CHEMICAL ENGINEERING TRANSACTIONS
VOL. 99, 2023
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Sauro Pierucci, Flavio Manenti
Copyright © 2023, AIDIC Servizi S.r.l.
ISBN 978-88-95608-98-3; **ISSN** 2283-9216
DOI: 10.3303/CET2399021

Quantitative Evaluation of the Probability of Success of Deliberate Attacks in the Offshore Oil&Gas Industry

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

[a]LISES - Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum - Università di 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)
M.Yang-1@tudelft.nl

Deliberate attacks (security attacks) pose a significant threat to offshore Oil&Gas critical infrastructures as they have the potential of triggering major event scenarios with severe consequences on people, property, and the surrounding environment. The standards API RP 70 and API RP 70I address security issues in the offshore Oil&Gas sector, providing a semi-quantitative approach to evaluate the actual level of security risk. However, as the credibility of security attacks grows, security risk assessments should be approached in a more systematic and quantitative way to measure vulnerabilities and determine the level of protection available in the site. In this context, the present study introduces a systematic quantitative procedure using Bayesian Network (BN) to calculate the probability of success of physical attacks and the role of preventive and mitigative response strategies. The procedure is applied to a case study allowing to show its potential for improving security in the offshore Oil&Gas industry.

1. Introduction

The Oil&Gas industry plays a vital role in modern society, with offshore platforms and pipelines being key components of the global energy infrastructure (Speight, 2014). History proves that offshore Oil&Gas critical infrastructures may be the target of security attacks (e.g., cyberattacks, terrorist attacks, etc.) aimed at causing high-severity scenarios such as loss of containment of hazardous materials, fires, explosions, etc. (Iaiani et al., 2022b). For instance, in March 1983, Iraqi aviation carried out an air attack on an Iranian offshore platform, resulting in a two-year oil spill that released a total of 1.9 million barrels of oil into the Persian Gulf (Kashubsky, 2011).
The security of offshore Oil&Gas critical infrastructures is addressed by standards API RP 70 (“Security for Offshore Oil and Natural Gas Operation”) and the API RP 70I (“Security for Worldwide offshore Oil and Natural Gas Operations”). These two publications are aimed at helping offshore oil and gas drilling and production operators and contractors in assessing their security needs during daily operations. In fact, these standards provide guidelines and a semi-quantitative method which falls under the so-called Security Vulnerability/Risk Assessment (SVA/SRA) methodologies, that is aimed at the evaluation and management of the security risks that an Oil&Gas facility might face (Reniers et al., 2018). However, as the credibility of security attacks grows, security risk assessments should be approached in a more systematic and quantitative (probabilistic) way to measure vulnerabilities and determine the level of protection available in the site (Aven and Renn, 2009). This quantitative approach should consider not only the technical aspects of the threat but also the broader context of the organization and its environment. Moreover, it should also be flexible and adaptable, allowing organizations to respond to changes in the threat landscape and to adjust their security measures accordingly. The security risk in probabilistic terms is defined as follows (Argenti et al., 2018):

$$R^i = f(P_1^i, P_2^i, C^i) \quad (1)$$

Paper Received: 14 December 2022; Revised: 26 March 2023; Accepted: 17 April 2023
Please cite this article as: Iaiani M., Tugnoli A., Cozzani V., Reniers G., Yang M., 2023, Quantitative Evaluation of the Probability of Success of Deliberate Attacks in the Offshore Oil&gas Industry, Chemical Engineering Transactions, 99, 121-126 DOI:10.3303/CET2399021

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

In this context, the present study proposes a systematic and quantitative approach using Bayesian Network (BN) to calculate the conditional probability of success of physical security attacks given an attempt (P_2^i in eq. 1). This method allows to consider both external (e.g., environmental conditions) and internal (e.g., physical barriers) elements in the organization in the assessment, as well as preventive and mitigative response strategies. The method is applied to a case study for demonstration of the results that can be achieved as regards security improvement of an offshore Oil&Gas critical infrastructure.

