A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore Oil&Gas facilities

Iaiani, Matteo; Tugnoli, Alessandro; Cozzani, Valerio; Reniers, Genserik; Yang, Ming

DOI
10.1016/j.oceaneng.2023.114010

Publication date
2023

Document Version
Final published version

Published in
Ocean Engineering

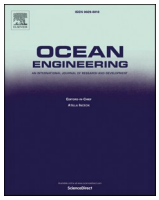
Citation (APA)
Iaiani, M., Tugnoli, A., Cozzani, V., Reniers, G., & Yang, M. (2023). A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore Oil&Gas facilities. *Ocean Engineering*, *273*, Article 114010. https://doi.org/10.1016/j.oceaneng.2023.114010

Ocean Engineering 273 (2023) 114010

Contents lists available at ScienceDirect

Ocean Engineering

journal homepage: www.elsevier.com/locate/oceaneng



A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore Oil&Gas facilities

Matteo Iaiani [a], Alessandro Tugnoli [a], Valerio Cozzani [a], Genserik Reniers [b], Ming Yang [b,*]

[a] LISES - Department of Civil, Chemical, Environmental, and Materials Engineering, Alma Mater Studiorum - University of Bologna, via Terracini n. 28, 40131, Bologna, Italy
[b] Safety and Security Science Section, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, the Netherlands

ARTICLE INFO

Handling Editor: Prof. A.I. Incecik

Keywords:
Security
Security attack
Offshore Oil&Gas industry
Bayesian network
Security risk
Quantitative assessment

ABSTRACT

Offshore Oil&Gas facilities are attractive targets of intentional malicious attacks (security attacks) that may trigger cascading events (e.g., the release and dispersion of hazardous material and/or energy, fires, explosions) with consequences on people, environment, and assets. The severity of these consequences is potentially similar to those arising from major accident scenarios originated by conventional safety-related causes. Current practice in managing the risk of security attacks mostly relies on qualitative or semi-quantitative procedures developed over the years in the offshore Oil&Gas industry. In the present study, a systematic quantitative procedure is developed, based on a Bayesian Network (BN) approach, for calculating the probability of success of physical security attacks, taking into account both preventive and mitigative security intervention strategies. The procedure addresses the specific framework of the offshore Oil&Gas industry. A case study concerning an offshore fixed Oil&Gas platform allowed us to demonstrate the quality of the results that can be achieved and their potential towards the improvement of the security of the installations considered.

1. Introduction

There is historical evidence of intentional malicious attacks (security attacks) targeting offshore Oil&Gas facilities (Iaiani et al., 2021a; Cordner, 2011; Harel, 2012) and related activities (Zhou et al., 2021; Meng et al., 2021; John et al., 2016; Zhou, 2022), carried out by a wide variety of adversaries who range from pacific protesters to hostile nation armies and terrorist organizations. Motivations of adversaries may include monetary gain, disruption of economic and political equilibria, revenge, challenge, or environmental awareness (Kashubsky, 2011; Bajpai and Gupta, 2007). In the specific case of the offshore Fluid Production sector, i.e., production of oil and/or gas from offshore wells, the adversaries may be particularly attracted by the specific company profile (e.g., multinational companies), by the socio-political location of the target installation, and/or by the severity of potential cascading events (consequence escalation) involving the gas and/or oil release triggered by the attack (Argenti et al., 2015; Chen et al., 2019; Reniers and Cozzani, 2013).

The security attacks can exploit the inherent hazard set by the presence of large quantities of hazardous materials (e.g., crude oil and natural gas processed) and cause severe impacts on humans, the environments, and the assets, which are comparable to the outcomes of major accidents originating from safety-related causes (Iaiani et al., 2021b; Vasilev, 2016; Steinhäusler et al., 2008) (e.g., the well-known accidents occurred at the Piper Alpha oil platform in 1988 (Shallcross, 2013) and at the Deepwater Horizon drilling rig in 2010 (Bozeman, 2011)). For example, in January 2006 in Nigeria, rebels attacked the Shell EA offshore oil platform and kidnapped four foreign oil workers from a support vessel anchored at the platform, causing its shutdown (Kashubsky, 2011). The adversaries also blew up crude oil pipelines, cutting supplies to the Forcados offshore export terminal.

The aforementioned events dramatically confirm that the physical security of offshore Oil&Gas facilities must be considered a major concern. According to Progoulakis and Nikitakos (2019), security of

Abbreviations: ASD, Adversary Sequence Diagram; ATT, Adversary Task Time; ATTr, Adversary Task Time remaining after the first detection; BN, Bayesian Network; CPT, Conditional Probability Table; DAG, Directed Acyclic Graph; EASI, Estimate of Adversary Sequence Interruption; ESD, Emergency Shutdown; PPS, Physical Protection System; RT, Response Time; SD, Standard Deviation; SIT, Security Intervention Time; SRA, Security Risk Assessment; SVA, Security Vulnerability Assessment.

* Corresponding author.
E-mail address: M.Yang-1@tudelft.nl (M. Yang).

https://doi.org/10.1016/j.oceaneng.2023.114010
Received 28 June 2022; Received in revised form 18 January 2023; Accepted 15 February 2023
Available online 27 February 2023

offshore Oil&Gas facilities is intended as "the process in which the operational (exploration and production) and engineering assets are actively and passively protected by stringent physical and operational measures in order to ensure resiliency and reduced degradation associated with security breaches".

Despite the panorama outlined, very few methodologies, mostly qualitative or semi-quantitative, have been developed over the years addressing physical security issues in offshore Oil&Gas facilities (Progoulakis and Nikitakos, 2019; Iaiani et al., 2022a). It is worth mentioning the two Recommended Practices (RP) specific for the offshore Oil&Gas sector that have been developed by the American Petroleum Institute, i.e., the API RP 70 ("Security for Offshore Oil and Natural Gas Operation") (American Petroleum Institute (API), 2010) and the API RP 70I ("Security for Worldwide offshore Oil and Natural Gas Operations") (American Petroleum Institute (API), 2012). These two publications are intended to assist the offshore Oil&Gas drilling and producing operators and contractors in assessing security needs during the performance of oil and natural gas operations, by providing guidelines and a semi-quantitative procedure that falls under the so-called Security Vulnerability/Risk Assessment (SVA/SRA) methodologies. The latter allow for a qualitative or a semi-quantitative assessment of the security risk through the characterization of the target facility, threat agents, attack modes, system vulnerabilities, and security countermeasures in order to support the impacts estimation of potential security attacks (Matteini et al., 2019). However, as the credibility of the security attacks increases, the assessment of security risks shall be dealt with more systematic approaches at a quantitative level in order to provide a metric of the existing vulnerability and of the available level of protection (Landucci and Reniers, 2019).

Over the years, Bayesian Networks have been increasingly adopted in the field of critical infrastructure security due to their ability to predict the probability of unknown variables or to update the probability of known variables (Khakzad et al., 2011; Charniak, 1991; Scutari and Denis, 2021). For example, Landucci et al. (2017) developed a probabilistic risk analysis approach supported by a BN model in order to assess the probability of attack success, taking into account also the attractiveness of the site. However, the method is intended for application in the Chemical and Process Industry (CPI) only, and it is path-independent, i.e., it is based on the simplifying assumption that the same set of elements of the Physical Protection System (PPS) is present along each potential attack path. Similarly, Argenti et al. (2018) developed a BN-based quantitative approach for the evaluation of the vulnerability of industrial facilities against security attacks, allowing for the evaluation of the conditional probability of having a specific damage given an attack attempt. The method takes into account only a single preventive security intervention strategy (i.e., the intervention of the security personnel), and it is specifically dedicated to CPI facilities. Moreover, the method does not provide guidelines for the construction of the case-specific BN. A further example is the quantitative security risk analysis methodology based on the SRA proposed by API RP 780 (American Petroleum Institute (API), 2013) developed by van Staalduinen et al. (van Staalduinen et al., 2017) in which a Bow-Tie model mapped into a Bayesian Network allows the calculation of the conditional probability of having a successful attack leading to a specific loss. However, the likelihood of having an attack attempt is calculated with a non-probabilistic approach and eventually combined with the other probabilities into an overall security risk value. The scope of the method is still the CPI, and the proposed procedure does not include a systematic approach for case-specific BN construction.

The present study aims to provide a systematic quantitative procedure based on the Bayesian Network (BN) approach for the calculation of the conditional probability of success of physical security attacks given the attempt. The procedure takes into account both preventive and mitigative security intervention strategies and it is intended for application in the specific context of the offshore Oil&Gas industry.

The following part of the paper is structured as follows: in Section 2, the security risk formulation is outlined. In Section 3, the proposed systematic quantitative procedure is described. In Section 4, an illustrative case study is presented and in Section 5 the discussion is reported. In Section 6 the conclusions are drawn.

2. Security risk formulation

In the process safety domain risk is usually defined as a scenario combination of consequences and associated probabilities or associated uncertainties (probability is typically interpreted as a "frequentist probability", thus as the fraction of time in which the event occurs and continuously repeats over time) (Mannan, 2012). In the security domain, risk is commonly defined by the triplet asset/value, threat, and vulnerability (Anthony and Cox, 2008) without any explicit reference to a probabilistic component. However, recently, Amundrud et al. (2017) analyzed the compatibility between safety and security risk frameworks concluding that also security risk may be defined by events-consequences and uncertainties as in the case of safety risk. Moreover, Kriaa et al. (2015) suggest that a suitable approach to express the uncertainties is to refer to probabilities.

