CHEMICAL ENGINEERING TRANSACTIONS
VOL. 91, 2022
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Valerio Cozzani, Bruno Fabiano, Genserik Reniers

ISBN 978-88-95608-89-1; **ISSN** 2283-9216
DOI: 10.3303/CET2291065

Assessing the Security of Offshore Oil&Gas Installations using Adversary Sequence Diagrams

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

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

Offshore Oil&Gas fluid production installations may be the target of intentional malicious acts (security attacks) carried out by adversaries of different nature and different motivations which may generate major events with severe consequences on workers, the environment and the property. The current study reviews the state of the art concerning the security of Offshore Oil&Gas operations, which is typically addressed according to best practices and qualitative or semi-quantitative methods. However, systematic approaches or guidelines in support of the analysis are still lacking. The current study investigates the possibility of using Adversary Sequence Diagrams (ASDs) as Security Vulnerability/Risk Assessment (SVA/SRA) supporting tools. A case study addressing a fixed Offshore Oil&Gas fluid production platform proved the ability of ASDs to provide credible attack modes within the Physical Protection System (PPS) that the adversaries have to perform in order to accomplish their objectives, as well as the security barriers that can potentially be effective in delaying and detecting the attacks, which are information required by SVA/SRA studies.

1. Introduction

Offshore Oil&Gas operations, and in particular the fluid production sector, i.e. production of oil and/or gas from offshore wells, may be the target of intentional malicious acts (security attacks) performed by a wide range of adversaries which may be particularly attracted by the specific company profile (e.g. the case of multinational companies) or by the socio-political location of the target installation (Argenti et al., 2015). Such adversaries span from pacific protesters promoting environmental awareness to hostile nation armies and terrorist organizations motivated by disruption of economic and political equilibria (Kashubsky, 2016). Intentional malicious acts (e.g. attacks involving incendiary or explosive devices) to Offshore Oil&Gas fluid production installations can exploit the inherent hazard set by the presence of large quantities of crude oil and natural gas that are processed every day and can cause scenarios of damage to people, environment and assets comparable to the ones of major accidents originating from safety-related causes (Harel, 2012). For example, in October 2007, a suicide boat rammed the tanker Silk Pride off the northern tip of Sri Lanka (MSI, 2021): the tanker, which was carrying a cargo of 265 tons of diesel fuel was set afire; 13 military and 12 civilians were rescued, while 3 military remained missing.
The aforementioned sporadic event and similar other security-related incidents that were collected and analyzed by Iaiani et al. (2021) in a previous work, dramatically confirm that security of Offshore Oil&Gas operations and in particular of Offshore fluid production installations must be considered as a major concern. According to Progoulakis and Nikitakos (2019), the security of such installations is intended as the process in which the operational (exploration and production) and engineering assets are actively and passively protected by physical and operational measures in order to ensure resiliency and reduce degradation associated with security breaches.
The current study reviews the state of the art concerning the security of Offshore Oil&Gas operations (Section 2) and investigates the role of Adversary Sequence diagrams (ASDs) as supporting tools for SVA/SRA assessments in Offshore Oil&Gas operations. The theoretical framework of ASDs is briefly discussed (Section 3) and a case study addressing a fixed Offshore Oil&Gas fluid production platform is used to show the potential

Paper Received: 25 January 2022; Revised: 27 March 2022; Accepted: 22 May 2022
Please cite this article as: Iaiani M., Tugnoli A., Macini P., Mesini E., Cozzani V., 2022, Assessing the Security of Offshore Oil&gas Installations Using Adversary Sequence Diagrams, Chemical Engineering Transactions, 91, 385-390 DOI:10.3303/CET2291065

use of ASDs in providing the information required in SVA/SRA assessments in Offshore Oil&Gas operations (Section 4).

