CHEMICAL ENGINEERING TRANSACTIONS
VOL. 86, 2021
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Sauro Pierucci, Jiří Jaromír Klemeš

ISBN 978-88-95608-84-6; **ISSN** 2283-9216

Analysis of Security Threats for Offshore Oil&Gas Operations

Matteo Iaiani, Namig Musayev, Alessandro Tugnoli*, Paolo Macini, Valerio Cozzani, Ezio Mesini

LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum – Università di Bologna, Italy
a.tugnoli@unibo.it

Offshore Oil&Gas operations are a key part of the supply of energy in many countries. Worldwide, about a third of the oil is produced offshore and, in Europe, more than 80% of the current Oil&Gas production takes place offshore. Offshore Oil&Gas installations may be the target of malicious acts aiming at causing severe impacts in terms of damage and media coverage, comparable to the outcomes of major accidents originating from safety-related causes. The attractiveness of such installations is linked to the high amount of hazardous substances handled, their socio-political location, and the possibility of obtaining proprietary information important for the business. In the present study, in order to frame a clear picture of the security threats affecting offshore Oil&Gas operations, a database of 2222 security-related incidents occurred in the last 49 years was developed and analysed. Itemized categories used to classify the events by industrial sector, security threats, attack modes, and final scenarios triggered by the malicious acts, were defined and analysed with Exploratory Data Analysis (EDA). Correlations among itemized categories were investigated using Correspondence Analysis (CA). Overall, the results show the concreteness of the security threats to offshore Oil&Gas installations.

1. Introduction

Offshore Oil&Gas operations may be the target of malicious acts perpetuated by various threat actors, ranging from disorganized pirates to hostile state-nations or state-sponsored organizations, that can be motivated by monetary gain, disruption of economic and political equilibria, revenge, challenge and environmental awareness (Kashubsky, 2011). In the case of offshore platforms, the threat actors may be particularly attracted by the specific company profile (multinational companies, companies with a leading position in a specific sub-sector, etc.) or by the socio-political location of the target plant (Argenti et al., 2015).
Besides the direct outcomes of an attack in terms of casualties and loss of production, the potential for release of large quantities of hazardous materials as a result of a malicious attack, defines scenarios of damage to people, environment and assets comparable to the outcomes of major accidents originating from safety-related causes (e.g. the well-known explosions occurred at the Piper Alpha oil platform in 1988 (Shallcross, 2013) and at the Deepwater Horizon drilling rig in 2010 (Bozeman, 2011)). For example, in March 1983 Iraqi aviation attacked an Iranian offshore platform, causing a two-year long oil spill that amounted to a total of 1.9 million barrels of oil dispersed in the Persian Gulf (Kashubsky, 2011).
The application of Security Risk Assessment (SRA) and Security Vulnerability Assessment (SVA) methods, that are experience-based qualitative, or semi-quantitative tools for assessing the security threats facing a facility, and evaluating risk-mitigation strategies (Matteini et al., 2019), can be supported by past incident analysis, for example as regards the phases of identification of the threat actors and related attack patterns, of the final scenarios that can be triggered by an attack, and of possible safety/security countermeasures. Examples of SRA/SVA methods are the CCPS methodology, the VAM-CF methodology, the API RP 780 methodology, and the RAMCAP methodology.
The present study aims at collecting and analyzing past security-related incidents (SIs) affecting industrial offshore Oil&Gas operations, retrieving data from a broad set of sources. The analysis focuses on time and geographical trends, security threats, industrial sectors, attack modes, final scenarios, and correlations

between them. Data was analysed using Exploratory Data Analysis (EDA), including Correspondence Analysis (CA), and the results can be used to support the application of SRA-SVA methods.