Based on the aforementioned considerations, the security risk can be defined as follows (Landucci et al., 2017; American Petroleum Institute (API), 2013):

$$R^i = f\left(P_1^i, P_2^i, C^i\right) \tag{1}$$

where:

R^i: security risk of a certain scenario i; P_1^i: probability of attempted attack against an asset according to scenario i; P_2^i: conditional probability of successful execution of the attack given the attempt according to scenario i; C^i: expected consequences of the attack according to scenario i.

Quantification of P_1^i requires data, knowledge, or modeling of the motivations, intents, characteristics, capabilities, and tactics of adversaries, as well as of the socio/political context of the target facility (Baybutt, 2017). For this reason, the background requirements fall largely into the domain of intelligence analysts, sociologists, and political analysts, rather than risk analysts. Therefore, as these analyses go beyond the specificity of the industrial sector to which the analyzed facility belongs, the approaches for the evaluation of P_1^i are largely inter-disciplinary, applicable to any critical infrastructure.

Quantification of P_2^i requires the understanding of how adversaries can reach the assets they are targeting through vulnerabilities in the system being attacked (Baybutt, 2017; Einarsson and Rausand, 1998) (the Physical Protection System (PPS) in case of physical attacks, and the IT (Information Technology) – OT (Operational Technology) in case of cyber-attacks (Iaiani et al., 2021c, 2021d)). In other words, it requires identifying the potential physical attack paths and cyber-attack paths that the adversaries have to carry out to generate damage to the target. This generally requires knowledge of multiple disciplines, including process engineering, control systems engineering, physical and cyber-security, and process safety. Therefore, unlike evaluation of P_1^i, the assessment of P_2^i strictly depends on the design of the PPS and/or of that of the IT-OT network, which may vary considerably (especially the PPS) for facilities belonging to different industrial sectors (e.g., offshore Oil&Gas platform are surrounded by water, making the attack paths inherently different from the ones targeting an onshore process facility): hence, the need for industrial sector-specific approaches for the evaluation of P_2^i.

Finally, quantification of C^i requires capabilities in modelling scenarios such as releases of hazardous materials, fires, explosions, and toxic dispersions, which are typical of process safety and risk analysts.

The present study proposes a systematic quantitative procedure based on the Bayesian Network (BN) for the evaluation of P_2^i in the context of the offshore Oil&Gas industry, filling the gap in the avail-

ability of methods specific for this industrial sector. The procedure is described in Section 3 and applied to an illustrative case study in Section 4.

3. Methods and tools

3.1. Bayesian Network: overview

According to Baybutt (2017) and Nguyen et al. (2016), security risk analysis is subjected to a form of uncertainty that is not present for accidents generated by safety-related causes and is difficult to address, namely, the behavior of adversaries. In fact, while the consequences of a security attack (e.g., terrorist attack or act of sabotage) may be predicted with some accuracy, the attack itself is subject to large uncertainty (Aven and Renn, 2009). The latter is defined by Aven and Renn (2009) as "the difficulty of predicting the occurrence of events and/or their consequences based on incomplete or invalid databases, possible changes of the causal chains and their context conditions, extrapolation methods when making inferences from experimental results, modeling inaccuracies, or variations in expert judgments".

Many authors agree that the Bayesian Network (BN) is a flexible tool for knowledge elicitation and reasoning under uncertainty (Misuri et al., 2019; Pearl, 1988), allowing a convenient procedure for a multitude of problems in which one wants to come to conclusions that are not warranted logically but, rather, probabilistically (Khakzad et al., 2011; Charniak, 1991). In fact, the capability for bidirectional interferences, combined with a rigorous probabilistic foundation, makes the BN modeling a suitable technique for accident analysis and more importantly, for the design and evaluation of protective measures (i.e., the security barriers in the security domain), replacing earlier ad hoc rule-based schemes (Fenton and Neil, 2019). As a matter of fact, BNs are increasingly used nowadays to construct system reliability models, risk management, and safety/security analysis based on probabilistic and uncertain knowledge (Khakzad et al., 2011). For example, Landucci and co-workers (Landucci et al., 2017; Argenti et al., 2018) and van Staalduinen and co-workers (van Staalduinen et al., 2017) adopted BN-modelling to assess the dependencies between internal and external factors affecting the detection, assessment, and neutralization of security attacks. Islam and co-workers (Islam et al., 2018) used BN-modelling to assess the reliability of human performance on maintenance activities on-board ships, developing a tool able to account for the uncertainty among the performance-affecting factors (e.g., environmental factors and operational factors) and the actions of seafarers.

Given this background, the BN modelling has been adopted in the proposed quantitative procedure to deal with the uncertainty posed by security attacks to offshore Oil&Gas facilities, as well as by the intrusion detection, assessment, and communication aspects. Moreover, the ability of BNs of being applied to forward and backward reasoning through evidence propagation along the network and probability updating, perfectly fits with the need of investigating the role of existing and new security barriers on the final probability of attack success.

BNs consist of both qualitative and quantitative parts. In particular, BNs are directed acyclic graphs (DAGs) in which the nodes represent variables, arcs signify direct dependencies (e.g., causal relationships, sequential order, etc.) between the linked nodes, and the conditional probability tables (CPTs) assigned to the nodes specify how strongly the linked nodes influence each other (Torres-Toledano and Sucar, 1998). The nodes with arcs directed from them are called parents, while the ones with arcs directed into them are called children. The nodes with no parents are also called root nodes, whereas the nodes with no children are known as leaf nodes.

Considering the conditional dependencies of variables, BN represents the joint probability distribution $P(U)$ of variables $U = \{G_1, \ldots, G_n\}$ as (Jensen and Nielsen, 2007):

$$P(U) = \prod_{i=1}^{n} P\left(G_i | Pa(G_i)\right) \tag{2}$$

where $Pa(G_i)$ is the parent set of variable G_i in the BN.

Accordingly, the probability of variable G_i is calculated as:

$$P(G_i) = \sum_{U \setminus G_i} P(U) \tag{3}$$

where the summation is taken over all the variables except G_i.

BNs take advantage of Bayes theorem to update the prior probabilities of variables given new observations, called evidence E, rendering the updated or posterior probabilities as (Jensen and Nielsen, 2007):

$$P(U|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)} \tag{4}$$

Overall, the popularity of BNs lies in the fact that they benefit from both qualitative modeling techniques (i.e., representation of dependencies within the set of variables through a network graphical structure) and quantitative modeling techniques based on the computation of CPT of every node (Khakzad et al., 2012).

3.2. Proposed quantitative procedure based on Bayesian Network

3.2.1. Overview

The quantitative procedure based on the Bayesian Network proposed in the present study (see flowchart in Fig. 2) is aimed at the calculation of the probability of successful execution of a security attack (physical) given the attack attempt (P_2), taking into account multiple security intervention strategies (both preventive and mitigative security intervention strategies). Therefore, it provides one key element for the estimation of the overall security risk of a facility (see eq. (1)) and provides useful information for the vulnerability assessment phase of SVA/SRA methodologies.

The core mechanism of the proposed procedure is that of the EASI (Estimate of Adversary Sequence Interruption) model, developed in the context of the security of nuclear power plants (see Fig. 1) (Garcia, 2007): once a physical intrusion takes place (i.e., an adversary begins his/her task), there is a timely execution of a security intervention strategy (preventive or mitigative) only in case the adversary task time remaining after the first detection that has resulted in a correct assessment and communication (ATTr), is higher than the response time (RT, defined as the sum of the time required for assessment and communication with the security intervention time (SIT), as shown in Fig. 1). The SIT is defined as the time required by the security response to intervene after communication, and it is generally the most significant contribution to the response time (assessment and communication times are often neglected). The reader is referred to (Garcia, 2007) for more details on the EASI model.

Similarly to what has been assumed in other SVA/SRA studies (see Section 2), also the present study is based on the assumption that in case of timely intervention of a preventive security strategy, the attack is assumed to be interrupted (i.e., the probability of attack neutralization is considered equal to 1).

The information to collect for the application of the proposed procedure consists in the following input data:

- the layout of the PPS of the facility analyzed (i.e., detection elements, physical barriers, and physical areas);
- SIT of each security intervention strategy available in the facility analyzed;
- quantitative data on probabilities of detection, of correct assessment of detection, and of alarm communication for the totality of detection, assessment, and communication elements present in the PPS analyzed;

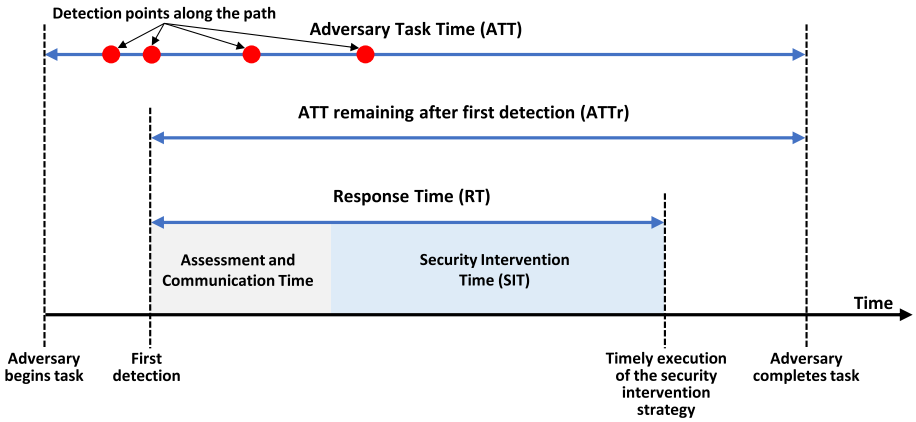


Fig. 1. *Timing model of EASI (Estimate of Adversary Sequence Interruption)* (Garcia, 2007).

