CHEMICAL ENGINEERING TRANSACTIONS
VOL. 111, 2024
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Valerio Cozzani, Bruno Fabiano, Genserik Reniers

ISBN 979-12-81206-11-3; **ISSN** 2283-9216
DOI: 10.3303/CET24111089

Security Management of Offshore Oil&Gas Installations: the Italian Experience

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

LISES – Department of Civil, Chemical, Environmental, and Materials Engineering, Alma Mater Studiorum – University of Bologna, via Terracini n.28, 40131 Bologna (Italy)
paolo.macini@unibo.it

Offshore Oil&Gas installations face unique security challenges due to their remote and often vulnerable nature, as dramatically confirmed by the large number of past incidents occurred worldwide in the offshore sector. This paper delves into the security management of these installations, with the specific focus on the Italian context. It explores the strategies implemented by Italian authorities and industry stakeholders to address security challenges in the offshore sector, pointing out the regulatory framework and industry standards. Additionally, the paper discusses methodologies for conducting a security risk assessment in offshore Oil&Gas facilities and identifies best practices for the adoption of security measures to enhance security resilience in this sector. By leveraging the Italian experience, this paper aims at providing insights and practical recommendations regarding the security management of offshore operations.

1. Introduction

In today's interconnected world, security stands as a paramount concern transcending various sectors, including industrial operations, and thus the need to safeguard against potential threats has never been more pressing. This is especially true in the maritime domain, where offshore operations face unique security challenges due to their remote and often vulnerable nature (Progoulakis & Nikitakos, 2019).

The large number of security-related incidents occurred in the offshore Oil&Gas sector registered in the last decades serves as tangible evidence that warrant the security-related concern worldwide (Iaiani et al., 2021), especially these years due to ongoing conflicts (e.g., the Ukraine crisis). In Italy, and more generally in Europe, the security incidents occurred in recent years in the offshore sector only concern civil protest actions carried out by environmental activists. Even if these incidents did not result in severe consequences for people and the environment so far, their potential in causing high-profile scenarios (e.g. major accident scenarios) cannot be underestimated. In fact, in other regions worldwide, e.g. in the area of the Strait of Malacca (between Indonesia and Malaysia) and in that of the Gulf of Guinea (Nigeria), there is historical evidence of intentional malicious attacks (security attacks) to offshore installations resulting in people injuries or fatalities and/or in extensive property and environmental damages (Daxecker & Prins, 2015). An example illustrating this issue occurred in January 2006 in Nigeria, where insurgents targeted Shell's EA offshore oil platform, leading to the abduction of four foreign oil workers from a support vessel anchored at the platform and to its subsequent shutdown. The insurgents then sabotaged crude oil pipelines, disrupting supplies to the Forcados offshore export terminal for several days (Kashubsky, 2011).

In this context, the present contribution presents the Italian panorama concerning the security management practices for offshore installations. Starting from a comprehensive analysis of the regulatory framework and of industry standards, the paper examines key strategies and measures implemented by the Italian authorities and industry stakeholders to address security challenges in offshore operations. Furthermore, the paper explores existing approaches for conducting security risk assessments in offshore environments, including threat analysis, vulnerability assessments, consequence analysis, and risk mitigation strategies. Best practices for the adoption of security barriers will also be discussed, drawing from both regional and international experiences to offer valuable insights for enhancing security resilience in offshore operations.

The insights provided in this paper contribute to a more comprehensive framework on security management practices in offshore operations, offering valuable lessons and best practices drawn from the Italian experience.