2. Methodology

Three main steps, typical of a past incident analysis, were followed: i) retrieval of data on past security-related incidents (SIs); ii) construction and population of a dedicated database; iii) analysis of the database.
The data sources from which SIs were collected are listed below:

- Open-source databases: Maritime Safety Information (MSI, 2021), Global Terrorism Database (GTD, 2021), The Repository of Industrial Security Incidents (RISI, 2015).
- Scientific literature: "A Chronology of Attacks on and Unlawful Interferences with Offshore Oil and Gas Installations, 1975 – 2010" (Kashubsky, 2011).
- Newspaper articles, web archives, extracts from books (used to integrate the information found in the above sources).

Two criteria were defined to include incidents in the database: 1) the incident should originate as a result of a malicious act aimed at interfering with normal operations; 2) the incident involves an industrial offshore Oil&Gas installation or offshore Oil&Gas transportation of hazardous chemicals as a primary objective. These criteria intentionally exclude fuels transported in fuel tanks to avoid the inclusion of events related to large fuel-propelled watercrafts such as cruise ships, container ships, and ferries.
The general structure of the database (see Figure 1) is adapted from Casson Moreno et al. (2018). Each entry in the database consists in the compilation of free text fields and itemized fields: free text fields allows retaining general details concerning the incident (e.g. date, location, data source, etc.), while itemized fields ("INDUSTRIAL SECTOR", "SECURITY THREAT", "ATTACK MODE", "FINAL SCENARIO", blue-shaded in Figure 1) help describe unambiguously a certain characteristic of the event. The categories and relative definitions for the itemized fields were adapted from Casson Moreno et al. (2018), Iaiani et al. (2020a), and the EU Directive 2013/30/EU (European Parliament and the Council).

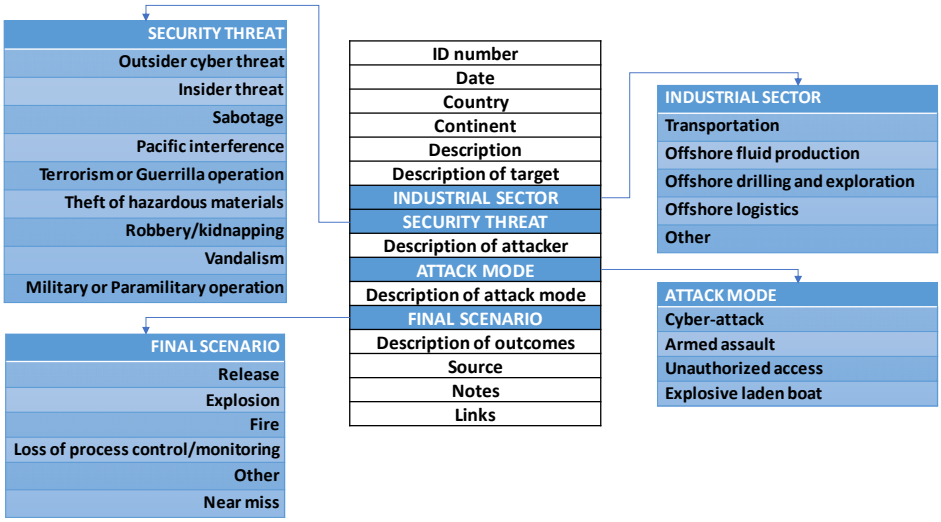

Figure 1: Database structure. The classes associated to each itemized field (blue-shaded) are reported.

The overall database was then investigated using Exploratory Data Analysis (EDA) (Tukey 1977), focusing on time and geographical trends, industrial sectors, security threats, attack modes, final scenarios, and correlations between them. In particular, the correlations were investigated by the application of the Correspondence Analysis (CA) (Greenacre, 2017), which aims at revealing the relative relationships between and within two groups of variables. The input data for the application of CA is given in the form of a contingency table, i.e. a table with row and column labels filled with the combined frequencies of the variables (i.e. number of SIs in the present study). Subsequently, the following main steps are computed (Greenacre, 2017): i) calculation of row/column profiles (sets of row/column relative frequencies) and masses (marginal total of a row/column, divided by the grand total of the table, used as weights in CA); ii) calculation of residuals (between expected values of row/column profiles from homogeneity hypothesis and their observed values); iii) calculation of X^2-distance and total inertia (weighted sum of squared distances), which are expression of how far the row/column profiles are to the average row/column profile; iv) reduction of dimensionality (Singular Value Decomposition to 1D/2D/3D); display of the projected row and column profiles (1D/2D/3D maps) in