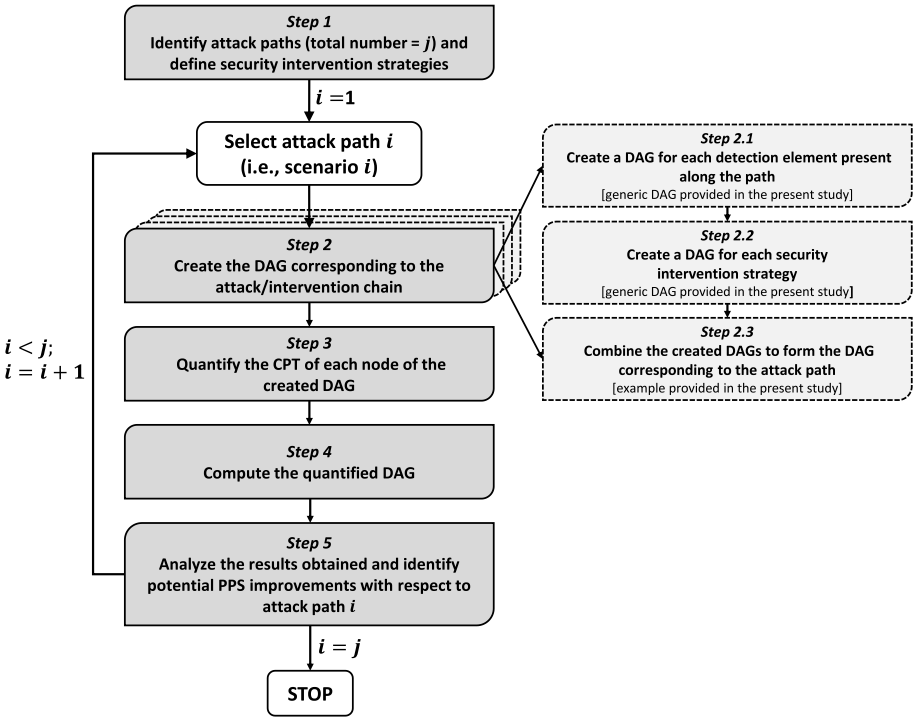


Fig. 2. Flowchart of the proposed systematic quantitative procedure based on Bayesian Network.

- quantitative data on marginal probabilities for each factor influencing the operation of the totality of detection, assessment, and communication elements present in the PPS analyzed;
- delay times for each physical barrier and physical area present in the PPS analyzed.

Overall, the proposed procedure is intended for application in the context of the offshore Oil&Gas industry and it consists in the application of 5 steps (see the flowchart shown in Fig. 2), each described in the following.

3.2.2. *Description of the proposed procedure*

Step 1 of the proposed procedure consists in the identification of the potential attack paths, i.e., the specific sequence of physical actions that the adversary has to carry out within the Physical Protection System (PPS) in order to accomplish his/her task (e.g., detonating explosives, etc.). The identification of the possible attack paths is required by both the classical SVA/SRA methodologies and the novel and more complex approaches that were recently proposed in the literature to address security issues (Iaiani et al., 2022b). In particular, the VAM-CF methodology (Jaeger, 2002), which is suitable for the Chemical and Process Industry (CPI), makes use of the Adversary Sequence Diagram (ASD) to this purpose. The suitability of the ASD in the context of the security of offshore Oil&Gas facilities was explored in a previous study of Iaiani et al. (2022a). The ASD is a tool developed in the context of the nuclear power industry (and later applied to the CPI) consisting in a graphical representation of the PPS of a facility, divided into physical areas and layers of protection between areas, allowing the systematic identification of all the possible attack paths that might be undertaken by adversaries to damage a specific target (Garcia, 2007). A generic scheme of an ASD is shown in Fig. 3. More detailed information on ASD modelling are reported in specific publications (Garcia, 2007; Jaeger, 2002) to which the reader is referred. Examples of application of the procedure concerning the identification of attack paths are provided by Garcia (2007) and Wadoud et al. (2018).

This step requires also the identification of the security intervention strategies potentially effective in preventing and/or mitigating each identified attack path among those available in the facility analyzed. A

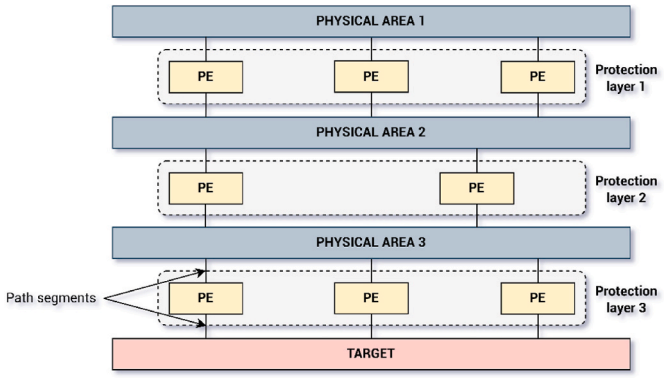


Fig. 3. *Generic scheme of an Adversary Sequence Diagram (ASD) according to* (Garcia, 2007). *PE: Path Element.*

security intervention strategy is intended as a response action aimed at delaying, interrupting an attack, and/or reducing the extent of its consequences. Examples of security intervention strategies for offshore Oil&Gas facilities include the intervention of the security force such as the Coast Guard, the activation of the abandon platform shutdown, and/or of the emergency shutdown. It is crucial to underline that a security intervention strategy may be effective against an attack path, but not for another. Therefore, they shall be tailored considering the features of each attack path.

Steps from 2 to 5 of the proposed procedure (see flowchart in Fig. 2) shall be carried out for each attack path identified in Step 1.

In particular, for a given attack path (i.e., attack path *i*), **Step 2** requires the creation of a DAG that represents all the elements of the attack/intervention chain, i.e., detection of adversaries, assessment of intrusion alarm, communication of intrusion, and intervention (Garcia, 2007). To support the systematic application of this step, it has been divided in 3 sub-steps.

The first (Step 2.1) consists in the creation, for each detection element effective in detecting the adversary performing the attack path under investigation (i.e., crossing physical areas and overcoming physical protection layers as identified from the ASD, see Fig. 3), of a DAG as the one provided in Fig. 4-a. This DAG is intended for direct application after tailoring with the specific case under assessment and it is formed by the detection node (D-node in the following), the assessment node (A-node in the following), both with or without their influencing factors (i.e., elements that influence the performance of the nodes to which they are connected), and the nodes corresponding to the timely intervention of each security intervention strategy considered effective against attack path *i*, given successful detection at the detection element under consideration (SD-node in the following).

Similarly, Step 2.2 consists in the creation, for each security intervention strategy (preventive and/or mitigative) considered effective against the attack path under consideration, of a DAG as the one provided in Fig. 4-b which is intended for direct application after tailoring with the specific case under assessment. Such DAG is formed by the communication node (C-node in the following) with or without its influencing factors, and the node corresponding to the timely intervention of the security intervention strategy under consideration (S-node in the following), given the successful detection in one or more of the detection elements along the considered path.

Finally, Step 2.3 provides for the combination of the DAGs created in

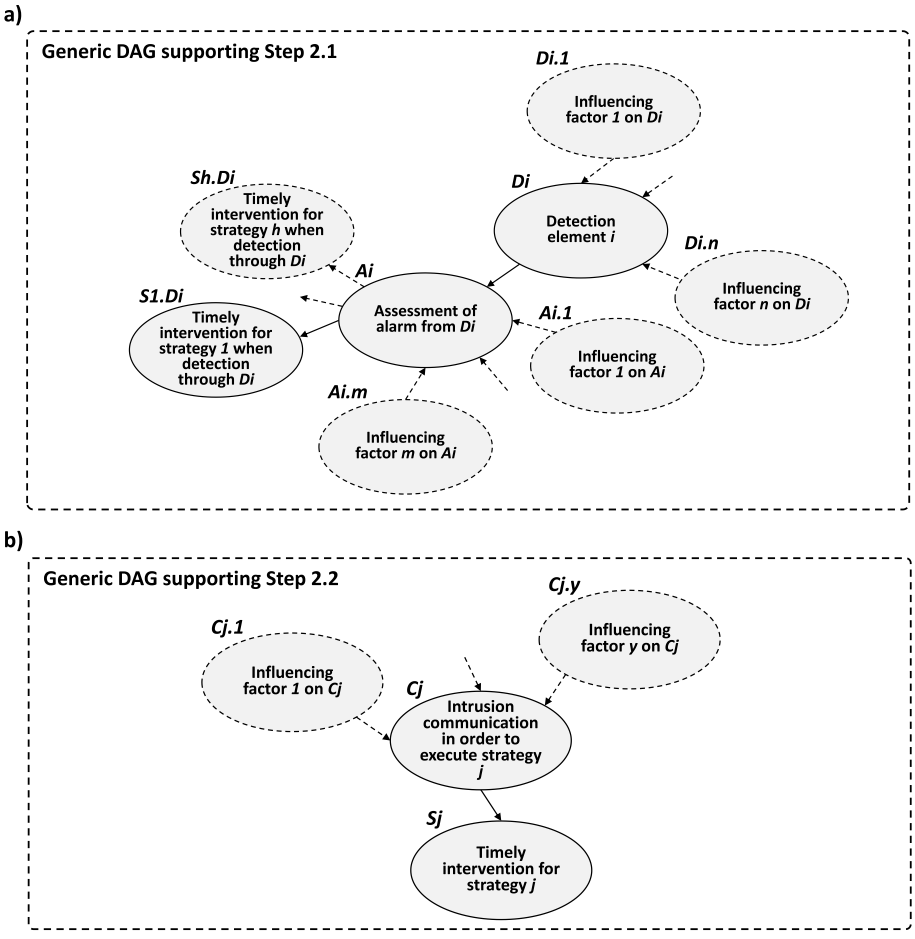


Fig. 4. Generic DAGs supporting application of Step 2.1 (Panel-a) and Step 2.2 (Panel-b) of the proposed procedure (see flowchart in Fig. 2).

the two previous sub-steps to form the required DAG for the attack path under consideration, which represents the dynamic of the attack/intervention chain. Fig. 5 reports an example of the output of this step. In particular, the figure shows a DAG which is the result of the combination of four DAGs (blue DAG refers to detection point 1, green DAG refers to detection point 2, violet DAG refers to security intervention strategy 1, yellow DAG refers to security intervention strategy 2).

