Process Safety and Environmental Protection 192 (2024) 926–945

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

journal homepage: www.journals.elsevier.com/process-safety-and-environmental-protection

Identification of security scenarios in offshore Oil&Gas production facilities based on past incident analysis

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

LISES – Laboratory of Industrial Safety and Environmental Sustainability, DICAM – Department of Civil, Chemical, Environmental and Materials Engineering, University of Bologna, via Terracini n.28, Bologna 40131, Italy

ARTICLE INFO

Keywords:
Offshore
Oil&Gas
Security
Past incident analysis
Scenario Identification
API RP 70

ABSTRACT

Offshore Oil&Gas installations may be attractive targets of intentional attacks due to their presence in socio-political sensitive areas, their economic significance, and the high impact of scenarios that can be triggered by the mismanagement of the hazardous substances handled (e.g., crude oil, natural gas, etc.). In the present study, a new dataset including 112 past security-related incidents that affected the offshore Oil&Gas sector in the last decades was developed and analyzed using Exploratory Data Analysis (EDA), Root Cause Analysis (RCA), and Attack Tree Analysis (ATA). Significant differences were found in the types of threats and attack modes, with terrorism identified as the primary threat, followed by robbery and kidnapping. The identified scenarios caused fatalities, injuries, and asset damages at the targeted facilities, underscoring their potential to cause severe impacts, comparable to the outcomes of safety-related accidents. Tables linking the specific contribution of the identified attack modes, scenarios, and consequences to the SVA workflow proposed by the API Recommended Practices 70 and 70I were obtained. Overall, the results obtained support the application of suitable Security Vulnerability/Risk Assessment (SVA/SRA) methodologies concerning the identification and characterization of adversaries, the definition of attack modes, the evaluation of effectiveness of existing security barriers, and the assessment of consequences.

1. Introduction

Offshore Oil&Gas operations may be targeted by intentional attacks performed by a wide range of adversaries, spanning from political organizations of protesters to terrorist organizations (Progoulakis and Nikitakos, 2019; Wang et al., 2022). Motivations for these adversaries could encompass monetary gain, disruption of economic and political stability, seeking revenge, pursuing challenges, and engaging in environmental activism. (Kashubsky, 2011). In the particular instance of the offshore Oil&Gas production sector (production of oil and/or gas from offshore rigs), potential threats may arise due to factors such as the company profile (e.g., multinational corporations) or the socio-political context of the facility attacked (Argenti et al., 2015). As an example, in January 2006 in Nigeria, insurgents targeted the Shell EA offshore oil platform, leading to the abduction of four foreign oil workers from a support vessel anchored at the platform and to its subsequent shutdown. Furthermore, the insurgents sabotaged crude oil pipelines, disrupting oil supply to the Forcados offshore export terminal (Kashubsky, 2011).

Offshore Oil&Gas installations may also be affected by cyber-attacks, i.e., attacks via the cyberspace targeting their IT (Information Technology, e.g., the corporate network) and/or OT (Operational Technology, e.g., the Basic Process Control System, BPCS, and the Safety Instrumented System, SIS) networks, with consequences that can severely impact the operability and/or system integrity of the target assets (El-Kady et al., 2023; Iaiani et al., 2023a; Yuan et al., 2023). For example, in the United States in 2003, some of the database servers collecting production data and the Human Machine Interface (HMI) workstations managing platform operations were affected by the Slammer worm causing loss of control, loss of operations supervision and loss of data collection (RISI, 2015).

Abbreviations: AM, Attack Mode; ATA, Attack Tree Analysis; BPCS, Basic Process Control System; CQ, ConseQuence; EDA, Exploratory Data Analysis; IACS, Industrial Automation and Control System; IT, Information Technology; OT, Operational Technology; RCA, Root Cause Analysis; SC, SCenario; SIS, Safety Instrumented System; SRA, Security Risk Assessment; ST, Security Threat; SVA, Security Vulnerability Assessment; WBIED, Water-borne Improvised Explosive Device.

* Corresponding author.
E-mail address: valerio.cozzani@unibo.it (V. Cozzani).

https://doi.org/10.1016/j.psep.2024.10.061
Received 16 June 2024; Received in revised form 6 October 2024; Accepted 17 October 2024
Available online 22 October 2024

The aforementioned sporadic incidents drastically confirm that security (both physical and cyber) of offshore Oil&Gas operations should be regarded as a significant issue. Actually, besides causing business outage, intentional attacks can exploit the inherent hazards associated with handling large quantities of hazardous substances, such as the natural gas and crude oil, leading to incidents that result in harm to individuals, the environment, and assets. The severity of the final consequences of such events may be comparable to those caused by major accidents arising from safety-related issues (e.g., the notable accidents that took place in 1988 at the Piper Alpha oil platform (Shallcross, 2013) and in 2010 at the Deepwater Horizon drilling rig (Bozeman, 2011)).

In this panorama, over the years, government agencies, research organizations and industries around the world developed best practices, guidelines, standards, and procedures for both the cyber and the physical security management of critical installations. For instance, the American Petroleum Institute (API) published two Recommended Practices (RP) specific for the Offshore Oil&Gas sector, the API RP 70 ("Security for Offshore Oil and Natural Gas Operation") (American Petroleum Institute, 2010) and the API RP 70I ("Security for Worldwide Offshore Oil and Natural Gas Operations") (American Petroleum Institute, 2012) which fall under the framework of Security Vulnerability Assessment (SVA) or Security Risk Assessment (SRA) methodologies, i.e. qualitative/semi-quantitative methods aimed at assessing the security (both physical and cyber) of critical installations (Reniers et al., 2018). An outline of the SVA approach proposed by the two aforementioned API standards for the offshore Oil&Gas sector is provided in Appendix C.

A review and comparison of the most common and non-proprietary SVA/SRA methodologies suitable also for the onshore chemical and process industry is provided in Matteini et al. (2019). They require the identification of all potential types of adversaries with their motivations, capabilities, and attack patterns, as well as the identification of the vulnerabilities present in the Physical Protection System (PPS) of the target facility and all the possible consequences of the physical scenarios triggered by such attacks (Fouzi et al., 2024). A similar workflow but focused entirely on cybersecurity of Industrial Automation and Control Systems (IACS, such as the BPCS and SIS), is proposed by the ISA/IEC 62443 series of standards (International Society of Automation & International Electrotechnical Commission, 2018). Security scenarios are also required as input information by quantitative approaches proposed in the literature to address security issues for the calculation of the probability of success of physical attacks to offshore Oil&Gas installations (Iaiani et al., 2023a). However, these methodologies and standards, even if requiring the identification of the security scenarios of concern, do not provide specific methods for their analysis apart some guide lists.

The analysis of past events that occurred in similar facilities (e.g., facilities belonging to the same industrial sector) is a valuable tool to gain lessons learnt and to support the risk identification step in the application of the above-cited methodologies (Lam and Tai, 2020). In this regard, the investigation of the available literature concerning the analysis of past security-related incidents that occurred in the offshore Oil&Gas industry revealed few contributions on this topic. In particular, Kashubsky (2011) provides the description of 60 security incidents involving offshore Oil&Gas installations worldwide from 1975 to 2010, while Benden et al. (2021) reports over 7500 maritime pirate attacks between 1993 and 2020, utilizing data from the International Maritime Bureau (IBM). However, in both cases, no statistical analysis of the incidents is conducted, hindering the easy retrieval of information to support SVA/SRA assessments for offshore installations. Also the studies conducted by Milch and Laumann (2019), by Konstandinidou et al. (2011), and by Iaiani et al. (2021c,b), even if consisting in the analysis of industrial incidents, they are not entirely suitable for deriving comprehensive data to support SVA/SRA assessments in the offshore Oil&Gas sector, as they present at least one of the following characteristics: main focus is on onshore industrial operations; scope is restricted to a single country; primary focus is on safety-related accidents rather than security-related incidents.

The present study aims at the collection and in-depth analysis of an extended dataset of past security-related incidents that affected Offshore Production facilities (i.e., facilities for the production of oil and/or gas from offshore reservoirs), retrieving information from different literature sources. The ultimate goal is to use the results of the dataset analysis to obtain specific insights to support the application of specific steps of the API RP 70 and API RP 70I workflow. This information includes threat types, types of attack modes perpetrated by the attackers, types of physical scenarios generated by the attacks, potential consequences for humans, assets, and surrounding environment, and role of safety/security barriers in the prevention or mitigation of the attacks. The analysis techniques applied include Exploratory Data Analysis (EDA), Root Cause Analysis (RCA), and Attack Tree Analysis (ATA).

The paper is structured as follows: the methodology applied to collect and analyze the security-related incidents of interest is outlined in Section 2. The features of the collected dataset, the results obtained from its analysis and the specific link with API RP 70/70I SVA workflow are presented and critically analyzed in Section 3. A discussion of the results is provided in Section 4, while some conclusions are drawn in Section 5.

2. Methodology

2.1. Dataset of security-related incidents

The starting point of the present study was the development and the population of a specific dataset including past security-related incidents that affected the Offshore Oil&Gas sector.

Fig. 1 shows the structure of each SRI-entry of the dataset: both free text fields and itemized fields were compiled. Free text fields allow for the retention of general details concerning the incident (i.e., "ID number", "Date", "Country", "Threat actor", "Attack description", "Reason of the attack", "Number of fatalities", "Number of injuries", "Extent of economic loss", "Security barriers", "Incident description", "Source", "Notes", "Links"), as available from the incident description in the original data source. Itemized fields are instead used to introduce an unambiguous classification of the SRIs (i.e., "Location", "Security threat", "Attack mode", "Scenario", "Consequence"), allowing for a systematic structured analysis.

Overall, all the classes considered for each itemized field (with the exception of the field "Location" as the categorization is based on the well-known classification into continents) are reported in the tables from A.1 to A.4 in Appendix A. For each itemized fields, the classification of each SRI was based on the match between the incident description and the definitions of the classes belonging to each itemized field.

The definitions of the terms "security threat", "attack mode", "scenario", and "consequence" adopted in the present study, which together form the incidental chain of events in the security domain, are reported in Table 1. It should be remarked that the definitions in Table 1 are intentionally broad, to avoid that a more stringent classification may lead to a misclassification or to an inaccurate representation of the data, as reported in the literature (Darbra et al., 2010).

It is important to remark that the accident description of some SRIs allowed for classification under more than one itemized class for the fields "Attack mode", "Scenario" and "Consequence". In these cases, multiple slots (e.g., "Consequence 1", "Consequence 2", "Consequence 3") were used in the dataset. The multiple slots are to be considered at the same level (i.e., no priority or ranking is implied by the progressive numbering of the itemized field).

The decision to avoid assigning a priority or weighting to the various categories aligns with the objective of providing robust data to support security risk analyses. Actually, in many cases security scenarios are not mutually exclusive. For example, the same adversary may execute multiple attack modes, leading to more than one physical damage scenario, all of which should be considered equally important. Moreover,

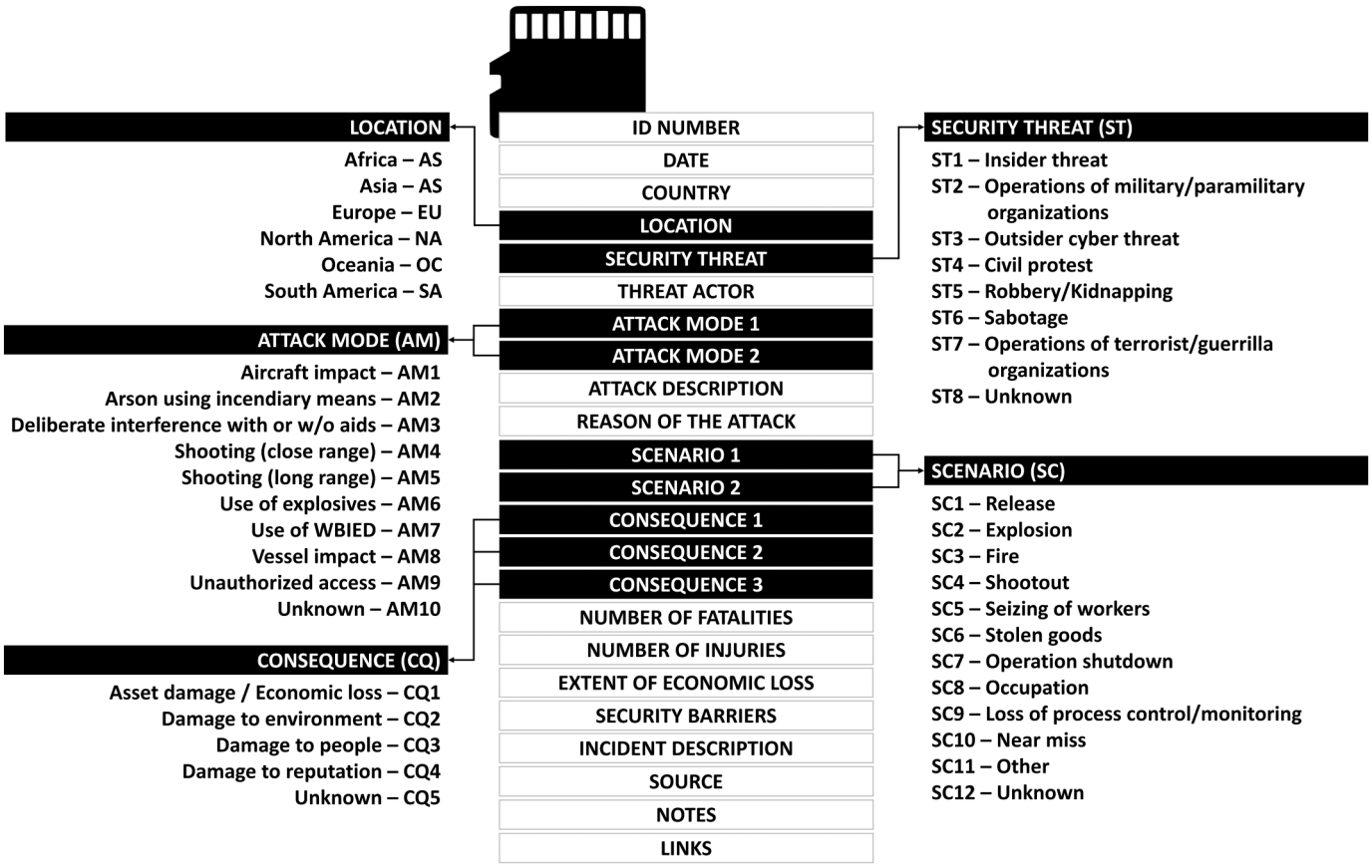

Fig. 1. Structure of each SRI-entry in the dataset (white boxes: free text fields, black boxes: itemized fields). ST-codes, AM-codes, SC-codes, and CQ-codes are defined in Table A.1, Table A.2, Table A.3, and Table A.4 in Appendix A respectively.

when evaluating consequences, it is essential to treat all potential impacts with the same level of significance, as they may potentially affect different targets (assets, people, the environment, and reputation).

Thus, while avoiding assigning a priority or a weight to the different categories indeed poses limitations to traditional approaches such as event tree analysis or similar methods that rely on mutually exclusive events, its application is well-suited to support the implementation of advanced methodologies. For instance, Bayesian Network-based methods and other advanced probabilistic techniques are better featured to handle scenarios where multiple consequences or attack modes should be considered simultaneously, as shown by several studies in the literature (Chen et al., 2024; Kong et al., 2024; Li et al., 2023; Meng et al., 2024; Ren and Yang, 2024; Sun et al., 2024).