order to be visualized and discussed. Therefore in CA, the points are profiles, the weights are the masses of the profiles, and the distances are X^2-distances. Some basic indications on how to interpret a correspondence 2D-map are given in section 3.4. The Matlab script used in the present work for the implementation and application of CA was developed by Seva et al. (2009). Since some classes identified in EDA contain a relatively low number of recorded entries, care shall be put into assigning rigorous statistical value to the results of the count. However, as common in cases of rare events and early warnings analysis (Paltrinieri et al. 2012), some general lessons can be learnt even from a limited number of events.

3. Results and discussion

3.1 The time trend and the location

Figure 2a shows the quinquennial time trend of the SIs collected in the database. Prior to the year 2000 only 36 SIs were recorded, justifiable by an increased attention to the practice of reporting security-related incidents after the "9/11" terrorist attacks in New York. For the following years, the time trend shows an average of 530 events per 5-year period, with a peak of 680 events recorded in the 2010-2014 period.
The geographical distribution of the incidents recorded is showed in figure 2b. Most of the incidents took place in Asia (1292, 60 %) followed by Africa (722, 32 %), South America (112, 5 %), Central America (32, 1 %), Europe (25, 1 %), and North America (17, < 1 %). Eighteen (18) of the SIs recorded could not be classified by continent, since they occurred on a body of water between two continents, such as the Bab el-Mandeb strait between Africa and Asia, or in open ocean. The geographical regions most affected resulted to be the Strait of Malacca (between Indonesia and Malaysia) and the Gulf of Guinea (mainly Nigeria), due to strategic location for international maritime shipping routes, in conjunction with a complex piracy issue, compounded in opportunistic attackers, organized criminal syndicates, and terrorist groups (Jin et al., 2019). Nigeria, and in general the Gulf of Guinea, is characterized by violent and frequent piracy and guerrilla attacks (Peters, 2020) affecting both the high number of offshore installations present in the region and ships used for transportation of hazardous materials or to support offshore operations.

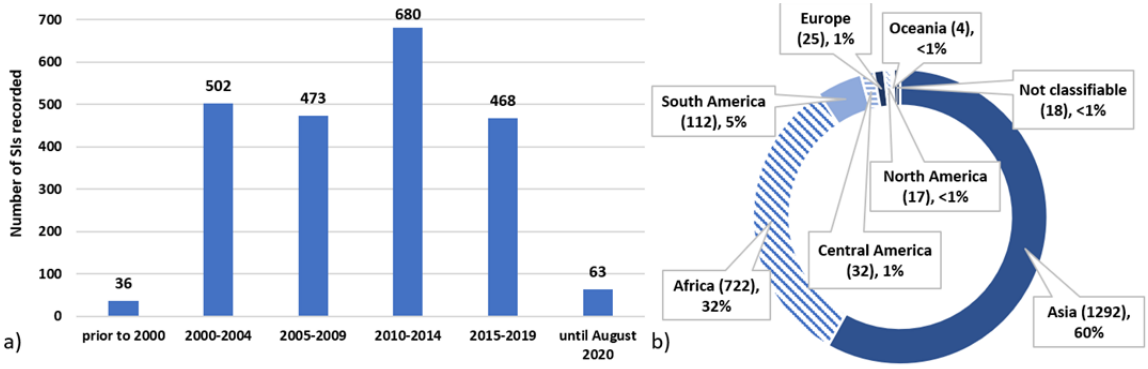

Figure 2: a) Quinquennial time trend of the incidents; b) Geographical distribution of the incidents.