To support the application of this step, the following guidelines are provided:

- The node corresponding to the outcome of the attack (AT-node in the following) shall be created (red node in Fig. 5).
- Each S-node shall be connected to the AT-node (green arcs in Fig. 5).
- Each SD-node shall be connected to its corresponding S-node (violet arcs in Fig. 5).
- Each A-node referred to a detection element shall be connected to any SD-node referred to a detection element located in a spatially subsequent point along the attack path under consideration (red arcs in Fig. 5). This is done to consider that the probability of timely intervention of a given security intervention strategy depends only on the first point along the physical path with successful detection and assessment.

Clearly, in addition to the above-required connections, case-specific dependencies may be present due to particular features of the PPS analyzed. Thus, they shall be appropriately represented with arcs within the DAG (e.g., some nodes may share the same influencing factors, blue arc in Fig. 5).

Each node created in Step 2, except for the AT node, has two states, one corresponding to the favorable condition and the other to the unfavorable condition. The AT-node has 2 states (i.e., *successful*, *not successful*) in case there are no mitigative security intervention strategies and 3 states (i.e., *successful without mitigated consequences*, *successful with mitigated consequences*, *not successful*) in case the latter are present.

Step 3 of the proposed procedure is aimed at the quantification of the CPT of each node of the DAG developed in Step 2, which means providing marginal probabilities for the root nodes and conditional probabilities for the non-root nodes. These are based on collection and analysis of massive field data or of former literature studies applicable to the case under assessment. Care must be taken in carrying out this step as the quality of the results that may be achieved by the application of the proposed procedure depends on the reliability of the input values of CPTs.

In order to support the application of this step, the following guidelines are provided:

- CPT of a D-node, A-node, C-node, and SD-node can be completed according to the following equation derived from the procedure of Argenti et al. (2018):

$$P = P_0 \prod_{h=1}^{Q} (X_h r_h) \tag{5}$$

where:

Q: number of influencing factors and variables that (independently) affect the performance of the element under assessment; P_0: baseline conditional probability representing the probability of the element under assessment successfully performing its function given that all influencing factors are in the favorable state (i.e., given that most favorable conditions to success are present); r_h: measure of the unfavorable impact on the baseline conditional probability P_0 from changing the state of the h-th influencing factor from the favorable state to the unfavorable state and assuming all other influencing factors are still in the favorable state; $X_h = 1$ if the h-th influencing factor is in its unfavorable state, while $X_h = 1/r_h$ if the h-th influencing factor is in its favorable state.

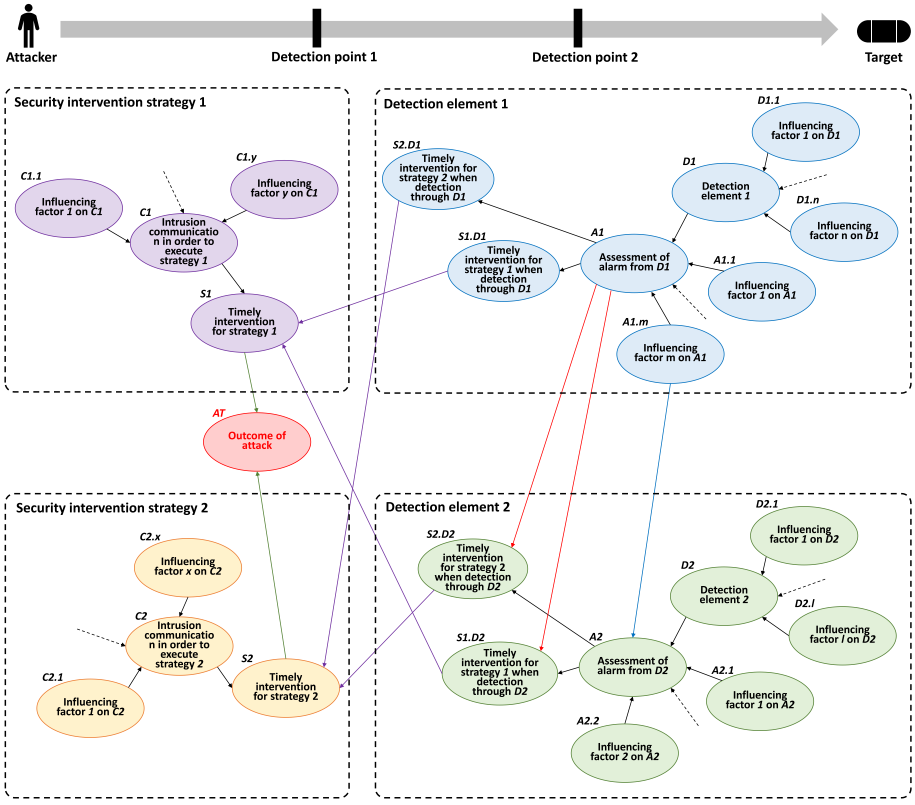


Fig. 5. Example of output of Step 2.3: combined DAG with two detection points along the attack path and two security intervention strategies potentially effective against it.

- The marginal probabilities of the influencing factors and of P_0 for a D-node, A-node, and C-node can be retrieved from experience-based judgments (expert elicitation), performance data (e.g., from field tests on the site or similar systems, real monitoring of plant operations, weather-marine conditions, vendor data, etc.), and/or from an intelligence agency. For example, Argenti et al. (2017) proposed a procedure to obtain performance estimates from expert responses to a survey, in agreement with the guidelines for expert consultation outlined by Cooke and Goossens (2000). Similarly, Yang et al. (2011) used Fuzzy Analytic Hierarchy Process (FAHP) to evaluate the weights of influencing factors with expert judgment. The use of real-time monitoring data to obtain improved statistics to be adopted within dynamic risk assessment is made by Ancione et al. (2020) and BahooToroody et al. (2020). An example of available datasets is the Copernicus Marine Environment Monitoring Service (Home CMEMS n.d, 2023), that provides free, regular, and systematic authoritative information on the state of the oceans and seas on a global and regional scale that can be used to retrieve statistics on weather-marine conditions.
- P_0 for a SD-node can be obtained according to the following equation (normal distribution for time parameters is assumed) which is at the basis of the EASI model (Garcia, 2007):

$$P_0 = \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_x^2}} exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2} \right] dx \tag{6}$$

$$x = ATTr - RT \tag{7}$$

where:

ATTr: Adversary Task Time remaining after detection in a given detection element; *RT*: Response Time referred to a given security intervention strategy.

- CPT of a S-node can be completed with 1-values when at least one SD-node is in its favorable state, with 0-values otherwise.
- CPT of the AT-node can be completed with 1-values when at least one S-node is in its favorable state, with 0 values otherwise.

In order to use the EASI model (Garcia, 2007), and thus to solve equations (6) and (7), standard deviations (SD) are required for both the security intervention times (SIT) and the delay times. This allows considering that guards and/or operators have a variable response time and that adversaries may take more or less time to cross physical areas and to penetrate physical barriers. SD values are obtained from field tests or measurements (e.g., collecting response intervention time data over several months), or from tabulated values reported in technical reports (e.g., the Hypothetical facility Exercise Handbook developed by the Hypothetical Atomic Research Institute (HARI) (Hypothetical Atomic Research Institute, 2013)). If such specific data are not available, it is suggested to use 30% of the estimated mean as SD: tests at Sandia National Laboratories have shown that the standard deviation of SITs and delay times can be conservatively estimated at 30% of the mean (Garcia, 2007).

Step 4 of the proposed procedure consists in computing the quantified DAG obtained from the previous step to calculate the probabilities of the nodes of interest, based on different evidence set in the graph. This is typically done using software for BN modelling. In particular, the software GeNIe Academic has been adopted in the present study.

Finally, **Step 5** of the proposed procedure is aimed at the analysis of the results obtained in Step 4 in terms of the vulnerability of the facility analyzed against the attack path under consideration (e.g., the identification of the elements that mostly influence the obtained probability values of the AT node). Possible PPS improvements (e.g., implementation of new countermeasures) are identified and proposed in this step.