Paper Received: 23 February 2024; Revised: 30 May 2024; Accepted: 15 June 2024
Please cite this article as: Iaiani M., Macini P., Tugnoli A., Cozzani V., Mesini E., 2024, Security Management of Offshore Oil&gas Installations: the Italian Experience, Chemical Engineering Transactions, 111, 529-534 DOI:10.3303/CET24111089

2. The EU and Italian regulatory frameworks

One of the key international bodies contributing to the enhancement of maritime security, including within the scope of the European Union's regulatory framework, is the International Maritime Organization (IMO) established in 1948. While the EU has implemented regulations and directives to bolster maritime security in response to various threats such as terrorism and piracy, the IMO serves as a global authority in setting standards and regulations for safe, secure, and environmentally responsible shipping operations. Through its conventions, codes, and guidelines, the IMO provides a comprehensive framework for addressing a wide range of maritime security issues, including those related to port and transportation security. Additionally, the IMO's initiatives extend beyond the EU's focus on port and transportation security to encompass offshore operations, such as drilling, exploration, and the production of crude oil and natural gas, ensuring a holistic approach to maritime security across the globe. The International Ship Port Security Code (ISPS) established in 2002 by the IMO is a pivotal component of this framework, aimed at enhancing security measures in ports and aboard ships worldwide.

With reference to the timeline shown in Figure 1-a), the EU Regulation 725/2004 (European Parliament and Council of the European Union, 2004), is the first regulation that it is worth to mention in the context of ship and port facility security in the EU member states. Enacted in March 2004, this regulation was prompted by the EU's recognition of international illicit actions, particularly terrorism, as significant threats to democracy, freedom, and peace, values central to the EU. It asserts the need for continuous monitoring and implementation of security measures to safeguard maritime transport within the EU and its citizens, as well as the marine environment, against intentional acts aimed at disrupting normal operations and harm people. It requires each member state to adopt a national program detailing applicable security measures, including specific security plans for ships and port facilities at different security levels. These levels range from maintaining minimum security measures to implementing specialized security measures in response to imminent security threats.

Additionally, Directive 2005/65/EC (European Parliament and Council of the European Union, 2005) complements Regulation 725/04 by extending security provisions to the entire port area, ensuring consistent high security levels across all European ports. Italy, in compliance with these regulations, has adopted the National Maritime and Port Security Program (PNSM) since 2007, periodically updating it to address evolving maritime security challenges. The PNSM aims to ensure the safety of passengers, crews, port operators, and infrastructures (including offshore GNL regasification terminals) while maintaining regular maritime transport operations. It coordinates the implementation of maritime security standards, it defines roles and responsibilities among authorities, law enforcement agencies, and maritime transport entities, and it provides operational criteria for security measures.

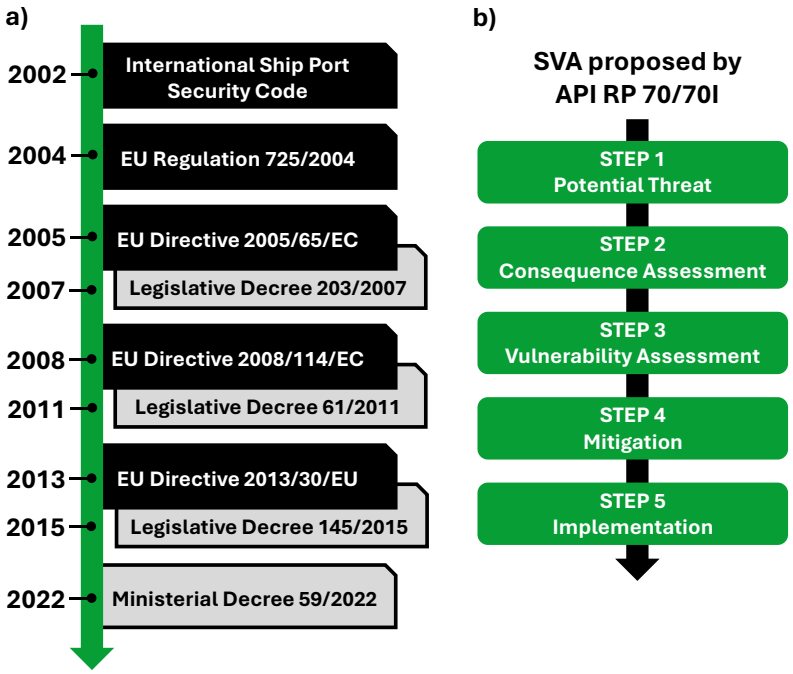

Figure 1 a) Timeline of main EU Directives and Italian transpositions in the field of safety and security of offshore installations; b) Flowchart of SVA methodology proposed by API RP 70 and API RP 70I.