3.2 The industrial sectors affected and the security threats

The distribution of the SIs by industrial sectors is shown in Figure 3a. The transportation sector resulted the most affected (1979 out of 2222, 89 %), followed by the offshore fluid production sector (100, 5 %), the offshore logistics sector (87, 4 %), and the offshore drilling and exploration sector (28, 1 %). Among the security threats (Figure3b), robbery/kidnapping (1472, 66 %) resulted the most recorded, followed by guerrilla operation/terrorism (86, 4 %), theft of hazardous materials (38, 2 %), and pacific interference (33, 1 %). The categories sabotage, insider threat, outsider cyber threat constitutes less than 10 incidents each. Almost a quarter of the incidents could not be categorized by security threat, and thus were labeled as "unknown", situation commonly encountered in failed assaults to ships, such as the attempted boarding of the Liberian-flag tanker Louise on 6 December 1999, where unidentified persons opened fire on the tanker after failing to board it (MSI, 2021), or in unclaimed attacks perpetrated by unknown assailants, such as the one occurred in Nigeria on 10 of June 2008, when fire was opened by unknown perpetrators upon an oil facility (Kashubsky, 2011). The preponderance of transportation-related SIs can be explained by the fact that ships are vulnerable to opportunistic attacks perpetrated by disorganized criminals, which are more common than organized, large-scale criminal acts. This could also justify why theft of personal belongings or equipment is more commonly encountered than theft of hazardous substances, such as in the case of syphoning of oil from tankers or well-heads, which requires a high level of knowledge and skill.

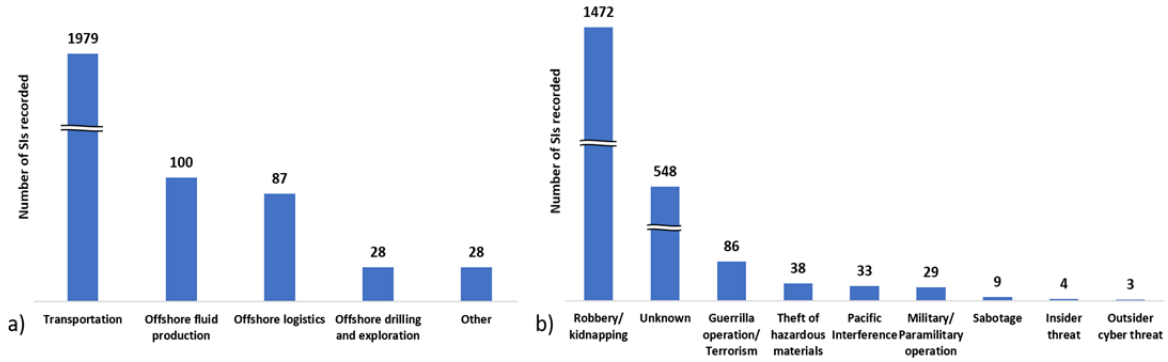

Figure 3: a) Distribution of the incidents by industrial sector; b) Distribution of the incidents by security threat.

3.3 The attack modes and final scenarios

Figure 4a shows the contingency table considering the attack modes and the final scenarios. The most common scenario is the absence of significant industrial accidents, indicated as “other” final scenario, with 2183 cases out of 2222: almost half of these SIs were caused by armed assaults (1084 out of 2183), followed by unauthorized accesses (33), use of explosive laden boats (9), cyber-attack (1), while the attack mode is unknown in the remaining SIs (1056). Such a high number of unclassifiable SIs by attack mode is due to the common practice in incident reporting of focusing on accident scenarios and outcomes of the events rather than on the attack modes perpetrated by the attackers. Eleven (11) cases of explosions were registered in the database, all related to armed assaults. For example, on 19 December 2007, in Nigeria, an oil company barge was blown up with dynamite by gunmen trying to hijack the vessel (MSI, 2021). In 4 records, a release of a hazardous substance was reported: 2 caused by armed assaults and 2 related to unknown attack modes. Three (3) cases of fire were registered, 2 caused by explosive laden boat attacks, such as the suicide attack perpetrated by Tamil separatists off Sri Lanka’s northern coast on 31 of October 2001, setting ablaze the oil tanker Silk Pride (GTD, 2021), and one of unknown attack mode. Two (2) cases of loss of process control/monitoring and 1 case of near miss (i.e. an event in which an incident scenario could have plausibly resulted if circumstances had been slightly different) were collected, all caused by cyber-attacks. For example, in 2003, database servers located on an offshore platform in the United States were infected by a SQL Slammer, a computer worm that caused the loss of process control view and data collection (RISI, 2015). In 18 SIs the source did not contain information on the final scenario, and thus labeled as “unknown”.