4. Illustrative case-study

4.1. Description of the hypothetical offshore Oil&Gas platform

A hypothetical fixed offshore Oil&Gas fluid production platform anchored directly to the seabed with jacket is considered in the case study, which is aimed at illustrative purposes only. The platform (see Fig. 6) is surrounded by a protected area (radius of 500 m) where free traffic is not allowed and by a monitored area (radius of 3 km) that is the largest area to be monitored by a long-range radar located on the platform, able to detect ships and other objects over the seabed. Floating barriers (i.e., floating booms suspended between buoys equipped with a net extending above and below the seawater surface) separate the two areas with the exception of a section dedicated to the passage of authorized ships (ship portal). The shore is located at a minimum distance of 5 km from the platform. Access to the landing deck of the platform (equipped with a video motion system for intrusion detection) is guaranteed by a docking point where ships can moor, and personnel can climb up through a ladder. Stairs allow access to the other four decks: cellar deck (with filters and safety systems), main deck (with utilities, control cabinets, control room, and main equipment such as separators and wellheads), auxiliary deck (with resting rooms for personnel), and helideck for helicopter landing.

4.2. Attack paths and security intervention strategies (Step 1)

Step 1 of the proposed procedure (see Section 3.2.2) requires the identification of the possible attack paths that might be carried out by an adversary and, for each attack path, the definition of the available security intervention strategies that can prevent it, or at least mitigate its consequences. The Adversary Sequence Diagram (ASD) tool was used for this purpose as suggested in the description of the procedure. For the sake of brevity, the reader is referred to a previous study (Iaiani et al., 2022a) where attack paths for the same platform were identified using ASD tool. A single attack path is considered in the following to illustrate the application of the procedure and to demonstrate the quality of the results that can be achieved. Fig. 7-a shows the specific sequence of actions (the attack path) that the adversary has to carry out (in terms of physical areas to cross and physical barriers to overcome) as obtained from the platform-specific ASD (Iaiani et al., 2022a). In particular, the adversary leaves the shore and crosses the monitored area by boat, enters the protected area through the ship portal, moors and climbs onto the landing deck through the docking point, climbs the stairs until reaching the gas/liquid separators where 50 kg of homemade explosive (TATP) are positioned and detonated.

Fig. 7-a also reports, for each physical area and physical barrier, the detection elements that can be effective in detecting the adversary, i.e., the long-range radar, the video motion system, and the employees present on board.

According to Vasilev (2016), an attack making use of explosives is very common for all spectrum of offshore constructions (thus including offshore Oil&Gas platforms) and is able to cause massive damage and loss of life. Moreover, Landucci et al. (2015) consider the quantity of 50 kg of explosive contained inside a backpack, a credible attack scenario for a single adversary. The reader is also referred to (Iaiani et al., 2022b), where reference attack modes (including the use of explosive devices) are characterized in terms of equipment and materials carried by the adversaries and validated using past security-related incidents.

The Coast Guard, with a station located 15 km away from the platform, can intervene in case of intrusion communication in order to interrupt the attack (preventive security intervention strategy). Moreover, as for security policy, in case of intrusion communication, the platform is also forced to shutdown (mitigative security intervention strategy) providing emergency closure of the producing conduits by closing the subsurface safety valves (SSSV).

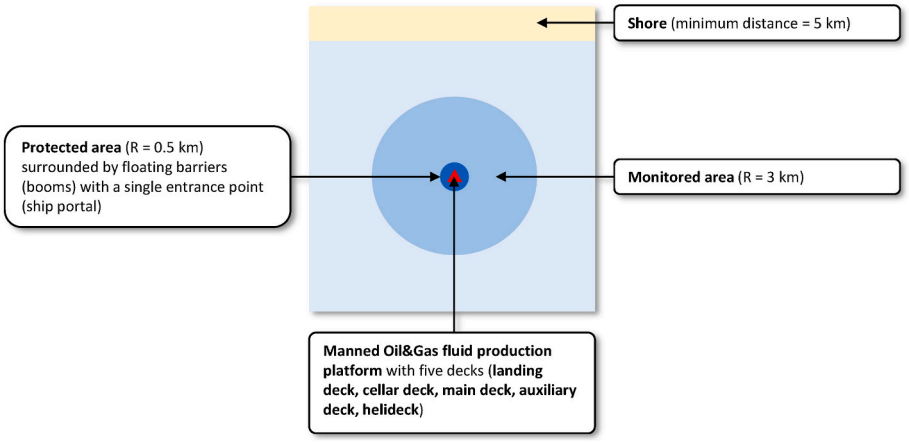


Fig. 6. The layout of the hypothetical offshore Oil&Gas fluid production platform considered in the case study.

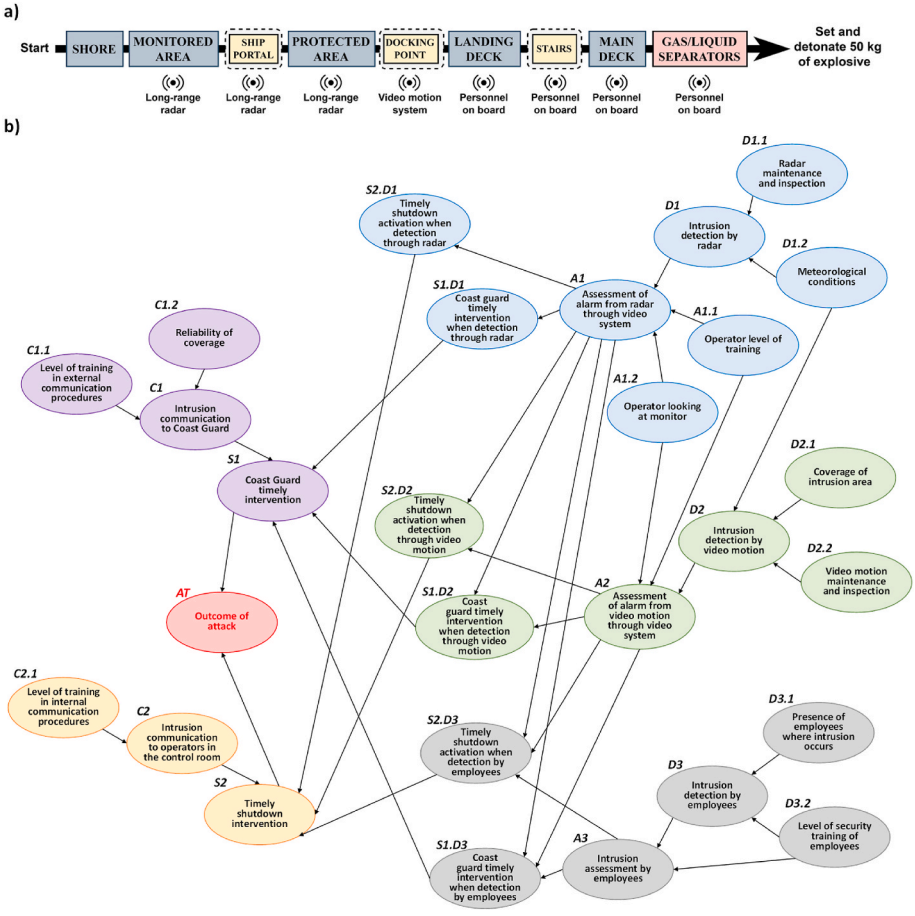


Fig. 7. (a) Attack path assessed in the case study as obtained from ASD; (b) Combined DAG obtained from the application of Step 2.

4.3. Developed DAG (Step 2) and CPT quantification (Step 3)

The combined DAG obtained from the application of Step 2 of the proposed procedure (see Section 3.2.2), corresponding to the attack path described above and the security intervention strategies potentially effective in preventing or mitigating it, is shown in Fig. 7-b.

The DAGs in blue, green, and gray colors are the ones obtained as output of Step 2.1, respectively for the long-range radar, the video motion system, and the employees on the platform, i.e., the detection elements present along the attack path considered. Similarly, the ones in violet and yellow colors are those obtained as output of Step 2.2, respectively referred to Coast Guard communication and timely intervention, and to communication to the control room operators and timely shutdown activation. Connections between the nodes have been made according to the guidelines provided in the description of Step 2 (see Section 3.2.2).

While maintenance and inspection of the radar (node D1 in Fig. 7-b) and the video motion system (node D2) have been reasonably considered independent (two separate nodes, D1.1 and D2.2), the node corresponding to meteorological conditions (node D1.2) is shared between the two detection elements, with the video motion system being also influenced by the coverage of intrusion area (node D2.1). Similarly, the

intrusion detection by employees (node D3) is influenced by the presence of employees where the intrusion occurs (node D3.1) and by the level of security training of employees (node D3.2), with the latter also influencing the intrusion assessment made by employees (node A3).

The operator level of training (node A1.1), and whether or not the operator is looking at the monitor (node A1.2) influence the assessment through the video system of the alarm from both (shared nodes) the radar and the video motion system (respectively nodes A1 and A2).

The communication to the Coast Guard (node C1) is influenced by the level of training of personnel in external communication procedures (node C1.1) and by the reliability of coverage (node C1.2). Similarly, the communication to the operators in the control room (node C2) is influenced by the level of training of personnel in internal communication procedures (node C2.1).

For the sake of clarity, the states that have been considered for each node displayed in the DAG of Fig. 7-b, are reported in Table 1.

Each CPT was filled (Step 3 of the proposed procedure) according to the equations reported in Section 3.2.2 using quantitative input data retrieved from the following sources:

- marginal probabilities for influencing factors and P_0 of D-nodes, A-nodes, and C-nodes were retrieved from Argenti et al. (2017) who provide performance data of physical security countermeasures that have been elicited from the consultation of experts, and by the Hypothetical facility Exercise Handbook (Hypothetical Atomic Research Institute, 2013);
- delay times for physical barriers in place were retrieved from the Hypothetical Facility Exercise Data Handbook (Hypothetical Atomic Research Institute, 2013);
- the typical range of speed of commercial boats was retrieved from McKenna et al. (2012);
- the typical range of speed of adversary by feet was retrieved from Wadoud et al. (2018).