2. The Bayesian Network (BN) modelling

Bayesian Networks (BNs) are directed acyclic graphs (DAG) where each node represents a variable, the connections between nodes (arcs) indicate relationships (such as causality or sequence), and the conditional probability tables (CPTs) assigned to nodes show the strength of these relationships (Charniak, 1991). Nodes with outgoing arcs are referred to as "parents" while those with incoming arcs are called "children". Nodes with no incoming connections are called "root nodes" and those with no outgoing connections are "leaf nodes".
Considering the conditional dependencies of variables, BN represents the joint probability distribution $P(U)$ of variables $U = \{G_1, \dots, G_n\}$ (Jensen and Nielsen, 2007):

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

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.

Bayesian Networks can be used for both forward and backward reasoning through the process of evidence propagation and probability updating. They utilize Bayes theorem to calculate the updated probabilities of variables (posterior probabilities) based on new observations (evidence E). In particular:

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

Many authors agree that BN is a suitable approach for knowledge elicitation and reasoning under uncertainty, that can be adopted for different problems in which one wants to come to conclusions that are not warranted logically but probabilistically (Khakzad et al., 2011).
In the present study, BN was used as baseline mathematical model in the proposed methodology (see Section 3) in order to address the uncertainty posed by physical security attacks to offshore Oil&Gas critical infrastructures and by the chain of events leading to a response intervention (i.e., detection of attackers, assessment of intrusion alarm, communication of intrusion to response force, response intervention).

3. Proposed methodology

3.1 Overview

The proposed methodology is a quantitative step-by-step procedure based on the Bayesian Network (BN) aimed at the calculation of the conditional probability of success of physical security attacks given an attempt (P_2^i in eq. 1). It is important to underline that the methodology is currently restricted to the scope of physical security due to the inherent differences between physical and cyber-attacks as regards attack paths ad system affected (Iaiani et al., 2022a) which lead to the need of dedicated approaches for the two disciplines.
The theoretical concept of the EASI (Estimate of Adversary Sequence Interruption) model is used as core-mechanism to address the attack/response interactions. In particular, according to EASI, a response strategy (preventive or mitigative) can be timely executed only when the time needed to the attacker to complete the

attack after the first successful detection, assessment and communication (named ATTr) is higher than the time required to the response strategy to be executed (named RT). Normal distribution for time parameters (i.e., ATTr and RT) is assumed in the assessment. In mathematical terms, the probability of timely intervention of a response strategy is:

$$P = \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_x^2}} exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right] dx, x = ATTr - RT \quad (5)$$

The reader is referred to (Garcia, 2007) for more details on the EASI model.
The information needed for application concerns the layout of the Physical Protection System (PPS), the RT of the available response strategies, the times required by attackers to overcome physical barriers in the PPS and to cross physical areas, probabilities of detection, of correct assessment of detection, and of alarm communication for the totality of detection / assessment / communication elements present in the PPS, and the marginal probabilities for each factor influencing operation of the totality of detection / assessment / communication elements present in the PPS.
The flowchart of the proposed methodology (5 steps) is shown in Figure 1a, which are briefly described in the following sub-section. The reader is referred to Iaiani et al. (2023) for more details on the methodology.