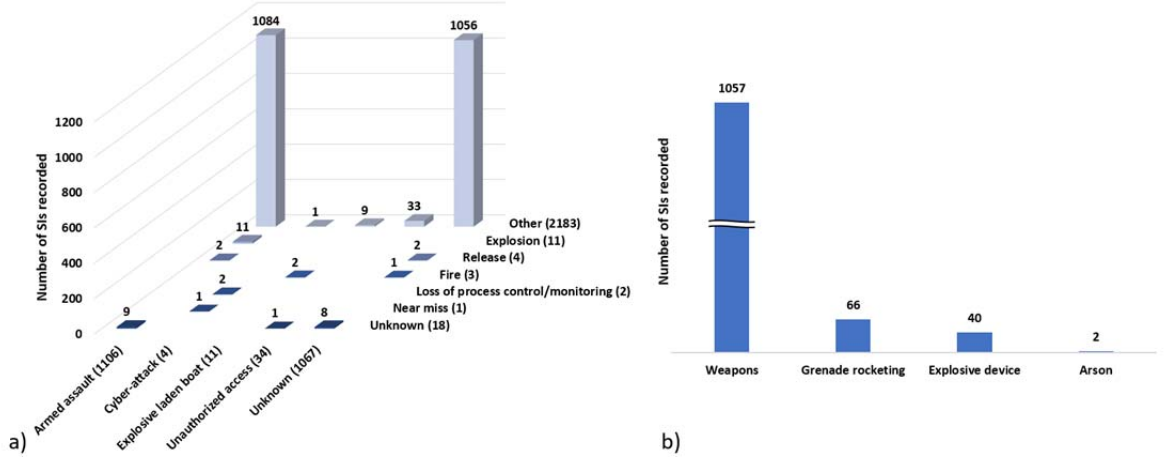

Figure 4: a) Distribution of the security threats with respect to the final scenarios; b) Armed assault attack mode subcategories

The information available in the records allowed to better detail the armed assault attack mode considering 4 sub-categories: armed assault with weapons, by grenade rocketing, with explosive devices, and by arson (Figure 4b). The majority of armed assaults displayed the use of weapons, with 1057 cases recorded, followed by the use of grenades launched by rockets (66 SIs). The use of explosive devices was found in a total of 40 SIs. An example of this attack mode occurred on January 2006 when Movement for the Emancipation of Niger

Delta (MEND) armed rebels kidnapped workers of the Shell's EA offshore oil platform and detonated explosives on crude oil pipes (Kashubsky, 2011). An arson was recorded in 2 incidents. Note that the total number of SIs shown in Figure 4b is higher than the number of SIs belonging to the armed assault category because in various cases more than one subcategory was present in a single SI.

3.4 Correlations between industrial sectors, security threats and attack modes

Figure 5 shows the 2D-maps of Correspondence Analysis (CA) displaying the points corresponding to the couples of itemized fields "SECURITY THREAT" vs "INDUSTRIAL SECTOR", and "SECURITY THREAT" vs "ATTACK MODE". A high degree of correlation is displayed by couples of points that are distant from the origin of the graph (which represents the average behavior of the dataset), and that form acute angles with it (Greenacre, 2017), together with a high cross-count of events belonging to the points considered.
From Figure 5a, the transportation sector results strongly correlated with the robbery/kidnapping security threat (red-circled), and weakly correlated with the theft of hazardous materials (yellow-circled). For this reason, when a security risk assessment is performed for operations concerning the transportation of hazardous substances, it is important to consider opportunistic attacks to ships during the threat identification phase. In the same way (Figure 5a), the offshore fluid production sector has a week correlation (yellow-circled) with the guerrilla operation/terrorism security threat. This could be explained by the fact that terrorist organizations are more attracted by fixed installations rather than by ships due to their strategic value and inherent hazard that can be exploited to trigger incidents with severe consequences for humans, the assets and the environment (i.e. major events).