The dataset was populated by retrieving data from the following sources:

- Open-source databases and reports on industrial accidents/incidents: the Worldwide Threats to Shipping Report (Office of Naval Intelligence, 2023), the Global Terrorism Database (START, 2020), the Repository of Industrial Security Incidents (RISI, 2015), the Worldwide Offshore Accident Databank (DNV GL Digital Solutions, 2015), the accidents reports RR566 and RR567 of the UK Health and Safety Executive (UK Health and Safety Executive, 2007a, 2007b), the Maritime Pirate Attacks Dataset (Benden et al., 2021), the database developed by the International Association of Oil&Gas Producers (IOGP, 2020), the ProcessNet Incident Database (Dechema, 2022), and the offshore security incident dataset of Iaiani et al. (2021a).
- Scientific literature: (Kashubsky, 2011; Konstandinidou et al., 2011).
- The web (Chaparro, 2022; Domínguez, 2022; Falcon Mega Solutions, 2022; Offshore Engineer, 2020; Safety4Sea, 2021).

Two inclusion criteria were applied to select the relevant data:

i. the incident shall originate as a result of an intentional attack aimed at interfering with normal operations;
ii. the incident involves an industrial offshore installation devoted to the production of oil and/or gas from offshore wells as a primary objective (offshore transportation, drilling and exploration are excluded).

The investigation of the above cited data sources was carried out by queries with specific sets of keywords (concerning threat type, incident type, industrial sector, installation type) that were translated into the language of the data source analyzed. In the creation of the dataset, particular attention was paid in avoiding the double counting of the events: specific checks were performed taking into consideration the date, country and type of company involved in the event. A total of 112 security-related incidents (SRIs) were included in the dataset (see Table B.1 in Appendix B).

2.2. Dataset analysis

A set of complementary techniques was used to carry out a structured analysis of the dataset, with the aim of identifying and characterizing the threat types, the threat actors, the attack modes, the generated scenarios and their consequences. This approach provides data useful for applying SVA and SRA methodologies, including offshore-specific approaches proposed by API RP 70 and API RP 70I, which are outlined in Appendix C.

In this study, Exploratory Data Analysis (EDA), Root Cause Analysis (RCA), and Attack Tree Analysis (ATA) were applied to analyze the SRIs.

Exploratory Data Analysis (EDA) is an approach of analysing datasets

Table 1
Definition of security threat, attack mode, scenario, and consequence and corresponding dataset itemized fields.

Term	Definition	Corresponding itemized field/s	Classes definition detailed in
Security threat	A security threat refers to an individual, group, organization, or government that has the intent or capability to cause harm to critical assets (American Petroleum Institute, 2013). It does not specify how the harm will be caused—this is determined by the **attack mode**. Examples include terrorist organizations and pirates.	"Security threat"	Table A.1 in Appendix A
Attack mode	The attack mode describes how the harm is executed, specifying the manner and means, including the weapon and the delivery method, that may be employed (American Petroleum Institute, 2013). It translates the intent of the threat actor into action, causing a particular event (the scenario). Examples include the detonation of explosive devices and shooting.	"Attack mode 1", "Attack mode 2"	Table A.2 in Appendix A
Scenario	The scenario refers to the physical events that result from the execution of the attack modes by the threat actors and that might lead to the loss of an asset (type and extent determined by the consequences) (American Petroleum Institute, 2013). Examples include releases of hazardous materials and seizing of workers.	"Scenario 1", "Scenario 2"	Table A.3 in Appendix A
Consequence	The consequence refers to the outcome of the scenario, describing the type and extent of the loss of an asset. It is commonly measured in four ways – human, economic, mission, and psychological – but may also include other factors such as impact on the environment (American Petroleum Institute, 2013). Examples include fatalities and economic losses.	"Consequence 1", "Consequence 2", "Consequence 3".	Table A.4 in Appendix A

to summarize their main characteristics, often using statistical graphics and other data visualization methods (Tukey, 1977). In the present study EDA was used to explore the following aspects:

- time trend: counting of SRIs was based on 5-years period;
- geographical distribution: counting of SRIs was based on itemized field "Location";
- security threats: counting of SRIs was based on itemized field "Security threat";
- attack modes perpetrated by the adversaries: counting of SRIs was based on itemized fields "Attack mode";
- scenarios triggered by the attacks: counting of SRIs was based on itemized fields "Scenario";
- consequences suffered by companies: counting of SRIs was based on itemized fields "Consequence".

Results were plotted either separately or cross-tabulating different aspects, using tools such as histograms, Venn diagrams, geographical maps and pie charts. Histograms were used to show the distribution of threats affecting offshore production assets over time. Venn diagrams were adopted to show the share of the security threats with respect to the attack modes and the scenarios. A geographic map was used to show the distribution of SRIs worldwide, together with pie charts displaying the share of the security threats in each continent.

Root Cause Analysis (RCA) is a systematic process used for identifying the root causes of a focus event, widely used in different fields of engineering, including accident/incident analysis (Wilson et al., 1993). RCA was applied in order to understand the motivations/reasons of the adversaries behind the attacks, which are considered the root causes of the SRIs (i.e., the focus events of interest in the present study). The understanding of such information is important since motivations affect the possibility of achieving different types of scenarios.

The RCA of the dataset was performed considering the information collected in the free text fields "Threat actor" and "Reason of the attack". Even if the incident descriptions are mainly focused on the scenarios triggered by the attacks, information on the motivations/reasons and capabilities of the threat actors was found in 66 out of 112 SRI reports.

According to the RCA-specific standard IEC 62740 (International Electrotechnical Commission, 2015), which lists all the possible tools and techniques for RCA application and data visualization, the Ishikawa diagram (more commonly known as "fishbone diagram" for its shape) was adopted.

Attack Tree Analysis (ATA) is a method of modelling threats against a specific target (Abdo et al., 2018). ATA makes use of attack trees (ATs) to summarize the results: they are conceptual diagrams, related to the established fault tree formalism (International Electrotechnical Commission, 2021), that represent the chain of security breaches leading to a top event (called security event in the security domain such as a scenario, a consequence or a combination of the two).

Attack trees were used to explore the role of the security barriers in interrupting the attacks perpetrated by the adversaries or, at least, in mitigating the consequences of the generated scenarios. Moreover, attack trees allow an in-depth characterization of the attack modes by the definition of the specific tools/means used by the adversaries to cause the scenarios.

In the present study, the attack modes considered in the development of the attack trees are the classes adopted in the itemized fields "Attack mode 1" and "Attack mode 2" of the dataset, all described in Table A.2 in Appendix A. They were identified from the analysis of the main SVA/SRA methodologies. In particular, analyzed sources include: SVA method proposed by Störfall-Kommission (2002), CCPS methodology (Center for Chemical Process Safety, 2003), VAM-CF methodology (Jaeger, 2002), API RP 780 SRA methodology (American Petroleum Institute, 2013), API RP 70 methodology (American Petroleum Institute, 2010), API RP 70I methodology (American Petroleum Institute, 2012), and RAMCAP methodology (Moore et al., 2007).

The information recorded in the free text fields "Attack description", and "Security barriers" of the dataset allowed to characterize the classes of attack modes in terms of the tool/means used by the adversaries and to identify the security barriers contrasting the attacks. Based on this information, two attack trees were developed: one considering a "major event" (see definition in Table 2) and the other considering a "non-major event" (see definition in Table 2) as security events of the trees.

Fig. 2 shows the contribution of the results of each analysis technique to the specific steps of API RP 70 and API RP 70I security risk assessment workflow, along with the dataset fields investigated to gather the required specific information in support of each step. In particular, the results support Step 1 (Potential Threat), Step 2 (Consequence Assessment), and Step 3 (Vulnerability Assessment) of the two aforementioned SVA methodologies. As outlined in Appendix C, Step 1 of API RP 70/70I involves identifying potential threats and possible attack modes. Step 2 involves the identification of scenarios resulting from intentional attacks and the evaluation of their consequences on people, assets, and the environment. Step 3 of API RP 70/70I involves identifying potential vulnerabilities related to security events, assessing existing countermeasures (safety/security barriers) and procedures, and evaluating their effectiveness in mitigating or interrupting intentional attacks. As clearly shown in Fig. 2, no support is provided for Step 4 (Mitigation) and Step 5 (Implementation), as these are standalone steps that rely on the results of the preceding steps (see Appendix C).

3. Results

In the following sections, the results obtained from the application of Exploratory Data Analysis (EDA), Root Cause Analysis (RCA), and Attack Tree Analysis (ATA) to the security-related incidents (SRIs) recorded in the dataset are reported and critically analyzed.

3.1. Identification of threat scenarios

The identification of the potential threat scenarios that may affect the assets of interest (i.e., facilities related to Offshore Production operations in the present study) is the first task to be performed according to Step 1 of the API RP 70 and API RP 70I workflow (see Fig. 2). To support this identification, suitable information on security threats was gathered by Exploratory Data Analysis (EDA, see Section 2.2).

The 2-D histogram in Fig. 3 shows the share of the security threats over time (5-year time slots are considered): the classes of security threats displayed in the figure are described in Table A.1 in Appendix A. It is important to remark that the 2021–2023 time period includes partial results, as it is not yet concluded (two years still left to complete the 5-year period). Thus, its comparison with the outcomes obtained for the other 5-year slots shall be considered with caution.

The most frequent type of security threat recorded over years is "Operation of terrorist/guerrilla organizations" (ST7, 42 SRIs, 38 % of the total), consisting in attacks performed by highly capable, well-organized and well-equipped organizations, aimed at causing high-impact events, not only in terms of casualties (damage to people), but also of impact on the media (damage to reputation). This security threat turned out to be by far the most relevant threat in the recent years (see time period from 2016 to 2020 in Fig. 3), making the security of Offshore Production operations of primary concern. Terrorism and guerrilla operations were also recorded in all the other time periods considered, even if in lower percentages with respect to the other security threats.

The second most recorded security threat is "Robbery/Kidnapping" (ST5, 29 SRIs, 29 % of the total), consisting in attacks aimed at stealing cash or valuable items, or extorting money by kidnapping or hostage taking. This security threat was recorded in all the time periods considered with a similar extent as the operation of terrorist and guerrilla organizations, except for the 2016–2020 time slot as highlighted above.

As shown in Fig. 3, all the other threats considered concern a number of events comprised between 2 % and 10 % of the total, thus showing a more limited occurrence.

The security threats typically performed by low equipped adversaries (e.g., acts of civil protest and sabotage) had a clear decrease after 2005, suggesting that security management processes (including cybersecurity processes supported by international standards such as ISO/IEC 27005 and ISA/IEC 62443) have been increasingly implemented over the years.

Overall, the time trend of the SRIs reported in Fig. 3 shows that a relatively small number of incidents was recorded before year 2000 (23 SRIs) if compared to that registered in the last two decades (89 SRIs). This is mainly justifiable by an increased attention to the practice of reporting security-related incidents after the "9/11" terrorist attacks in New York, which deeply affected the awareness of security attacks worldwide. A peak of incidents was recorded during the 5-year period 2006–2010 (40 SRIs) due to a high activity of the guerrilla group called MEND (Movement for the Emancipation of the Niger Delta) in Nigeria in the years 2006 and 2007, causing a roughly one-third reduction of Nigeria's oil production (Hanson, 2007).

Fig. 4 shows the world map with the geographic distribution of the SRIs: in each continent, the distribution of the security threats is reported. By far, the majority of the incidents took place in Africa (80 SRIs, 73 % of the total). In particular the Gulf of Guinea (Nigeria) resulted the most affected area: this is due to the strategic location for international maritime routes, in conjunction with a complex piracy issue, compounded in opportunistic attackers, organized criminal syndicates, and terrorist groups (Daxecker and Prins, 2015; IBM Piracy Reporting Centre, 2023; International Maritime Organization, 2023). In facts, as reported in the pie chart for Africa, terrorist and guerrilla attacks are the SRI most frequently occurred over the years (36 SRIs), followed by acts of robbery and/or kidnapping (29 SRIs).

Asia resulted the second most affected by security attacks targeting Offshore Production operations (16 SRIs, 14 % of the total). In particular, the area of the Strait of Malacca (between Indonesia and Malaysia), which is, similarly to the Gulf of Guinea, strategic for maritime shipping routes (Daxecker and Prins, 2015; International Maritime Organization, 2023). Operations of military/paramilitary organizations was found to be the main threat in this continent (10 SRIs), followed by terrorism and guerrilla operation (4 SRIs).

Europe (5 SRIs, 4 % of the total), North America (4 SRIs, 4 % of the total), and South America (6 SRIs, 5 % of the total) resulted less affected by security attacks to assets related to Offshore Production operations. This might be ascribed to a greater attractiveness of onshore installations (e.g., chemical and petrochemical plants) rather than of offshore installations for adversaries aimed at triggering scenarios with severe consequences on humans, environment, and the assets, as evidenced and discussed in a previous study by Iaiani et al. (2021c,b). In fact, with the exception of South America, where increasing piracy

Table 2
Definitions of the top events "Major event", "Non-major event" considered in the present study (European Parliament and Council, 2013).

Top Event	Definition
Major event	An event that: a. involves an explosion, fire, loss of well control, or release of oil, gas or dangerous substances involving, or with a significant potential to cause, fatalities or serious personal injury; b. leads to serious damage to the installation or connected infrastructure involving, or with a significant potential to cause, fatalities or serious personal injury; c. results in any major environmental damage as an outcome of the events above. For the purposes of the definition above an installation that is normally unattended shall be treated as if it were attended.
Non-major event	An undesired event which cannot be classified as "Major event".

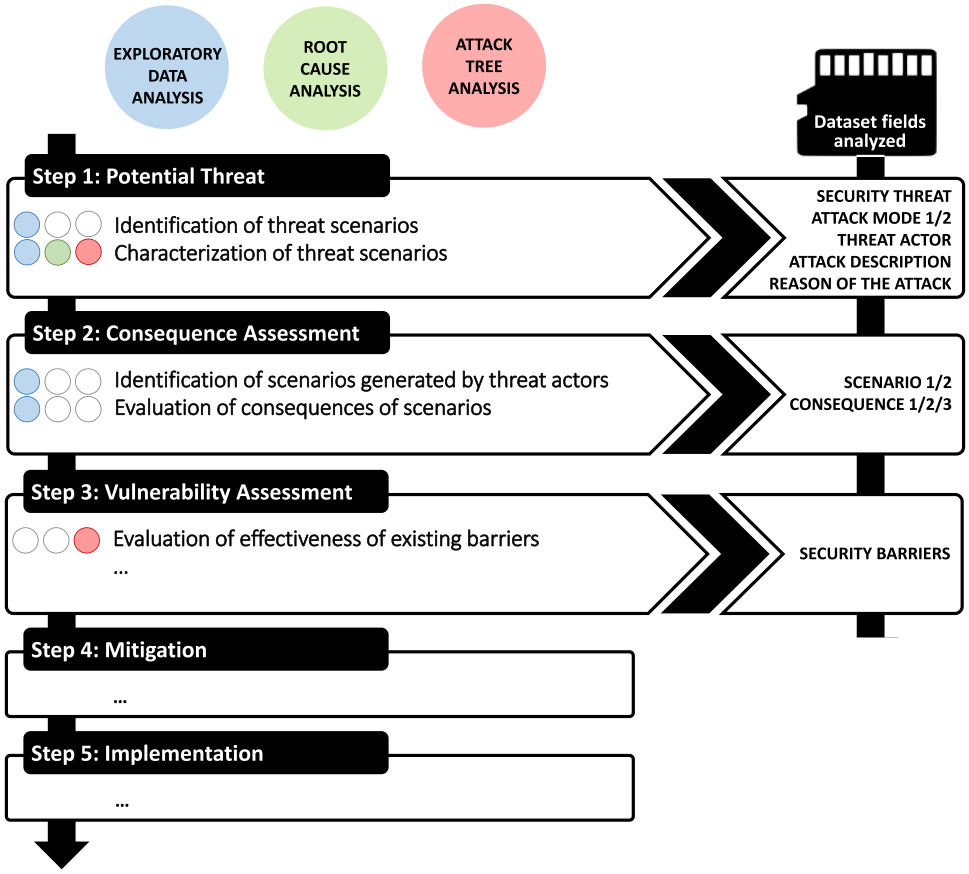

Fig. 2. Techniques used in the structural analysis of the dataset to support specific steps of the API RP 70/70I workflow. The scheme also reports the fields of the dataset analyzed to gather the specific information of interest for each step.

