







Comprehensive Risk Classification and Mitigation in the Petroleum Cyber-Physical Systems of the Oil and Gas Industry

Zina Oudina^{1*}, Ahmed Dib², Mohamed Amine Yakoubi³, Makhlof Derdour⁴

¹ Embedded Systems Laboratory, Badji Mokhtar University, Annaba 23000, Algeria

² Networks and Systems Laboratory, University of Badji Mokhtar Annaba, Annaba 23000, Algeria

³ Laboratoire de Recherche en Informatique, University of Badji Mokhtar Annaba, Annaba 23000, Algeria

⁴ LIAOA Laboratory, Oum El Bouaghi University, Oum El Bouaghi 04000, Algeria

Corresponding Author Email: zina.oudina@univ-annaba.org

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijssse.140110>

ABSTRACT

Received: 24 November 2023

Revised: 19 January 2024

Accepted: 23 January 2024

Available online: 29 February 2024

Keywords:

petroleum cyber-physical systems (CPSs), oil and gas (O&G), risk, vulnerability analysis, mitigation, security approach

The oil and gas (O&G) industry is the engine of the global economy. Oil and gas production passes through axes related to exploration, research, extraction, transportation, and finally the final manufacturing of energy products. All these stages permeate some risks that threaten both the human factor and the material factor. The oil industry merged with the fourth technological industry 4.0, which included multiple technologies and systems, the most important of which is the cyber-physical system (CPS), which some researchers have named petroleum cyber-physical systems if it is embodied within this industry. CPSs are collaborative systems formed of autonomous and smart devices that can handle data flows and activities while maintaining integrated physical objects. Several risks confront the energy field, with the potential to interrupt critical supply lines, hurt the environment, and trigger a financial catastrophe. In the field of O&G, there are very few scientific studies that are exposed to risks in a complementary and comprehensive manner, including only those that focus on cyber-attacks and their causes. There is a lack of comprehension and in-depth studies of all types of threats in all their aspects that surround cyber-physical systems within this field. Some risk classifications are based on internal and external risks, while others are based on the influencing and causative aspects in a general way. This study deals with the classification of risks: 1) classification of risk for the global industry of O&G. 2) in terms of the fact that the cyber-physical system is the most important component in the O&G industry and that these risks are either physical, cyber, or related to permissibility and authorization in the O&G field. A security approach is also presented that leads to mitigating the impact of risks in oil and gas zones.

1. INTRODUCTION

The product chain of an oil and gas firm is frequently separated into three parts: upstream, midstream, and downstream. The terms upstream and midstream apply to crude oil transportation and storage by pipelines, trains, ships, or trucks, respectively. Finally, completed goods are produced downstream. Industry 4.0 enables the integration of multiple industrial technologies into ICT, remotely maintains Supervisory Control and Data Acquisition (SCADA) systems [1], and supervises operations in real-time via actuators and smart sensors [2]. ICS is also utilized to monitor machinery and provide real-time process monitoring [3].

Cyber-physical systems (CPS) have been employed in a range of oil-related tasks, where CPS optimization approaches can aid in petroleum exploration, production, and management [4].

Most oil and gas production facilities are situated in remote locations with challenging weather. For these systems, it is especially important that monitored metrics are communicated through the air, fixed (optic or copper) lines, or satellite. It's

also crucial to have remote control of equipment that is installed on-site, such as valves, pumps, hydraulic and pneumatic control systems, safety instrumented systems (SISs), emergency stop systems, and fire detection apparatus. Since all of the systems are run by software, external remote services may act as attack surfaces for intruders aiming to get access to internal network resources from faraway places. Furthermore, remote operations are frequently managed by digital systems, which are susceptible to cyberattacks including hacking, phishing, and malware. One important issue is that hackers may get unauthorized access to the distant system and cause damage or disruption.

Khan et al. [5] released research on dependable IoT-based architectures for the O&G industry. They provide alternative architectures for functional applications in both upstream, middle, and downstream oil field services, as well as security concerns.

The energy industry confronts a wide range of risks and hazards that could interrupt critical supply lines, hurt the environment, or even trigger a financial catastrophe, necessitating dealing with and addressing the problems. In

literature, the focus is on cyber-physical attacks. There are very few academic works that specifically address cyber security issues in the oil and gas industries. Nonetheless, some publications address various cyber security dangers to this industry. Hacquebord and Pernet [6] survey risks to the oil and gas industry and present a study of known hacker groups and their cyber-attacks against the oil and gas industry. It issued a survey on (O&G) as cyber threats in the study of Dragos [7] and cataloged cyber organizations and state actors that attack (O&G) facilities. Lobo [8] produced a comprehensive cyber risk technical evaluation tailored for the upstream subsector of the oil and gas industry, and they present an extensive analysis of threats, common assaults, and even catalog an enormous list of upstream cyber-security events. In the study of Radmand et al. [9], they propose a taxonomy of wireless sensor network cyber-security threats in the O&G industries, and they present common wireless network security criteria and link them to probable attacks on wireless networks utilized in O&G ICS. It focuses solely on wireless technologies. The US Department of Energy issued Risk Management Guidance for Energy Infrastructure, which applies to the O&G field [10]. In the study of McLaughlin et al. [11], the SCADA system and its detailed architecture were described. The SCADA communication protocols, critical control system protection, and security assessment are also presented.

According to Sergiopoulos et al. [12], there has been no systematic method for documenting, charting, and categorizing cyber security breaches in the oil and gas sector. Furthermore, the historical record highlights the vulnerability of the oil and gas operational technology infrastructure to cyberattacks.

In the petroleum field literature, there is a paucity of risk modeling and feasible mitigation strategies. Also, there is no classification of the full possible risk in the O&G sector. There are currently two categories of risk: 1) risks that are internal or external, and 2) general classifications that include natural disasters, geopolitical conflicts, and operational incidents. These ratings do not address every potential risk and do not emphasize every aspect or cause of risk. Also, there are simply reports, instructions, and guidelines, with no systematic and comprehensive compilation of all relevant hazards and risks.

This study contributes to: 1) risk classification for the entire industry of O&G. 2) classification in terms of the fact that the cyber-physical system is the most important component in the O&G industry and that these hazards are either physical, cyber, or connected to permissibility and authorization for O&G companies. 3) proposes a security approach for securing oil and gas zones. The goals of this study are:

(1) Recognize potential risks in the oil and gas industry and provide systematic classification.

(2) How to bridge the gap between the risk's awareness and defense by proposing a security solution that led to the mitigation of impact and aid for protection against risks, which is a multifaceted security approach that is divided into three parts.

The paper is organized as follows: Section 2 describes risk classification and distinguishes two types of classification. The first is for the entire (O&G) business, which is based on aspects such as HSE, human, business, and security. The second classification is related to the cyber-physical system in the O&G area. Also, the significance of risk identification and classification, along with some empirical data and a case study, are presented in this section. Section 3 gives an overview of mitigating the impact of risk in petroleum CPS. Section 4

proposes a multifaceted security approach for securing oil and gas zones, which includes three phases, and some challenges for implementing oil and gas standards are highlighted. The discussion and conclusion are presented in sections 5 and 6.

2. RISK CLASSIFICATION

The petroleum and natural gas industries are complex environments that include onshore and offshore industries, upstream and downstream pipelines, and more. These organizations are all part of the same industry, yet each has its own set of risks and potential hazards to avoid. This industry remains vulnerable to a wide range of risks, including natural disasters, geopolitical tensions, operational incidents, cyber-attacks, unauthorized access, etc. Existing classifications are: 1) internal and external risks; and 2) classification in general: natural disasters, geopolitical tensions, and operational incidents. These ratings are in-depth, do not highlight all aspects and causes of risk, and do not cover all risks that may occur. This is why every area of this industry should have comprehensive coverage and analytical studies of concerns, risks, and threats. Through this research, we offer a general classification of the risks that threaten this field, which can be a principle for analytical studies on which each domain is based separately, such as marine oil, land petroleum, or transport. We also propose a classification that is related to the petroleum physical cyber systems, which are the result of integrating the smart technological industry with the petroleum industry.

Our proposed classification is:

- (1) Risk classification for the entire industry of O&G.
- (2) Classification in terms of the fact that the cyber-physical system is the most important component in the O&G industry and that these hazards are either physical, cyber, or connected to permissibility and authorization for O&G firms.

2.1 Risk classification for the entire industry of O&G

The field of oil and gas is considered one of the largest vital sectors, which is the backbone of major economies in the world and is linked to the environment and the ocean because its extraction and production are hard work in a difficult environment that may be mountainous, marine, or in rugged areas. Operation in this field is based on human, material, and equipment factors. Our classification of risk is based on those aspects: environment, human, business, and security.

2.1.1 HSE (Health, Safety, and Environment) risks

Health. The O&G sector uses and exposes workers to a variety of large and dangerous products, equipment, and materials. The most typical workplace dangers that affect a worker's health are:

(1) Highway car incidents cause 4 out of every 10 workplace fatalities for employees.

(2) According to the OSHA IMIS Database, 3 out of every 5 fatal on-site incidents are caused by being struck by, caught in, or caught between moving objects (such as moving or falling machinery, moving vehicles, high-pressure lines, etc.) [13].

(3) Explosions and Fires: This industry works with combustible gases and vapors like hydrogen sulfide and well gases that can escape from trucks, production equipment, or surface equipment (shale shakers).