2. Security management framework for Offshore Oil&Gas operations

The European and American scenarios regarding the security of Offshore Oil&Gas operations (including the Offshore Oil&Gas fluid production sector) are quite different, similarly to what happens in the safety context (Mannan, 2012). In the United States the issue is covered by three institutions: the Department of Homeland Security (DHS), the US Coast Guard (USCG), and the Department of Energy (DOE). In particular in 2002, the DHS promulgated the Maritime Transportation and Security Act of 2002, which required vessels and port facilities to conduct SVA and to develop security plans such as passenger, vehicle and baggage screening procedures, security patrols, personnel identification procedures, access control measures, etc. Later, the USCG enforced legislation requirements for security of Offshore Oil&Gas assets through the Navigation and Vessel Inspection Circular n. 03 03 (2009) and n. 05 03 (2003). Both NVICs cover the required submittal of security related documentation (plan, assessments, etc.) to ensure compliance to the Maritime Transportation and Security Act of 2002. Within the DHS, the Transportation Security Administration (TSA) is among other tasks charged with the security of transportation of hazardous materials by any mode, including water (e.g. vessels) and pipelines.

The American Petroleum Institute (API) published two Recommended Practices (RPs) specific for the Offshore Oil&Gas sector, the API RP 70 ("Security for Offshore Oil and Natural Gas Operation") (API, 2010) and the API RP 70I ("Security for Worldwide Offshore Oil and Natural Gas Operations") (API, 2012) which fall under the framework of Security Vulnerability Assessment (SVA) and Security Risk Assessment (SRA) methodologies, i.e. qualitative / semi-quantitative methods aimed at determine if existing security measures (security barriers) present in the Physical Protection System (PPS) are adequate or need improvement (Matteini et al., 2019).

In Canada, the security of Offshore Oil&Gas operations is administered by the Marine Transportation Security Act (MTSA) (1994) and its Marine Transportation Security Regulations (MTSRs) (2004), whose enforcement is guaranteed by Transport Canada (TC), the main government body authorized to regulate security at offshore facilities such as oil and gas drilling platforms. MTSRs provide a framework to detect security threats and take measures to prevent security incidents that could affect marine vessels and their facilities. The MTSRs apply Canadian and foreign-flagged vessels as well as marine facilities and port authorities and take a risk-based approach in enhancing security by ensuring that submitted marine facility and vessel security plans address risks identified within their SVA/SRA assessments (e.g. API RP 70 and API RP 70I).

The European Union (EU) covers the subject of security of Oil&Gas assets through the concept of Critical Infrastructure Protection (CIP). The EU Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, classifies Oil&Gas fluid production facilities as European Critical Infrastructure (ECI); nevertheless, it does not cover Oil&Gas exploration facilities. In addition to the aforementioned directive, the European Union published the EU Directive 2013/30/EU which focuses on the safety of Offshore Oil&Gas operations: however, despite it does not address directly security aspects, it covers the safety and environmental implications of the aftermath of an accident that may have resulted due to a security breach.

Moreover in Europe, the specific field of cybersecurity (i.e. security against cyber-attacks) is object of the NIS Directive (EU 2016/1148) which requires the development of national cybersecurity capabilities and increased EU-level cooperation in protecting essential services (Oil&Gas fluid production is included) and digital services. Particularly in Norway, the Norwegian Oil and Gas Operations Committee, the Norwegian Oil and Gas Security network, and the HSE Managers Forum, have developed the Recommended Guideline 091 (2015) with the aim of securing the oil and gas supply chain by initiating measures to prevent unauthorized materials and personnel reaching the installations. Similarly, the cybersecurity issues in Oil&Gas operations are covered by the other two Recommended Guidelines, i.e. the 104 (2009) and the 110 (2009).

Generally speaking, the best practices and methodologies for the security assessment of Oil&Gas operations cited above do not provide any practical method that can help authorities and practitioner to conduct the analysis, only occasionally some guide lists are reported. For example, despite the SVA approach proposed by API RP 70 and API RP 70I (see flowchart in Figure 1a) require the identification of all possible adversaries and attack modes (Step 1 in Figure 1a), of the physical scenarios triggered by such attacks and their consequences on people, the environment and the physical assets (Step 2 in Figure 1a), of the vulnerabilities of the PPS that can be exploited by the adversaries to perform the attacks (Step 3 in Figure 1a), and of the mitigation strategies to implement (Step 4 in Figure 1a), they do not address the methodological framework to systematically perform such assessment. Therefore in this panorama, the current study is aimed at filling the outlined gap by