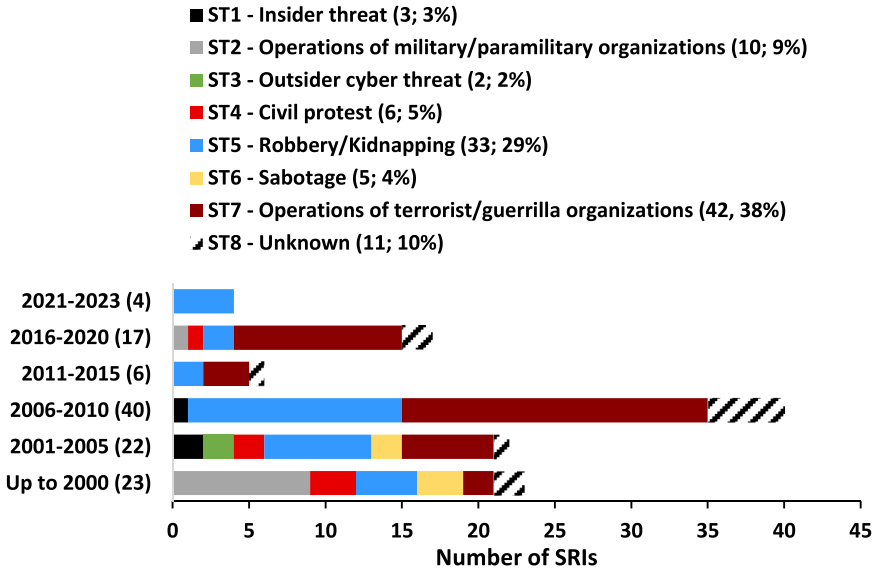

Fig. 3. Share of the security threats over time (5-year time intervals are considered).

activity has been recorded in the last two years in the Southern Gulf of Mexico (Stelzer, 2022), civil protest and sabotage are the most recorded threats in these continents. However, as discussed above, these threats are deemed not to cause high-profile scenarios as terrorist or guerrilla groups aim. The higher attractiveness of onshore plants may be justified by both the easiness in accessing the sites as they are not surrounded by water, and their increased visibility due to the presence of highly populated areas nearby (e.g., population living nearby the plant).

Finally, due to the lower number of installations related to Offshore Production operations, no incident was recorded in Oceania.

Overall, the results useful for the application of Step 1 of API RP 70 and API RP 70I workflow (see Fig. 2) as regards the identification of the minimum set of potential threat scenarios, are summarized in Table 3. It is important to remark that these outcomes are the result of the analysis

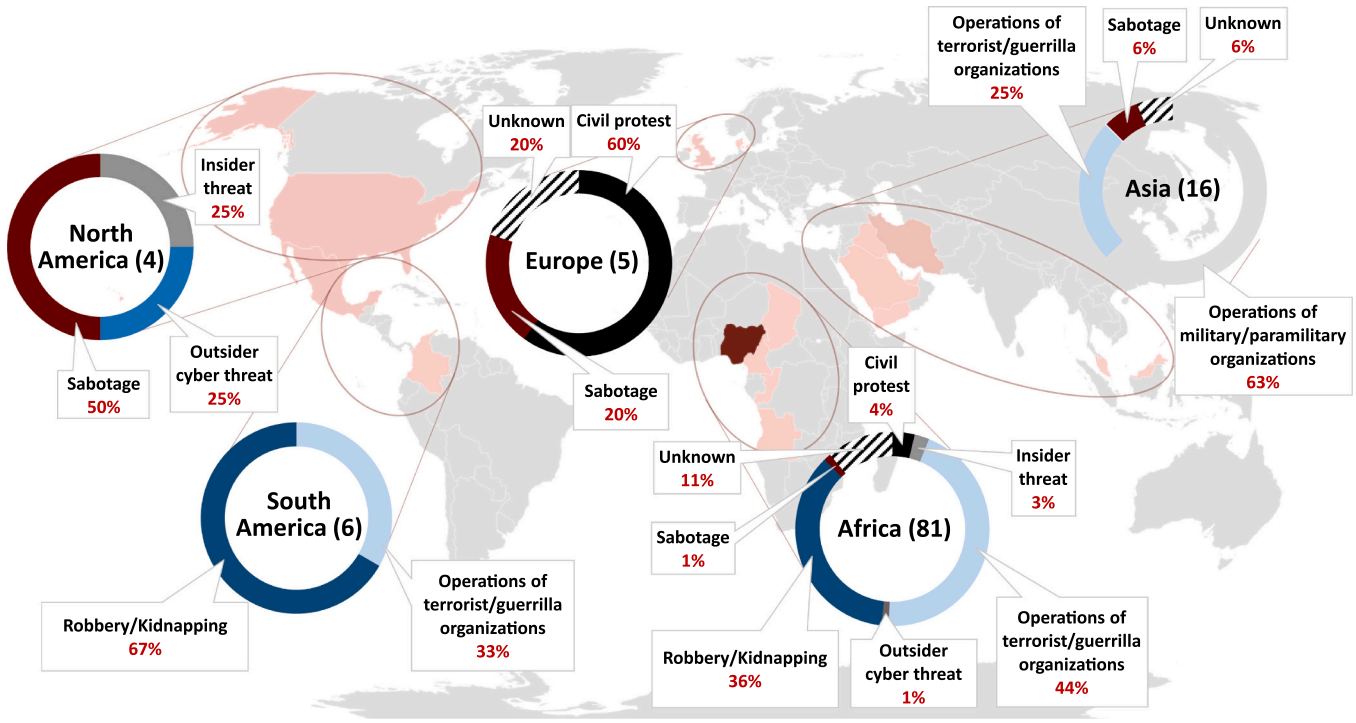

Fig. 4. World map reporting the geographical distribution of the SRIs. The distribution of the security threats in each continent is reported.

Table 3
Results of the past incident analysis supporting Step 1 of API RP 70 and API RP 70I as regards the identification of the minimum set of threat scenarios according to the dataset analyzed.

Location of the installation of interest	Minimum set of potential security threats suggested for consideration in SVA/SRA
Africa	"Operations of terrorist/guerrilla organizations"; "Robbery/Kidnapping"
Asia	"Operations of military/paramilitary organizations"; "Operations of terrorist/guerrilla organizations";
Europe, North America, South America, Oceania	"Civil protest"; "Sabotage"

of an incident dataset which inherently lacks information due to both under-reporting of incidents and the fact that they are rare events: therefore, the past incidents validate some scenarios but do not exclude the others.

For example, with reference to Table 3, if an offshore facility is located in Africa, threats from terrorist or guerrilla organizations and from robbers or kidnappers (e.g., pirates) should be considered in a SVA/SRA study for that facility (e.g., in the list of threats identified in Step 1 of API RP 70/70I). These results align with findings from Kashubsky and Morrison (2013), who emphasize the prominence of piracy and theft in African waters. Similarly, for a European offshore installation, sabotages and civil protests should be taken into account as possible security threats in the SVA/SRA process.

3.2. *Characterization of threat scenarios*

According to Step 1 of API RP 70 and API RP 70I, the identified potential threat scenarios shall be characterized in terms of the attack modes performed by the treat actors (the adversaries), the means adopted in attacks, and the reasons/motivations behind the attacks. To support the characterization, suitable information was gathered by Exploratory Data Analysis (EDA, see Section 2.2), Root Cause Analysis (RCA, see Section 2.2), and Attack Tree Analysis (ATA, see Section 2.2) (see Fig. 2).

RCA allowed gaining insight into the types of threat actors and motivations behind the attacks. Fig. 5 shows the Ishikawa ("fishbone") diagram displaying the security threats as main rib branches, the types of threat actors as secondary rib branches, and the reasons/motivations as tertiary rib branches. Numbers in brackets refer to the number of occurrences of the information of interest in the dataset. It shall be noted that, as more than one descriptor may apply to the single SRI, the numbers on one branch may not sum up consistently with SRI counting.

The "Operations of terrorist/guerrilla organizations" security threat includes acts performed by criminals (adversaries belonging to syndicates or similar illegal organizations), guerrillas (adversaries belonging to small independent group taking part in irregular fighting), terrorists (adversaries belonging to an organization designated of terrorist matrix in at least one country all around the world), and regionalists/nationalists (adversaries belonging promoting ideals of regionalism/nationalism). Financial discontent and gaining political power and influence were found the reasons driving the attacks performed by guerrillas, together with an act of strength in the context of an ongoing conflict. The latter characterizes also acts performed by terrorist organizations, along with motivations related to religious extremism, territorial autonomy, and obtaining political power and influence. Regionalists or nationalists, instead, were found driven by political decentralization and territorial autonomy, but also by the promoting of environmental awareness.

Regionalists and nationalists turned out to be adversaries belonging also to the "Robbery/Kidnapping" threat. These acts were also carried by criminals, popular protesters, activists, and armed militants, mainly driven by financial discontent and monetary gain.

Acts of "civil protest" were found to be performed by protesters and people belonging to non-profit organizations, especially when motivated by the promotion of environmental awareness. Similarly, a hostile nation army in an act of show of strength turned out to be a potential adversary in case of "Operations of military/paramilitary organizations" security threat.

When "Insider threat" is considered, disgruntled employees (i.e., employees dissatisfied with their job) moved by financial discontent, were reported. Given the fact that they generally have knowledge of

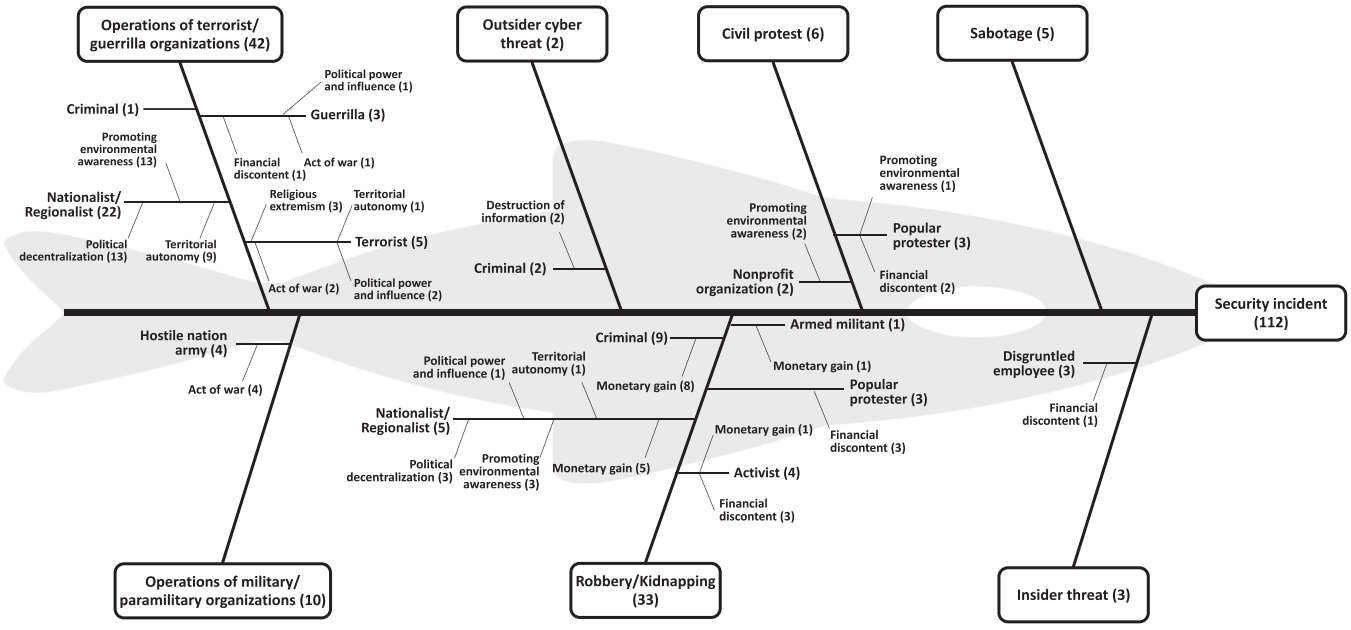

Fig. 5. Ishikawa diagram (fishbone diagram) displaying the results of RCA. Security threats, type of threat actors (adversaries), and reasons/motivations are reported respectively in main, secondary, and tertiary rib branches.

both the process and the equipment, they turn out to be a very critical threat, able to cause severe damages.

Finally, cyber-criminals targeting the IT-OT network with cyber-attacks aimed at corrupting and destroying information were found as potential adversaries belonging to "Outsider cyber threat".

EDA (see Section 2.2) allowed gaining information on the attack modes (AMs) adopted by the adversaries identified through RCA. The AM-classes considered in the present study are described in Table A.2 in Appendix A.

Fig. 6 shows the share of the attack modes with respect to the security threats considered in the present study. The majority of the adversaries belonging to "Operations of terrorist/guerrilla organizations" threat performed attacks involving the shooting at close range (AM4, 15 SRIs) and the detonation of explosive devices (AM6, 15 SRIs): a single incident reported the adoption of both the AMs (overlap). Therefore, AM4 and AM6 are deemed very likely attack modes that shall be considered in the context of a SVA/SRA study. However, there is historical evidence of other types of attacks performed by terrorists and/or guerrillas such as the detonation of large amounts of explosives contained inside vessels (AM7, 3 SRIs), deliberate interferences (AM3, 2 SRIs), and incendiary attacks (AM2, 1 SRI). In 9 incidents, an unauthorized access (AM9), as defined in Table A.2 in Appendix A, was recorded.

The latter attack mode is the most frequently reported AM in case of "Robbery/Kidnapping" (28 SRIs) with a overlap of two incidents reporting shooting at close range (AM4, 4 SRIs). This is not surprising, as adversaries belonging to this security threat are characterized by an intent of stealing cash or valuable items or extorting money by kidnapping people present on the platform (sometimes with the use of small/medium firearms such as handguns), and thus they are not used to perform attacks that have the potential of generating major event scenarios as several AMs considered in the present study do (i.e., AM1, AM2, AM4, AM5, AM6, AM8 defined in Table A.2 in Appendix A). Therefore, AM9 shall be considered when characterizing robbers and/or kidnappers in the context of a SVA/SRA study.

The long-range shooting (AM5, 7 SRIs) is the most frequently recorded AM in case of "Operations of military/paramilitary organizations" threat, followed by attacks making use of explosives (AM6, 3 SRIs, with an overlap of 2 SRIs with AM5) and by attacks consisting in the ramming of structural parts of the platforms with vessels (AM8, 2 SRIs). This confirms that the adversaries belonging to this threat are well-equipped and potentially able to cause damages with severe consequences such as major event scenarios.

Only unauthorized accesses (AM9, 6 SRIs) were recorded in case of "Civil protest": this is not surprising, since adversaries belonging to this threat class are characterized by non-violent means of interference. Similarly, deliberate interference (AM3, 2 SRIs) is the only attack mode that was recorded for "Outsider cyber threat", while in case of "Insider threat" and "Sabotage" also unauthorized accesses (AM9) were reported in the incident records. It is important to underline that, in case of insiders, this is possible as well since they might not have access to all the areas of the facility.

More details concerning the attacks performed by the adversaries were retrieved through application of ATA (see Section 2.2). In particular, given the potential severity of consequences of the scenarios that can be triggered by the attack modes considered in the present study, two attack trees (ATs) were developed: one leading to a "major event" (see definition in Table 2) as a security event (i.e., the top event of the tree in the security domain, see Fig. 7), and the other leading to a "non-major event" (see definition in Table 2) as a security event (Fig. 8). The two ATs also display the security barriers that turned out to be able to contrast or mitigate specific AMs, that will be further discussed in Section 5.