(4) Chemical exposure occurs in restricted places such as petroleum storage and other tanks, mud pits, reserve pits, and other dug locations where workers typically operate. Workers are exposed to both health hazards, such as asphyxiation, and harmful chemical products.

Safety. Safety risks may be related to extraction activities, equipment, or humans. As per the United States Department of Labor, oil and gas extraction activities are associated with certain safety risks [13], such as human accidents, vehicle accidents, explosions and fires, equipment hazards, and electrical hazards.

Personnel operating on offshore (O&G) facilities, as well as seafarers in general, are potentially exposed to the unpredictability of wind and sea conditions, vessel motion, noise, vibration, poor air quality, hazardous chemicals, intense physical labor, and cramped workspace [14, 15].

Environment. There are four stages of oil and gas exploration and production [16]:

(1) A geological and geographical survey is required to determine the potential of an oil well for commercial viability.

(2) Exploration is a critical step for determining rig placement, exploratory drilling, plugging the well, destroying production wells, and so on.

(3) One of the major stages is development and production, which involves platform commissioning, pipeline installation, production drilling, pipeline maintenance, and so on.

(4) Decommissioning is the ultimate stage of oil and gas production. When the well is drained, this includes removing the platform and plugging the well.

All of these stages have a direct impact on the environment [16]. Examples include the impact of seismic surveys on aquatic species and the interruption of fisheries. Pollution emissions are affected by rig placement during the exploration stage. Development and production have an impact on operational discharges, accident spillage, and physical disturbances. emissions from operations, other impacts:

(1) In the Arctic region and in areas of the sea ice cover, there are untapped potentials for exploration, and there are difficulties and obstacles in extracting hydrocarbons [17].

(2) The use of seismic surveys for exploration has sparked worries about their effects on marine life due to the loud noise they generate. This noise can evict marine species from their habitat, alter their behavior, muddle safety related to equipment and human communication, induce stress, and, at close ranges, even harm their hearing systems [17].

(3) Oil leak incidents occur during oil exploration and transportation in the offshore petroleum industry. The worry with oil leaks is that they cause enormous contamination in the ocean, which causes a variety of economic and environmental issues [18].

According to the United States Department of Labor, oil and gas extraction activities pose:

specific environmental and safety risks [13], such as hazardous chemicals, hydrocarbon gases and vapors (HGVs) and low oxygen environments, temperature extremes, and naturally occurring radioactive material (NORM).

(1) Climatic risk: The volume of petroleum operations will be influenced by meteorological circumstances. For example, borehole operations are extremely dangerous when it rains or snows, while petroleum operations are extremely risky when it is extremely hot.

(2) Geologic risk: The structure and complexity of the

petroleum pool, its abundance and reserves, its nature, its burial depth, its initial formation pressure, its permeability, its active porosity, its cave and fault conditions, and its underground rock hardness will all have an impact on how well the petroleum operation goes.

2.1.2 Security risks

Cyber. Expanded automation, expanded computer network connectivity, and increased use of cloud computing services expose O&G companies to increasing cyber-security vulnerabilities.

In the study of Mahmoud et al. [19], cyber-attacks are classified as denial of service (DoS) assaults, deception attacks, and replay attacks. In the O&G field, attacks are directed at the operating domain [20]. The majority of attacks in this sector are denial of service (DoS) attacks, which endanger system availability by flooding the connecting device with requests to jam communication channels and prevent valid requests [21]. In 2012, one of the world's largest oil firms was the victim of a massive cyberattack. Shamoon, a debilitating wiper infection, made tens of thousands of the company's computer servers inoperable [22]. Another illustration of the Black Energy malware, which evolved from a trojan to a new piece of malware delivering the KillDisk payload, is a piece of malware that has evolved through time. It targeted the power plant Prykarpattya Oblenergo as well as other Ukrainian electricity distribution companies [23]. However, we cannot overlook the ransomware attacks that are increasingly prevalent in multiple sectors. Techniques such as network traffic or system call analysis can be used to detect this type of attack upon its appearance [24].

Piracy. Piracy is regionally based [25], and it is influenced by a number of factors such as unpredictable political environments, ineffective governments, a lack of economic development, poverty, and the capacity to reward in order to prosper [26]. By 2007, attacks on offshore infrastructure and piracy had become common in the Gulf of Guinea [27]. The offshore petroleum industry has also been impacted by pirate activity off the east coast of Africa.

Terrorism. Oil-producing nations are more susceptible to terrorism because oil installations are prime targets for terrorist attacks that aim to have a greater impact and disrupt the external interests of powerful nations. It makes use of data from the oil industry and terrorist attacks [28].

2.1.3 Human risks

Employees. Quality, operational level, cultural level, personnel age composition, and overall quality are important for the employee in the O&G organization. The lack of these characteristics is the main cause of the risks caused by human errors. Many studies suggest that drilling events are caused by people and that human error has played a substantial role in the prevalence and severity of the consequences [29].

Managers and organizations. Petroleum operations will be impacted by the management skills, charisma, and leadership of managers. These characteristics also relate to organizational risk. Petroleum operations will be impacted by these elements, such as illogical organizational structures, inadequate staffing, and irrational responsibility distribution. Organizational risk will have an impact on the operating period and can impact the economic effectiveness of the company.

Lack of training. Engineers and staff are frequently untrained or undertrained in cyber security [30].

2.1.4 Business risks

Financial risk. Oil and gas are products, and their prices are significantly more volatile than those in other markets. In addition to the actual price of raw materials, the underlying expenses of harvesting and refining natural resources have a considerable impact on their pricing. Furthermore, petroleum operations have a long cycle, a broad geographical dispersion, a huge number of personnel, and a large quantity of funds.

Economic and market risk. Taxation is a key tool for the government to manage oil and gas production, supply, and demand, which directly influence the level of profits of petroleum enterprises.

Supply and demand shocks are a risk for oil and gas firms, especially because energy facilities require large amounts of capital and time to ramp up to full capacity. Concerns have been raised about any disruption in the global supply of oil and gas (O&G), which might have an impact on oil prices and, by extension, the global economy [31].

2.2 Risk related to petroleum CPS in the O&G industry

2.2.1 Physical risks for petroleum CPS

Physical hazards are those that threaten facilities, equipment, and the human factor and cause physical damage to them, such as destruction, burning, and vandalism. In the oil and gas industry, we consider that any damage that may be caused to facilities, storage equipment, storage levels, and transportation equipment is physical damage [32]. In this context, we can mention the most important physical risks as follows:

Tank attacks. The treated gas and water are held in settling tanks until they may be exported. The oil tank level spooping Attacks are outfitted with level control sensors that send data to avoid tank overfilling. The major purpose of this approach is to deceive sensors into reporting that the tank level is lower than it actually is [31].

Wellhead production data exfiltration. By using malicious software such as trojans on hacked control station workstations, an attacker could gain access to sensitive information such as wellhead production data. The use of Domain Generation Algorithms (DGA) in creating communications between bots and their Command and Control (C&C) servers is one example that led to obtaining sensitive information [32].

Drone attacks. Physical attacks are also a problem; just recently, a drone attack on the world's largest refinery crippled 5% of the world's global oil supply [33].

2.2.2 Cyber risks for petroleum CPS

Numerous threats were faced upstream, such as during the exploration phase, when malware entered through network storage nodes to steal competitive seismic data for an offshore field that was up for bid. As in the development phase, a pre-deployed rogue program begins dictating drilling parameters, resulting in well deviation and other well integrity difficulties. Through the production and abandonment phases, a masked worm in SCADA arbitrarily adjusts the speed of motor pumps, resulting in suboptimal production and well damage.

Cyber-attacks are occurring on the industrial control systems (ICS) of O&G firms, putting worker safety, reputation, and operations, as well as the environment, at risk. Whether hackers use spyware to target field bidding data, malware to infect production control systems, or denial of service to block the flow of information through control systems, they are becoming increasingly sophisticated and, particularly concerning, launching coordinated attacks on the industry. In

this sense, the following are the most well-known cyber risks:

(1) Denial-of-service (DoS) attacks: Unavailability attacks in ICS components can render O&G systems inaccessible if vulnerabilities are successfully exploited [34].

(2) Command Injection: Common network attacks on ICS include blocking or replaying command or reporting messages (DoS) [35].

(3) Data exfiltration: Data exfiltration is the unlawful disclosure of sensitive or confidential information. Data exfiltration can be committed by either an outsider or an insider of a company [36].

(4) Data tampering: An offensive operation may occur within another offensive operation, and the intention is to obscure the larger operation, mislead the data, and deceive the defender [37]. It is called data tempering, and we consider it an indirect attack.

2.2.3 Authorization risks for petroleum CPS

This danger is tied to both human and material factors. Any human access to facilities and the use of any material not allowed in the field of exploitation, production, or discipline. Even unauthorized access to data can be used to abuse the lack of cryptography in protocols or communication channels.

Internal authorization and access (employees).

(1) Employees' lack of threat awareness, coercion or blackmail, or even the sale of company security information on the dark web for profit can raise network vulnerability and constitute a critical risk. In 2017, for example, an employee in the Middle East used a USB drive to download and watch a movie on a critical infrastructure computer. The user was unaware that this activity resulted in the distribution of malware later called Copperfield by Nyotron, the company in charge of detecting it. Data leakage, network scanning, and remote control of an ICS workstation were all caused by Copperfield [38].