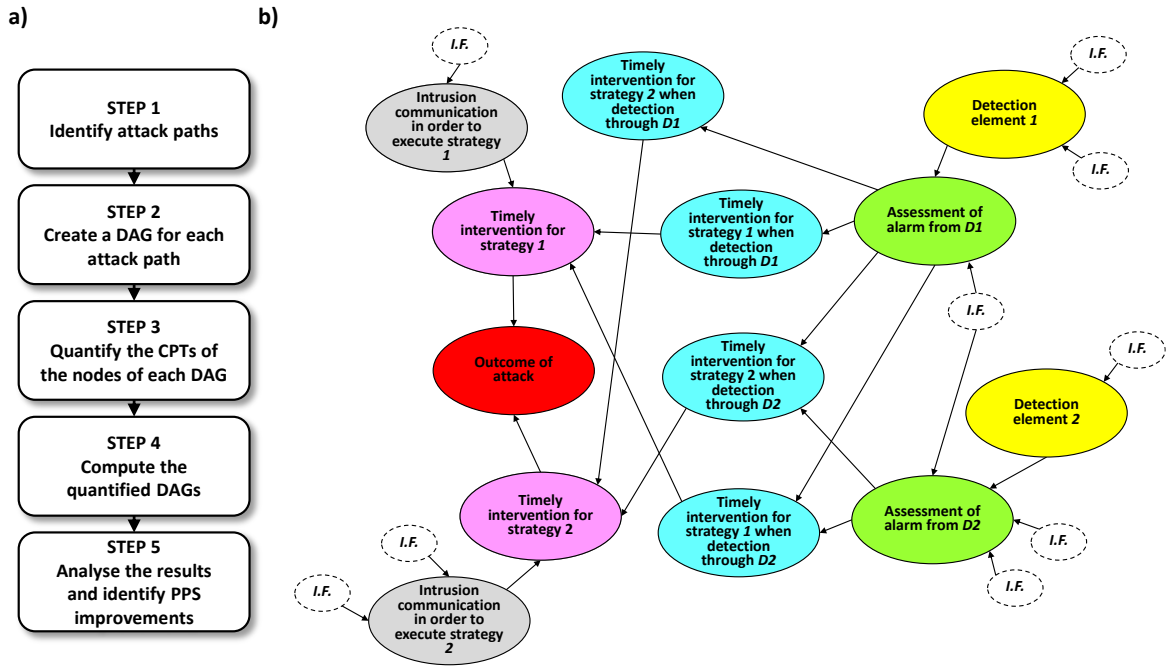

Figure 1: a) Flowchart of the proposed methodology; b) Example of generic DAG with two detection points along the attack path and two response strategies potentially effective in preventing/mitigating it. I.F.: Influencing Factor.

3.2 Description of the methodology

In Step 1 (see Figure 1a) the possible attack paths are identified. The latter are defined as the set of the specific actions that attackers have to carry out in order to accomplish their attack: these actions typically include overcoming physical barriers in the PPS, crossing physical areas, and executing the final attack (e.g., detonating explosives, setting fire, etc.) once the target asset has been reached. The Adversary Sequence Diagram (ASD) tool is suggested to this purpose. Its suitability for the offshore Oil&Gas industry has been discussed in a previous work of the authors (Iaiani et al., 2022b).

In Step 2 (see Figure 1a), the DAG corresponding to each identified attack path is created. The DAG shall display all the dependencies among detection elements along the path, assessment elements, communication elements, and the available response strategies that can be effective in preventing or mitigating the attack under assessment. Factors influencing the operations of the aforementioned elements shall be considered as well and properly connected within the network. Figure 1b shows an example of a generic DAG corresponding to an

attack path with two detection points along the path and two response strategies contrasting it. Detection nodes (in yellow) are connected to assessment nodes (in light green) which are in turn connected to the nodes corresponding to timely intervention of a response strategy (in light blue) when detection occurs in a specific detection point. All the latter nodes are connected, together with the communication node (in grey), to the one corresponding to the timely intervention of the response strategy when detection occurs in at least one detection point along the path (in violet) that are in turn connected to the node of the outcome of the attack (in red) which is the one of interest in the present study.

In Step 3 (see Figure 1a) the Conditional Probability Table (CPT) of each node in the DAG is quantified, that means to provide marginal probabilities for the root nodes and conditional probabilities for the non-root nodes. This process is based on collection and analysis of massive field data (e.g., from field tests on the site or similar sites, real monitoring of process operations, data from vendor, etc.), or of former literature studies applicable to the case under assessment. The set of equations that can be used to combine this data in order to quantify CPTs, are provided in Iaiani et al. (2023).

In Step 4 (see Figure 1a) each quantified DAG is computed. This way, based on the evidence set in the graph, the probabilities of the states of the nodes of interest are calculated. The computation is done with the aid of a BN-based software. In the present study, GeNIe Academic was used.

