 2nd Edition. Elsevier. ISBN: 9780128016534.

World Port Source (WPS) (2019), "World port source", available at: www.worldportsource.com/ports/maps/OMN_Port_of_Qalhat_3945.php (accessed 18 December 2019).

Yang, T. and Hung, C.C. (2007), "Multiple-attribute decision-making methods for plant layout design problem", *Robotics and Computer-Integrated Manufacturing*, Vol. 23 No. 1, 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*, Vol. 25 No. 4, pp. 551-561.

Zadeh, L.A. (1965), "Fuzzy sets", *Information and Control*, Vol. 8 No. 3, pp. 338-353.

Further reading

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

Corresponding author
Noorul Shaiful Fitri Abdul Rahman can be contacted at: noorul@imco.edu.om