(2) A risk exists due to the lack of strong authentication and authorization procedures for personnel and any software entities.

(3) Many studies believe that drilling events are caused by humans and that human error has played a significant role in incidence and consequence aggravation.

External access (third parties or foreign and attackers). Third-party SCADA systems must be monitored for dependability risks such as firmware changes, misconfigurations, open ports, communication failures, equipment faults, and others.

The risks here revolve around the possibility of operating these systems remotely, through strangers from the company, or through professional attackers. External remote services may serve as attack surfaces for adversaries seeking to get first access to internal network resources from distant locations [39].

Using the TRISIS framework, Xenotime created a disruption at an O&G plant in Saudi Arabia in 2017. This malware was designed to attack the Triconex safety controllers [7]. It employed backdoor malware to shut down the facility's industrial systems.

Table 1 summarizes the most significant and well-known risks associated with the CPS and system structure in the oil and gas industry.

Many studies have cited events and accidents in the O&G industry; we categorized this event using our proposed risk classification in petroleum CPS. Table 2 shows some O&G industry events.

Table 1. Well-known risks associated with the CPS and system structure in the oil and gas industry

Components in O&G	Description	Risks	Impact
ICS	<ul style="list-style-type: none"> - Cyber-attacks on O&G systems might be allocated to different ICS architectural layers. - Devices and embedded components such as RTU, PLC, and relays are found in the hardware layer. - The firmware layer is between the hardware and software layers. It consists of the operating system that is used by midstream and downstream controllers, systems, and field equipment. - The software layer of an ICS includes all of the programs used to monitor and control machines and peripheral systems, as well as other software platforms and human machine interfaces. - The network layer contains: firewalls, modems, routers, remote access points. [7] and wireless sensors use S-MAC, LMAC or B-MAC protocols. - Layer of Processing: The dynamic properties of the intended ICS model must be followed by the ICS procedures [52]. 	<ul style="list-style-type: none"> - Hardware Layer: Tampering attacks and physical attacks [32, 39] - Supply chain attacks as hardware trojans in any stage of the supply chain [40-42]. - Unpatched legacy/end-of-life equipment. - Firmware Layer: firmware injection [40, 43] attacks - Software Layer: injection, malware attacks, remote code execution [32, 39]. - Unpatched operating systems [44]-SQL injection, malwares attacks [45], XSS and CSRF Attacks [46]-Buffer overflows [45, 46]. - Improper access control or authentication processes in software used in ICSs [47-49] - Network Layer: Dos attacks and jamming attacks. - MODBUS lacks of secure channel [48]. - FINS protocol for PLC lacks encryption in data exchanges [49] <ul style="list-style-type: none"> - Absence of network partitioning - Layer of Processing: ICS-centric attacks [52] <ul style="list-style-type: none"> - Field Bus Layer: Telnet intrusions [56] intrusion from outside the local network, which may affect both routine and aberrant login attempts and command/response exchanges, DoS attacks 	<ul style="list-style-type: none"> - Third-party devices may present unforeseen vulnerabilities in both upstream and downstream infrastructures [40] - Disruption of ICS operation - Disruption of ICS operation <ul style="list-style-type: none"> - Affect ICS process - Compromised OT processes, commands and data - ICS exposed to network attacks [50] - Attackers can get access to field devices and control-related systems [51] - Attackers operate machinery, alter production, losses in revenue, performance degradation [53, 54]
	SCADA	<ul style="list-style-type: none"> - SCADA Components: Three Layers (field bus, Industrial Ethernet, Business Management) [55]. - SCADA communication protocols such as Modbus-TCP Distributed Network Protocol (DNP3), IEC-60870-5-104 and the Inter-Control Center Protocol (ICCP, IEC60870-6) [57]. 	<ul style="list-style-type: none"> - Industrial Ethernet Layer: DoS attacks, integrity attacks, and phishing attacks [58]. - Attacks on the PLC: Cryptographic attacks, Replay attacks, Fragmentation attacks. - Business Management Layer: onan attack, DoS attacks <ul style="list-style-type: none"> - Sensor misconfigurations [59]
IOT	<ul style="list-style-type: none"> - The use of IoT devices spread across all layers. - O&G IoT systems enable real-time monitoring and control of activities throughout the value chain. 	<ul style="list-style-type: none"> - Failures caused by the interaction of smart gadgets and legacy equipment - Absence of access control or encryption on IoT device links <ul style="list-style-type: none"> - Using insecure open source code and implementations 	<ul style="list-style-type: none"> - Denial of Services and integrity incidents - Affecting the overall infrastructure ecosystem [60]
Protocols	<ul style="list-style-type: none"> - Field device communication protocols (ZigBee, 6LoWPAN, and so on) [32]. 	<ul style="list-style-type: none"> - Vulnerable to denial-of-service, man-in-the-middle, and spoofing attacks [39, 61] - Sensors: Spoofing attacks that result tank overflow and containment breach - Temperature or pressure sensors: Data tampering attacks 	<ul style="list-style-type: none"> - Unavailability - Integrity incidents
Hardware	<ul style="list-style-type: none"> - Access control hardware (smart cards, RFID, etc.), server hardware (RACKs, CPUs, etc.), sensors, actuators, RTUs, PLCs, routers, valves, ATGs, slaves, et. - WSN security issues in all layers (from hardware to application layer). 	<ul style="list-style-type: none"> - PLC, safety instrumented system, and actuators: DoS attacks - PLC, pumps, actuators: Command injection attacks - controlled simulated attacks: can target all hardware in all layers 	<ul style="list-style-type: none"> - Explosion, loss of life, environmental damage - Bad product quality, revenue loss. - Exposing sensitive information, injecting false information into actuator states, causing DoS, shut down, restart, or even require reprogramming [60, 62]

2.3 Significance of risk identification and classification

Many case studies in the literature that focus on risk analysis and assessment in the oil and gas sector, such as in the studies

of Shah et al. [63], Khadem et al. [64], and Zand [65], have proved that risk identification and resource allocation are the basis of the risk management process and the key to the protection action plan.

Table 2. Events in oil and gas industry

Event	Year	Risk Type
A trojan was opened from within the Gazprom organization, and the attackers had direct access of the Russian gas supplier's full control system.	1999	Cyber
Changes in the historical database, PRV not properly designed and failed to open, caused a pressure spike, pipeline rupture, explosion when an automatic valve shut in a 16' Olympic Pipeline Company gasoline in Bellingham, Washington, USA. Three persons were killed, Property damage was estimated to be \$58.5 million.	1999	Cyber
PDVSA attack on ICS and affect reduction in oil production	2002	Cyber
Critical alarms, control instrumentation at British Petroleum's (BP) Texas City refinery presented erroneous indicators, failing to notify operators to the excessive amount of volatile hydrocarbons in the raffinate splitter tower. This caused an explosion that killed 15 people, forced the refinery to close for a year, cost BP \$1 billion damages.	2005	Authorization
Alarms and communications on the Baku-Tbilisi-Ceyhan pipeline in Turkey were disrupted, causing over-pressurization and the leaking of more than 30,000 barrels of crude oil.	2008	Physic
Mr Mario Azar, an IT consultant who was dissatisfied not hired for post in Pacific Energy Resources' Networks Operations Centre (NOC) in Long Beach, California, but who keeps access rights, stopped the leak detection system on three offshore sites. A single NOC can control up to 50 oil platforms, allowing for a centralized approach.	2008	Authorization
An explosion in Bayamon, Puerto Rico, was blamed on a 'glitch' in the facility's computerized monitoring system, according to investigators. Due to a faulty tank meter, a storage tank being filled with gasoline from a ship parked in San Juan harbour overflowed constantly until the vapour cloud collided with an igniting source. For three days.	2009	Physic
A rig en way from South Korea to Brazil was infected with computer malware and required 19 days to repair. While this is not an attack, it does demonstrate the possibility of loss as a result of a cyber incident.	2010	Cyber
A Night Dragon attack disabled proxy settings, used remote tools to steal sensitive data, operational production systems (ICS), financial docs pertaining to field exploration, bidding data on the assets.	2011	Authorization
Shamoon virus was used to launch a cyber attack against Saudi Aramco, causing damage to at least 30,000 machines. It propagated rapidly and wiped out entire systems while distorting the master boot record, rendering the computer useless. The strike attempted to disrupt Saudi oil and gas production and prevent resources from flowing to international markets. It had no direct influence on oil production, refining, transportation, or safety operations.	2012	Cyber
Televant, a provider of remote administration, monitoring technologies to the energy industry, was the target of an advanced persistent threat that infiltrated its internal firewall and security mechanisms.	2012	Authorization
Cyber attacks were launched against dozens of Norwegian energy corporations, including Statoil. The attackers have not been recognized, and their intentions are unknown.	2014	Cyber
The Indestroyer malware shut down the power grid in Kiev, Ukraine (Sandworm). Indestroyer, with minor adjustments, is capable of targeting other types of critical infrastructure including pipeline control system.	2016	Cyber
Oil rig malware attacks in Saudi Arabia results a data exfiltration.	2016	Cyber
Triton (aka Trisis) malware was developed to target equipment built by Schneider Electric, a business that sells equipment used in oil and gas facilities, as well as nuclear energy facilities and manufacturing factories on occasion.	2017	Cyber
Gaza cybergang attack on MENA region.	2017	Cyber
Two face webshell attack on min of oil.	2017	Cyber
Lycieum spear phishing in middle east.	2019	Cyber

According to Shah et al. [63], constructing new oil and gas pipelines (OGPs) without studying the potential risk factors (RFs) that influence the safety of these pipes creates time and expense overruns in these projects. In the field of oil and gas, to prevent project failure, it is vital to appropriately manage the related risks [64]. Reducing future delays and cost overruns in oil and gas projects involves conducting risk analysis and developing risk management measures [65].