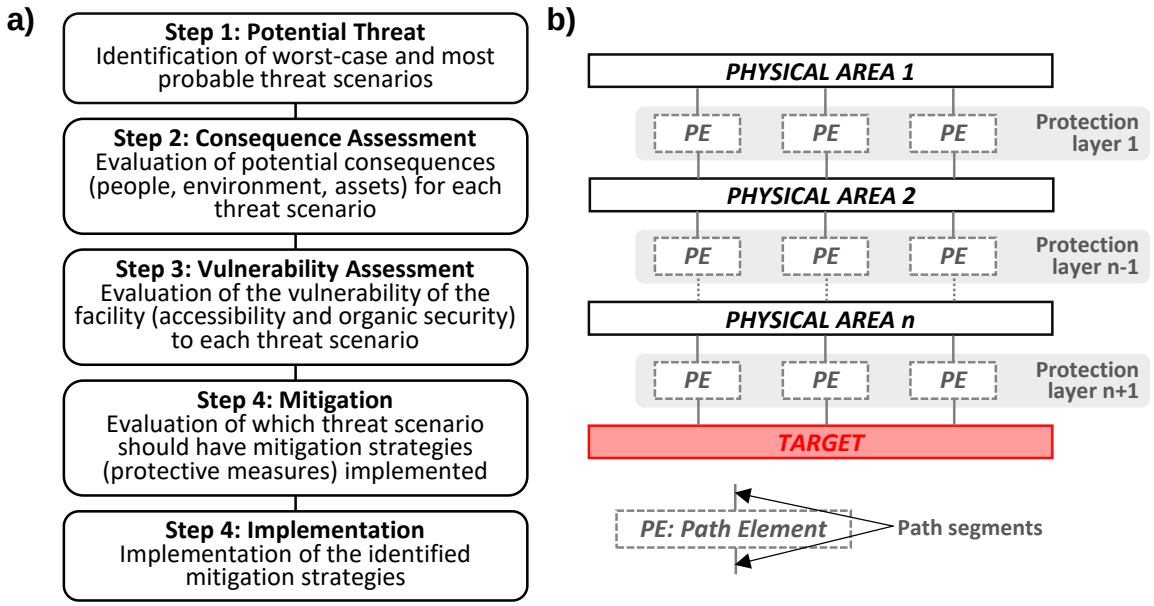

Figure 1: (a) Flowchart of SVA proposed by API RP 70 and API RP 70I; (b) ASD concept.

investigating the role of Adversary Sequence Diagrams (ASDs) in supporting available SVA/SRA studies for the assessment of Offshore Oil&Gas operations assets such as the SVA proposed by API RP 70 and API RP 70I (see Figure 1a). In fact, while the use of ASDs is well consolidated in the security assessment of nuclear power plants and of onshore chemical and process plants (e.g. see VAM-CF methodology (Jaeger, 2002)), no available studies were found in the literature addressing the use of ASDs in the assessment of Offshore Oil&Gas operations.

3. Adversary Sequence Diagram (ASD): theoretical framework

Adversaries accomplish their objective by moving along a path through a facility (an Offshore Oil&Gas fluid production facility in the current study) and defeating elements of the Physical Protection System (PPS) encountered along the path (ZOU et al., 2021). The Adversary Sequence Diagram (ASD) is a graphic representation that is used to help evaluate the effectiveness of the PPS at a facility (see the generic ASD shown in Figure 1b). It identifies the paths which adversaries can follow to accomplish sabotage or theft.

The ASD models a PPS by identifying the path elements (PEs) which compose protection layers between adjacent physical areas (see Figure 1b). Each protection layer consists of a number of path elements (see Figure 1b) which are the basic building blocks of a PPS such as personnel and vehicle gateways, emergency exits, shipping/receiving doorways, etc. Path segments (see Figure 1b) model the entries and the exits between physical areas through the PEs.

The basic concept for an ASD is shown in Figure 1b: an adversary attempts to defeat a path element in each protection layer as he/she moves along a path through the facility to the target. Clearly, in a typical facility, there are usually hundreds of alternative paths an adversary might take to reach a target, and further, each path can be traveled in many ways using force, deceit, or stealth tactics to defeat the various detection and delay components located along a path. Thus, each path consists of a specific set of adversary actions that, if accomplished, will result in the achievement of the adversary objective.