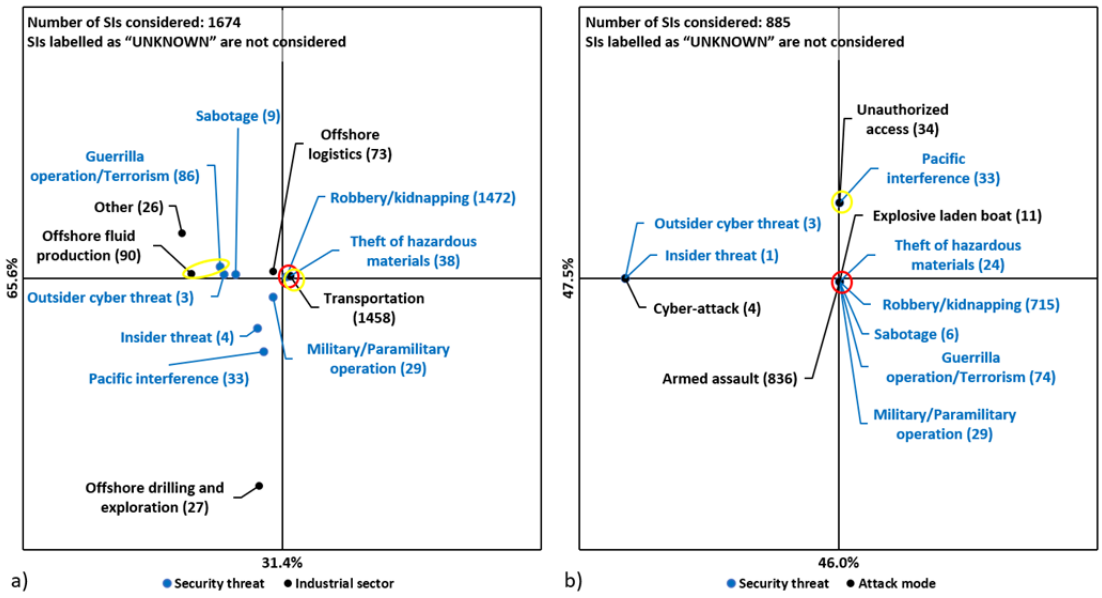

Figure 5: Correspondence 2D-maps from CA (number in brackets refer to the total SIs recorded): a) "SECURITY THREAT" vs "INDUSTRIAL SECTOR"; b) "SECURITY THREAT" vs "ATTACK MODE".

As regards the attack modes, Figure 5b shows a strong correlation between armed assaults and the robbery/kidnapping security threat (red-circled) and a weaker correlation between the unauthorized accesses and the pacific interference security threat (yellow-circled). This information could be useful in the definition of attacker capabilities and of effective countermeasures in the framework of SRA/SVA methodologies.
The application of CA did not show other relevant associations among categories. Nevertheless, it can be noted that the outsider cyber threat category by definition makes use of cyber-attacks, even if attack modes involving physical actions could be used (e.g. unauthorized physical access in the control room to use an infected USB stick) (Iaiani et al., 2020b). Note that the two correlations "transportation-robbery/kidnapping" and "armed assault-robbery/kidnapping" are considered strong even if near to the origin of the graph due to high numerosity of SIs recorded belonging to these categories with respect to the others.