Creating safe and secure systems in the oil and gas industry requires detecting and categorizing all types of risk. Risk classification facilitates the definition of roles and duties within the oil and gas organization, as well as the identification of vulnerable regions and their causes. This simplifies risk minimization and protection. The aim of this study is to identify potential risks in the oil and gas sector and to offer a methodical classification based on findings from published research as well as guidelines and reports.

The current risk classification in the literature fails to take into account all relevant industry aspects and elements, such as in the study of Zand [65]. The authors conducted a case

study to highlight some of the most critical risk elements associated with oil and gas projects, as well as recommendations for risk reduction. The argument is based on publicly available material and covers two independent projects in Iran and Qatar. Furthermore, they provided a framework that suggests recognizing and evaluating risks as early in the project life cycle as is feasible. The types of risk introduced in the study of Zand [65] are construction, operational, regulatory, and financial. They overlooked the human element, as well as the organization's overall safety and security.

In reality, human, material, and equipment aspects are the foundation of operations in the oil and gas sector and power the global economy while being encircled by the natural environment. All activities in the oil and gas sector should be carried out safely and securely. Based on those factors - environment, human, business, and security - we categorize risk. Table 3 shows the findings of published papers in each risk class.

Table 3. The findings of published papers in each risk class

Cyber Risk	HSE Risk	Human Risk	Business Risk
[6-24, 32-43, 45-47, 49-61]	[13-18, 31-33, 66, 67]	[7, 13-15, 29, 30, 38, 39, 66]	[31, 63-65]

It is worth noting that the majority of studies focus on cyber security concerns and HSE risks rather than other types of risks.

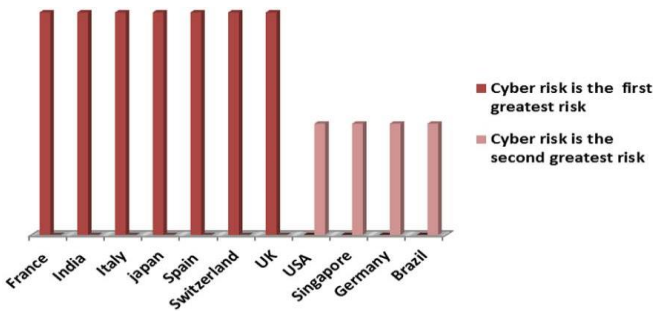


Figure 1. The rank of cyber security risk for many countries

2.3.1 Empirical data

According to the Federal Service for Ecological, Technological, and Atomic Supervision's (Russian Federation) analysis, there will be 36 risk events in the oil and gas sector (for Russia) between 2021 and 2022, with a total of 285 firms [68]. According to the Allianz Risk Barometer report [69], business interruption and supply chain disruption are ranked as the second greatest risk at 34%. It ranks second only to cyber events (34%), highlighting the significance of the digital economy, the threat of ransomware and extortion, and the rise of cyber-based conflicts. The report notes the close relationship between cyber risk and business interruption. Figure 1 presents the rank of cyber security risk for many countries.

The second classification offered in this study is for CPS, in terms of the fact that the cyber-physical system is the most essential component in the O&G firm and that the risks are either physical, cyber, or related to permissibility and authorization for O&G enterprises. Figure 2 depicts some events in the oil and gas industry; the event information is reported in Table 2.

2.3.2 Case study

Our paper suggested HSE as a risk class for the global oil

and gas industry. We use the Qatar Petroleum Organization's Health, Safety, and Environmental Conservation and Protection Policy [70] as a case study.

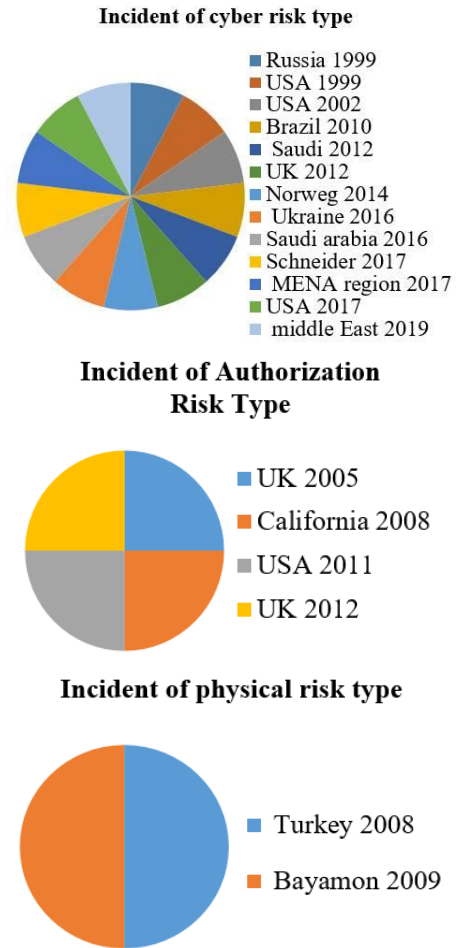


Figure 2. Some events in the oil and gas industry

We consider that the identification of fears and risks aids in the use of appropriate mitigation solutions and treats the kind of danger and weakness with the appropriate protection and solution. This is the case for Qatar Petroleum (QP), which considers HSE as a type of risk and The QP HSE Regulations for Contractors are documents that address the management of HSE in QP contracts and consist of procedures for managing HSE in contracts and guidelines that outline the overall process while also providing tools, templates, and guidance to QP professionals. Table 4 presents a brief summary of QP HSE regulations for contractors.

Table 4. A brief summary of QP HSE regulations for contractors

Defining Objectives	Identifying HSE Risk	Mitigation and HSE Rules
To develop and explain the minimal HSE requirements that contractors, workers, and subcontractors must meet while working for QP in order to ensure workplace safety, safeguard the health of all affected parties, and protect the environment.	-Requirement s identification (health, safety) for personal and material requirement, environment requirement. -Hazard Identification -Risk Assessment and Control.	- Maintain all guarding devices provided by the manufacturer of equipment/machinery to protect personnel from the inherent hazards connected with the operation of spinning machinery. Guiding systems include pulley and v-belt coverings, as well as a grinding disc guard. - Protect humans from harm by creating and maintaining effective defenses against the radiation dangers that arise from these sources. - List of other rules in the study of Balogun and Andaila [70].

3. RISK MITIGATION IN THE OIL AND GAS INDUSTRY

History has shown that oil and gas OT infrastructure is susceptible to cyberattacks. Many surveys, such as the study [62], emphasize dangers and risk reduction in different ways and with different goals. Alcaraz and Zeadally [71] discuss CPS vulnerabilities and prospective threats, as well as mitigating remedies. They presented a testbed for finding vulnerabilities in SCADA protocols in the study of Sayegh et al. [49].

An overview of ICS security and protocol-related (Modbus/TCP, DNP3, IEC 61850) and sensor/actuator vulnerabilities is presented, along with recommended security solutions to mitigate their risk [72].

Most statistics indicate that operator error or illegal activity is what causes accidents. Therefore, the petroleum industry should improve staff education and engage in a variety of inspection, advocacy, and communication activities.

Malware mitigation, intrusion, and anomaly detection are suggested for security and privacy in the study of Chen et al. [73]. To lower the danger of permitted access, facilities should put strong authentication and authorization procedures in place for all software entities and their workers.

In the study of Marzooq and Rashid [74], they studied ways to raise safety awareness and showed how a person's consciousness and behaviors have a big impact on their safety, actions, and capacity to deal with risks at work.

The O&G industry is strongly encouraged to adhere to standards. In order to make the methods understandable to design engineers, they illustrate IEC61508 compliance in oil and gas applications with an emphasis on steam turbines and provide a strategy for reliability analysis of intricate safety-structured systems [75].

The National Institute of Standards and Technology (NIST) explained by Stouffer et al. The study [47] how organizations should design and implement security programs and security strategies for the Industrial Control System (ICS). It highlighted how existing IT security knowledge, programs, and practices should be coordinated and integrated into new programs. It was suggested that the unique needs and characteristics of ICS technologies and surroundings be taken into account. It is also suggested that organizations regularly examine and update their ICS security plans and procedures to reflect changes in technologies, operations, standards, and regulations, as well as particular facility security demands.

There is a widespread belief among security experts that it is impossible to defend the perimeter of their IT systems, and the focus is shifting from defense to detection and rapid response. The energy sector is vulnerable to a variety of threats that can have serious consequences for operations, safety, and the environment.

Some defense approaches and risk management strategies concentrated on basic gaps in the literature and frequently discovered reports from real-world cyberattacks. In the previous part, we classified existing risks in the oil and gas industry into physical, cyber, and authorization categories. To lower each category of risk, we recommend combining associated safety and health standards, as well as cyber and environmental norms and regulations. The most important standard is ISO 20815:2008, an international standard for production assurance and dependability management in the petroleum, petrochemical, and natural gas industries. It includes production assurance principles in drilling,

exploitation, processing, and transportation systems and operations.

