Ingénierie des Systèmes d'Information
Vol. 29, No. 2, April, 2024, pp. 469-478
Journal homepage: http://iieta.org/journals/isi

Identifying and Addressing Trust Concerns in Cyber-Physical Systems for the Oil and Gas Industry

Zina Oudina[1*], Makhlouf Derdour[2], Ahmed Dib[3], Mohamed Amine Yaakoubi[4]

[1] Embedded Systems Laboratory, Computer Science Department, Badji Mokhtar University, Annaba 23000, Algeria
[2] LIAOA Laboratory, Computer Science Department, University of Oum El Bouaghi, Oum El Bouaghi 04000, Algeria
[3] Networks and Systems Laboratory, Computer Science Department, University of Badji Mokhtar Annaba, Annaba 23000, Algeria
[4] Laboratoire de Recherche en Informatique, Computer Science Department, University of Badji Mokhtar Annaba, Annaba 23000, Algeria

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

https://doi.org/10.18280/isi.290208

Received: 4 July 2023
Revised: 25 November 2023
Accepted: 7 December 2023
Available online: 25 April 2024

Keywords:
Cyber-physical systems (CPSs), trust CPS, trust concerns, oil and gas(O&G), risk mitigation

ABSTRACT

Crude oil and natural gas constitute key sources of energy that foster the growth of many other industries and facilitate many facets of modern life and the global economy. The Petroleum Cyber-Physical System (CPS) is reshaping the oil and gas (O&G) sector environment. Considering how much output data an oil well generates, the global view of the oil field is assisted by petroleum CPS efficiency techniques. Several risks face the energy industry and have the ability to disrupt crucial supply lines, harm the environment, and precipitate a financial crisis. Those risks involve communication breakdowns, cyber-attacks, environmental dangers, and human errors. Business risks include supply and demand hazards as well as pricing depending on geopolitical and economic factors. The scientific community is concentrated on how to build a confident and modern CPS. Definitions of concerns, the causes of fears of all kinds, and a practical defensive plan are absent from the literature on petroleum and natural gas. Also, cyber security for oil and gas assets has yet to be extensively studied. This study presents the general trust concerns in CPS as well as their extension to the context of the oil and gas industry. We categorized trust concerns according to several factors, including functional, human, business, and trust. The concerns are presented as a collection of properties, and their connectivity was demonstrated. A concern was classified, and the sources are published papers in the literature as well as best practices reports, directives, and recommendations. This study discovered that identifying and addressing concerns in the oil and gas industry is an essential step for risk management, as well as defense and mitigation techniques, and is a key gadget for improving CPS quality and dependability across this crucial economic sector.

1. INTRODUCTION

Petroleum Cyber-physical Systems (CPS) are currently used in several operations within the oil industry. Petroleum CPS techniques can help with management, production, and exploration [1].

An oil and gas company's product chain is often split into three segments: upstream, midstream, and downstream. While midstream involves the movement and storage of crude oil via pipelines, trains, ships, upstream refers to the procedures involved in oil discovery and production. Lastly, the manufacturing of completed goods downstream.

The integration of various industrial technologies with ICT is made possible by Industry 4.0, which also uses actuators and smart sensors to manage processes in real-time and remotely maintain Supervisory Control and Data Acquisition (SCADA) systems [2, 3]. Additionally, real-time process tracking and equipment control are provided by ICS [4]. CPS in the petroleum industry is capable of precisely simulating fluid flow throughout the entire reservoir and exploiting large field data remotely acquired at production wells [5].

Identifying the concerns and risks is necessary since the energy sector is vulnerable to several hazards that could damage the environment, or cause an economic meltdown. In literature, many concerns within the oil and gas industry are studied. In the study of Petersen et al. [6], reliability, energy usage, and regulation were among the concerns raised by WSN use. They also determined the technological prerequisites for WSN implementation inside the boundaries of the oil and gas sector. Concerns about infrastructure reliability, accidents, and terrorist attacks are presented in the study of Flouri et al. [7]. For safety concern, Sklet [8] present the definition, illustration, analysis, the improvement of safety obstacles during the offshore oil and gas manufacturing and operational phase.