The resulting CPTs are based on literature data and have illustrative purposes limited to the current case study.

According to the guidelines provided by Garcia (2007) and summarized in section 3.2.2, a standard deviation (SD) of 30% was assumed for the SIT and for the delay times of barriers for which an estimated value was not reported in the literature analyzed.

As an example, Table 2 reports the input data and the calculations that have been carried out in order to fill in the CPT of node D1 ''Intrusion detection by radar''.

4.4. Computing of the developed quantified DAG (Step 4)

The computing (Step 4 of the proposed procedure) of the quantified DAG shown in Fig. 7-b was performed using the software GeNIe Academic.

The probabilities obtained for the non-root nodes of the DAG in case no evidence was set in the network, are reported in Table 3. It is important to underline that for the considered attack path, the damage of the gas/liquid separator is deemed to be certain according to the standoff distances (i.e., the minimum distance from the asset of interest and the location where the attack takes place without causing damage) calculated by Landucci et al. (2015) for different quantities and types of improvised explosive materials (including the TATP). In fact, a damage is always possible at 0 m from an equipment (whether it is an atmospheric vessel, pressurized vessel, or a pressurized horizontal vessel) considering the detonation of 50 kg of TATP, and it can be assumed to be the one of maximum extent (worst-case scenario, i.e., instantaneous release of the entire vessel content). Therefore, for the case study, a successful attack means having a specific loss of containment (LOC) from the gas/liquid separator, and thus the obtained probabilities for the AT-node are actually a combination of P_2 and C in eq. (1).

In order to investigate the effect on the probabilities of the states of the AT-node (*Successful without mitigated consequences, Successful with mitigated consequences, Not successful*) of having a successful detection in the sea (i.e., by the long-range radar), at the docking point (i.e., by the video motion system), or on the platform (i.e., by the employees on board) with consequent correct assessment of the alarm, as well the effect of each influencing factor taken in its unfavorable state, different evidence in the DAG has been set. In particular, all these elements were investigated separately, i.e., only one evidence has been set at a time. The results of each computing, taking into consideration all the cases just mentioned, are shown in Fig. 8, whose analysis (Step 5 of the proposed procedure) is part of the discussion section.

5. Discussion

The present study proposes a systematic quantitative procedure based on the Bayesian Network (BN) for the calculation of the conditional probability of success of physical security attacks given the attempt (P_2 in eq. (1), see Section 2), taking into assessment both preventive and mitigative security intervention strategies. The procedure fills the existing gap in the availability of systematic quantitative methods able to assess the risk related to physical security issues in offshore Oil&Gas facilities, providing the reader with guidelines for the case-specific BN construction. However, given its generic nature, the proposed procedure can be customized and applied to a wider range of critical infrastructures (e.g., security of airports).

The application of the proposed procedure to the hypothetical fixed offshore Oil&Gas fluid production platform considered in the illustrative case study proved the quality of the results that can be achieved in supporting the application of the vulnerability assessment phase within SVA/SRA, providing important insights on the degree of vulnerability of the platform assessed, as well as information on the most critical weaknesses present in its Physical Protection System (PPS) thanks to the probability update feature of BNs.

In particular, with reference to Table 3, the interruption of the attack considered (i.e., reaching the platform by boat and detonating explosives planted on the gas/liquid separators located in the main deck) by the intervention of the Coast Guard turned out to be not possible (probability of the state *Attack not successful* of the AT-node is 0%). This

Table 1
List of the states adopted for each node (for node IDs refer to Fig. 7-b).

Node ID	State 1	State 2	State 3
D1, D2, D3	Detection	No detection	
D1.1, D2.2	Sufficiently frequent	Not sufficiently frequent	
D1.2	Favorable	Unfavorable	
D2.1	Complete	Partial	
A1, A2, A3	Assessed detection	No assessed detection	
A1.1, D3.2, C1.1, C2.2, C2.1	High	Low	
A1.2, D3.1	Yes	No	
S1.1, S1.2, S1.2, S2.2, S1.3, S2.3, S1, S2	Timely	Not timely	
C1, C2	Communication	No communication	
A	Successful without mitigated consequences	Successful with mitigated consequences	Not successful

Table 2
Example of data and method applied for the quantification of the CPT of node D1 (see Fig. 7-b). Numerical data were retrieved from (Argenti et al., 2017) and (Hypothetical Atomic Research Institute, 2013); the equation used is (5) (Argenti et al., 2018).

Input data for quantification of CPT of node D1				
Node ID	Node name	Variable ID	Variable	Median of elicited values
D1.1	Radar maintenance and inspection	$MP_{1.1}$ $r_{1.1}$	Marginal probability of carrying out adequate maintenance and inspection Measure of negative impact on the probability of having detection from changing the maintenance and inspection to the unfavorable state and assuming that meteorological conditions remain in a favorable state	0.875 0.2
D1.2	Meteorological conditions	$MP_{1.2}$ $r_{1.2}$	Marginal probability of meteorological conditions being favorable to detection Measure of negative impact on the probability of having detection from changing the meteorological conditions to the unfavorable state and assuming that radar maintenance and inspection remains in a favorable state	0.85 0.7
D1	Intrusion detection by radar	CP_1	Conditional probability of successful detection given radar maintenance and inspection and meteorological conditions in favorable state	0.1
Calculations for quantification of CPT of node D1				
Radar maintenance and inspection	Sufficiently frequent		Not sufficiently frequent	
Meteorological conditions	Favorable	Unfavorable	Favorable	Unfavorable
Detection	CP_1	$CP_1 \bullet r_{1.2}$	$CP_1 \bullet r_{1.1}$	$CP_1 \bullet r_{1.1} \bullet r_{1.2}$
No detection	$1- CP_1$	$1- CP_1 \bullet r_{1.2}$	$1- CP_1 \bullet r_{1.1}$	$1- CP_1 \bullet r_{1.1} \bullet r_{1.2}$
CPT of node D1 quantified				
Radar maintenance and inspection	Sufficiently frequent		Not sufficiently frequent	
Meteorological conditions	Favorable	Unfavorable	Favorable	Unfavorable
Detection	0.1	0.07	0.02	0.014
No detection	0.9	0.93	0.98	0.986

Table 3
Results of the quantitative analysis of the developed quantified DAG with no evidence set. Only probabilities of main nodes are reported (for node IDs see Fig. 5).

Node ID	States	Probability
D1	Detection	9%
	No detection	91%
A1	Assessed detection	6%
	No assessed detection	94%
D2	Detection	83%
	No detection	17%
A2	Assessed detection	59%
	No assessed detection	41%
D3	Detection	67%
	No detection	33%
A3	Assessed detection	57%
	No assessed detection	43%
C1	Communication	89%
	No communication	11%
C2	Communication	93%
	No communication	7%
S1	Timely	0%
	Not timely	100%
S2	Timely	29%
	Not timely	71%
A	Successful without mitigated consequences	71%
	Successful with mitigated consequences	29%
	Not successful	0%

is due to the much higher time required by the Coast Guard to intervene (RT of 1080 s) if compared to the total time required by the adversaries to accomplish the attack (ATT of 494 s), calculated from the first point where they can potentially be detected, i.e., from the beginning of the monitored area, even considering possible deviation from the mean values (standard deviation of 30% was assumed). Therefore, the attack path considered resulted in being very critical for the platform analyzed, making mitigation of its consequences (e.g., through platform emergency shutdown and blowdown activation) of paramount importance to reduce the extent of the outcomes in terms of damage to people, to the environment, and to the other assets (potential for man-made cascading events (Chen et al., 2019; Reniers and Cozzani, 2013)). Actually, a timely activation of the emergency shutdown system (ESD) is possible even if with a relatively low probability (around 29%, see Table 3): in fact, the much lower time required for activating the platform ESD (RT of 120 s) compared to that of Coast Guard intervention (1080 s), makes the execution of this intervention strategy more likely.

Clearly, no security intervention is possible if no detection occurs, and thus, intrusion detection plays a fundamental role in preventing and mitigating security attacks. Among the detection elements present along the attack path considered, the video motion system present in the docking point of the platform is the most effective in detecting the adversaries (success probability of 83%, see Table 3), followed by the detection by employees (success probability of 67%), and finally the long-range radar (success probability of 9%). However, the role that a detection element has on the final outcome of an attack does not depend only on its absolute probability of detection, but also on the specific point along the path where it is able to detect the adversaries: in fact, it influences the time remaining to the adversary to accomplish the attack (ATTr). For this reason, it is interesting to analyze the effect on the outcomes of the attack that each detection element and related assessment have. This was possible thanks to the probability update feature of BNs. In particular, with reference to Fig. 8, in case the adversary is detected by the radar system and the alarm is correctly assessed, there is a non-zero probability of attack interruption (around 4%), and a probability of having mitigated consequences through timely platform ESD activation, of about 89% (this means that the probability of successful attack without mitigated consequences is around 7%). Similarly, when the adversary is detected by the video motion system and the alarm is correctly assessed, the probabilities of attack interruption, attack mitigated, and attack successful without mitigation are 0%, 46%, and 54% respectively, while in the case of intrusion detection and assessment by employees these probabilities are 0%, 29%, and 71% respectively. In the case of the hypothetical platform considered in the case study, this result clearly evidences the importance of the detection of adversaries in the sea, in particular when they enter the monitored area: in fact, this leads to a very high probability of mitigation of attack consequences through the activation of the platform ESD and a non-zero probability of Coast Guard timely intervention for attack interruption. For this reason, the radar turned out to be a very important detection element in the prevention and mitigation of the attack path considered for the hypothetical