We can summarize the most important measures, proposals, and recommendations in the field of protecting gas and oil facilities in the following group of points, which we have arranged according to their importance from our point of view:

- (1) Identify and classify safety and security concerns in O&G firms.
- (2) Identify the weaknesses and causes of vulnerability and responsibility.
- (3) Setting the safety and security objectives.
- (4) Develop a safety and security plan, combining safety with security standards.
- (5) Industrial control system availability and integrity are assured with a strong and modern cyber strategy.
- (6) Early detection of attacks and managing time for response and defense.
- (7) To prevent physical manipulation, employ hardware security safeguards.
- (8) Incorporate end-to-end encryption and embedded security in all processes.
- (9) Implement authentication and access control mechanisms.
- (10) Every facility must implement appropriate network segmentation.
- (11) Assure employee training and raise their awareness.

4. A PROPOSED SECURITY APPROACH FOR SECURING OIL AND GAS ZONES

4.1 Secured oil and gas zone

A secured zone is a collection of logical or physical assets that all have the same security criteria within the oil and gas organization. A zone has a distinct boundary with other zones. A zone's security policy is often implemented by a combination of measures located both at the zone's perimeter and within the zone. Zones can be hierarchical in the sense that they can be made up of subzones (ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models, 29 October 2007).

4.2 Phases of the proposed security approach

This subsection proposes a multifaceted approach, which is divided into three parts. The first part identifies systems, architectures, and risks in the oil and gas zone. The second phase involves integrating industrial Next-Generation Firewalls (NGFW) for SCADA and ICS systems. The third phase involves incorporating oil and gas industry standards into the security life cycle of oil and gas zones. Figure 3 depicts the security approach, which focuses on the following security goals:

- (1) Securing the zone perimeter.
- (2) Protect the oil and gas zone from common risks.
- (3) Prevents unauthorized access and reduces access to data and resources.

4.2.1 Phase one: Identifying systems, architectures, and risks in the oil and gas zone and gaining visibility over assets

This phase includes recognizing and describing locations, types, quality, and total assets, as well as having complete visibility over OT assets such as field devices, SCADA

systems, and network visibility. Also, a complete collection of data and specifications for all PLC, RTU, DCS, and SCADA devices, as well as operating systems and related vulnerabilities, is presented in Table 1.

The segmentation of networks and using various technologies are the most utilized strategies for vulnerability mitigation and control in the sphere of oil and gas [76]. We separated the petroleum zone into systems (ICS, SCADA) to boost its security, as mentioned in Figure 3. The objective behind system identification is to partition the system into discrete security subzones and add layers of protection to separate the system's most critical components. Figure 3 presents ICS and SCADA components.

Regarding risk identification as a key task in this phase, we classified risk for petroleum CPS in Section 2 as physical, cyber, and authorization risks.

4.2.2 Phase two: Using Industrial Next-Generation Firewalls (NGFW) for SCADA and ICS systems

A firewall is a network security device that monitors and restricts network traffic based on predefined security rules (Wikipedia). The idea of using industrial NGFWs for secure

systems in the oil and gas zone is the cover of the technology's subzone (ICS, SCADA). Next-Generation Firewalls (NGFW) are industrial threat security firewalls that provide visibility, control, and automatic real-time analytics detection. The firewall's objective is to reduce the risk of unwanted access (or network traffic) and adhere to the philosophy of minimum permission and continuous surveillance of all traffic.

How is integrating industrial NGFWs into SCADA and ICS Systems?

Large, complicated systems, such as aged industrial machinery and dispersed networks, can be found in ICS/SCADA environments. In order to design an acceptable solution, it is necessary to analyze the needs and complexity of the ICS and SCADA environments before implementing firewalls.

The ICS and SCADA environments should only allow users to access the designated areas. When moving to a different network level, safeguarding the access by incorporating a firewall on each side prevents unauthorized access. Figure 4 shows ICS and SCADA, which are divided into network levels and are based on the ISA-99 standard.

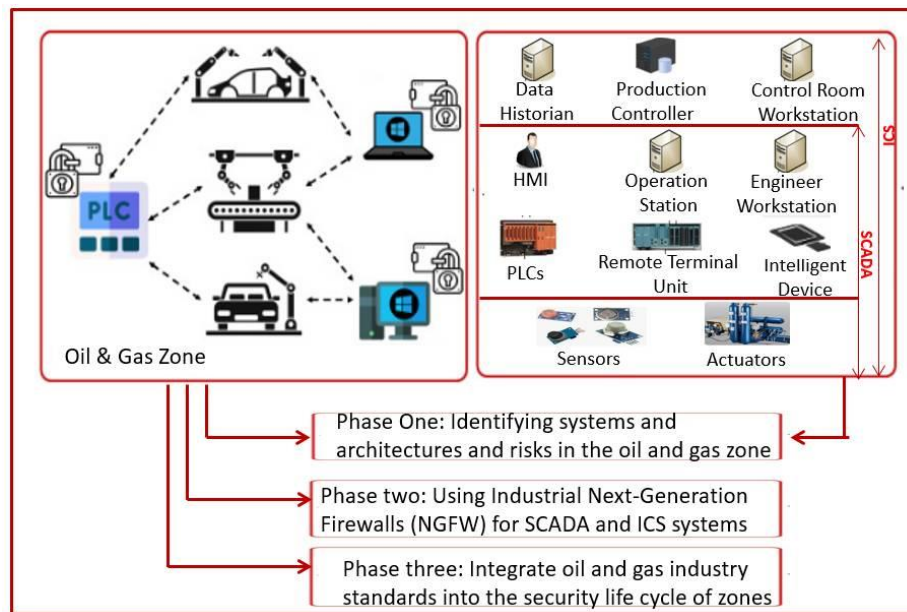


Figure 3. Multifaceted security approach for oil and gas zones

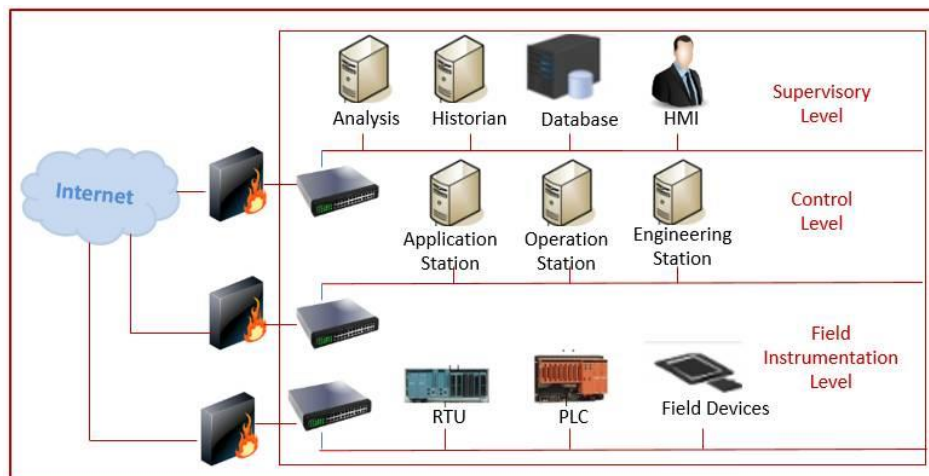


Figure 4. Industrial Next-Generation Firewalls (NGFWs) for ICS and SCADA

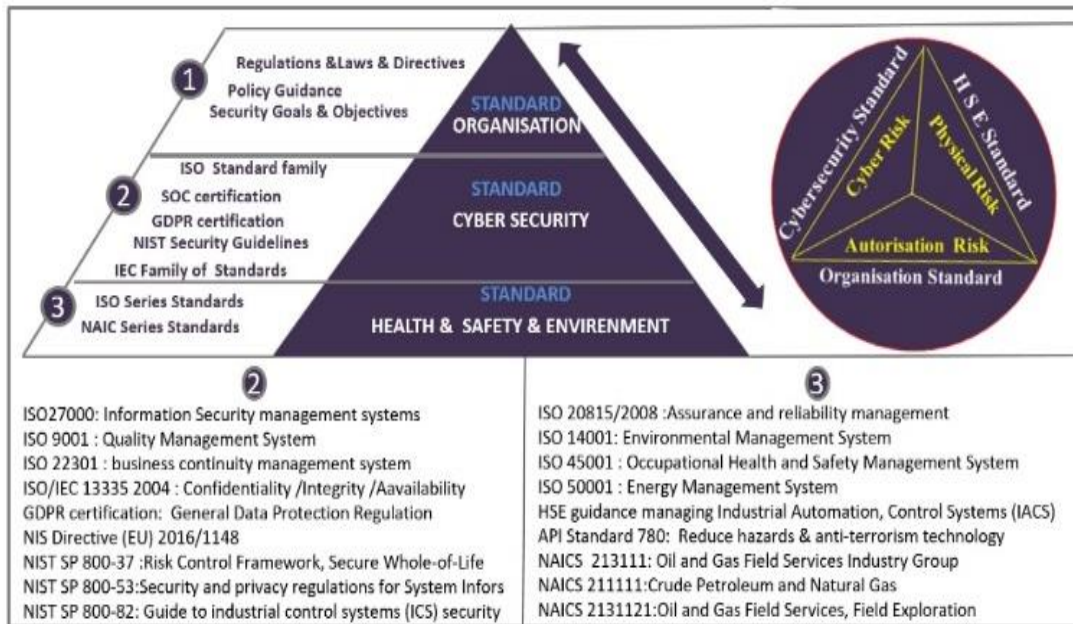


Figure 5. Risk in oil and gas zones and related standards: 1) Organization standards for authorization risks 2) cybersecurity standards for cyber risks; and 3) HSE standards for physical risks

We employed an industrial NGFW with an integrated transparent mode. Traffic is reviewed against ASA firewall policies, such as access rules, in this mode, and any traffic identified for blocking by these policies is dropped. A subset of the traffic is then inspected per FirePOWER inspection policies, and any traffic marked for blocking is deleted.