Addressing trustworthiness and reliability in CPS is one way to reduce fears in the petroleum sector. A majority of contributions handled trust and trustworthiness issues from a

security perspective. Oudina and Derdour [9] described a workable and effective MBSE technique for building trust in CPS, offering direction for the reliability analysis procedure. In the study of Anwar and Ali [10], A technique focused on trust to safeguard cyber-physical systems has been proposed. which cited internal trust as elements such as sensors, actuators, and communication networks, and outside trust that is linked to the physical environment of the CPS. In the study of Mohammadi et al. [11], they presented a framework for needs and development techniques that take trustworthiness into account when designing CPS. A trust degree framework for cyber-physical systems is developed and the requirements for each degree are classified. Also, they mentioned the use of this framework in all fields [12].

The confidence in petroleum cyber-physical systems (CPS) and the risks facing the oil and gas sector have been important areas of concern. The focus of the scientific community is on developing a confident and modern CPS. The literature on the petroleum and natural gas industries lacks definitions of concerns and sources of all types of fears, as well as a workable defense strategy. Also, cyber security for oil and gas assets has yet to be extensively studied [13]. There is no defense system that can truly guard against all types of risks while still ensuring the reliability of the petroleum CPS.

Familiarity with fears and fulfillment of requirements should ensure trust as a system quality [12]. Controls against risks that could jeopardize CPS's operations should be built into the system. A set of resources, concerns, risks, or controls should be identified. This procedure is crucial for modeling the security and reliability of CPS [9]. Establishing safe, secure, and trustworthy systems in the oil and gas sector involves identifying and categorizing trust concerns. It is simpler to identify susceptible areas and their causes, as well as to define roles and duties within the oil and gas organization, owing to the classification of concerns. This makes the process of mitigating risk easier.

The goal of this paper is to analyze trust concerns and outline the whole collection of trust fears and needs that lead to the development of the intended trust quality in CPS from the early design phase. Each concern class is a collection of qualities that may be related to one or more aspects, such as human, business, functional, or trustworthy. The specification of the properties set for each fear type reveals the interconnectivity of the categorized trust concerns. The study also addresses the classification of trust concerns in the energy industry and shows how concern identification can aid in risk mitigation.

The remainder of the paper is: Section 2 gives an overview of trust in cyber-physical systems. Section 3 presents the classification of trust concerns for cyber-physical systems. In Section 4, the trust concerns for cyber-physical systems in the O&G industry are presented. Section 5 shows how concern identification can help with risk mitigation. Section 6 presents the paper's conclusion.

2. OVERVIEW OF TRUST CYBER PHYSICAL SYSTEMS

Many definitions exist for a trusted system, including the degree to which it enforces a given security policy and has been trusted by the user, who feels secure using it and trusts it to complete tasks without surreptitiously executing harmful or illegal applications.

A trust system is a protection mechanism that operates on a level-based security framework. Creating a secure system is always an objective; this system will be trusted or trustworthy to some degree, depending on its characteristics ("Ola Flygt"; "Linnaeus University").

If the requirements of availability, confidentiality, integrity, and security and safety are satisfied, a cyber-physical system is referred to as a trust system. According to their definition [14], trust is the degree of confidence or conviction that the other person will act appropriately and not take advantage of opportunities. The CPS is a system that meets a set of prerequisites as well as compulsory features and proprieties that ensure the CPS's trustworthiness [12].

Petroleum CPS can be manipulated for extraction activities in the oil and gas environment, which might be dangerous and hazardous. It involves lengthy workdays, challenging working conditions, and sophisticated machinery that puts nearby individuals at danger and could seriously injure them. CPS should ensure trust properties such as safety to protect human life, security to protect data confidentiality, and availability to ensure system functionality for an extended period of time.

3. CLASSIFICATION OF TRUST CONCERNS FOR CYBER PHYSICAL SYSTEMS

Trust, as a quality of CPS, is based on a set of functional and non-functional properties and judgments. Whereas the requirements are a translation of the concerns and are avoided and mitigated by achieving the necessary properties of the system, our classification of trust concerns is based on the combination of many aspects:

3.1 Functional concerns

CPS combines computing and physical operations, with physical operations being supervised and managed by networks and embedded computers. In the CPS, diverse equipment are connected via wireless networks. Groups of sensors and actuators are used to establish communication. Therefore, concerns about CPS functionality are related to a variety of aspects and components, including communication, controlling, sensing, and devices.