Italy transposed Directive 2005/65/EC in 2007 through Legislative Decree No. 203 of November 6, 2007 (Italian Government and Parliament, 2007), designating the General Command of the Coast Guard of the Ministry of Infrastructures and Sustainable Mobility as the national contact point for port security. This decree also outlines specific requirements for port security assessments, security plans, and training exercises to test response capabilities. Additionally, Directive 2008/114/EC (Council of the European Union, 2008), transposed in Italy by Legislative Decree 61/2011 (Italian Government and Parliament, 2011), addresses the protection of critical infrastructures across the EU, including those in the energy and transportation sectors. It establishes common criteria for identifying and evaluating critical infrastructures, emphasizing the need to prioritize the protection against terrorist threats. Italy has partially implemented this directive, but formal designations of national critical infrastructures are pending. The ongoing revision of Directive 2008/114/EC aims to strengthen the resilience of critical entities across various sectors, reflecting the evolving risk landscape, including hybrid threats, natural disasters, and pandemics. In Italy, the Critical Infrastructure Secretariat, under the Prime Minister's Office, oversees activities related to the identification and designation of European critical infrastructures and coordinates Italy's position in ongoing EU negotiations regarding critical infrastructure protection.
Finally, Directive 2013/30/EU (European Parliament and Council of the European Union, 2013) addresses offshore activities related to hydrocarbon exploration and production, establishing minimum safety standards to prevent major accidents and mitigate environmental risks. Italy transposed this directive into national law through Legislative Decree No. 145 of August 18, 2015 (Italian Government and Parliament, 2015), enhancing offshore safety measures to protect marine ecosystems and minimize the impact of potential accidents, also by preparing a mandatory document (Report on Major Hazards) containing a risk assessment and an emergency response plan. This decree does not directly address security aspects, it covers the safety and environmental implication of the aftermath of an accident that may have resulted due to a security breach.
Last in the timeline, in 2022 Italy implemented an update of the National Maritime Security Program against intentional unlawful actions (PNSM), approved by the Interministerial Committee for the Security of Maritime Transport and Ports (CISM) on October 21, 2021, through the Ministerial Decree on March 17, 2022, No. 59 (Italian Ministry of Infrastructure and Sustainable Mobility, 2022).