The implementation of the suggested NGFW integration is based on the following steps:

- (1) Divide ICS and SCADA into network layers based on the ISA-99 standard.
- (2) Select the transparent mode of NGFW.
- (3) Logging and inspection of SCADA protocols and ICS by Next Generation SCADA protocols include Distributed Network Protocol Version 3 (DNP3), which can use TCP, UDP, or both. Another option is Modbus/TCP. c) The Open Platform Communications Unified Architecture (OPC UA).
- (4) Alerts for malformed traffic.
- (5) Configuration tasks are completed via the management client.

The applications of Next-Generation Firewalls (NGFW) include:

- (1) Encryption capabilities.
- (2) Whitelisting.
- (3) VPN.
- (4) Intrusion detection.
- (5) Deep Packet Inspection.

To maintain cyber security and the security lifecycle, the following actions should be completed:

- (1) Upgrading antivirus signatures.
- (2) Applying security updates to Windows servers.
- (3) Using intrusion detection systems (IDS) that can detect malicious or suspicious network activity.

4.2.3 Phase three: Integrate oil and gas industry standards into the security life cycle of oil and gas zones

Organizations in the oil and gas industry are increasingly having to deal with many kinds of threats. We proposed in this phase to integrate oil and gas standards into the security life cycle of oil and gas zones. We previously classified risks in

the petroleum industry as physical, cyber, and authorization. Figure 5 (assembled by the authors) depicts the risks and related standards for the oil and gas perimeter.

We divided the oil and gas perimeter into three virtual axes: perimeter access, physical perimeter, and cyber perimeter. This phase proposes the protection of those axes and the key standards that may relate.

Protection of perimeter access. There is a requirement for technological measures that monitor entry into petroleum zones. Physical access or logical access is possible, and the organization should address authorization protection.

All oil and gas companies have rules, laws, policies, guidelines, and directives that help them achieve their security goals and objectives. Securing logical access includes authentication procedures, ACLs inside network components, intrusion detection and prevention systems (IDS and IPS) signatures, and situational awareness tools.

For securing physical access, organizations may use the following common procedures to avoid unwanted physical access to perimeters and system impacts:

- (1) Forbid unauthorized physical access to critical locations.
- (2) Forbid unauthorized physical modification, manipulation, theft, or other removal or damage of existing systems, infrastructure, or communications interfaces.
- (3) Forbid unauthorized communication eavesdropping, or other potentially detrimental impact, such as a USB memory device, wireless access point, Bluetooth, or cellular device.
- (4) Manage access to the ICS and server rooms.
- (5) Physical access requires multifactor authentication (key card, card-and-personal identification number (PIN), or biometric).
- (6) Employing cameras and motion detectors to monitor entry.
- (7) Notifying of any device manipulation, such as power removal, device resets, cabling modifications, or the addition or use of removable media devices.

Protection of Physical Perimeter. It is vital to address the

physical protection of the petroleum zone, its components, infrastructure, and humans as part of the overall security of the zone's environment.

Many zone facilities' security is strongly linked to safety, with the primary purpose of keeping people out of potentially hazardous circumstances while allowing them to conduct their jobs or carry out emergency measures. Physical security controls are any physical measures mandated by organizational rules and directives in accordance with the oil and gas industry's HSE standards.

The key standards for the protection of the physical perimeter are:

(1) ISO 45001/2018: The worldwide standard ISO 45001 for occupational health and safety helps shield workers and guests from illnesses and accidents related to their jobs.

(2) API Standard 780 is employed by pipeline operators, which makes it easier to conduct security risk assessments (SRAs), which are intended to identify and reduce hazards. Approved as a suitable anti-terrorism technology by the Department of Homeland Security (DHS).

(3) HSE guidance on managing Industrial Automation and Control Systems (IACS).

Protection of the cyber perimeter. Communication breakdowns and cyberattacks are threats that SCADA and ICS systems must overcome to maintain their safety and dependability. In order to guarantee that SCADA systems in the oil and gas sector are reliable and safe, Gosnadzor [68] offered an examination of the fundamental security and reliability design process. To ensure the design of safe SCADA and ICS, as well as secure operation in oil and gas zones, the IT and OT security lifecycles in the oil and gas sector should be maintained and accorded with a set of security standards.

The key standards of cyber security are:

(1) The NIST Cybersecurity Framework is the preeminent framework utilized by organizations across all industries; natural gas and oil companies are increasingly focusing enterprise-wide programs on the NIST CSF. It was used to strengthen critical infrastructure security.

(2) (ISO) 27000: The most well-known standard in the family, it specifies the standards for information security management systems.

(3) ISO 9001: Quality Management System.

(4) The International Electrotechnical Commission's (IEC) 62443 is a leading set of standards for industrial control systems (ICS) security. It is widely used in the oil and gas sector and may be used for any kind of ICS.

(5) SOC certification: system and organization controls.

(6) GDPR certification: General Data Protection Regulation.

(7) NIS Directive (EU) 2016/1148.

To carry out this phase:

(1) Safety procedures and processes need to be defined, including safety procedures for various operations within the perimeter, such as drilling, transportation, and refining. Develop an emergency response plan for various eventualities, such as spills, fires, and accidents. Provide employees training on safety measures and risk awareness.

(2) Compliance: Implement local and international HSE rules and perform regular audits and evaluations.

(3) Measurement: Create customized methods to monitor HSE performance and conduct regular inspections, assessments, and audits.

4.3 Challenges

Integrating several oil and gas standards into the security life cycle of zones presents substantial challenges. There is a link between applying safety and cybersecurity requirements and Petroleum and Gas Authority legislation and controls.

(1) Objectives and methods: Aligning standard objectives and procedures is a challenging task. HSE standards are focused on standardizing, preventing, and mitigating the impacts of material and hardware failures or systematic errors that can lead to hazardous occurrences and accidents that endanger the environment and human health. The cybersecurity standard focuses on preventing or mitigating the effects of acts that may jeopardize the confidentiality, integrity, or availability of information or systems. The organization standard focuses on preventing or minimizing unwanted access to systems and data within the oil and gas perimeter using access rules, regulations, and laws.

(2) Standards compliance and application should ensure that cybersecurity measures do not impair functional safety performance or vice versa. Some security measures or techniques, such as encryption or authentication methods, may boost security while also adding delay or complexity to the reaction time or availability of the safety function.

(3) It is critical to undertake a holistic review throughout the lifecycle phases to guarantee that oil and gas standards are integrated and consistent with one another. Close collaboration and coordination are required among the various stakeholders involved in the design, implementation, and testing of industrial systems [77]. It also necessitates ongoing monitoring and enhancement of both functional safety and cybersecurity.

5. DISCUSSION

The oil and gas sector faces a variety of hazards, with cyber being one of the most critical due to the industry's reliance on increasingly interconnected IT and OT systems. For Addressing these difficulties and improving oil and gas cybersecurity are vital for protecting critical infrastructure and systems, ensuring safety, and ensuring the industry's operational continuity. We attempted to close the gap in this field by implementing a thorough risk classification for the domain of oil and gas and highlighting existing mitigation and industry best practices.

The security of assets and key infrastructure in the oil and gas industry is challenging, and no clear and practical solution can truly carry and guard against all risks in this field.

In this study, we presented a multifaceted security approach that is divided into three parts, the first of which is the reconfiguration and assessment of infrastructure that may exist in the oil and gas zone.

The second phase will focus on integrating new-generation industrial firewalls into SCADA and ICS systems in the oil and gas industry. This integration aids in the segmentation of the network of zones into levels so that each one can be secured and separated from the others. Firewalls, strong perimeter defenses, intrusion detection and prevention systems (IDS), and secure network topologies can all help to protect critical systems from unauthorized access.

The final phase focused on meeting and strengthening several oil and gas standards, which can significantly aid in managing ever-changing threats.

The proposed security approach's purpose is to protect vital infrastructure, provide business continuity, avoid cyber threats, manage various risks, and monitor and regulate activities in zone networks.

6. CONCLUSION

Industrial cyber security is critical for removing many of the main risks associated with the oil and gas industry's new trends and difficulties. To mitigate risks, it is critical to raise awareness of all types of existing dangers. This paper provides a risk classification for the entire industry of O&G and a classification of risk related to the petroleum cyber-physical system. Both risk classifications seek to aid in the establishment of a framework for assessing the complete risk profile of the oil and gas industry, as well as cyber risk connected to CPS in particular. Such profiles could be used to simplify the careful provision of cyber-related insurance coverage for oil and gas facilities.