Functional concerns included: Functionality, physical, communication, control, actuation, sensing, and environment.

- Functionality: The concerns are related to the services provided by a CPS. Some functions are solely physical CPS attributes.
- The communication concerns are related to the exchange of information between the CPS and other entities.
- The controlling concern is about the ability of CPS to control a property of a physical part.
- As critical components of the CPS, actuators and their associated concerns deal with how the CPS can affect change in the physical world.
- The sensing concerns are related to how CPS exploits the physical information collected by sensors to bridge real and cyber spaces.
- Interaction of CPS functionality with the domain and industry environment.

3.2 Human concerns

The human is the important actor that confirms the trustworthiness of CPS, and its requirements ought to be in accordance with the needs of the user [12]. The fear is that when utilizing the system, the user will be made aware of any discrepancies between the system's development and their requirements. This could cause the user to lose faith in the system and ultimately reject it. Human concern includes the following attributes:

- Interaction: How humans interact with the complexity of CPS. The interfaces improve the learning and human interaction.
- Usability: How CPS is used by humans.
- Satisfaction: How CPS achieves its functional goals successfully and the contentment of users (ISO 9241-210).

3.3 Business concerns

The business is liable for the foundational aspects and expenses required for CPS development, as well as the cost of training staff members. Accreditation is mandatory for the cyber physical system to ensure its regulation. Time to market is another business concern because it is tied to the availability of CPSs and their deployment.

- Regulation: regulation and accreditation requirements.
- Time to market: the length of time needed to bring a CPS from need realization to deployment.
- Cost: foundational or monetary requirements by the CPS throughout its development cycle.

3.4 Trust concerns (trust as a qualities)

According to the trust degrees framework [12], we divided the set of trust concern into three subsets (security, trustworthy, trust).

3.4.1 CPS security concerns

(1) Safety concerns about capacity of the CPS to guarantee that there won't be any disastrous effects on the lives, health, property, or data of stakeholders, or the natural environment.

(2) Security concerns about the capacity of the CPS to guarantee that every one of its procedures, systems, and services is shielded from unauthorized and unintentional access, alteration, harm, loss, or use, either internally or externally. As security sub-properties:

- Confidentiality: Maintaining approved access and disclosure limitations.
- Integrity: Protection against improper system change or destruction, including non-repudiation and authenticity.
- Availability: The ability to access and use a system in a timely and dependable manner.

3.4.2 CPS trustworthy concerns

(1) Privacy concerns about the CPS's ability to prevent entities (humans, computers) from accessing data that is created, stored in, or transited through a CPS or any of its elements; privacy plays a vital role in enhancing the credibility of the system. Users have access to and control over their personal information.

(2) Performance: The ability of the CPS to reach needed operational targets and the quality that characterizes how well a service performs. The extent to which a system or element performs its intended activities within specified restrictions, like quickness, precision, or memory utilization (IEEE-610.12) [15].

(3) Dependability: a grouping of sub-properties (Accuracy, Availability, Robustness, Reliability, Scalability, and Maintainability). The capability is supported by the service it provides. A proper and predictable execution was performed as expected. There are various aspects to dependability, including:

- Availability: Ready for application
- Reliability: Uninterrupted provision of services
- Safety: Not experiencing disastrous effects on the environment
- Confidentiality: Absence of information distribution that is not authorized
- Integrity: Absence of inappropriate information tampering
- Maintainability: Ability to adapt and change
- Compatibility: Concerns about the connectivity between hardware and software from various sources without requiring changes

3.4.3 Trust concerns

(1) Usability fears about the ability of CPS to be effectively employed to satisfy operational objectives and user needs (adapted from ISO 9241-210.) Complex systems combining physical and cyber components make it harder to meet usability norms.

(2) Correctness entails system behavior that complies with user requirements, such as user expectations on trustworthiness and standards.