In Step 5 (see Figure 1a) the results are analysed and potential improvements of the PPS (e.g., possibility for additional barriers) are proposed.

4. Case study

4.1 Description of the case study

An unmanned fixed Oil&Gas fluid production platform is considered. It is surrounded by two different zones: a monitored area with a 3 km radius that is monitored using a long-range radar located on the platform and a restricted area with a 500 m radius where free traffic is prohibited. Floating barriers separate the two areas except for a designated section for authorized ship passage. The shore is located at least 5 km away from the platform. Access to the platform landing deck, which is equipped with a video motion detection system, is granted via a docking point where ships can moor and personnel can climb up. Stairs provide access to the other four decks. The Coast Guard, with a station located 8 km away from the platform, can intervene in case of intrusion communication in order to interrupt the attack (preventive security intervention strategy).

4.2 Results and discussion

For the sake of brevity, the reader is referred to a previous study of the authors (Iaiani et al., 2022b) where attack paths for the same platform were identified using ASD tool (Step 1). In the following, a single attack path is considered for illustrative purposes: attackers leave the shore by boat, cross monitored area, enter restricted area, reach the platform, access the third deck where gas/liquid separators are located, detonate 50 kg of homemade explosive.
The DAG corresponding to such attack path (Step 2) is shown in Figure 2, where detection elements (radar and video motion), assessment of intrusion alarm, communication of intrusion to Coast Guard and its intervention, and the related influencing factors (e.g., meteorological conditions, maintenance and inspection, etc.) are connected according to the guidelines reported in Section 3.2. The states of each node in the DAG are shown in Figure 3.
Quantification of each conditional probability table (CPT) of the DAG in Figure 2 (Step 3) was carried out according to the equations provided in Iaiani et al. (2023) with performance data retrieved from literature sources, such as Argenti et al. (2017) and the Hypothetical facility Exercise Handbook (Hypothetical Atomic Research Institute (HARI), 2013).
The results of the computation of the quantified DAG (Step 4), without any evidence set, are shown in Figure 3 in terms of the probability of each state. It should be noted that, based on the research conducted by Iaiani et al. (2022a), the damage of the gas/liquid separators in the considered attack path is certain. As a result, in the case study, a successful attack entails a specific loss of containment from the gas/liquid separator: thus, the probabilities for the AT-node are a combination of P_2 and C in eq. (1).
In particular, the interruption of the considered attack by the intervention of the Coast Guard resulted to be unlikely (2% chance of attack not successful, see the results of the AT node in Figure 3) even if the Coast Guard response time (RT of 540 s) is comparable to the time needed to the attackers to complete the attack (ATTr of 494 s) after detection at the beginning of the monitored area. This is because the probability of detection of the

long-range radar, i.e. the first detection point along the considered attack path, is only 9%. Much more reliable is the video motion system (probability of detection of 83%): however, if detection occurs at this point of the attack path, the ATTr is equal to 116 s, much lower than the time required to the Coast Guard to intervene, making the intervention not timely. For this reason, the attack path considered in the case study is very critical for the platform analyzed, making mitigation strategies (e.g., forcing the platform to shutdown before attackers detonate the explosives) crucial to minimize damage to people (the platform is unmanned but personnel may be present e.g. for maintenance and inspection), the environment, and assets and to prevent cascading events. Moreover, the results highlight the importance of the detection in the sea (at the beginning of the monitored area) and thus the need of more reliable long-range detection elements.