The paper also bridges the gap between the risk's awareness and defense by presenting long-term mitigations that aid in protection against risks. The proposed security approach ensures the security of the oil and gas perimeter. This approach considers the interconnectivity of physical and digital components within the oil and gas zone, seeking to comprehensively protect all parts within this perimeter.

The proposed solution is a multifaceted security approach that includes the configuration and evaluation of potential infrastructure in the oil and gas zone as an initial phase. In the second phase, the oil and gas industry's SCADA and ICS systems are integrated with industrial new-generation firewalls. that facilitate the division of the zone network into distinct and secure levels and shield vital systems from unwanted access. The final phase concentrated on achieving and reinforcing compliance with oil and gas standards, which can greatly help in handling constantly evolving risks.

For future work, we are planning on implementing the strategy of zero-trust in the oil and gas industry.

REFERENCES

- [1] Alcaraz, C., Zeadally, S. (2013). Critical control system protection in the 21st century. *Computer*, 46(10): 74-83. <https://doi.org/10.1109/MC.2013.69>
- [2] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J. (2018). A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, 20(4): 3453-3495. <https://doi.org/10.1109/COMST.2018.2855563>
- [3] Giraldo, J., Cárdenas, A., Quijano, N. (2016). Integrity attacks on real-time pricing in smart grids: Impact and countermeasures. *IEEE Transactions on Smart Grid*, 8(5): 2249-2257. <https://doi.org/10.1109/TSG.2016.2521339>
- [4] Zhou, J., Li, L., Vajdi, A., Zhou, X., Wu, Z. (2021). Temperature-constrained reliability optimization of industrial cyber-physical systems using machine learning and feedback control. *IEEE Transactions on Automation Science and Engineering*, 20(1): 20-31. <https://doi.org/10.1109/TASE.2021.3062408>
- [5] Khan, W.Z., Aalsalem, M.Y., Khan, M.K., Hossain, M.S., Atiquzzaman, M. (2017). A reliable Internet of Things based architecture for oil and gas industry. 2017 19th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South), pp. 705-710. <https://doi.org/10.23919/ICACT.2017.7890184>
- [6] Hacquebord, F., Pernet, C. (2019). Drilling deep: A look at cyberattacks on the oil and gas industry. *Trend Micro Research*.
- [7] Dragos. (2019). Global Oil and Gas Cyber Threat Perspective. <https://www.dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf>.
- [8] Lobo, F. (2018). Upstream oil & gas cyber risk: Insurance technical review. *Lloyd's Market Assoc.:* London, UK.
- [9] Radmand, P., Talevski, A., Petersen, S., Carlsen, S. (2010). Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries. 2010 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, WA, Australia, pp. 949-957. <https://doi.org/10.1109/AINA.2010.175>
- [10] DOE. (2011). Risk Management Guide. PM - Office of Project Management Oversight and Assessments. Available at <https://www.directives.doe.gov/>.
- [11] McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.R., Maniatakos, M., Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5): 1039-1057. <https://doi.org/10.1109/JPROC.2015.2512235>
- [12] Stergiopoulos, G., Gritzalis, D.A., Limnaios, E. (2020). Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns. *IEEE Access*, 8: 128440-128475. <https://doi.org/10.1109/ACCESS.2020.3007960>
- [13] Oil and gas extraction - hazards. *Occupational Safety and Health Administration*. <https://www.osha.gov/oil-and-gas-extraction/hazards>, accessed on Nov. 22, 2023.
- [14] Haward, B.M., Lewis, C.H., Griffin, M.J. (2009). Motions and crew responses on an offshore oil production and storage vessel. *Applied Ergonomics*, 40(5): 904-914. <https://doi.org/10.1016/j.apergo.2009.01.001>
- [15] Oldenburg, M., Hogan, B., Jensen, H.J. (2013). Systematic review of maritime field studies about stress and strain in seafaring. *International Archives of Occupational and Environmental Health*, 86: 1-15. <https://doi.org/10.1007/s00420-012-0801-5>
- [16] Chandrasekaran, S. (2016). *Health, Safety, and Environmental Management in Offshore and Petroleum Engineering*. John Wiley & Sons.
- [17] Levantesi, S., Levantesi, S., Bongioanni, M., Bongioanni, M., Olivieri, F., Olivieri, F. (2020). Oil and gas exploration poses severe risks to marine species, better management is needed. *LifeGate*. <https://www.lifegate.com/oil-and-gas-seismic-surveys-risks-to-marine-life>.
- [18] Rink, K., Chen, C., Bilke, L., Liao, Z., Rinke, K., Frassl, M., Kolditz, O. (2018). Virtual geographic environments for water pollution control. *International Journal of Digital Earth*, 11(4): 397-407. <https://doi.org/10.1080/17538947.2016.1265016>
- [19] Mahmoud, M.S., Hamdan, M.M., Baroudi, U.A. (2019). Modeling and control of cyber-physical systems subject

- to cyber attacks: A survey of recent advances and challenges. *Neurocomputing*, 338: 101-115. <https://doi.org/10.1016/j.neucom.2019.01.099>
- [20] Avanzini, G.B., Spessa, A. (2019). Cybersecurity verification approach for the oil & gas industry. In *Offshore Mediterranean Conference and Exhibition*, Ravenna, Italy.
- [21] Taylor, J.M., Sharif, H.R. (2017). Security challenges and methods for protecting critical infrastructure cyber-physical systems. In *2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, Avignon, France, pp. 1-6. <https://doi.org/10.1109/MoWNeT.2017.8045959>
- [22] Finkle, J., Finn, T., Wagstaff, J. (2016). Shamoon virus returns in Saudi computer attacks after four-year hiatus. Reuters. <https://www.reuters.com/article/us-cyber-saudi-shamoon-targets-idUSKBN13Q4AX/>.
- [23] Wilhoit, K. (2016). Killdisk and BlackEnergy Are Not Just Energy Sector Threats. Online: <http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats>.
- [24] Dib, A., Ghazi, S., Mehdi, M.M.S. (2023). Ransomware attack detection based on pertinent system calls using machine learning techniques. *International Journal of Computer Networks & Communications (IJCNC)*, 15(4): 123-145. <https://doi.org/10.5121/ijcnc.2023.15408>
- [25] Kamal-Deen, A. (2015). The anatomy of Gulf of Guinea piracy. *Naval War College Review*, 68(1): 93-118.
- [26] Murphy, M.N. (2007). Small boats, weak states and dirty money: Contemporary piracy and maritime terrorism's threat to international security. Doctoral dissertation, Reading University.
- [27] Nincic, D. (2009). Maritime piracy: Implications for maritime energy security. *Journal of Energy Security*, 3(1).
- [28] Lee, C.Y. (2018). Oil and terrorism: Uncovering the mechanisms. *Journal of Conflict Resolution*, 62(5): 903-928. <https://doi.org/10.1177/0022002716673702>
- [29] Amir-Heidari, P., Maknoon, R., Taheri, B., Bazyari, M. (2016). Identification of strategies to reduce accidents and losses in drilling industry by comprehensive HSE risk assessment—A case study in Iranian drilling industry. *Journal of Loss Prevention in the Process Industries*, 44: 405-413. <https://doi.org/10.1016/j.jlp.2016.09.015>
- [30] Gol Mohammadi, N., Paulus, S., Bishr, M., Metzger, A., Könnecke, H., Hartenstein, S., Weyer, T., Pohl, K. (2014). Trustworthiness attributes and metrics for engineering trusted internet-based software systems. In: Helfert, M., Desprez, F., Ferguson, D., Leymann, F. (eds) *Cloud Computing and Services Science. CLOSER 2013. Communications in Computer and Information Science*, vol 453. Springer, Cham. https://doi.org/10.1007/978-3-319-11561-0_2
- [31] Mohammed, A.S., Reinecke, P., Burnap, P., Rana, O., Anthi, E. (2022). Cybersecurity challenges in the offshore oil and gas industry: An Industrial Cyber-Physical Systems (ICPS) perspective. *ACM Transactions on Cyber-Physical Systems (TCPS)*, 6(3): 1-27. <https://doi.org/10.1145/3548691>
- [32] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*. US Dept. of Commerce, National Institute of Standards and Technology.
- [33] Kalin, S., Gamal, R.E., Zhdannikov, D. (2019). Attacks on Saudi oil facilities knock out half the kingdom's supply. Reuters.
- [34] Ing. Punzenberger Copa-data GmbH dos vulnerabilities: CISA. Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/ics-advisories/icsa-12-013-01>.
- [35] Krishna Moorthy, U., Anding, D., Ng, C. L., Songli, S., Sahak, S., Baharudin, M.H. (2020). Alternative method to supply pneumatic air to an unmanned platform, in the event of the platform's instrument gas system is on downtime. In *SPE Annual Technical Conference and Exhibition*, p. D031S021R002. <https://doi.org/10.2118/201522-MS>
- [36] Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M.A., Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications*, 101: 18-54. <https://doi.org/10.1016/j.jnca.2017.10.016>
- [37] Zhang, F., Kodituwakku, H.A.D.E., Hines, J.W., Coble, J. (2019). Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, 15(7): 4362-4369. <https://doi.org/10.1109/TII.2019.2891261>
- [38] Iaa1- Operation Copperfield, Nyotron, <https://www.darkreading.com/attacks-breaches/another-cyberattack-spotted-targeting-mideast-critical-infrastructure-organizations>. 2019.
- [39] Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B. (2018). *Mitre att&ck: Design and philosophy*. Technical Report, The MITRE Corporation.
- [40] Zerdazi, I., Fezari, M., Bayart, M. (2019). Evolution and vulnerability in SCADA systems. https://www.researchgate.net/publication/345497237_Evolution_and_Vulnerability_in_SCADA_Systems.
- [41] Tsoutsos, N.G., Konstantinou, C., Maniatakos, M. (2014). Advanced techniques for designing stealthy hardware trojans. In *Proceedings of the 51st Annual Design Automation Conference*, pp. 1-4. <https://doi.org/10.1145/2593069.2596668>
- [42] Jin, Y., Maniatakos, M., Makris, Y. (2012). Exposing vulnerabilities of untrusted computing platforms. 2012 IEEE 30th International Conference on Computer Design (ICCD), Montreal, QC, Canada, pp. 131-134. <https://doi.org/10.1109/ICCD.2012.6378629>
- [43] Gao, W., Morris, T., Reaves, B., Richey, D. (2010). On SCADA control system command and response injection and intrusion detection. 2010 eCrime Researchers Summit, Dallas, TX, pp. 1-9. <https://doi.org/10.1109/ecrime.2010.5706699>
- [44] Kovacs, B. (2023). Hackers can exploit Siemens control system flaws in attacks on power plants. *SecurityWeek*. <https://www.securityweek.com/hackers-can-exploit-siemens-control-system-flaws-attacks-power-plants/>.
- [45] Deresford. (2010). The sauce of utter pwnage. <http://thesauceofutterpwnage.blogspot.com/>.
- [46] Stouffer, K., Falco, J., Scarfone, K. (2011). *Guide to*