The numbers in brackets in Fig. 8 refer to the number of SRIs validating a specific attack mode. It is important to remark that the sum of the numbers in brackets in the branches corresponding to the AMs exceeds the number of SRIs validating the two security events, due to the presence of overlaps in the attack modes (as previously discussed).

In case of deliberate interferences with or without the use of aids (AM3), three different patterns were recorded. The first consisted in the threatening of people (2 SRIs) who were manning the platform to force them to start process shutdown leading to production outage. The second consisted in a false attack notification that led operators to activate emergency responses (2 SRIs). The third consisted in a cyber-attack targeting the IT-OT system of the platform (3 SRIs).

The use of hand-held firearms (the information contained in the records did not allow to discriminate between rifles and handguns) covers the totality of the cases of shooting at close distance (AM4) that were

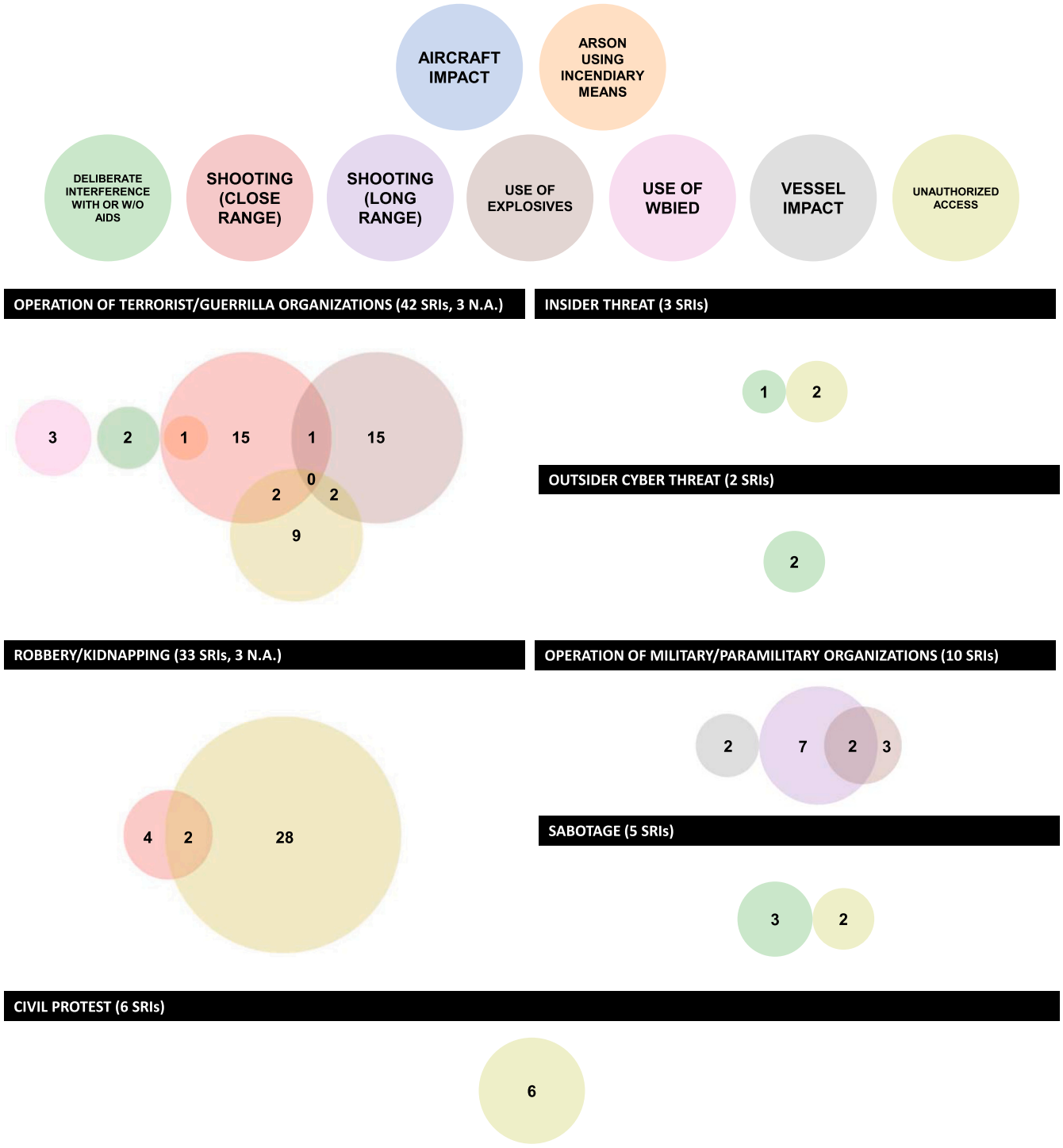

Fig. 6. Venn diagrams displaying the share of the attack modes (see definitions in Table A.2 in Appendix A) with respect to the security threats (see definitions in Table A.1 in Appendix A).

recorded (21 SRIs). On the other hand, when the shooting occurred at long distance (i.e., adversaries did not access the platform, AM5), gunshots coming from both air (military aircraft, 3 SRIs) and water (military warship, 4 SRIs) environments were recorded. No information on the specific weapon used was available in the reports of the incidents. Also hand-held firearms were recorded for this attack mode.

When attacks involving explosives (AM6) are considered, the use of military explosives (2 SRIs) and hand grenades (1 SRI) were reported. These explosives are generally safe to handle, have high energy density and a long shelf life, and are generally adopted by well-equipped adversaries such as militia, armies and terrorist organizations. The used of homemade explosives (less efficient, but more easily achievable) such as ANFO (Ammonium Nitrate – Fuel Oil) or TATP (Triacetone Triperoxide Peroxyacetone) was not reported in the records. Moreover, in a single incident, a system for remote activation of the bomb (unknown explosive material) was reported. Due to its complexity, also this case is expected to be adopted by well-equipped adversaries.

The branches associated with the detonation of large amounts of explosives inside vessels (AM7) are of particular interest. In fact, two patterns were found. The first consisted in a suicide attack as adversaries

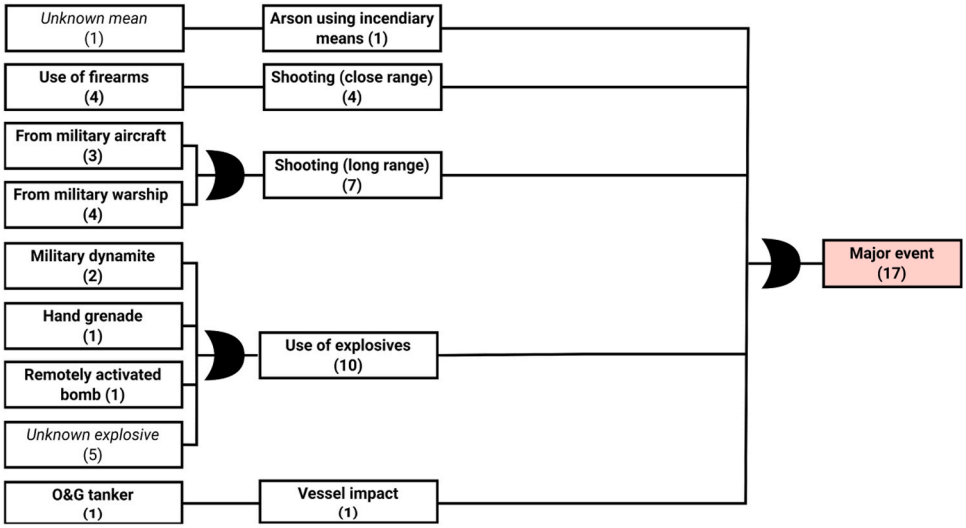

Fig. 7. Attack Tree developed considering a "Major event" as a Security Event. Number in brackets refer to the number of SIs.

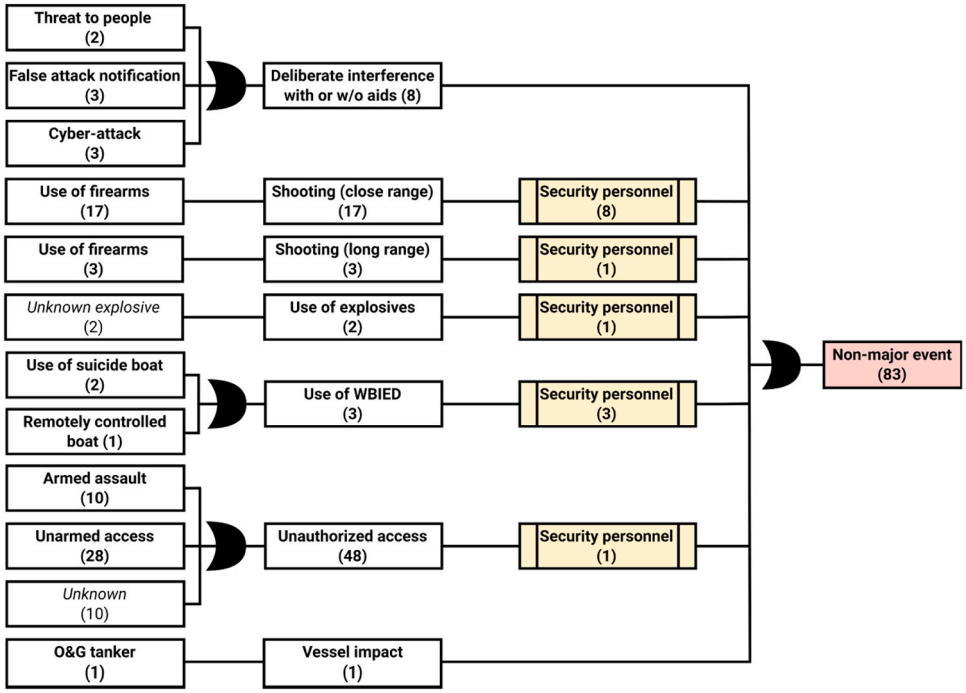

Fig. 8. Attack Tree developed considering a "Non-major event" as a Security Event. Number in brackets refer to the number of SIs.

directly triggered the explosive and died because of the explosion (2 SRIs). The second consisted in a boat controlled and detonated remotely (1 SRI). The latter attack pattern is particularly critical for unmanned facilities, due to the absence of personnel on board able to interrupt the advance.

In both the two SRIs reporting "Vessel impact" (AM8) as attack mode, an Oil&Gas tanker was responsible of ramming the targeted offshore production platforms.

Finally, both armed (10 SRIs) and unarmed (28 SRIs) accesses were recorded in case of adversaries accessing the platform without authorization (AM9) and not resulting in performing any other relevant actions, as reported in the two attack trees. Clearly enough, these situations did not lead to the occurrence of major event scenarios.

Overall, the information supporting the application of Step 1 of API RP 70 and API RP 70I workflow (see Fig. 2) with respect to the characterization of the threat scenarios, is summarized in Table 4. As highlighted above, these outcomes are the result of the analysis of an incident dataset which inherently lacks information due to both the under-reporting of incidents and to their rare occurrence. Thus, on the one hand, the scenarios that are not supported by historical evidence might still be possible. On the other hand, the actual occurrence of the scenarios proposed in the present study in past events (whether they are security threats, attack modes, physical scenarios, consequences, etc.) provides a validation, requiring taking such scenarios into consideration in the context of a SVA/SRA study.

For example, with reference to Table 4, if an insider threat (e.g., a disgruntled employee driven by discontent) is identified as possible security threat in a SVA/SRA study (e.g., in Step 1 of API RP 70/70I), potential attacks such as deliberate interferences (e.g., cyber-attacks or physical actions aimed at causing damage to the installation) and

Table 4
Results of the past incident analysis supporting Step 1 of API RP 70 and API RP 70I as regards the characterization of the threat scenarios.

Security threat	Potential adversary	Reasons/ Motivations	Potential attacks
"Insider threat"	Disgruntled employee	Discontent (e.g., financial)	"Deliberate interference with or w/o aids" (e.g., cyber-attack, physical actions) "Unauthorized access" (e.g., in prohibited areas)
"Operations of military/ paramilitary organizations"	Hostile nation army	Act of war	"Shooting (long range)" (e.g., from aircraft/warship) "Use of explosives" (e.g., military dynamite, hand grenades, remotely activated bombs)
"Outsider cyber threat"	Cyber criminal	Destruction of information	"Deliberate interference with or w/o aids" (Cyber-attack targeting IT-OT system)
"Civil protest"	Nonprofit organization; Popular protesters	Promoting/ protesting a/for given causa (e.g., environmental awareness)	"Unauthorized access" (physical occupation of the platform).
"Robbery/ Kidnapping"	Criminals; Activists	Monetary gain	"Shooting (close range)" (e.g., using rifles and handguns)
"Sabotage"	N.A.	N.A.	"Deliberate interference with or w/o aids" (e.g., physical actions)
"Operations of terrorist/ guerrilla organizations"	Terrorist organization; Guerrilla group	Political power and influence; Religious extremism;	"Shooting (close range)" (e.g., using rifles and handguns) "Use of explosives" (e.g., military dynamite, hand grenades, remotely activated bombs) "Use of WBIED" (e.g., suicide boat, remotely controlled boat)

unauthorized accesses to restricted areas should be considered to characterize such threat.

Similarly, if the threat of religious extremism terrorist organization is identified, attacks like shooting at close range (e.g., with rifles or handguns), using explosives (e.g., military-grade dynamite or hand grenades), and water-borne improvised explosive devices (WBIEDs) should be taken into account as possible attack modes within the SVA/ SRA process to develop security scenarios of concern for the installation (e.g., in Step 1 of API RP 70/70I). These results align with Harel (2012) who underscores the increasing threat posed by terrorists employing WBIEDs and direct assaults on offshore platforms. Similar considerations can be applied to each of the security threats listed in the table.

3.3. Consequence assessment: scenarios generated by threat actors

The identification of the physical scenarios generated through the attacks perpetrated by the threat actors (the adversaries) is part of Step 2 of the API RP 70 and API RP 70I workflow (see Fig. 2). To support this identification, suitable information was gathered by the application of Exploratory Data Analysis (EDA, see Section 2.2) and Attack Tree Analysis (ATA, see Section 2.2).

Similarly to the analysis of the attack modes (see Section 3.2), the results from EDA are shown using Venn diagrams in order to display the overlap between the SC-categories investigated (more than one SC may be triggered in a single attack). The latter are defined in Table A.3 in Appendix A. According to the definitions provided in Table 2, the scenarios from SC1 to SC3 fall under the category "major event", while those from SC5 to SC12 fall under the category "non-major event". The SC4 (shootout) scenario falls under the category "major event" if causes a fatalities or serious personal injury, otherwise it should be considered as a "non-major event".

Fig. 9 shows the share of the physical scenarios with respect to the security threats considered in the present study. The most frequently observed scenario that followed attacks performed by terrorist organizations or guerrilla groups (ST7) are explosion (SC2, 15 SRIs) and shootout (SC4 14 SRIs), with a little overlap between them. Nevertheless, cases of seizing of workers (SC5, 5 SRIs), of operation shutdown (SC7, 3 SRIs), of near miss (SC10, 3 SRIs), and of stolen goods (SC6, 1 SRI), were also recorded.

In the case of "Robbery/Kidnapping" (ST5), almost the totality of the records reported scenarios of seizing of workers (SC5, 25 SRIs), with overlap with shootout (SC4, 4 SRIs), stolen goods (SC6, 7 SRIs), and operation shutdown (SC7, 3 SRIs). As expected, due to both the reasons/ motivations and the attack modes performed by this type of adversaries (see Section 3.2), no major events as defined in Table 2 were recorded.

When the category of insiders is assessed, it is worth considering separately the cyber-insiders from the ones who do not interfere with the IT-OT network of the target facility. In the previous case, seizing of workers (SC5, 2 SRIs) followed the attacks. In the latter case, loss of process control and monitoring (SC9, 1 SRI) was registered.