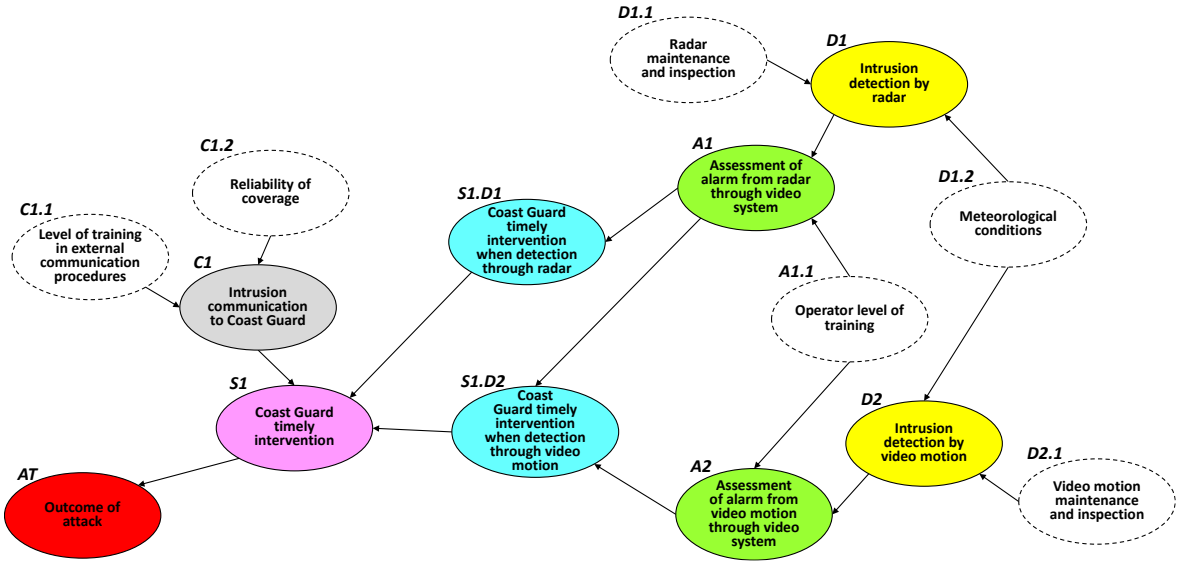

Figure 2: DAG obtained for the attack path considered in the case study.

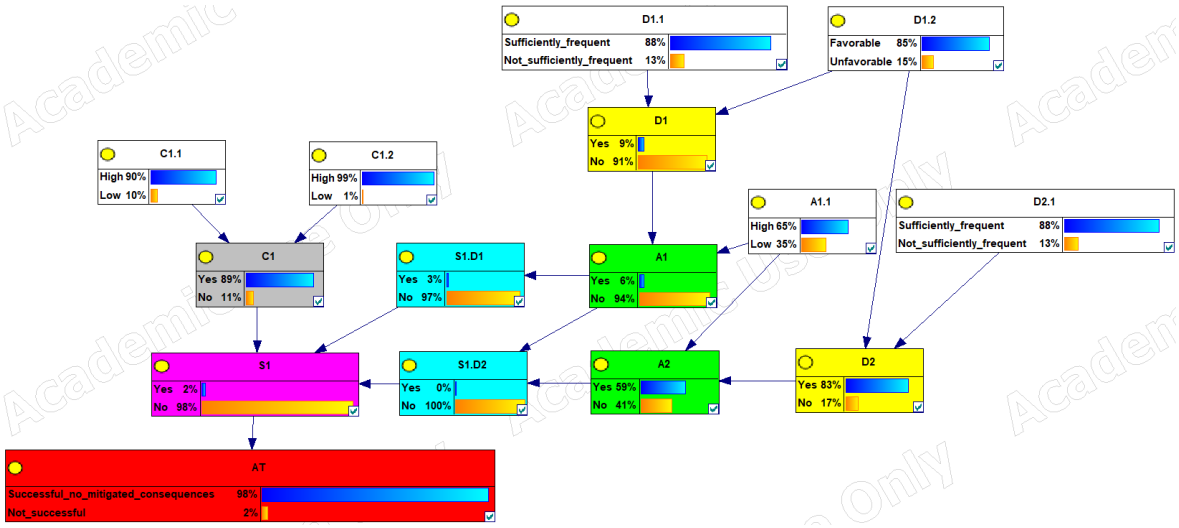

Figure 3: Results of the computation of the DAG using GeNIe Academic software.