In order to create a site-specific ASD, three main steps have to be followed: i) modeling the facility by separating it into adjacent physical areas separated by a protection layer controlling movement between areas; ii) defining path elements that make up the protection layers between the adjacent areas; iii) assign probability of detection (p_D) and delay time (t_D) for each path element and each physical area.

In the current study, the possibility of modelling an Offshore Oil&Gas fluid production platform using the ASD concept shown in Figure 1b and discussed above is demonstrated through a case study (see Section 4): however, the definition of a systematic approach based on ASDs and ASD quantification with probability of detections and delay times is out of the scope and it will be part of future developments.

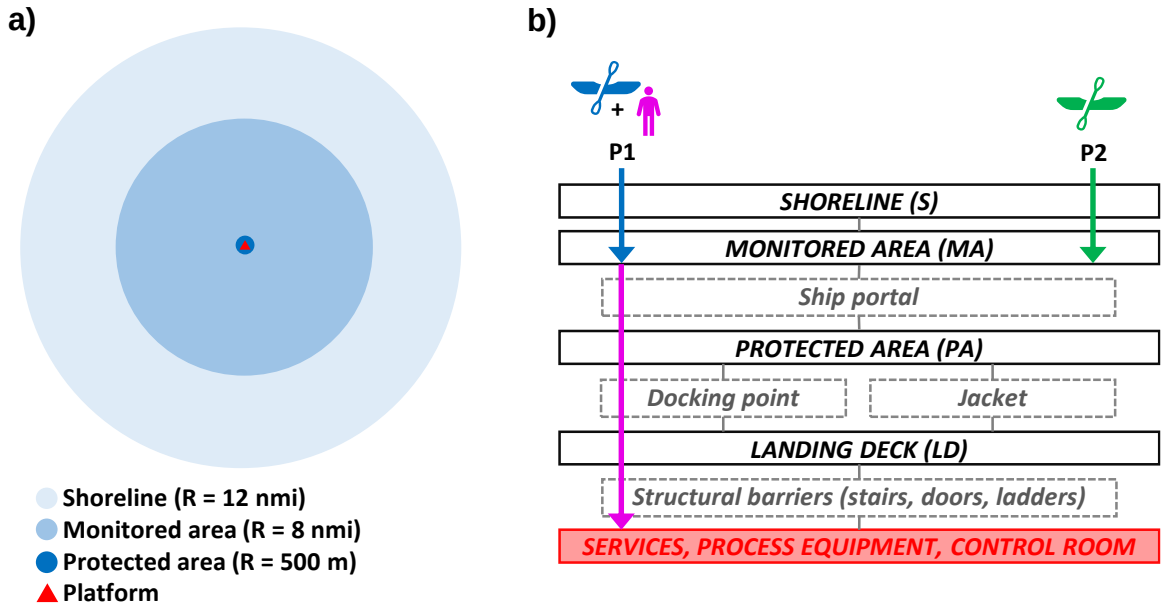

Figure 2: (a) Simplified scheme of the physical areas surrounding the platform; (b) Site-specific ASD displaying physical paths P1 and P2.

4. Case study

A fixed Offshore Oil&Gas fluid production platform anchored directly to the seabed with jacket is considered in the case study. The platform (see Figure 2a) is surrounded by a protected area (PA, radius of 500 m) where free traffic is not allowed, by a monitored area (MA, radius of 8 nmi) that is the largest area to be monitored by a long-range radar present in the platform, and finally by the shoreline (S) which extends to the coast. Access to the landing deck (LD) of the platform (equipped with a short-range closed-circuit television system, CCTV) is guaranteed by a docking point where ships can moor and personnel can move upstairs.

The site-specific ASD developed from the layout described above is shown in Figure 2b: the physical areas, the path elements, and the target (i.e. services, process equipment and the control room in the platform) are linked according to the ASD concept shown in Figure 1b and discussed in Section 3: as already stated, no quantification of the ASD components is provided as it is out of the scope of the current study.

The analysis of the ASD allowed to identify two main paths (called P1 and P2) that can be followed by an adversary in order to damage the target located at the platform, all shown using colored segments in Figure 2b and all described in Table 1 which also reports the security barriers which are effective in delaying (DE) and/or detecting (DT) the adversaries for each path.

In particular, given the great distance from the coast to the location of the platform (12 nmi, i.e. about 22,2 km), each of the two identified paths is considered in part (P1) or entirely (P2) carried out by the use of boat.