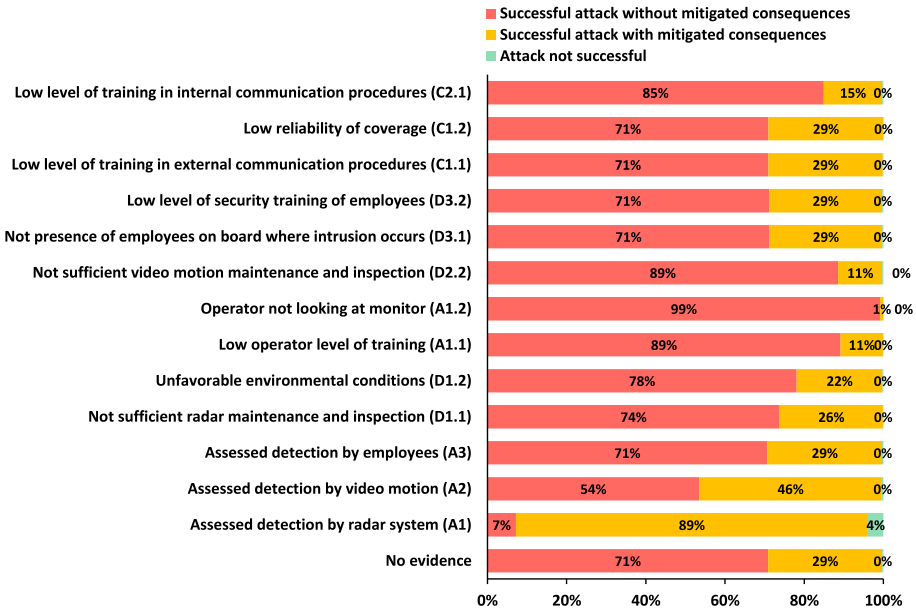


Fig. 8. Probabilities of the states of the AT-node obtained by the computing of the developed quantified DAG with different evidence set.

platform in case of successful detection. However, as already stated, the probability of detection through the radar system and that of the correct assessment of the produced intrusion alarm are around 9% and 6%, respectively (see Table 3), meaning that the chances of detection in the sea are low. Therefore, efforts and resources should be spent on the adoption of more reliable intrusion detection systems in the sea as they may deeply decrease the security risk of the platform analyzed against the attack assessed herein.

As remarked above, the detection element which mainly influences the outcome of the attack is the video motion system due to its much higher probability of detection (83%). The detection occurs in a position where the shutdown activation can still be timely. Therefore, an insufficient maintenance of the video system (i.e., the influencing factor specific of the node D2) strongly affects the probabilities calculated for the AT node (probability of unmitigated attack of 89% vs. the 71% calculated in case of no evidence set). Clearly, an operator who does not look at the monitor makes the assessment of the detection by the radar and the video motion impossible, and thus no prevention and mitigation can occur (probability of unmitigated attack of 99% vs. the 71% calculated in case of no evidence set).

On the contrary, the detection of adversaries by employees on board, despite having a relatively high probability of success (67%), turned out to be quite ineffective, as the time remaining for the adversaries to accomplish their actions when they are already on board is lower or comparable (considering a standard deviation of 30%) to the less-time-requiring shutdown activation. This is why a poor level of security training for employees, as well as the absence of employees where the intrusion occurs (i.e., the influencing factors associated to node D3 taken in their unfavorable states) do not affect the probabilities calculated for the AT-node (see Fig. 8).

Clearly, the communication of the assessed intrusion detection to the port captaincy and/or to operators in the control room is essential in order to initiate the execution of the respective security intervention strategy, i.e., the intervention of the Coast Guard and the platform shutdown activation. With reference to Fig. 8, a low level of training in internal communication procedures deeply affects the outcome of the attack as it indirectly affects the platform shutdown activation, which turned out to be the only effective security intervention strategy against the attack considered (probability of unmitigated attack of 85% vs the 71% calculated in case of no evidence set). On the contrary, a low level of training in external communication procedures and a low reliability of coverage (i.e., the influencing factors of the communication to port captaincy taken in their unfavorable state) do not influence the outcome of the attack as a timely intervention of the Coast Guard was found to be unlikely also in case of detection in the sea.

It is important to point out that despite the above discussion is specific for the results obtained from the analysis of a single security attack path (the one described in Section 3.2), they can be in part generalized for the hypothetical platform analyzed. In fact, the probability of timely intervention of the Coast Guard will be almost zero for any other type of attack that requires a shorter time to be accomplished by an adversary (e.g., an attack consisting in the shooting of gas/liquid separators from long distance, such as from the inside of the monitored area). Moreover, attacks that do not involve physical access to the platform are also critical since only the radar system (probability of detection of 9%) is potentially able to detect adversaries, making intrusion detection and security intervention extremely unlikely.

Overall, the results that can be obtained through the application of the proposed procedure support decision-makers to prioritize resources and help companies achieve continuous improvement in security performance, allowing them to identify, assess, and address vulnerabilities, prevent or mitigate security attacks, enhance training and response capabilities, and maintain and improve relationships with key stakeholders and authorities.

The quality of the results obtained by applying the proposed procedure (e.g., the probability of success of a given physical security attack scenario, the most vulnerable elements along the attack path, etc.) is limited by the reliability of the data used in the quantification of each CPT for a specific facility. Data retrieved from field test on the site or on similar systems, which are the most reliable, may be unavailable or cumbersome to obtain, especially in ex-ante studies (e.g., the design of a new facility). Use of data from the literature, as demonstrated in the case study, is however feasible in many practical cases, though a careful scrutiny is advised to assess data applicability to the specific case (e.g., the actual presence of employees in an area of interest shall be checked according to the actual manning plan of the platform). The use of Bayesian Network allows the easy update of the results once new information becomes available over time for the site (e.g., analysis of data from live monitoring of weather-marine conditions on the actual site allows improved statistics concerning this aspect).

The proposed procedure may be demanding in terms of time and resources required for its application if a large number of attack paths is

credible for the assessed facility. However, the modular nature of the steps of the procedure allows in perspective the possibility of automatization by software tools. Notably, the sub-steps from 2.1 to 2.3 may benefit from the future development of specific data libraries.

The application of the procedure is currently restricted to the scope of physical security attacks. Cyber-attacks to the IT (Information Technology) and OT (Operational Technology, e.g., BPCS – Basic Process Control System and SIS – Safety Instrumented System) of the assessed facility are not considered due to inherent differences in the attack path. Future developments may also address the analysis of multiple attack paths, including cyber-attacks, in the context of a probabilistic security vulnerability assessment of an offshore Oil&Gas facility.

6. Conclusions

A systematic quantitative procedure based on the Bayesian Network (BN) for the calculation of the probability of success of physical security attacks to offshore Oil&Gas facilities has been developed, filling the existing gap in the availability of systematic quantitative methods able to accounts for security issues in these facilities. Unlike similar methodologies intended for application in different industrial sectors, the developed procedure is able to address both preventive (e.g., response of the security force) and mitigative (e.g., emergency shutdown (ESD) activation) security intervention strategies in the assessment, and, due to its generic nature, can be customized and applied to a wider range of critical infrastructures (e.g., security of airports).

The results of the developed procedure provide valuable support to the application of vulnerability assessment phase of Security Vulnerability/Risk Assessment (SVA/SRA) methodologies, including the SVA approach proposed by API RP 70 and API RP 70I recommended practices, which is specific for the offshore Oil&Gas industry. In particular, the support to SVA/SRA concerns: (*i*) the calculation of one of the three contributions to the value of the security risk of the facility assessed; (*ii*) the identification of the most critical attack path (i.e., the one with the lowest probability of interrupted and/or mitigated attack) which determine the overall effectiveness of the Physical Protection System (PPS); (*iii*) the identification of the vulnerabilities present in the PPS that can facilitate the adversaries to accomplish their tasks; (*iv*) the definition of potential design improvements towards a more secure PPS.

The quality of the results that can be achieved through the application of the developed procedure was proved by an illustrative case study addressing a hypothetical fixed offshore Oil&Gas platform with reference to a single attack path for the sake of brevity (i.e., reaching the platform by boat and detonating explosives planted on the gas/liquid separators located in the main deck).

CRediT authorship contribution statement

Matteo Iaiani: Conceptualization, Methodology, Formal analysis, Investigation, Writing – original draft. **Alessandro Tugnoli:** Conceptualization, Methodology, Formal analysis, Supervision, Writing – review & editing. **Valerio Cozzani:** Methodology, Writing – review & editing, Validation. **Genserik Reniers:** Writing – review & editing, Validation. **Ming Yang:** Methodology, Supervision, Writing – review & editing, Validation.

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.

Data availability

Data will be made available on request.

Acknowledgments

This work was supported by MITE (Ministero della Transizione Ecologica, Itlay).