3. Methodologies to assess security risks in offshore installations

Within the regulatory framework outlined in the previous section, professional organizations and governmental authorities have proposed, over the years, methodological frameworks to identify, assess, and manage security risks in industrial critical infrastructures, including offshore Oil&Gas facilities. These methods fall under the so-called Security Vulnerability Assessment (SVA) and Security Risk Assessment (SRA) methodologies, which thus serve as practical approaches for ensuring compliance with regulatory requirements.
A review of the main non-proprietary SVA/SRA methodologies is provided in Bajpai & Gupta (2018). For the specific field of offshore Oil&Gas operations, the American Petroleum Institute (API) published two Recommended Practices, the API RP 70 “Security for Offshore Oil and Natural Gas Operations” (American Petroleum Institute, 2010) and the API RP 70I “Security for Worldwide Offshore Oil and Natural Gas Operations” (American Petroleum Institute, 2012) that propose a semi-quantitative workflow to conduct a SVA (see the flowchart in Figure 1-b)).
In Step 1, the scenarios that could be a potential threat to the offshore facility under assessment shall be identified (both worst-case scenarios and most probable scenarios should be considered). Examples of threat scenarios reported in the reference sources of the methodology include an “Externally attack the facility by ramming with a vessel / by launching or shooting weapons from a distance / by moving explosives adjacent to the platform” or “Intrude and/or take control of facility and open valves / takes hostages / kills people”.
In Step 2 the potential consequences of each considered threat scenarios shall be evaluated. This is done with the aid of a rank-based matrix (three levels, i.e., moderate, significant, catastrophic): the consequence level is assigned based on the potential for death or injury, significant economic impact or significant environmental impact (in assessing the environmental impact, the facility location in relation to sensitive natural resources should be considered).
In Step 3, each facility owner/operator shall evaluate each scenario in terms of the facility’s vulnerability to an attack. The initial evaluation of vulnerability should be viewed with only existing strategies and protective measures, designed to lessen vulnerabilities, which are already in place. After the initial evaluation has been performed, a comparison evaluation can be made with new strategies and protective measures (mitigations) considered. The two elements that shall be taken into account in assessing vulnerability are accessibility and organic security: the first is related to the physical and geographic barriers that deter the threat without organic security, while the second is the ability of facility personnel to deter the attack (it may include security plans, communication capabilities and plans, intrusion detection systems and point of embarkation plans). A three-levels rank is adopted for both accessibility and organic security: definition of each rank level is provided in the reference sources of the methodology.

In Step 4, the facility owner/operator should determine which scenarios should have mitigation strategies (protective measures) implemented. This is done using the matrix shown in Figure 2 based on consequence level and total vulnerability score. “Consider” means that mitigation strategies should be developed on a case-by-case basis; “Document” means that the scenario may not need a mitigation measure and therefore needs only to be documented; “Mitigate” means that mitigation strategies, such as security protective measures and/or procedures, should be considered to reduce risk for that scenario.
In Step 5, the facility owner/operator should develop and implement practical mitigation strategies for those situations that score a “Consider” or “Mitigate”. Multiple mitigation strategies may need to be considered.

		Total Vulnerability Score		
		2	3-4	5-6
Consequence Level	Catastrophic	Consider	Mitigate	Mitigate
	Significant	Document	Consider	Mitigate
	Moderate	Document	Document	Consider

Figure 2 Vulnerability & Consequence matrix adopted by API RP 70 and API RP 70I SVA methodology.

The workflow here described, as well as that of most SVA/SRA methodologies, lacks systematic practical procedures for scenario identification, providing only occasionally checklists for sample security scenarios (as it occurs for the API RP 70 and API RP 70I SVA methodology). Moreover, these methods are often semi-quantitative and rely heavily on expert judgment, resulting in non-reproducible security assessments. Additionally, some methodologies are specific to single industrial sectors, limiting their applicability to broader critical industrial infrastructure. This fostered academic institutions to develop quantitative systematic approaches in support to existing methodologies: a review of these novel methods is provided in Iaiani et al. (2022).
The Authors themselves published a study (Iaiani et al., 2023) proposing a step-by-step quantitative methodology based on the Bayesian Network modelling aimed at the quantification of the probability of success of security attacks given the attempt (this is one of the three contributions of the security risk in its probabilistic formulation), to which the reader is referred to gain more details. The methodology allows for a systematic identification of the attacks that can be performed by threat actors through the use of the Adversary Sequence Diagram (ASD) tool that was developed and adopted for this purpose in the context of the nuclear power industry (Garcia, 2007). The application of the methodology to a fixed Oil&Gas production platform proved its ability in supporting API RP 70 and API RP 70I SVA as regards the identification of the most critical threat scenarios, the identification of the vulnerabilities in the Physical Protection System (PPS) of the analyzed facility, and the definition of potential design improvements towards a more secure PPS.