Overall, the accuracy of results obtained using the proposed methodology in terms of the probability of success of physical security attack scenarios and the identification of the most vulnerable elements, is limited by the reliability of data used in quantifying each CPT for a specific facility. Reliable data, such as that obtained from field tests, may not always be available. However, data from literature can be used, but with caution to ensure applicability to the specific case. The use of Bayesian Network allows the easy update of the results as new

information emerges over time for a site. For instance, by analysing data from real-time monitoring of the weather-marine conditions on the site, more accurate statistics regarding this aspect can be obtained.
The proposed methodology may require significant time and resources if many attack paths are credible for the facility under analysed. However, it is modular and may be automated with software tools, overcoming this limitation. Currently, the methodology is restricted to physical security attacks and does not consider cyber-attacks (i.e., attacks to the IT – Information Technology – and OT – Operational Technology – systems). Future developments may address the analysis of multiple attack paths in the context of a probabilistic Security Vulnerability/Risk Assessment (SVA/SRA) study of an offshore Oil&Gas critical infrastructure, including cyber-attacks to their IT-OT systems.

5. Conclusions

A quantitative step-by-step methodology based on the Bayesian Network (BN) for the calculation of the conditional probability of success of security attacks to offshore Oil&Gas critical infrastructures is proposed. The attack/response interactions (i.e., the actions that attackers have to carry out to damage the target, the detection of intrusion, the assessment of intrusion alarm, the communication of intrusion, and the response intervention) are modelled using the EASI (Estimate of Adversary Sequence Interruption) mathematical framework. Unlike the majority of available approaches addressing security issues in the offshore Oil&Gas industry, the proposed methodology is able to address in the assessment both preventive and mitigative response strategies and can be customized to a wider range of critical infrastructures, including the chemical and process industry.
The application of the proposed methodology to a case study proved the quality of the outputs in providing valuable support to existing Security Vulnerability/Risk Assessment (SVA/SRA) procedures such as the one proposed by standards API RP 70 and API RP 70I which are specific for offshore Oil&Gas operations. Support concerns the calculation of the probability of success of a given attack path and the identification of the most vulnerable elements of the Physical Protection System (PPS).

References

Argenti F., Landucci G., Cozzani V., Reniers G., 2017, A study on the performance assessment of anti-terrorism physical protection systems in chemical plants, Safety Science, 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, Reliability Engineering and System Safety, 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 Analysis, 29, 587–600. https://doi.org/10.1111/J.1539-6924.2008.01175.X

Charniak E., 1991, Bayesian Networks without tears, Artificial Intelligence Magazine, 12, 50–63.

Garcia M.L., 2007, The Design and Evolution of Physical Protection Systems, 2nd ed., Butterworth-Heinemann.

Hypothetical Atomic Research Institute (HARI), 2013, Hypothetical Facility Exercise Data Handbook.

Iaiani M., Tugnoli A., Cozzani V., 2022a, Identification of reference scenarios for security attacks to the process industry, Process Safety and Environmental Protection, 161, 334–356. https://doi.org/10.1016/j.psep.2022.03.034

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, 114010. https://doi.org/10.1016/J.OCEANENG.2023.114010

Iaiani M., Tugnoli A., Macini P., Mesini E., Cozzani V., 2022b, Assessing the Security of Offshore Oil&Gas Installations using Adversary Sequence Diagrams, Chemical Engineering Transactions, 91, 385–390. https://doi.org/10.3303/CET2291065

Jensen F.V., Nielsen T.D., 2007, Bayesian networks and decision graphs, 2nd ed., Springer, New York.

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.

Khakzad N., Khan F., Amyotte P., 2011, Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches, Reliability Engineering and System Safety, 96, 925–932. https://doi.org/10.1016/J.RESS.2011.03.012

Reniers G., Khakzad N., van Gelder P., 2018, Security Risk Assessment in the Chemical and Process Industry, De Gruyter.

Speight J.G., 2014, Handbook of Offshore Oil and Gas Operations, 1st ed., Gulf Professional Publishing.