4. Conclusions

In the present study a database collecting 2222 past security-related incidents that affected offshore Oil&Gas

operations was populated and analysed, retrieving data from open-source databases, scientific literature, and the web. Exploratory Data Analysis (EDA), including Correspondence Analysis (CA), were used in the analysis. The time trend shows a significant increase in the number of incidents recorded after year 2000, making security of offshore Oil&Gas operations an issue of major concern. Geographically, the Gulf of Guinea (Africa) and the Strait of Malacca (Asia) resulted the most affected areas by security attacks due to the strategic location for international maritime shipping routes and the presence of a high number of offshore Oil&Gas operations. Important differences were found in the distribution of incidents among the industrial sectors with the transportation sector dominating (almost 89 % of the events recorded) due to the vulnerability to opportunistic attacks displayed by watercrafts. Although historical evidence of major events triggered by security attacks to offshore Oil&Gas installations was recorded, the majority of final scenarios resulted in non-industrial impacts (labelled as “other”, such as theft of personal belongings of workers, documents, equipment, kidnapped workers for ransom, protests). Similar correlations, due to the extensive use of watercrafts, were found for the transportation sector and the offshore logistics sector with the robbery/kidnapping security threat, and the armed assault attack mode, showing that pirates do not differentiate among different types of targets, but generally display a more opportunistic approach. The offshore fluid production sector was found correlated with high-motivated and well-equipped guerrilla operation and terrorism security threats. Overall, the results obtained confirmed the concreteness of security attacks to offshore Oil&Gas operations and provide baseline information useful for the application of security assessment techniques such as SRA-SVA methodologies.

Acknowledgments

This work was supported by INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro) in the framework of the 4th SAF€RA call.

References

Argenti F., Landucci G., Spadoni G., Cozzani V., 2015. The assessment of the attractiveness of process facilities to terrorist attacks. Saf. Sci. 77, 169–181.

Bozeman B., 2011. The 2010 BP Gulf of Mexico oil spill: Implications for theory of organizational disaster. Technol. Soc. 33, 244–252.

Casson Moreno V., Reniers G., Salzano E., Cozzani V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.

Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC.

Greenacre M., 2017, Correspondence Analysis in Practice, 3rd ed., Chapman and Hall/CRC (Ed), New York.

GTD - Global Terrorism Database, 2021, <www.start.umd.edu/gtd/access/> accessed 01.08.21.

Iaiani M., Casson Moreno V., Tugnoli A., Cozzani V., 2020a. Analysis of security-related events in the chemical and process industry. Proc. 30th Eur. Saf. Reliab. Conf. 15th Probabilistic Saf. Assess. Manag. Conf.

Iaiani M., Tugnoli A., Casson Moreno V., Cozzani V., 2020b. Analysis of past cybersecurity-related incidents in the process industry and the like. Chem. Eng. Trans. 83, 163–168.

Jin M., Shi W., Lin K.C., Li K.X., 2019. Marine piracy prediction and prevention: Policy implications. Mar. Policy 108, 103528.

Kashubsky M., 2011. A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975 – 2010. Perspect. Terror. 5.

Lorenzo-Seva U., van de Velden M., Kiers H.A.L., 2009. Car: A MATLAB package to compute correspondence analysis with rotations. J. Stat. Softw. 31, 1–14.

Matteini A., Argenti F., Salzano E., Cozzani V., 2019. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab. Eng. Syst. Saf. 191, 106083.

MSI - Maritime Safety Information, 2021, <https://msi.nga.mil/Piracy> accessed 01.08.21.

Paltrinieri N., Dechy N., Salzano E., Wardman M., Cozzani V., 2012. Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management. Risk Analysis 32(8), 1404–1419.

Peters B.C., 2020. Nigerian piracy: Articulating business models using crime script analysis. Int. J. Law, Crime Justice 62, 100410.

RISI - The Repository of Industrial Security Incidents, 2015, <www.risidata.com/Database> accessed 01.08.21.

Shallcross D.C., 2013. Using concept maps to assess learning of safety case studies - The Piper Alpha disaster. Educ. Chem. Eng. 8, e1–e11.

Tukey J.W., 1977, Exploratory Data Analysis, Addison-Wesley Publishing Company, Reading (USA).