Loss of operations control and supervision (SC9, 2 SRIs) is the only consequence recorded following the cyber-attacks performed by outsider cyber adversaries (ST3). Nevertheless, as shown by (Iaiani et al., 2023), also major scenarios are possible when the OT system is maliciously manipulated (either remotely or physically, e.g. inducing over-pressurization of equipment leading to a breach and consequent release of the hazardous process fluids).

On the contrary, releases (SC1, 2 SRIs), explosions (SC2, 4 SRIs), and fires (SC3, 5 SRIs) (i.e., the major event scenarios) were recorded as a direct consequence of attacks performed by military/paramilitary organizations (ST2), along with operation shutdown (SC7, 1 SRI) which is not classified as a major event. A near miss (SC10) was also recorded. Given the similarity in the attack modes, it is not surprising that these consequences were also registered for the "Operations of terrorist/ guerrilla organizations" security threat.

As expected in case of adversaries performing civil protests (ST4), the totality of records reported the physical occupation of the platform (SC8, 6 SRIs), while "Sabotage" (ST6) reported also cases of near miss (SC10, 2 SRIs) and cases of consequences labelled as "other" (SC11, 2 SRIs).

The two attack trees (ATs) that were developed by the application of the ATA to the overall dataset (see Fig. 7 and Fig. 8) allowed linking the attack modes to the physical scenarios caused by them, which, in this case, are grouped into the two wider categories "major event" and "non-major event" (see definitions in Table 2).

The AT developed for "Major event" (Fig. 7) shows that there is historical evidence of incendiary attacks (AM2), shooting at both close and long range (AM4 and AM5), of attacks consisting in the detonation of explosive devices (AM6), and in the ramming of platforms with vessels (AM8), that are able to cause a major event scenario as defined in Table 2. In particular, these attack modes cause a damage when the attack vector associated with each of them (i.e., heat load for incendiary attacks, overpressure for attacks involving explosives, and projectile impact for shooting attacks) is sufficiently intense considering the specific features of the target installation such as the material, the equipment thickness, etc. (Iaiani et al., 2022b, 2024a). The findings of a previous study on past security-related incidental scenarios in the onshore context (Iaiani et al., 2022b) suggest that ignition of a released

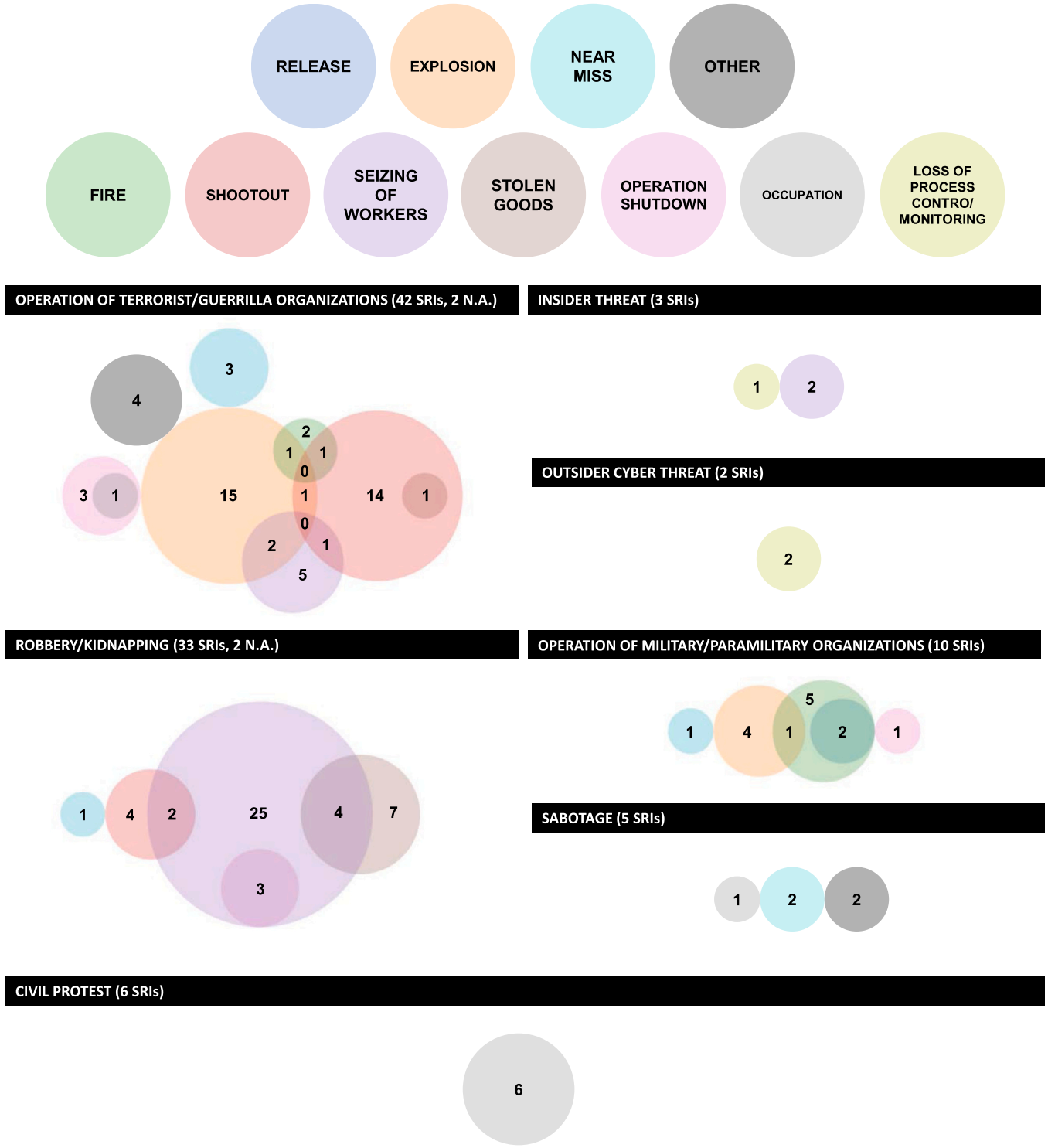

Fig. 9. Venn diagrams displaying the share of the scenarios (see definitions in Table A.3 in Appendix A) with respect to the security threats (see definitions in Table A.1 in Appendix A).

flammable substance (widely handled in Offshore Oil&Gas Fluid Production operations) is likely in case of arsons (certain ignition source), less likely in case of detonation of explosives, and unlikely in case of shootings. These results are deemed applicable also to the case of the offshore Oil&Gas industry given the similarities in the attack modes perpetrated by the adversaries and equipment design.

Although no incident collected has reported a major event originated by the detonation of a WBIED (Water-borne Improvised Explosive Device, AM7), this attack mode is deemed to be likely to cause a loss of containment, as it shares the same attack vector of attacks carried out using explosive devices (i.e., the overpressure). Similarly, also the breach corresponding to deliberate interferences with or without the use of aids (AM3) was not validated by past incidents. However, according to Iaiani et al. (2021c; 2023a,b), cyber-attacks that manage to affect the OT system (e.g., the Basic Process Control System (BPCS) or the Safety Instrumented System (SIS)) may cause a major event when the malicious manipulations are able to overcome the safety/security barriers in place (both active/procedural and passive/inherent safeguards).

The AT developed for "Non-major event" (Fig. 8) show that most of the attacks consisted in armed or unarmed unauthorized accesses to the platforms. Relevant cases of shooting with hand-held firearms at close distance were also recorded, followed by deliberate interferences with or without the use of aids (cyber-attacks, threats to people working on platforms, false attack alarms). The remaining attacks recorded consisted in the shooting at distance, in the detonation of explosives, also contained inside boats controlled remotely or driven by suicidal adversaries, and in the ramming of structural parts of platforms using vessels. What could be surprising is that most of the cited attacks have the potential of causing a major event scenario as defined in Table 2. However, two reasons could be ascribed to the fact that this did not occur in the incidents validating these attacks. First of all, the extent of damage depends on the intensity of the attack vector (heat load, overpressure, and projectile kinetic energy) at the target surface, which is function, among all, of the distance between the point where the attack takes place and the target, of the source of the attack vector (e.g., type of arson, explosive, projectile, etc.), and of the characteristics of target (e.g., material, thickness, etc.). Therefore, a major event scenario (e.g., a breach on the gas/liquid separators present on platforms), only occurs if the intensity of the attack vectors is sufficient to generate it. This issue is discussed by Iaiani et al. (Iaiani et al., 2022a; 2024b) for shooting attacks with handguns and rifles, in Iaiani et al. (2022b) for incendiary attacks, and in Landucci et al. (2015) for attacks involving explosives. A second issue preventing extended damage to occur is the presence of both safety and security barriers (e.g., security personnel), able to mitigate or even interrupt the attacks, as discussed in Section 5.

None of the incidents collected in the developed dataset reported aircraft impacts (AM1). Nevertheless, depending on the characteristics of the impact and of the two elements involved (the aircraft and the target), both major and non-major event scenarios are deemed possible outcomes of such attacks.

The information supporting the application of Step 2 of API RP 70 and API RP 70I workflow (see Fig. 2) concerning the identification of the physical scenarios generated by the attacks carried out by the threat actors (the adversaries) are summarized in Table 5.

Table 5
Results of the past incident analysis supporting Step 2 of API RP 70 and API RP 70I concerning the identification of the minimum set of physical scenarios generated by the attacks and the evaluation of their consequences.

Security threat	Potential scenarios	Potential consequences
"Insider threat"	"Loss of process control/ monitoring"	"Asset damage / Economic loss"
	"Seizing of workers"	"Damage to people"
"Operations of military/ paramilitary organizations"	"Release"; "Fire"; "Explosion"	"Asset damage / Economic loss"; "Damage to environment"; "Damage to people"
"Outsider cyber threat"	"Loss of process control/ monitoring"	"Asset damage / Economic loss"
"Civil protest"	"Occupation"	"Asset damage / Economic loss"; "Damage to reputation"
"Robbery/Kidnapping"	"Seizing of workers", "Shootout"	"Damage to people"
	"Stolen goods", "Operation shutdown"	"Asset damage / Economic loss"
"Sabotage"	"Operation shutdown", "Other"	"Asset damage / Economic loss"
"Operations of terrorist/ guerrilla organizations"	"Release"; "Fire"; "Explosion"	"Asset damage / Economic loss"; "Damage to environment"; "Damage to people"

3.4. Consequences of the scenarios

The evaluation of the consequences in terms of damage to people, environment, assets and reputation of the physical scenarios generated through the attacks is still part of Step 2 of the API RP 70 and API RP 70I workflow (see Fig. 2). To support this evaluation, suitable information was gathered by application of EDA.

Fig. 10 shows the distribution of the consequences classes (defined in Table A.4 in Appendix A) suffered by facilities for each category of physical scenario (SC) considered. Also in this case, more than one consequence class can be recorded in the dataset for the same SRI record as they are not mutually exclusive (multiple consequences can be associated to the same SC).

As expected, the major event scenarios (i.e., release, explosion, fire) were reported to cause asset damages and economic losses (CQ1) to the facility. Unfortunately, the information in the incident records did not allow to discriminate the extent of economic loss in monetary terms. In case of fires, also damages to people (CQ3) were recorded. Even if no records reported fatalities or injuries caused by an explosion (deflagration/detonation of an explosive or the physical explosion of an equipment item), also this physical scenario has the potential for such outcomes. Environmental damages (CQ2) were also recorded in case of the release of hazardous substances (e.g., release of crude oil to the sea).

Asset damages and economic losses (CQ1) were found to frequently occur also in case of non-major event scenarios. Nevertheless, even if not reported in the dataset entries, their extent is deemed to be smaller than that of major events as, for the latter, the repair or replacement of the damaged installation is a cost that adds to that of the production outage.

Shootouts and seizing of workers reported damages to people (CQ3) as a consequence. Differently, only reputation damages were registered in case of pacific physical occupations, but this outcome is probably affected by the under-reporting of information in the incident records (more attention is given to final targets such as people and environment, rather than to company reputation).

Overall, the information from the dataset analysis that can be used to support the application of Step 2 of API RP 70 and API RP 70I workflow (see Fig. 2) with respect to the evaluation of the consequences of the physical scenarios generated by the intentional attacks, is summarized in Table 5. As highlighted in the other sections, due to both the under-reporting of the incidents and the fact that they are rare events, these results do not represent all the possible scenarios that can be generated by the attacks performed by the threat actors, but shall be intended as a minimum set to be considered. A clear example is the case of cyber-attacks for which no major event scenarios were recorded for the offshore Oil&Gas production sector but have the potential of causing releases of hazardous materials also from the equipment units typically

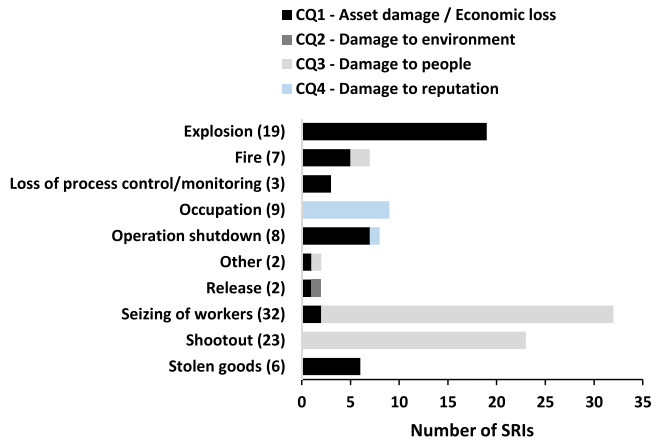

Fig. 10. Share of the consequences (CQs) suffered by the facilities for each physical scenario (SC).

present in offshore platforms (Iaiani et al., 2023a,b). As a result, Table 5 reports only the scenarios and consequences derived from the past incident analysis carried out in the present study, providing a valid rationale to consider these events in the context of a SVA/SRA study as starting reference scenarios. In case both non-major and major events scenarios are reported for a given security threat, only the latter are included in the table, according to the worst-case scenario principle commonly adopted in security risk assessment.

For example, with reference to Table 5, if an insider (e.g., a disgruntled employee) performing a cyber-attack has been identified in a SVA/SRA study (e.g., in Step 1 of API RP 70/70I) as possible security threat for the installation under assessment, the relevant physical scenarios to be considered (e.g., in Step 2 of API RP 70/70I) should include loss of process control/monitoring, which could lead to possible asset damages and economic losses due to impossibility of maintaining operational and/or safety conditions.

Similarly, if the threat from military or paramilitary organizations performing attacks such as long-range shooting or the use of explosives is identified in the threat assessment phase of SVA/SRA, the scenarios to be considered in the consequence assessment should include the release of hazardous material, potentially leading to fire or explosion. These scenarios could result in a significant asset damage, harm to the environment, and casualties, depending on the scale of the attack, the vulnerabilities and location of the installation, and the presence of personnel. These types of attacks and their severe consequences are further corroborated by the findings of Bajpai and Gupta (2007), who highlight the severe environmental and economic damage that the use of explosives can cause in offshore oil and gas installations.

3.5. Vulnerability Assessment

The evaluation of each threat scenario in terms of the facility vulnerability to an attack is part of Step 3 of the API RP 70 and API RP 70I workflow (see Fig. 2). As reported in the reference sources of the two recommended practices, two primary elements should be considered in the assessment: accessibility and organic security. The first is related to the physical and geographic barriers that deter the threat actors (e.g., floating barriers, platform structural elements, etc.), while the second refers to the ability of the facility personnel in interrupting or mitigating the attack (it may include security plants, communication capabilities, intrusion detection systems, etc.).