References

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.
Amundrud, Ø., Aven, T., Flage, R., 2017. How the definition of security risk can be made compatible with safety definitions, 101177/1748006X17699145 231:286–94. https://doi.org/10.1177/1748006X17699145.
Ancione, G., Paltrinieri, N., Milazzo, M.F., 2020. Integrating real-time monitoring data in risk assessment for crane related offshore operations. J. Mar. Sci. Eng. 8, 532. https://doi.org/10.3390/JMSE8070532, 2020;8:532.
Anthony, L., Cox, T., 2008. Some limitations of "risk = threat × vulnerability × consequence" for risk analysis of terrorist attacks. Risk Anal. 28, 1749–1761. https://doi.org/10.1111/J.1539-6924.2008.01142.X.
Argenti, F., Landucci, G., Spadoni, G., Cozzani, V., 2015. The assessment of the attractiveness of process facilities to terrorist attacks. Saf. Sci. 77, 169–181. https://doi.org/10.1016/j.ssci.2015.02.013.
Argenti, F., Landucci, G., Cozzani, V., Reniers, G., 2017. A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. Saf. Sci. 94, 181–196. https://doi.org/10.1016/J.SSCI.2016.11.022.
Argenti, F., Landucci, G., Reniers, G., Cozzani, V., 2018. Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. Reliab. Eng. Syst. Saf. 169, 515–530. https://doi.org/10.1016/j.ress.2017.09.023.
Aven, T., Renn, O., 2009. The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism risk. Risk Anal. 29, 587–600. https://doi.org/10.1111/J.1539-6924.2008.01175.X.
BahooToroody, A., De Carlo, F., Paltrinieri, N., Tucci, M., Van Gelder, P.H.A.J.M., 2020. Bayesian regression based condition monitoring approach for effective reliability prediction of random processes in autonomous energy supply operation. Reliab. Eng. Syst. Saf. 201, 106966 https://doi.org/10.1016/J.RESS.2020.106966.
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.
Baybutt, P., 2017. Issues for security risk assessment in the process industries. J. Loss Prev. Process. Ind. 49, 509–518. https://doi.org/10.1016/J.JLP.2017.05.023.
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.
Charniak, E., 1991. Bayesian networks without tears. Artif Intell Mag 12, 50–63.
Chen, C., Reniers, G., Khakzad, N., 2019. Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: a dynamic graph approach. Reliab. Eng. Syst. Saf. 191, 106470 https://doi.org/10.1016/j.ress.2019.04.023.
Cooke, R., Goossens, L., 2000. Procedures Guide for Structured Expert Judgment. European Commission.
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.
Einarsson, S., Rausand, M., 1998 185 1998. An approach to vulnerability analysis of complex industrial systems. Risk Anal. 18, 535–546. https://doi.org/10.1023/B:RIAN.0000005928.84074.E4.
Fenton, N., Neil, M., 2019. Risk Assessment and Decision Analysis with Bayesian Networks, second ed. CRC Press/Taylor & Francis Group.
Garcia, M.L., 2007. The Design and Evolution of Physical Protection Systems, second ed. Butterworth-Heinemann.
Harel, A., 2012. Preventing terrorist attacks on offshore platforms: do states have sufficient legal tools? Harvard Natl Secur J 4, 131–184.
Home CMEMS n.d. https://marine.copernicus.eu/(accessed January 16, 2023).
Hypothetical Atomic Research Institute (HARI), 2013. Hypothetical Facility Exercise Data Handbook.
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., Casson Moreno, V., Reniers, G., Tugnoli, A., Cozzani, V., 2021b. Analysis of events involving the intentional release of hazardous substances from industrial facilities. Reliab. Eng. Syst. Saf. 212, 107593 https://doi.org/10.1016/J.RESS.2021.107593.
Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021c. Major accidents triggered by malicious manipulations of the control system in process facilities. Saf. Sci. 134, 105043 https://doi.org/10.1016/J.SSCI.2020.105043.
Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021d. Analysis of cybersecurity-related incidents in the process industry. Reliab. Eng. Syst. Saf. 209 https://doi.org/10.1016/j.ress.2021.107485.
Iaiani, M., Tugnoli, A., Macini, P., Mesini, E., Cozzani, V., 2022a. Assessing the security of offshore Oil&Gas installations using adversary sequence diagrams. Chem Eng Trans 91, 385–390. https://doi.org/10.3303/CET2291065.

Iaiani, M., Tugnoli, A., Cozzani, V., 2022b. Identification of reference scenarios for security attacks to the process industry. Process Saf. Environ. Protect. 161, 334–356. https://doi.org/10.1016/j.psep.2022.03.034.
Islam, R., Khan, F., Abbassi, R., Garaniya, V., 2018. Human error probability assessment during maintenance activities of marine systems. Saf Health Work 9, 42–52. https://doi.org/10.1016/j.shaw.2017.06.008.
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.
Jensen, F.V., Nielsen, T.D., 2007. Bayesian Networks and Decision Graphs, second ed. Springer, New York.
John, A., Yang, Z., Riahi, R., Wang, J., 2016. A risk assessment approach to improve the resilience of a seaport system using Bayesian networks. Ocean. Eng. 111, 136–147. https://doi.org/10.1016/J.OCEANENG.2015.10.048.
Kashubsky, M., 2011. A chronology of attacks on and unlawful interferences with, offshore oil and gas installations, 1975 – 2010. Perspect Terror 5, 139–167.
Khakzad, N., Khan, F., Amyotte, P., 2011. Safety analysis in process facilities: comparison of fault tree and Bayesian network approaches. Reliab. Eng. Syst. Saf. 96, 925–932. https://doi.org/10.1016/J.RESS.2011.03.012.
Khakzad, N., Khan, F., Amyotte, P., Cozzani, V., 2012. Domino effect analysis using Bayesian networks. Risk Anal. 33, 292–306. https://doi.org/10.1111/J.1539-6924.2012.01854.X.
Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. 139, 156–178. https://doi.org/10.1016/J.RESS.2015.02.008.
Landucci, G., Reniers, G., 2019. Preface to special issue on quantitative security analysis of industrial facilities. Reliab. Eng. Syst. Saf. 191, 106611 https://doi.org/10.1016/j.ress.2019.106611.
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.
Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf. Environ. Protect. 110, 102–114. https://doi.org/10.1016/j.psep.2017.06.019.
Mannan, S., 2012. Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control, fourth ed. Butterworth-Heinemann: Elsevier, UK.
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 https://doi.org/10.1016/j.ress.2018.03.001.
McKenna, M.F., Katz, S.L., Condit, C., Walbridge, S., 2012. Response of commercial ships to a voluntary speed reduction measure: are voluntary strategies adequate for mitigating ship-strike risk? Coast. Manag. 40, 634–650. https://doi.org/10.1080/08920753.2012.727749.
Meng, X., Sun, B., Zhu, D., 2021. Harbour protection: moving invasion target interception for multi-AUV based on prediction planning interception method. Ocean. Eng. 219 https://doi.org/10.1016/J.OCEANENG.2020.108268.
Misuri, A., Khakzad, N., Reniers, G., Cozzani, V., 2019. A Bayesian network methodology for optimal security management of critical infrastructures. Reliab. Eng. Syst. Saf. 191, 106112 https://doi.org/10.1016/j.ress.2018.03.028.
Nguyen, T.H., Sinha, A., Tambe, M., 2016. Conquering Adversary Behavioral Uncertainty in Security Games: an Efficient Modeling Robust Based Algorithm. AAAI Conf. Artif. Intell., Phoenix (AZ).
Pearl, J., 1988. Probabilistic Reasoning in Intelligent Systems. Morgan Kaufmann. https://doi.org/10.1016/C2009-0-27609-4.
Progoulakis, I., Nikitakos, N., 2019. Risk assessment framework for the security of offshore oil and gas assets, 2019 Conf Proc IAME 1–25.
Reniers, G., Cozzani, V., 2013. Domino Effects in the Process Industries: Modelling, Prevention and Managing. Elsevier. https://doi.org/10.1016/C2011-0-00004-2.
Scutari, M., Denis, J.-B., 2021. Bayesian Networks with Examples in R, second ed. Chapman and Hall/CRC.
Shallcross, D.C., 2013. Using concept maps to assess learning of safety case studies - the Piper Alpha disaster. Educ. Chem. Eng. 8, e1–11. https://doi.org/10.1016/j.ece.2013.02.001.
Steinhäusler, F., Furthner, P., Heidegger, W., Rydell, S., Zaitseva, L., 2008. Security risks to the oil and gas industry: terrorist capabilities. Cent Contemp Confl 7, 1–10.
Torres-Toledano, J.É.G., Sucar, L.E., 1998. Bayesian networks for reliability analysis of complex systems. Lect. Notes Comput. Sci. 1484, 195–206. https://doi.org/10.1007/3-540-49795-1_17.
van Staalduinen, M.A., Khan, F., Gadag, V., Reniers, G., 2017. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. Reliab. Eng. Syst. Saf. 157, 23–34. https://doi.org/10.1016/j.ress.2016.08.014.
Vasilev, V.S., 2016. Some specifics of reducing the IED risk in offshore security environment. Micea Cel Batran" Nav Acad Sci Bull 19, 116–127.
Wadoud, A.A., Adail, A.S., Saleh, A.A., 2018. Physical protection evaluation process for nuclear facility via sabotage scenarios. Alex. Eng. J. 57, 831–839. https://doi.org/10.1016/J.AEJ.2017.01.045.
Yang, M., Khan, F.I., Sadiq, R., 2011. Prioritization of environmental issues in offshore oil and gas operations: a hybrid approach using fuzzy inference system and fuzzy analytic hierarchy process. Process Saf. Environ. Protect. 89, 22–34. https://doi.org/10.1016/J.PSEP.2010.08.006.
Zhou, X., 2022. A comprehensive framework for assessing navigation risk and deploying maritime emergency resources in the South China Sea. Ocean. Eng. 248, 110797 https://doi.org/10.1016/J.OCEANENG.2022.110797.
Zhou, X.Y., Liu, Z.J., Wang, F.W., Wu, Z.L., 2021. A system-theoretic approach to safety and security co-analysis of autonomous ships. Ocean. Eng. 222 https://doi.org/10.1016/J.OCEANENG.2021.108569.