In path P1 (see Table 1 and Figure 2b) an adversary is expected to reach the protected area by boat and then to continue swimming until he/she reaches the landing deck of the platform: there, once arrived at the target location, he/she carries out the actual attack. The latter may consist in the detonation of explosive devices (e.g. Ammonium Nitrate (AN) – Fuel Oil (ANFO) mixtures or Triacetone Triperoxide Peroxyacetone (TATP)) or in deliberate interferences without the use of tools (e.g. closing/opening of manual valves) or using them (e.g. ramming equipment and/or instrumentation). The duration of the path in water depends on the boat speed (from the coast to the protected area) and on the adversary ability to swim (from protected area to the landing deck), while the duration of the path on the platform depends on the location of the target (inside a closed area such as the control room, or outside; platform level to be reached, etc.) and on the type of attack. Adversary detection is given in water by the long-range radar system (up to the monitored area, see Figure 2a), and on the platform by the Closed-Circuit Television system (CCTV), also known as video surveillance, and by operators at work that may notice something abnormal.

Table 1: Description of paths P1 and P2 identified from the ASD shown in Figure 2b.

Path	Sequence of actions	Detection (DT) elements	Delay (DE) elements
P1	*A.1* Adversary crosses shoreline (S) by boat	None	Distance from coast to MA
	A.2 Adversary crosses monitored area (MA) by boat	Long-range radar located on platform	Distance from MA to PA
	A.3 Adversary crosses protected area (PA) by swimming and reaches the platform	Long-range radar located on platform	Distance from PA to platform
	A.4 Adversary climbs onto the landing deck (LD) through the docking point	Short-range CCTV system on platform	Docking point on LD
	A.5 Adversary reaches the target on platform and performs the attack (detonation of explosive device, deliberate interference with or without the use of tools)	Short-range CCTV system on platform, operators at work	Structural elements (ladders, stairs, doors), time required to plant an explosive device or to open/close manual valves.
P2	*A.1* Adversary crosses shoreline (S) by boat	None	Distance from coast to MA
	A.2 Adversary crosses monitored area (MA) by boat and performs the attack (detonation of large quantity of explosive material present on boat – WBIED)	Long-range radar located on platform	Distance from MA to PA, time required to reach a safe-zone (in case of non-suicide attack)

In path P2 (see Table 1 and Figure 2b) an adversary is expected to reach the protected area by boat and then to perform the attack which consists in the detonation of a large amount of explosive material (e.g. ANFO mixtures or TATP) contained inside the boat (Water-Borne Improvised Explosive Device – WBIED), sufficient to generate an overpressure capable of damaging the platform. Therefore, the long-range radar is the only detection element present along the path (CCTV is ineffective since attackers do not access the platform), while as for path P1, delay is due to the distance that adversaries have to cover in water (from the coast to the protected area) with additional delay time in case the boat is not driven remotely and the attack is not suicidal (in this case the attackers must reach a safe zone before detonation). Generally speaking, the prevention from this type of attack is very challenging since WBIED have to be destroyed or diverted over very long distances, making P2 a very critical path.

Overall, the site-specific ASD that was developed for the Offshore Oil&Gas fluid production platform considered in the case study (see Figure 2) has been proven to be a very useful and practical tool to easily identify and model a credible set of attack modes and the corresponding sequences of actions within the PPS that the adversaries have to perform in order to accomplish their objectives (i.e. the identified physical paths), as well as to identify the security barriers that can potentially be effective in delaying and detecting the adversaries. For this reason, given the discussion in Section 2, this information can support Step 1 (“Potential Threat”) and Step 3 (“Vulnerability Assessment) of the SVA approach proposed by API RP 70 and API RP 70I (see Figure 1a). Therefore, the results obtained in the current study pave the way for future developments that will be devoted to the definition of a systematic quantitative ASD-based approach to be integrated in SVA/SRA studies of Offshore Oil&Gas fluid production facilities in order to practically support the application of such assessments as regards the characterization of the attacks, the evaluation of effectiveness of security barriers, and the estimation of the probability of success of an attack. However, it is important to underline that given the different core mechanism of cyber-attacks (strongly dependent on the design of the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS)) compared to the one of physical attacks, ASDs are not deemed to be perfectly suitable for the identification of the cyber-related paths and thus cyber-attacks will be not addressed in future developments concerning ASDs. Dedicated approaches for cyber-risk and path identification can be found in Iaiani et al. (2021b) and Iaiani et al. (2021c).