Unfortunately, the entry records in the dataset did not report any detail concerning accessibility, while some information regarding organic security was retrieved from the description of 35 incidents collected. In particular, in 5 SRIs, preventive evacuation plans were activated, resulting in the total or partial abandonment of the platform: clearly, this barrier is only effective in safeguarding human life, and not in preserving the environment and/or the assets. However, in 3 out of the 5 incidents, both injuries and fatalities were reported: this is ascribed to the time needed for crew evacuation, especially in the case of large platforms with hundreds of employees onboard. Moreover, the evacuation process was possibly started only after the attack has been executed by the threat actors (Iaiani et al., 2023c).

In the remaining 30 incidents, the intervention of the security force (navy) was recorded as a result of the communication of a threatening circumstance by the operators working on the platform or of standard patrol surveillance in place. In 14 out of the 30 SRIs, the security force succeeded in interrupting and/or mitigating the attacks perpetrated by the threat actors, while in the other 16 cases the intervention was not on time or ineffective. In particular, the attacks interrupted and/or mitigated consist in the shooting at both close and long rage, in the detonation of explosives devices on the platform, and in the use of WBIED. These attacks, thanks to the intervention of the security force, resulted in a non-major event scenario (see the attack tree shown in Fig. 8) even if they have the potential to cause a breach in the equipment units typically used in offshore Oil&Gas platforms, with the consequent release of oil and/or natural gas (major event scenario).

Overall, these findings did not provide valuable information to directly support the application of existing SVA/SRA studies, but they highlighted the critical role of timely security force intervention in interrupting or mitigating attacks. This intervention is only successful when threat actors are detected early enough in their attack path, such that the time remaining to complete their task is greater than the security force's response time. Otherwise, the attack proceeds unhindered, posing a significant challenge in detecting adversaries at sea, as discussed by Iaiani et al. (2023c).

As a complement to these findings, Kashubsky and Morrison (2013) emphasize the role of exclusion zones and ship routing measures as preventive strategies against unauthorized accesses. They propose extending the typical 500-meter exclusion zone into a layered system consisting of a 15-nautical-mile cautionary zone, where vessels are monitored but not restricted, a 5-nautical-mile restricted zone, where access is limited and requires prior authorization, and a 1–2.5-nautical-mile exclusion zone, where unauthorized vessels are completely prohibited from entering (any breach triggers immediate response measures). This is also supported by Cordner (2011), who discusses the need for regional cooperation in establishing broader exclusion zones and strategic risk management frameworks to mitigate growing security risks in the Asia-Pacific region due to increased maritime activity.

4. Discussion

The Security Vulnerability Assessment (SVA) methodology proposed by API RP 70 and API RP 70I (see description in Appendix C) emphasizes the importance of past incident analysis as a useful tool in deriving insights for the security risk assessment process. In fact, by examining historical data, it is possible to validate through evidence key security scenarios and support the development of mitigation strategies to enhance future preparedness from the information of past events.

However, it is important to remark that the results shown in the previous section do not claim to be exhaustive. Since the analysis was based on a relatively low number of recorded SRIs (i.e., 112, see Table B.1 in Appendix B), specific attention was devoted to assessing the actual statistical value of the results. However, as demonstrated in several studies analysing past events (Ovidi et al., 2020; Paltrinieri et al., 2012; Paltrinieri and Reniers, 2017; Planas et al., 2015; Skogdalen and Vinnem, 2012; Zhu et al., 2017), important insights and lessons learnt can still emerge even from a limited number of records. Although there is a possibility that some findings may appear intuitively obvious due to the characteristics of the data, the ability to empirically confirm these trends is particularly significant in the context of risk management. In fact, such validation plays a key role in supporting strategic decision-making, as it provides solid justification for targeted investments and resource allocation to mitigate the identified risks (Reniers and Brijs, 2014).

Given the data scarcity limitation, the analysis of past incidents could benefit from integration with predictive approaches to achieve a more comprehensive assessment of security risks. In fact, this integration not only allows for the consideration of emerging and evolving threats that may not have occurred yet but remain plausible, but also helps to account for potential gaps in historical records, where incidents might have occurred but were not captured due to underreporting. By combining these approaches, a more comprehensive and robust assessment of security risks can be achieved. An example of such integration can be found in Iaiani et al. (2023b), where a comprehensive framework for cyber risk assessment is proposed for the chemical and process industry, combining the results of the analysis of 82 past cybersecurity incidents (Iaiani et al., 2021b) with a predictive methodology (POROS 2.0 – Process Operability Analysis of Remote manipulations through the cOntrol System (Iaiani et al., 2023a)) to generate a facility-specific list of cybersecurity-related scenarios. This integrated perspective ensures a forward-looking analysis.

This aspect is also highlighted in other recent studies. For instance, Larsen et al., (2022) developed a model that examines the factors influencing deck officers' perception of cyber risks in offshore operations, enabling to predict how evolving cyber risks are perceived by key personnel, which in turn supports the implementation of proactive security measures to address future threats. Similarly, Kulev and Torres (2022), by simulating the impact of cyber-attacks on offshore wind farms, demonstrated how anticipating the manipulation of critical parameters can enhance preparedness against emerging cyber risks.

A further issue concerns the use of Attack Tree Analysis (ATA) for categorizing and describing attack modes. While ATA can be a valuable tool in characterizing attacks, in complex and dynamic scenarios, it may oversimplify the possible attack patterns and interactions and fail to capture the evolving nature of emerging threats. As with the challenges mentioned earlier, these limitations can also be overcome by integrating ATA with predictive methodologies, such as Bayesian networks (BN) or machine learning models. For example, in a previous study (Iaiani et al., 2024a), the authors proposed a preliminary version of a BN-based methodology to systematically identify security scenarios from historical datasets, capturing the full network of cause-effect relationships with the flexibility to update the network as new information becomes available.

In perspective, the application of advanced approaches proposed in recent years can be applied to integrate the results of the present study beyond state-of-the-art methodologies. For example, Ayyildiz and Erdogan (2024) applied spherical fuzzy decision-making analysis to evaluate risk mitigation strategies in offshore wind farms. Although this approach focuses on a different sector, it provides a structured method that can be applied also in the security domain to assess and prioritize mitigation strategies aimed at reducing the impact of potential threats.

Fouzi et al. (2024) present a systematic review of chemical safety and security risk management approaches, focusing on organizational and technology-based strategies to enhance threat detection and prevention. Similarly, Yuan and co-workers (2023) proposed cost-effective approaches that optimize the maintenance of safety and security barriers, ensuring the continuous protection of critical infrastructure (including offshore installations) while minimizing costs. Moreover, Zhu and Liyanage (2021) and Ding et al. (2024) discussed the adoption of real-time monitoring systems and AI-based threat detection systems to enhance the response to both physical and cyber threats in the offshore Oil&Gas industry, proving their effectiveness.

Men et al. (2022) proposed a Pareto-based multi-objective network design approach aimed at minimizing various risks, including security risks, associated with the transportation of hazardous materials by road. Although originally developed for onshore applications, this method could potentially be adapted to the offshore Oil&Gas sector, specifically for optimizing maritime transportation routes and reducing security risks such as piracy attacks.

Overall, the combination of the results obtained in this study through past incident analysis with these advanced techniques is the way forward to create a more comprehensive framework for identifying vulnerabilities and developing effective risk mitigation strategies against security threats to offshore Oil&Gas installations (e.g., as required in Steps 3 and 4 of API RP 70/70I, outlined in Appendix C).

5. Conclusions

A dataset of 112 past security-related incidents that affected offshore Oil&Gas production infrastructures in the last fifty years was collected and analyzed using a structured set of techniques, including Exploratory Data Analysis, Root Cause Analysis, and Attack Tree Analysis. The results obtained provide specific ad-hoc support to the steps "Potential Threat", "Consequence Assessment", and "Vulnerability assessment" of the SVA approach proposed by the API Recommended Practices 70 and 70I (specific for the offshore Oil&Gas sector) and were summarized into guiding tables. The tables include a reference list of the minimum set of cases, validated by the analysis of the dataset, that shall be considered for application in SVA/SRA. Thus, the results support the thorough analysis of all the SRI aspects, reducing the possibility of oversights or underestimation of security risks.

Terrorism is highlighted as the primary concern for offshore Oil&Gas facilities, followed by acts of robbery and kidnapping, that resulted in several high-profile incidents, especially in the areas of the Gulf of Guinea (Africa) and the Strait of Malacca (Asia). The analysis of the attack modes outlined the prevalent tactics, as close-range shootings and both armed and unarmed unauthorized accesses on platforms, offering comprehensive insights on the behaviour of the threat actors.

Important differences were found in the physical scenarios generated by the attacks: attacks by terrorist or guerrilla groups often led to explosions and shootouts, whereas incidents involving robbers and kidnappers primarily revolved around theft of valuable items and worker seizures. A relevant number of attacks performed by military and paramilitary organizations resulted in the occurrence of a major event scenario such as a release of hazardous materials, an explosion, and/or a fire, while loss of process control resulted the outcome of cyber-criminal actions. Both fatalities and injuries, as well as asset damages and economic losses were the consequences suffered by the targeted facilities, proving that security attacks to offshore Oil&Gas infrastructures have the potential of causing severe damages, comparable to that occurring in safety-related accidents. Therefore, the overall results obtained in the present study, besides providing valuable support to the application of the SVA workflow proposed by API RP 70 and API RP 70I, evidence that integrating security risks into comprehensive risk analyses is imperative for a holistic understanding of all the risks and for an effective use of resources aimed at risk prevention and mitigation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by Ministero dello Sviluppo Economico (MISE), Direzione Generale per le Infrastrutture e la Sicurezza dei Sistemi Energetici e Geominerari (DGISSEG) in the framework of the project «Security degli Impianti Offshore».

Appendix A. Definitions of dataset itemized fields

Table A.1
Definitions of the classes considered for the itemized field "Security threat".

ST code	Security Threat	Definition
ST1	Insider threat	The attacker is an insider, i.e., an individual who normally has authorized access to the assets of the company (e.g., employee, contractor, business partner, vendor, etc.). The motivation is related to working dissatisfaction or possibility of gaining personal advantage (e.g., stealing items or materials). Insider threat refers both to physical security and cybersecurity.
ST2	Operations of Military / Paramilitary organizations	An interference in normal operations or damage to people, equipment or installations perpetrated by a regular or irregular army. In the latter case, however, the organizational structure, tactics, training, subculture, and often function are similar to those of a professional military organization.
ST3	Outsider cyber threat	Attacker characterized by an attack, via cyberspace, targeting the IT-OT system of a facility with the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. Usually, the malwares used by the attackers were not tailored for industrial control systems, but they breached the company network protection compromising operations. Examples include hackers and cyber criminals.
ST4	Civil protest	Group of people such as non-violent environmental activists, indigenous activists, labour activists, striking workers and anti-government protesters that interfere with normal operations without the use of violence.
ST5	Robbery/Kidnapping	Events collected in this category are characterized by an attack mode aimed at stealing cash or valuable items or extorting money by kidnapping or hostage taking. Examples include single robbers/kidnappers or criminal groups.
ST6	Sabotage	Events collected in this category are characterized by an attack mode aimed at disrupting normal operations, but not defined in their threatening agent, as well as in their driving motivations. Examples include single saboteurs or non-organized groups of people.
ST7	Operations of terrorist/guerrilla organizations	Terrorist organizations or criminal groups, highly capable, well organized and equipped, focused on targeting a facility with the aim of causing a high-impact event, not only in terms of casualties, but also on media. Unlike military and paramilitary organizations, they operate clandestinely and use violence or intimidation against civilians or non-combatants to achieve political, ideological, or religious goals. Operations performed by guerrillas are included.
ST8	Unknown	An interference in normal production activities has been achieved via certainly intentional acts, but no more details were given concerning attackers or motivations of the act. This category refers both to physical security and cybersecurity.

Table A.2
Definitions of the classes considered for the itemized fields "Attack mode 1" and "Attack mode 2".

AM code	Attack Mode	Definition
AM1	Aircraft impact	Aircraft impact aimed to release hazardous substances or damage/destroy important parts of the installation.
AM2	Arson using incendiary means	Incendiary attacks using an incendiary device (e.g., fuel tank either available on site or brought in by the attacker).
AM3	Deliberate interference with or w/o aids	Deliberate acts involving simple operations without the use of instruments, or deliberate interference using tools and aids that are present on site, or prepared destruction of installation parts by force using heavy tools.
AM4	Shooting (close range)	Interference at close distance, using different types of small/medium weapons (e.g., handguns and rifles).
AM5	Shooting (long range)	Interference at distance, using different types of heavy weapons (e.g., missiles, bazookas, bombs dropped from airplanes or drones).
AM6	Use of explosives	Use explosives (e.g., Triacetone Triperoxide Peroxyacetone – TATP, Ammonium Nitrate Fuel Oil – ANFO, or dynamite) to blow up equipment or pipework or to blow up load-bearing structures to cause the collapse.
AM7	Use of Water-borne Improvised Explosive Devices (WBIED)	Use of a vessel (e.g., boat, barge, etc.) carrying explosives (e.g., Triacetone Triperoxide Peroxyacetone – TATP, Ammonium Nitrate Fuel Oil – ANFO, or dynamite) to blow up equipment, pipework or load-bearing structures.
AM8	Vessel impact	Vessel (e.g., boat, barge, etc.) impact (e.g., ramming) aimed to release hazardous substances or damage/destroy important parts of the installation.
AM9	Unauthorized access	Physically accessing a property/area without authorization. The attack does not result in an attack method listed in this table or the adversaries performed other actions in addition to those reported in this table.
AM10	Unknown	The information available in records do not provide details on the attack mode.

Table A.3
Definitions of the classes considered for the itemized fields "Scenario 1" and "Scenario 2".

SC code	Scenario	Definition
SC1	Release	Scenario consisting in the discharge of a chemical from its containment, i.e., the process and storage equipment in which it is kept, without any further consequence such as an explosion or a fire (e.g., leak from vessel or pipework, catastrophic rupture).
SC2	Explosion	Scenario consisting in a physical and/or chemical explosion or in the deflagration or detonation of an explosive device.
SC3	Fire	Scenario consisting in a pool fire, jet fire, fireball, flash fire, flame, or in a non-hazardous material fire (paper, plastic, solid structures, etc.).
SC4	Shootout	Scenario consisting in a shooting battle between armed groups, or between one armed and one unarmed group.
SC5	Seizing of workers	Scenario during which hostages are taken among the workers in the facility, or during which workers are kidnapped.
SC6	Stolen goods	Goods of workers, cash or equipment belonging to the facility went missing, including hijacked vessels, helicopters or other transportation means.
SC7	Operation shutdown	Production and/or operation interruption, without the occurrence of a release of hazardous substances, a fire, or an explosion.
SC8	Occupation	Presence onboard of unauthorized people without major interaction with process/assets.
SC9	Loss of process control/ monitoring	Scenario consisting in the physical or cyber interference with the OT system (software and hardware), without the occurrence of a release of hazardous substances, a fire, or an explosion.

(*continued on next page*)

Table A.3 (*continued*)

SC code	Scenario	Definition
SC10	Near miss	Scenario not resulting in one of the scenario cases of the current table, but the attack perpetrated by the attackers had clear potential to result in at least one of such scenarios.
SC11	Other	Scenario that cannot be classified by the other definitions in this table.
SC12	Unknown	The information available in records do not provide details on the scenario.

Table A.4
Definitions of the classes considered for the itemized fields "Consequence 1", "Consequence 2", and "Consequence 3".

CQ code	Consequence	Definition
CQ1	Asset damage / Economic loss	Physical and economic damages due to loss of an asset for the affected facility, whether it is a loss of production capability, loss of equipment and property, including loss of sensitive data. Loss of life is not included.
CQ2	Damage to environment	Damages to the ecosystems due to air and/or water pollution, or land contamination.
CQ3	Damage to people	Injury or fatality of people.
CQ4	Damage to reputation	Damage to the reputation of the Company affected with potential impacts to the ability of the Company to sustain business position.
CQ5	Unknown	The information available in records do not provide details on the consequence.