4. Best practices to enhance offshore security

In the following, best practices concerning protective measures are proposed, based on the result of a study performed in the framework of the Italian project "Sicurezza operazioni a mare" supported by Ministero dell'Ambiente e della Sicurezza Energetica (MASE), Direzione Generale Infrastrutture e Sicurezza (DGIS). Their implementation is aimed at enhancing the security level of offshore hydrocarbon production and natural gas liquefaction and storage facilities. In fact, these measures can be considered in the context of SVA/SRA methodologies as potential new barriers to be implemented to reduce risk of assessed threat scenarios (e.g., Step 5 of API RP 70 and API RP 70I SVA methodology). The following actions may be considered for implementation (main sources analyzed are reports 474R, 494R, 496R, 497R, 512R, and 555R of the International Association of Oil and Gas Producers (IOGP)):

A. Conduct a comprehensive SVA/SRA

This should be performed for each platform/rig to identify potential threats comprehensively, including both regular operations and special activities such as loading, diving, pipeline laying, drilling, LNG unloading operations for regasification terminals. Risk assessment should involve the identification of potential threat scenarios, assessing asset vulnerability and attractiveness, and evaluating the potential impact of an attack on worker safety, environmental damage, and facility. The SVA workflow described in previous Section can be adopted to this purpose.

B. Implement security measures

This includes security protocols, surveillance systems, communication systems (both internal to operators in the control room, and external, to the security response force), alarm systems, personnel training policies,

evacuation plans. Specific procedures, including shutdown protocols, should also be defined to secure the facility in case of loss of control due to an external attack (cyber or physical attack).

C. Inform and train personnel

Employee responses during stressful situations can significantly impact the outcomes of an attack, potentially rendering facilities more vulnerable. Therefore, personnel on board should be informed and trained on predictable threats, security protocols, and appropriate response measures to ensure they can effectively manage emergencies. Regular drills should be conducted. Moreover, protocols for personnel behavior during attacks should adhere to the following principles: i) Employees must refrain from aggressive actions against assailants, with the prohibition of weapons, particularly firearms, aboard facilities; ii) Technical and private security personnel should abide by Voluntary Principles on Security and Human Rights when engaging assailants; iii) When an intrusion occurs, personnel should adopt a low-profile to avoid incidents jeopardizing health, safety, or life; iv) Armed security personnel should be stationed separately from oil and gas operations on dedicated vessels or platforms nearby, minimizing risks and potential conflicts.

D. Adopt defense-in-depth strategy

The control of maritime areas surrounding offshore installations should be conducted through various levels of protection and defense utilizing concentric circles around the asset (e.g., separated by floating barriers), which should allow the interposition of a dedicated security vessel between intruders and the target in case of an attack. The restricted navigation area (typically 500 meters in diameter) designated around offshore installations in Italy, which is outlined on nautical charts, must be rigorously enforced as even non-hostile boats such as fishing vessels navigating in these areas, could enable an aggressor to blend in. Hence, immediate removal of any unauthorized vessel is necessary to maintain effective control of the area. For offshore floating regasification terminals, reference can be made to the regulations applied to Offshore Loading Terminals (OLT). These terminals are typically considered ships and are subject to navigation safety regulations in their surrounding areas, often extending from the port jurisdiction. Such regulations may include prescribed exclusion zones for navigation safety, as outlined by regional technical committees or port authorities: these zones typically consist of concentric circles around the terminal, with various levels of monitoring and control extending to different distances from the terminal itself.

E. Monitor adjacent areas

Monitoring the marine area around offshore installations is crucial for deterring hostile activities and promptly detecting intruders. Methods include observation points on platforms, surveillance from supply boats, and dedicated security vessels. The observation bridge on platforms can serve as an observation post equipped with radar monitors, closed-circuit TVs, and night vision systems. Various equipment options like long-range binoculars, radar systems, communication devices, and drones enhance surveillance capabilities. Marine security vessels, such as patrol boats, play a crucial role in maintaining control of offshore waters, acting as a deterrent and providing early warning through effective detection.