- industrial control systems (ICS) security. NIST Special Publication, 800(82): 16-16.
- [47] iSIGHT Intelligence, F. (2016). Overload: Critical lessons from 15 years of ICS vulnerabilities.
- [48] Ádámkó, É., Jakabóczy, G., Tamás, S.P. (2018). Proposal of a secure modbus RTU communication with Adi Shamir's secret sharing method. *International Journal of Electronics and Telecommunications*, 64(2): 107-114. <https://doi.org/10.24425/119357>
- [49] Sayegh, N., Chehab, A., Elhadj, I.H., Kayssi, A. (2013). Internal security attacks on SCADA systems. In 2013 Third International Conference on Communications and Information Technology (ICCIT), Beirut, Lebanon, pp. 22-27. <https://doi.org/10.1109/ICCITechnology.2013.6579516>
- [50] Valasek, C., Miller, C. (2014). Adventures in automotive networks and control units. Technical White Paper, IOActive.
- [51] Nelson, T., Chaffin, M. (2011). Common cybersecurity vulnerabilities in industrial control systems. Control Systems Security Program.
- [52] Slowik, J. (2019). Evolution of ICS attacks and the prospects for future disruptive events. Threat Intelligence Centre Dragos Inc.
- [53] Khorrami, F., Krishnamurthy, P., Karri, R. (2016). Cybersecurity for control systems: A process-aware perspective. *IEEE Design & Test*, 33(5): 75-83. <https://doi.org/10.1109/MDAT.2016.2594178>
- [54] Rajput, P.H.N., Rajput, P., Sazos, M., Maniatakos, M. (2019). Process-aware cyberattacks for thermal desalination plants. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, pp. 441-452. <https://doi.org/10.1145/3321705.3329805>
- [55] Wang, C., Fang, L., Dai, Y. (2010). A simulation environment for SCADA security analysis and assessment. In 2010 International Conference on Measuring Technology and Mechatronics Automation, Changsha, China, pp. 342-347. <https://doi.org/10.1109/ICMTMA.2010.603>
- [56] Oman, P., Phillips, M. (2008). Intrusion detection and event monitoring in SCADA networks. In: Goetz, E., Sheno, S. (eds) Critical Infrastructure Protection. ICCIP 2007. IFIP International Federation for Information Processing, vol 253. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-75462-8_12
- [57] Pidikiti, D.S., Kalluri, R., Kumar, R.K.S., Bindhumadhava, B.S. (2013). SCADA communication protocols: vulnerabilities, attacks and possible mitigations. *CSIT*, 1: 135-141. <https://doi.org/10.1007/s40012-013-0013-5>
- [58] Giani, A., Karsai, G., Roosta, T., Shah, A., Sinopoli, B., Wiley, J. (2008). A testbed for secure and robust SCADA systems. *ACM SIGBED Review*, 5(2): 1-4. <https://doi.org/10.1145/1399583.1399587>
- [59] Ciepiela, P. (2016). Digitization and Cyber Disruption in Oil and Gas.
- [60] Johansson, E., Sommestad, T., Ekstedt, M. (2008). Security issues for SCADA systems within power distribution. <https://www.diva-portal.org/smash/get/diva2:495747/FULLTEXT01.pdf>.
- [61] Force, J.T., Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. NIST Special Publication, 800(53): 8-13. <http://dx.doi.org/10.6028/NIST.SP.800-53r4>
- [62] Stergiopoulos, G., Gritzalis, D.A., Limnaios, E. (2020). Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns. *IEEE Access*, 8: 128440-128475. <https://doi.org/10.1109/ACCESS.2020.3007960>
- [63] Shah, R., Kraidi, L., Matipa, W., Borthwick, F. (2022). Investigation of the risk factors causing safety and delay issues in oil and gas pipeline construction projects. In: Batako, A., Burduk, A., Karyono, K., Chen, X., Wyczółkowski, R. (eds) Advances in Manufacturing Processes, Intelligent Methods and Systems in Production Engineering. GCMM 2021. Lecture Notes in Networks and Systems, vol 335. Springer, Cham. https://doi.org/10.1007/978-3-030-90532-3_24
- [64] Khadem, M.M.R.K., Piya, S., Shamsuzzoha, A. (2018). Quantitative risk management in gas injection project: A case study from Oman oil and gas industry. *Journal of Industrial Engineering International*, 14: 637-654. <https://doi.org/10.1007/s40092-017-0237-3>
- [65] Zand, E.D. (2009). Risk analysis in oil and gas projects: A case study in the Middle East. Doctoral dissertation, Massachusetts Institute of Technology.
- [66] Lavasani, S.M., Ramzali, N., Sabzalipour, F., Akyuz, E. (2015). Utilisation of Fuzzy Fault Tree Analysis (FFTA) for quantified risk analysis of leakage in abandoned oil and natural-gas wells. *Ocean Engineering*, 108: 729-737. <https://doi.org/10.1016/j.oceaneng.2015.09.008>
- [67] Fetisov, V., Gonopolsky, A.M., Davardoost, H., Ghanbari, A.R., Mohammadi, A.H. (2023). Regulation and impact of VOC and CO₂ emissions on low-carbon energy systems resilient to climate change: A case study on an environmental issue in the oil and gas industry. *Energy Science & Engineering*, 11(4): 1516-1535. <https://doi.org/10.1002/ese3.1383>
- [68] Gosnadzor (2023). Official site of the Gosnadzor. Available online at <https://www.gosnadzor.ru/>, accessed on February 10, 2023.
- [69] E2-69- Barometer, A.R. (2023). Identifying the major business risks for 2023. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf>.
- [70] Balogun, T.G., Andaila, A.M. (2012). Development and implementation of a health safety and environmental management system in the Qatar petroleum drilling department. In SPE International Production and Operations Conference & Exhibition, Doha, Qatar. <https://doi.org/10.2118/156118-MS>
- [71] Kholidy, H. A. (2021). Autonomous mitigation of cyber risks in the Cyber-Physical Systems. *Future Generation Computer Systems*, 115(10): 171-187. <https://doi.org/10.1016/j.future.2020.09.002>
- [72] Krotofil, M., Gollmann, D. (2013). Industrial control systems security: What is happening? 2013 11th IEEE International Conference on Industrial Informatics (INDIN), Bochum, Germany, pp. 670-675. <https://doi.org/10.1109/INDIN.2013.6622964>
- [73] Chen, X., Zhou, Y., Zhou, H., Wan, C., Zhu, Q., Li, W., Hu, S. (2016). Analysis of production data manipulation attacks in petroleum cyber-physical systems. 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, TX, pp. 1-7. <https://doi.org/10.1145/2966986.2980091>
- [74] Marzooq, A.A., Rashid, H.A. (2023). The impact of

- safety priorities on the economic management of projects: A review. *International Journal of Safety & Security Engineering*, 13(1): 21-29. <https://doi.org/10.18280/ijssse.130103>
- [75] Catelani, M., Ciani, L., Luongo, V. (2013). Safety analysis in oil & gas industry in compliance with standards IEC61508 and IEC61511: Methods and applications. In 2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Minneapolis, MN, USA, pp. 686-690. <https://doi.org/10.1109/I2MTC.2013.6555503>
- [76] Oudina, Z., Derdour, M, Dib, A., Aouidate, A.A. (2023). Model based system engineering for trust SCADA and ICS systems in oil & gas industry. 2023 5th International Conference on Pattern Analysis and Intelligent Systems (PAIS), Sétif, Algeria, pp. 1-8. <https://doi.org/10.1109/PAIS60821.2023.10321993>
- [77] Oudina, Z., Derdour, M. (2023). Toward modeling trust cyber-physical systems: A model-based system engineering method. *International Journal of Advanced Computer Science and Applications*, 14(7): 441-452.