Appendix B. The dataset

Table B.1
List of security-related incidents (SI) recorded in the dataset. For each SI, year, location, security threat, attack mode, scenario, consequence, and data source are reported. AF: Africa; AS: Asia; EU: Europe; NA: North America; SA: South America. For other codes see **Table A.1**, **Table A.2**, **Table A.3**, and **Table A.4** in Appendix A.

ID	Year	Location	Security Threat	Attack Mode	Scenario	Consequence	Source
#01	1899	NA	ST6	AM9	SC11	CQ1	(Kashubsky, 2011)
#02	1975	EU	ST6	AM3	SC10	CQ5	(Kashubsky, 2011)
#03	1977	AF	ST7	AM3	SC12	CQ5	(Kashubsky, 2011)
#04	1981	NA	ST6	AM3	SC10	CQ5	(Kashubsky, 2011)
#05	1981	AS	ST2	AM8	SC7	CQ1	(DNV GL Digital Solutions, 2015)
#06	1983	AS	ST2	AM5	SC1; SC3	CQ1; CQ3	(Kashubsky, 2011)
#07	1983	AS	ST2	AM5	SC2; SC3	CQ1; CQ2	(DNV GL Digital Solutions, 2015)
#08	1983	AS	ST2	AM8	SC2	CQ1	(DNV GL Digital Solutions, 2015)
#09	1983	AS	ST2	AM5	SC1; SC3	CQ1	(DNV GL Digital Solutions, 2015)
#10	1985	AS	ST2	AM5	SC3	CQ1	(DNV GL Digital Solutions, 2015)
#11	1987	AS	ST8	AM10	SC12	CQ5	(START, 2020)
#12l	1987	AS	ST2	AM5; AM6	SC2	CQ1	(Kashubsky, 2011)
#13	1988	AS	ST2	AM5	SC3	CQ1; CQ3	(DNV GL Digital Solutions, 2015)
#14	1988	AS	ST2	AM5; AM6	SC2	CQ1	(Kashubsky, 2011)
#15	1995	EU	ST4	AM9	SC8	CQ4	(Kashubsky, 2011)
#16	1998	AF	ST4	AM9	SC8	CQ4	(Kashubsky, 2011)
#17	1999	AF	ST8	AM9	SC7	CQ4	(Office of Naval Intelligence, 2023)
#18	1999	AF	ST5	AM9	SC5; SC6	CQ1; CQ3	(Kashubsky, 2011)
#19	1999	AF	ST5	AM9	SC5	CQ3	(Kashubsky, 2011)
#20	1999	AF	ST5	AM9	SC5	CQ3	(Kashubsky, 2011)
#21	2000	EU	ST4	AM9	SC8	CQ4	(Office of Naval Intelligence, 2023)
#22	2000	AF	ST5	AM9	SC5	CQ3	(Kashubsky, 2011)
#23	2000	SA	ST7	AM9	SC11	CQ5	(Office of Naval Intelligence, 2023)
#24	2001	AS	ST6	AM3	SC11	CQ5	(Office of Naval Intelligence, 2023)
#25	2001	AF	ST5	AM9	SC5	CQ1; CQ3	(Kashubsky, 2011)
#26	2002	AF	ST5	AM9	SC5	CQ3	(Office of Naval Intelligence, 2023)
#27	2002	AF	ST5	AM9	SC5	CQ1; CQ3	(Office of Naval Intelligence, 2023)
#28	2003	AF	ST8	AM9	SC8	CQ4	(Office of Naval Intelligence, 2023)
#29	2003	AF	ST4	AM9	SC8	CQ4	(Office of Naval Intelligence, 2023)
#30	2003	AF	ST5	AM9	SC5	CQ3	(Office of Naval Intelligence, 2023)
#31	2003	AF	ST7	AM3	SC11	CQ5	(Office of Naval Intelligence, 2023)
#32	2003	AF	ST4	AM9	SC8	CQ4	(Office of Naval Intelligence, 2023)
#33	2003	AF	ST5	AM9	SC5	CQ3	(Office of Naval Intelligence, 2023)
#34	2003	AF	ST1	AM9	SC5	CQ3	(Kashubsky, 2011)
#35	2003	NA	ST3	AM3	SC9	CQ1	(RISI, 2015)
#36	2004	AF	ST5	AM4	SC4	CQ3	(Office of Naval Intelligence, 2023)
#37	2004	AS	ST7	AM7	SC7	CQ1	(START, 2020)
#38	2004	AS	ST7	AM7	SC10	CQ5	(Kashubsky, 2011)
#39	2004	AF	ST1	AM9	SC5	CQ3; CQ4	(Office of Naval Intelligence, 2023)
#40	2004	AF	ST7	AM9	SC11	CQ5	(Office of Naval Intelligence, 2023)
#41	2004	AS	ST7	AM9	SC5	CQ3	(Kashubsky, 2011)
#42	2004	AF	ST3	AM3	SC9	CQ1	(RISI, 2015)

(*continued on next page*)

Table B.1 (*continued*)

ID	Year	Location	Security Threat	Attack Mode	Scenario	Consequence	Source
#43	2005	AF	ST6	AM9	SC8	CQ4	(Office of Naval Intelligence, 2023)
#44	2005	AF	ST5	AM9	SC5; SC7	CQ1; CQ3	(Kashubsky, 2011)
#45	2005	AF	ST7	AM9	SC7; SC8	CQ1	(Kashubsky, 2011)
#46	2006	AF	ST7	AM6; AM9	SC2; SC5	CQ1; CQ3	(Kashubsky, 2011)
#47	2006	AF	ST7	AM2; AM4	SC3; SC4	CQ1; CQ3	(Kashubsky, 2011)
#48	2006	AF	ST7	AM9; AM6	SC5; SC2	CQ1; CQ3	(Kashubsky, 2011)
#49	2006	AF	ST5	AM9	SC5; SC7	CQ1; CQ3	(Kashubsky, 2011)
#50	2006	AF	ST5	AM9	SC5	CQ3	(Kashubsky, 2011)
#51	2006	AF	ST5	AM10	SC12	CQ5	(START, 2020)
#52	2006	AF	ST5	AM9	SC5; SC6	CQ1; CQ3	(Office of Naval Intelligence, 2023)
#53	2007	AF	ST5	AM9	SC5; SC7	CQ1; CQ3	(Kashubsky, 2011)
#54	2007	AF	ST5	AM9	SC5	CQ3	(Kashubsky, 2011)
#55	2007	AF	ST5	AM9	SC5	CQ3	(Office of Naval Intelligence, 2023)
#56	2007	AF	ST5	AM4; AM9	SC4; SC5	CQ1; CQ3	(Kashubsky, 2011)
#57	2007	AF	ST7	AM9	SC5	CQ1	(Office of Naval Intelligence, 2023)
#58	2007	AF	ST7	AM4; AM9	SC4; SC6	CQ1; CQ3	(Office of Naval Intelligence, 2023)
#59	2008	EU	ST8	AM10	SC11	CQ5	(Kashubsky, 2011)
#60	2008	AF	ST7	AM4	SC4	CQ3	(Office of Naval Intelligence, 2023)
#61	2008	AF	ST7	AM4	SC4	CQ3	(Office of Naval Intelligence, 2023)
#62	2008	AF	ST8	AM5	SC4	CQ3	(Kashubsky, 2011)
#63	2008	AF	ST8	AM4	SC4	VQ3	(START, 2020)
#64	2008	AF	ST7	AM4; AM9	SC4; SC5	CQ3	(START, 2020)
#65	2008	AF	ST8	AM4	SC4	CQ3	(START, 2020)
#66	2008	AF	ST8	AM5	SC4	CQ3	(Kashubsky, 2011)
#67	2008	AF	ST7	AM6	SC2	CQ1; CQ3	(Office of Naval Intelligence, 2023)
#68	2008	AF	ST7	AM4	SC4	CQ3	(Office of Naval Intelligence, 2023)
#69	2008	NA	ST1	AM3	SC9	CQ1	(RISI, 2015)
#70	2009	AF	ST5	AM9	SC6	CQ1	(Office of Naval Intelligence, 2023)
#71	2009	AF	ST7	AM4	SC10	CQ5	(Office of Naval Intelligence, 2023)
#72	2009	AF	ST7	AM4	SC4	CQ3	(Office of Naval Intelligence, 2023)
#73	2009	AF	ST7	AM4	SC4	CQ3	(Kashubsky, 2011)
#74	2009	AF	ST7	AM6	SC2	CQ1	(Kashubsky, 2011)
#75	2009	AF	ST7	AM4	SC4	CQ3	(Kashubsky, 2011)
#76	2009	AF	ST7	AM6	SC2; SC3	CQ1; CQ3	(Kashubsky, 2011)
#77	2009	AF	ST7	AM6	SC2	CQ1	(Kashubsky, 2011)
#78	2009	AF	ST7	AM6; AM4	SC2; SC4	CQ1; CQ3	(START, 2020)
#79	2010	AF	ST5	AM4; AM9	SC4; SC5	CQ3	(Kashubsky, 2011)
#80	2010	AF	ST5	AM9	SC5	CQ3	(Office of Naval Intelligence, 2023)
#81	2010	AF	ST5	AM9	SC5	CQ3	(Office of Naval Intelligence, 2023)
#82	2010	AF	ST5	AM9	SC5	CQ3	(Office of Naval Intelligence, 2023)
#83	2010	AF	ST5	AM9	SC5	CQ1; CQ3	(Kashubsky, 2011)
#84	2010	AF	ST7	AM4	SC4	CQ3	(Kashubsky, 2011)
#85	2010	AF	ST7	AM6	SC2	CQ1	(Office of Naval Intelligence, 2023)
#86	2011	AF	ST7	AM6	SC2	CQ1	(Office of Naval Intelligence, 2023)
#87	2011	AF	ST7	AM6	SC2	CQ1	(Office of Naval Intelligence, 2023)
#88	2013	AF	ST5	AM10	SC12	CQ5	(Office of Naval Intelligence, 2023)
#89	2014	AF	ST5	AM4	SC4	CQ3	(Office of Naval Intelligence, 2023)
#90	2015	AF	ST7	AM4	SC4	CQ3	(Office of Naval Intelligence, 2023)
#91	2015	AF	ST8	AM5	SC4	CQ3	(Office of Naval Intelligence, 2023)
#92	2016	AF	ST7	AM4	SC4	CQ3	(Office of Naval Intelligence, 2023)
#93	2016	AF	ST7	AM10	SC7	CQ1	(Office of Naval Intelligence, 2023)
#94	2016	AF	ST7	AM10	SC11	CQ3	(Office of Naval Intelligence, 2023)
#95	2016	AF	ST7	AM10	SC12	CQ5	(Office of Naval Intelligence, 2023)
#96	2016	AF	ST7	AM4	SC4	CQ1; CQ3	(Office of Naval Intelligence, 2023)
#97	2016	AF	ST7	AM6	SC2	CQ1	(Office of Naval Intelligence, 2023)
#98	2016	AF	ST7	AM6	SC2	CQ1	(Office of Naval Intelligence, 2023)
#99	2016	AF	ST7	AM6	SC2	CQ1	(Office of Naval Intelligence, 2023)
#100	2016	AF	ST7	AM6	SC2	CQ1	(Office of Naval Intelligence, 2023)
#101	2016	AF	ST8	AM9	SC12	CQ5	(START, 2020)
#102	2017	AS	ST7	AM7	SC10	CQ5	(Office of Naval Intelligence, 2023)
#103	2017	AF	ST5	AM9	SC6	CQ1	(Office of Naval Intelligence, 2023)
#104	2017	AS	ST2	AM6	SC10	CQ5	(Office of Naval Intelligence, 2023)
#105	2020	AF	ST8	AM4	SC10	CQ5	(Office of Naval Intelligence, 2023)
#106	2020	AF	ST5	AM9	SC5	CQ3	(Office of Naval Intelligence, 2023)
#107	2020	SA	ST7	AM6	SC2	CQ1	(START, 2020)
#108	2020	EU	ST4	AM9	SC8	CQ4	(Offshore Engineer, 2020)
#109	2021	SA	ST5	AM9	SC6	CQ1	(Safety4Sea, 2021)
#110	2022	SA	ST5	AM9	SC5	CQ1; CQ3	(Chaparro, 2022)
#111	2022	SA	ST5	AM9	SC5	CQ1; CQ3	(Falcon Mega Solutions, 2022)
#112	2022	SA	ST5	AM10	SC10	CQ5	(Domínguez, 2022)

Appendix C. – Outline of the SVA approach proposed by API RP 70/70I

The SVA approach outlined in API RP 70 and API RP 70I is structured into 5 steps.

Step 1 (Potential Threat) requires the identification of potential threats and the related types of attack through which a given asset could be targeted. These include external attacks such as ramming a vessel into the platform, underwater sabotage by divers, or even the illicit takeover of the facility by intruders.

Step 2 (Consequence Assessment) involves evaluating the physical damage scenarios that could be triggered by the attacks carried out by the threat actors. For each scenario, a consequence score is assigned based on the potential impacts that can be caused, which may range from moderate – causing minimal operational or environmental damage – to catastrophic, leading to significant loss of life, severe economic disruption, and/or long-term ecological harm.

Step 3 (Vulnerability Assessment) involves evaluating the facility's susceptibility to the identified security scenarios (threat – attack – physical damage scenario). Two key factors are assessed: the facility's accessibility, which refers to how easily an attacker could reach the site (this relates to physical and geographic barriers), and organic security, which reflects the facility's internal capacity to deter or respond to an attack (this relates to security procedures, including response protocols). A vulnerability score is then assigned based on the level of these two factors.

In Step 4 (Mitigation), uses the results of the vulnerability and consequence assessments to determine appropriate mitigation strategies aimed at reducing the risk associated with each security scenario. These strategies may include reinforcing access controls, upgrading surveillance systems, or improving the training and preparedness of security personnel. This is guided by the combination of the vulnerability score and the consequence score of each scenario.

Finally, Step 5 (Implementation) focuses on the effective execution and documentation of the selected mitigation measures, ensuring they are fully incorporated into the facility's operational practices.

References

Abdo, H., Kaouk, M., Flaus, J.M., Masse, F., 2018. A safety/security risk analysis approach of industrial control systems: a cyber bowtie – combining new version of attack tree with bowtie analysis. Comput. Secur 72, 175–195. https://doi.org/10.1016/j.cose.2017.09.004.

American Petroleum Institute (API), 2010. API RP 70: Security for Offshore Oil and Natural Gas Operations.

American Petroleum Institute (API), 2012. API RP 70I: Security for Worldwide Offshore Oil and Natural Gas Operations.

American Petroleum Institute (API), 2013. API RP 780: Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries.

Argenti, F., Landucci, G., Spadoni, G., Cozzani, V., 2015. The assessment of the attractiveness of process facilities to terrorist attacks. Saf. Sci. https://doi.org/10.1016/j.ssci.2015.02.013.

Ayyildiz, E., Erdogan, M., 2024. A comprehensive approach to evaluate risk mitigation strategies in offshore wind farms using spherical fuzzy decision making analysis. Ocean Eng. 311, 118881. https://doi.org/10.1016/j.oceaneng.2024.118881.

Bajpai, S., Gupta, J.P., 2007. Securing oil and gas infrastructure. J. Pet. Sci. Eng. 55, 174–186. https://doi.org/10.1016/j.petrol.2006.04.007.

Benden, P., Feng, A., Owell, C., Dalla Riva, G.V., 2021. Crime at sea: a global database of maritime pirate attacks (1993–2020). J. Open Humanit. Data 7, 19. https://doi.org/10.5334/johd.39.

Bozeman, B., 2011. The 2010 BP Gulf of Mexico oil spill: implications for theory of organizational disaster. Technol. Soc. 33, 244–252. https://doi.org/10.1016/j.techsoc.2011.09.006.