F. Strengthen assets

If deemed necessary based on risk analysis, assets should be reinforced to prevent intrusions, buy time for rescue teams, and protect personnel from hostile fire. Priority is given to reinforcing the physical protection of human resources and process equipment with a protective barrier (e.g., security doors, gates, lightening system, etc.). Protection must meet security and operational needs without blocking escape routes or critical access points. However, it is important to underline that integrating security into design is crucial, as modifications to existing installations is costly and less effective. Assets strengthening should also involve unmanned sites.

5. Conclusions

In the context of an increasing concern worldwide towards security issues in industrial critical infrastructures, including offshore Oil&Gas facilities, the present contribution outlines the regulatory frameworks at both the EU and Italian levels, detailing specific directives and regulations aimed at enhancing maritime security and addressing offshore security concerns.

The methodologies available to assess security risks are then discussed, with the particular focus on the one proposed by API Recommended Practices API RP 70 and API RP 70I as it is specific for offshore Oil&Gas operations. Limitations and existing challenges are also drawn, highlighting the contributions from academia in terms of quantitative systematic approaches in support to the existing methodologies.

Lastly, the present study presents best practices for protective barriers to enhance security of maritime operations, drawing from recent reports and recommendations. These practices include conducting comprehensive security assessments, implementing security measures, informing and training personnel,

adopting defense-in-depth strategies, monitoring adjacent areas of facilities, and strengthening assets as necessary. Overall, the insights provided in the present study contribute to provide a more comprehensive framework on security management practices in offshore operations, offering valuable lessons and best practices drawn from the Italian experience.

Acknowledgments

This work was supported by Ministero dell'Ambiente e della Sicurezza Energetica (MASE), Direzione Generale Infrastrutture e Sicurezza (DGIS) in the framework of the project "Sicurezza operazioni a mare".

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.

Bajpai S., Gupta J.P., 2018, Security risk assessment: Some techniques, Chapter In: G. Reniers, N. Khakzad, & P. Van Gelder (Eds.), Security Risk Assessment in The Chemical and Process Industry, de Gruyter, 75–92.

Council of the European Union. (2008), Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345.

Daxecker U.E., Prins B.C., 2015, Searching for sanctuary: Government power and the location of maritime piracy, International Interactions, 41(4), 699–717.

European Parliament and Council of the European Union, 2004, Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, Official Journal of the European Union, L129.

European Parliament and Council of the European Union, 2005, Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security, Official Journal of the European Union, L310.

European Parliament and Council of the European Union, 2013, Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC, Official Journal of the European Union, L178.

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

Iaiani M., Musayev N., Tugnoli A., Macini P., Cozzani V., Mesini, E., 2021, Analysis of security threats for offshore oil&gas operations, Chemical Engineering Transactions, 86, 319–324.

Iaiani M., Tugnoli A., Cozzani V., 2022, Identification of reference scenarios for security attacks to the process industry, Process Safety and Environmental Protection, 161, 334–356.

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.

Italian Government and Parliament, 2007, Legislative Decree 203/2003: Attuazione della direttiva 2005/65/CE relativa al miglioramento della sicurezza nei porti, Gazzetta Ufficiale.

Italian Government and Parliament, 2011, Legislative Decree 61/2011: Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione, Gazzetta Ufficiale.

Italian Government and Parliament, 2015, Legislative Decree 145/2015: Attuazione della direttiva 2013/30/UE sulla sicurezza delle operazioni in mare nel settore degli idrocarburi e che modifica la direttiva 2004/35/CE, Gazzetta Ufficiale.

Italian Ministry of Infrastructure and Sustainable Mobility, 2022, Decree 59/2022: Regolamento recante disciplina del funzionamento del Comitato di sicurezza finanziaria e delle categorie di documenti formati o comunque rientranti nella disponibilità del Comitato, Gazzetta Ufficiale.

Kashubsky M., 2011, A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975 – 2010, Perspectives on Terrorism, 5(5/6), 139–167.

Progoulakis I., Nikitakos N., 2019, Risk Assessment Framework for the Security of Offshore Oil and Gas Assets, Proceedings of the IAME 2019 Conference, 1–25.