5. Conclusions

The current study reviews the state of the art concerning the security of Offshore Oil&Gas operations showing important differences between the American and the European scenarios. Generally, security of Offshore Oil&Gas installations is addressed by best practices and qualitative / semi-quantitative methodologies (e.g. Security Vulnerability Assessment (SVA) or Security Risk Assessment (SRA) methodologies) which do not provide any systematic approach or guideline in support of the analysis.
In order to fill this gap, the role of Adversary Sequence Diagrams (ASDs) as supporting tools for SVA/SRA studies was investigated. A case study addressing a fixed Offshore Oil&Gas fluid production platform allowed to demonstrate the quality of ASDs in providing information required by the SVA approach proposed by API RP 70 and API RP 70I (which are specific for Offshore Oil&Gas operations). This information concerns the identification of a set of reliable attack modes, of the corresponding sequences of actions that the adversaries have to perform within the Physical Protection System (PPS) in order to accomplish such attacks, and of the security barriers which are potentially effective in delaying and detecting the attacks. Thus, an ASD-based approach is believed to help authorities and practitioners in conducting a SVA/SRA of Offshore Oil&Gas installations. For this reason, the current study paves the way for future development of systematic approaches based on quantified ASDs to be integrated in SVA/SRA studies of Offshore Oil&Gas fluid production facilities (e.g. SVA method proposed by API RP 70 and API RP 70I) in order to practically support the application of such assessments as regards the characterization of the attacks, the evaluation of the effectiveness of security barriers, and the estimation of the probability of success of an attack.

Acknowledgments

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

References

American Petroleum Institute (API), 2012, API RP 70I - Security for Worldwide Offshore Oil and Natural Gas Operations.
American Petroleum Institute (API), 2010, API RP 70 - Security for Offshore Oil and Natural Gas Operations.
Argenti F., Landucci G., Spadoni G., Cozzani V., 2015, The assessment of the attractiveness of process facilities to terrorist attacks, Safety Science, 77, 169–181.
Garcia M.L., 2007, The Design and Evaluation of Physical Protection systems, 2nd ed, UK: Butterworth–Heinemann.
Harel A., 2012, Preventing terrorist attacks on offshore platforms: Do states have sufficient legal tools?, Harvard National Security Journal, 4, 131–184.
Iaiani M., Musayev N., Tugnoli A., Macini P., Cozzani V., Mesini E., 2021a, Analysis of Security Threats for Offshore Oil&Gas Operations, Chemical Engineering Transactions, 86, 319–324.
Iaiani M., Tugnoli A., Bonvicini S., Cozzani V., 2021b, Major accidents triggered by malicious manipulations of the control system in process facilities, Safety Science, 134, 105043.
Iaiani M., Tugnoli A., Macini P., Cozzani V., 2021c. Outage and asset damage triggered by malicious manipulation of the control system in process plants, Reliability Engineering & System Safety, 213, 107685.
Jaeger C.D., 2002, Vulnerability assessment methodology for chemical facilities (VAM-CF), Chemical Health and Safety, 9, 15–19.
Kashubsky M., 2016, Offshore Oil and Gas Installations Security: An International Perspective - Maritime and Transport Law Library, Informa Law from Routledge.
Mannan S., 2012, Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control, 4th ed., Elsevier, UK: Butterworth-Heinemann.
Maritime Safety Information (MSI), 2021, <https://msi.nga.mil/Piracy> accessed 02.24.2021.
Matteini A., Argenti F., Salzano E., Cozzani V., 2019, A comparative analysis of security risk assessment methodologies for the chemical industry, Reliability Engineering & System Safety, 191, 106083.
Progoulakis I., Nikitakos N., 2019, Risk Assessment Framework for the Security of Offshore Oil and Gas Assets, Proc. IAME 2019 Conf., 1–25.
ZOU B., LI M., YANG M., 2021, Vulnerability learning of adversary paths in Physical Protection Systems using AMC/EASI, Progress in Nuclear Energy, 134, 103666.