Center for Chemical Process Safety (CCPS), 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites.

Chaparro, L., 2022. Pirates Are Holding Up Mexico's Oil Rigs at Gunpoint [WWW Document]. URL ⟨https://www.vice.com/en/article/dy78y7/gulf-of-mexico-pirates-pemex-oil-rig⟩ (accessed 1.3.24).

Chen, X., Ma, X., Jia, L., Zhang, Z., Chen, F., Wang, R., 2024. Causative analysis of freight railway accident in specific scenes using a data-driven Bayesian network. Reliab Eng. Syst. Saf. 243. https://doi.org/10.1016/j.ress.2023.109781.

Cordner, L., 2011. Managing regional risk: Offshore oil and gas safety and security in the Asia-Pacific region. Aust. J. Marit. Ocean Aff. 3, 15–24.

Darbra, R.M., Palacios, A., Casal, J., 2010. Domino effect in chemical accidents: Main features and accident sequences. J. Hazard Mater. 183, 565–573. https://doi.org/10.1016/j.jhazmat.2010.07.061.

Daxecker, U.E., Prins, B.C., 2015. Searching for sanctuary: Government power and the location of maritime piracy. Int. Interact. 41, 699–717. https://doi.org/10.1080/03050629.2015.1016159.

Dechema, 2022. ProcessNET - Incident Database [WWW Document]. URL ⟨https://processnet.org/en/⟩ (accessed 12.15.23).

Ding, X., Wang, H., Zhang, X., Ma, C., Zhang, H.F., 2024. Dual nature of cyber–physical power systems and the mitigation strategies. Reliab Eng. Syst. Saf. 244. https://doi.org/10.1016/j.ress.2024.109958.

DNV GL Digital Solutions, 2015. The Worldwide Offshore Accident Databank (WOAD).

Domínguez, N.G., 2022. Frustran petroleros ataque pirata con chorros de agua [WWW Document]. URL ⟨https://www.milenio.com/estados/frustran-petroleros-ataque-pirata-chorros-agua⟩ (accessed 1.3.24).

El-Kady, A.H., Halim, S., El-Halwagi, M.M., Khan, F., 2023. Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Saf. Environ. Prot. 173, 384–413. https://doi.org/10.1016/j.psep.2023.03.012.

European Parliament and Council, 2013. 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. J. Eur. Commun. L178, 66–106.

Falcon Mega Solutions, 2022. 10 Armed Pirates attacked Oil Platform in the Gulf of Mexico [WWW Document]. URL ⟨https://www.linkedin.com/pulse/10-armed-pirates-attacked-oil-platform-gulf-mexico-/⟩ (accessed 1.3.24).

Fouzi, N.F.R., Aziz, H.A., Yaakub, N., 2024. Systematic review of chemical safety and chemical security risk management approach. Process Saf. Environ. Prot. 183, 676–686. https://doi.org/10.1016/j.psep.2024.01.035.

Hanson, S., 2007. MEND: The Niger Delta's Umbrella Militant Group [WWW Document]. Counc. Foreign Relat. ⟨https://web.archive.org/web/20090720004429/http://www.cfr.org/publication/12920/⟩ accessed 12.13.23.

Harel, A., 2012. Preventing terrorist attacks on offshore platforms: Do states have sufficient legal tools? Harvard National Security. Journal 4, 131–184.

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021c. Analysis of Cybersecurity-related Incidents in the Process Industry. Reliab Eng. Syst. Saf. 209, 107485. https://doi.org/10.1016/j.ress.2021.107485.

Iaiani, M., Tugnoli, A., Cozzani, V., 2022b. Identification of reference scenarios for security attacks to the process industry. Process Saf. Environ. Prot. 161, 334–356. https://doi.org/10.1016/j.psep.2022.03.034.

Iaiani, M., Musayev, N., Tugnoli, A., Macini, P., Cozzani, V., Mesini, E., 2021a. Analysis of security threats for offshore oil&gas operations. Chem. Eng. Trans. 86, 319–324. https://doi.org/10.3303/CET2186054.

Iaiani, M., Sorichetti, R., Tugnoli, A., Cozzani, V., 2022a. Projectile perforation models for the vulnerability assessment of atmospheric storage tanks. Process Saf. Environ. Prot. 161, 231–246. https://doi.org/10.1016/j.psep.2022.03.025.

Iaiani, M., Tugnoli, A., Cozzani, V., 2023b. Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry. Process Saf. Environ. Prot. 172, 69–82. https://doi.org/10.1016/j.psep.2023.01.078.

Iaiani, M., Tugnoli, A., Cozzani, V., 2023a. Process hazard and operability analysis of BPCS and SIS malicious manipulations by POROS 2.0. Process Saf. Environ. Prot. 176, 226–237. https://doi.org/10.1016/j.psep.2023.06.024.

Iaiani, M., Tugnoli, A., Cozzani, V., Reniers, G., Yang, M., 2023c. A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore Oil&Gas facilities. Ocean Eng. 273, 114010. https://doi.org/10.1016/J.OCEANENG.2023.114010.

Iaiani, M., Tugnoli, A., Cozzani, V., 2024a. Using Bayesian Network To Analyze Incident Datasets. In: Kolowrocki, Krzysztof, Dabrowska, Ewa (Eds.), Advances in Reliability, Safety and Security. ESREL 2024 Collection of Extended Abstracts Part 1, pp. 23–24.

Iaiani, Matteo, Sorichetti, R., Tugnoli, A., Cozzani, V., 2024b. Modelling standoff distances to prevent escalation in shooting attacks to tanks storing hazardous materials. Reliab Eng. Syst. Saf. 241, 109689. https://doi.org/10.1016/j.ress.2023.109689.

Iaiani, Matteo, Moreno, V.C., Reniers, G., Tugnoli, A., Cozzani, V., 2021b. Analysis of Events Involving the Intentional Release of Hazardous Substances from Industrial Facilities. Reliab Eng. Syst. Saf., 107593 https://doi.org/10.1016/j.ress.2021.107593.

IBM Piracy Reporting Centre, 2023. IMB raises concern on resurgence of maritime piracy and armed robbery in Gulf of Guinea in 2023 mid-year report [WWW Document]. URL ⟨https://www.icc-ccs.org/index.php/1333-imb-raises-concern-on-resurgence-of-maritime-piracy-and-armed-robbery-in-gulf-of-guinea-in-2023-mid-year-report⟩ (accessed 12.13.23).

International Association of Oil&Gas Producers, 2020. IOGP database.

International Electrotechnical Commission (IEC), 2015. IEC 62740: Root Cause Analysis (RCA).

International Electrotechnical Commission (IEC), 2021. IEC 61025: Fault Tree Analysis (FTA).

International Maritime Organization, 2023. Reports on acts of piracy and armed robbery against ships - Annual Report 2022.

International Society of Automation (ISA), International Electrotechnical Commission (IEC), 2018. ISA/IEC 62443 Series of Standards: Industrial Automation and Control Systems Security.

Jaeger, C.D., 2002. Vulnerability assessment methodology for chemical facilities (VAM-CF). Chem. Health Saf. 9, 15–19. https://doi.org/10.1016/S1074-9098(02)00389-1.

Kashubsky, M., 2011. A Chronology of attacks on and unlawful interferences with, offshore oil and gas installations, 1975 – 2010. Perspectives on. Terrorism 5, 139–167.
Kashubsky, M., Morrison, A., 2013. Security of offshore oil and gas facilities: exclusion zones and ships' routeing. Aust. J. Marit. Ocean Aff. 5, 1–10. https://doi.org/10.1080/18366503.2013.10815725.
Kong, D., Lin, Z., Li, W., He, W., 2024. Development of an improved Bayesian network method for maritime accident safety assessment based on multiscale scenario analysis theory. Reliab Eng. Syst. Saf. 251. https://doi.org/10.1016/j.ress.2024.110344.
Konstandinidou, M., Nivolianitou, Z., Kefalogianni, E., Caroni, C., 2011. In-depth analysis of the causal factors of incidents reported in the Greek petrochemical industry. Reliab Eng. Syst. Saf. 96, 1448–1455. https://doi.org/10.1016/j.ress.2011.07.010.
Kulev, N., Torres, F.S., 2022. Simulation of the impact of parameter manipulations due to cyber-attacks and severe electrical faults on Offshore Wind Farms. Ocean Eng. 260, 111936. https://doi.org/10.1016/j.oceaneng.2022.111936.
Lam, C.Y., Tai, K., 2020. Network topological approach to modeling accident causations and characteristics: analysis of railway incidents in Japan. Reliab Eng. Syst. Saf. 193, 106626. https://doi.org/10.1016/j.ress.2019.106626.
Landucci, G., Reniers, G., Cozzani, V., Salzano, E., 2015. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliab Eng. Syst. Saf. 143, 53–62. https://doi.org/10.1016/j.ress.2015.03.004.
Larsen, M.H., Lund, M.S., Bjørneseth, F.B., 2022. A model of factors influencing deck officers' cyber risk perception in offshore operations. Marit. Transp. Res. 3, 100065. https://doi.org/10.1016/j.martra.2022.100065.
Li, H., Ren, X., Yang, Z., 2023. Data-driven Bayesian network for risk analysis of global maritime accidents. Reliab Eng. Syst. Saf. 230. https://doi.org/10.1016/j.ress.2022.108938.
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. https://doi.org/10.1016/j.ress.2018.03.001.
Men, J., Chen, G., Zhou, L., Chen, P., 2022. A pareto-based multi-objective network design approach for mitigating the risk of hazardous materials transportation. Process Saf. Environ. Prot. 161, 860–875. https://doi.org/10.1016/j.psep.2022.03.048.
Meng, H., Hu, M., Kong, Z., Niu, Y., Liang, J., Nie, Z., Xing, J., 2024. Risk analysis of lithium-ion battery accidents based on physics-informed data-driven Bayesian networks. Reliab Eng. Syst. Saf. 251. https://doi.org/10.1016/j.ress.2024.110294.
Milch, V., Laumann, K., 2019. The influence of interorganizational factors on offshore incidents in the Norwegian petroleum industry: Challenges and future directions. Reliab Eng. Syst. Saf. 181, 84–96. https://doi.org/10.1016/j.ress.2018.09.002.
Moore, D.A., Fuller, B., Hazzan, M., Jones, J.W., 2007. Development of a security vulnerability assessment process for the RAMCAP chemical sector. J. Hazard Mater. 142, 689–694.
National Consortium for the study of terrorism responses to terrorism (START), 2020. Global Terrorism Database (GTD) [WWW Document]. URL ⟨https://start.umd.edu/data-tools/global-terrorism-database-gtd⟩ (accessed 11.8.23).
Office of Naval Intelligence, 2023. Worldwide Threats to Shipping Report [WWW Document]. URL ⟨https://msi.nga.mil/Piracy⟩ (accessed 10.24.23).
Offshore Engineer, 2020. Greenpeace Activists "Occupy" Oil Platform in Danish North Sea [WWW Document]. URL Greenpeace Activists "Occupy" Oil Platform in Danish North Sea (accessed 1.3.24).
Ovidi, F., van der Vlies, V., Kuipers, S., Landucci, G., 2020. HazMat transportation safety assessment: Analysis of a "Viareggio-like" incident in the Netherlands. J. Loss Prev. Process Ind. 63, 103985. https://doi.org/10.1016/j.jlp.2019.103985.
Paltrinieri, N., Reniers, G., 2017. Dynamic risk analysis for Seveso sites. J. Loss Prev. Process Ind. 49, 111–119. https://doi.org/10.1016/j.jlp.2017.03.023.
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 Anal. 32, 1404–1419. https://doi.org/10.1111/j.1539-6924.2011.01749.x.
Planas, E., Pastor, E., Casal, J., Bonilla, J.M., 2015. Analysis of the boiling liquid expanding vapor explosion (BLEVE) of a liquefied natural gas road tanker: The Zarzalico accident. J. Loss Prev. Process Ind. 34, 127–138. https://doi.org/10.1016/j.jlp.2015.01.026.
Progoulakis, I., Nikitakos, N., 2019. Risk assessment framework for the security of offshore oil and gas assets. Proc. IAME 2019 Conf. 1–25.
Ren, C., Yang, M., 2024. Risk assessment of hazmat road transportation accidents before, during, and after the accident using Bayesian network. Process Saf. Environ. Prot. https://doi.org/10.1016/j.psep.2024.08.062.
Reniers, G., Brijs, T., 2014. Major accident management in the process industry: An expert tool called CESMA for intelligent allocation of prevention investments. Process Saf. Environ. Prot. 92, 779–788. https://doi.org/10.1016/j.psep.2014.02.003.
Reniers, G., Khakzad, N., Van Gelder, P., 2018. Security Risk Assessment in the Chemical and Process Industry.
Safety4Sea, 2021. Pirates attack oil platform in the Gulf of Mexico [WWW Document]. URL ⟨https://safety4sea.com/pirates-attack-oil-platform-in-the-gulf-of-mexico/⟩ (accessed 1.3.24).
Shallcross, D.C., 2013. Using concept maps to assess learning of safety case studies - The Piper Alpha disaster. Educ. Chem. Eng. 8, e1–e11. https://doi.org/10.1016/j.ece.2013.02.001.
Skogdalen, J.E., Vinnem, J.E., 2012. Combining precursor incidents investigations and QRA in oil and gas industry. Reliab Eng. Syst. Saf. 101, 48–58. https://doi.org/10.1016/j.ress.2011.12.009.
Stelzer, A., 2022. Piracy in the Southern Gulf of Mexico: Upcoming Piracy Cluster or Outlier? E-International Relations.
Störfall-Kommission (SFK), 2002. SFK–GS–38 - Combating Interference by Unauthorised Persons.
Sun, X., Hu, Y., Qin, Y., Zhang, Y., 2024. Risk assessment of unmanned aerial vehicle accidents based on data-driven Bayesian networks. Reliab Eng. Syst. Saf. 248. https://doi.org/10.1016/j.ress.2024.110185.
The Repository of Industrial Security Incidents (RISI) [WWW Document], 2015. URL ⟨https://www.risidata.com/Database⟩ (accessed 12.8.23).
Tukey, J.W., 1977. Exploratory Data Analysis. Addison-Wesley.
UK Health and Safety Executive, 2007a. RR567 - Accident statistics for floating offshore units on the UK Continental Shelf 1980-2005.
UK Health and Safety Executive, 2007b. RR566 - Accident statistics for fixed offshore units on the UK Continental Shelf 1980-2005.
Wang, Y., Li, Y., Yin, F., Wang, W., Sun, H., Li, J., Zhang, K., 2022. An intelligent UAV path planning optimization method for monitoring the risk of unattended offshore oil platforms. Process Saf. Environ. Prot. 160, 13–24. https://doi.org/10.1016/j.psep.2022.02.011.
Wilson, P.F., Dell, L.D., Anderson, G.F., Gaylord, F., 1993. Root Cause Analysis: A Tool for Total Quality Management. Wisconsin. ASQ Quality Press, Milwaukee.
Yuan, S., Reniers, G., Yang, M., Bai, Y., 2023. Cost-effective maintenance of safety and security barriers in the chemical process industries via genetic algorithm. Process Saf. Environ. Prot. 170, 356–371. https://doi.org/10.1016/j.psep.2022.12.008.
Zhu, C., Zhu, J., Wang, L., Mannan, M.S., 2017. Lessons learned from analyzing a VCE accident at a chemical plant. J. Loss Prev. Process Ind. 50, 397–402. https://doi.org/10.1016/j.jlp.2017.11.004.
Zhu, P., Liyanage, J.P., 2021. Cybersecurity of offshore oil and gas production assets under trending asset digitalization contexts: a specific review of issues and challenges in safety instrumented systems. Eur. J. Secur. Res. 6, 125–149. https://doi.org/10.1007/s41125-021-00076-2.