Table 1. The related properties for each concern type

Concern	Factors	Related Properties
Functional	CPS Functionality	Dependability, Performance
	Physical	Maintainability, Reliability
	Communication	Integrity
	Sensing	Dependability
	Actuation	Dependability
	Control	Dependability
Human	Interaction	Learnability
	Usability	Effectiveness
	Satisfaction	Efficiency of use
Business	Regulation	Security (compliance, Assurance)
	Time to market	Dependability (availability, reliability)
	Cost	Utility, Value (computing value equals utility divided by costs)
	Quality	Usability (satisfaction, learnability, effectiveness, efficiency of use)
Trust	Security	Safety, Security
	Trustworthy	Privacy Performance Dependability Compatibility
	Trust	Usability Correctness

Table 1 presents the related properties for each concern type.

Some properties can be part of and related to many concerns at the same time, such as performance and dependability, which are related to functional and trustworthy concerns. The interconnection of concerns is presented in Figure 1.

Each type of concern is a set of properties, and the merger of this trust concern can be presented as the union of many groups of trust properties that should meet to guarantee the trust quality in CPS. Our proposed formula is expressed as follows:

- Ct: The total of trust concerns
- Cf: Functional concerns (properties of CPS required by functional concern)
- Cb: Business concerns (properties of CPS required by business concern)
- Ch: Human concerns {properties of CPS required by human concern}
- Ctr: Trustworthiness concern as quality {properties of CPS required by trustworthiness concern that divided into three subset: Secured, trustworthy, trusted}

$$Ct = Cb \cup Ch \cup Ctr \cup Cf \quad (1)$$

The multiplicity of concerns is defined as the union of groups. The composition of a set of concerns is interpreted as the sum of the properties required by each concern in the set.

- Sp: Set of properties
- P: Property
- n: Total number of trust properties

$$SP = \sum_{k=0}^{n} P \quad (2)$$

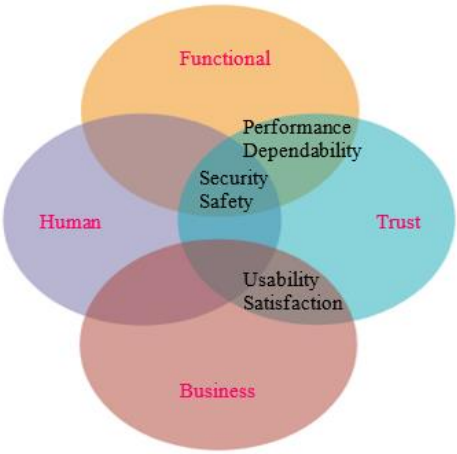

Figure 1. Concerns intersection

4. TRUST CONCERNS IN CYBER-PHYSICAL SYSTEMS FOR THE O&G INDUSTRY

We tried to identify trust concerns in the context of the oil and gas industry using the prior classification of trust concerns in CPS.

4.1 Human concerns for O&G

Projects in the oil and gas industry have the possibility to be hazardous to people, property, and the environment if they are not controlled and regulated [16]. There are obvious human security and safety risks linked to oil and gas production. Oil leaks and gas flaring are two major threats to human security [17] and directly impact their safety. Some hazards, such as natural hazards [18], which are harmful due to geographic and climatic factors, represent a serious risk to anyone working in this sector.

As far as the human aspect is concerned, the complicated nature of the drilling process dictates numerous dangers. Many studies [19-22] consider that human mistake has greatly contributed to the exacerbation of drilling incidents, and that drilling events are caused by people.

Humans are a key actor in trust quality; from the side, they are the final users of the system, and in this case, they will judge the functionality and quality of CPS, which is related to satisfaction propriety that is included in trust concern. On the other side, if the user of CPS is an employee in the oil and gas industry, he will interact directly with CPS, and if there is an error in system operation or a lack in the user's learnability, here we talk about usability and learnability properties that relate to trust concerns.

The concern related to the human factor in this case has two aspects: the first is the fear for the human being in terms of his safety and security. The second aspect is the fear of him and the mistakes he makes, whether he is a worker in the oil field or a dealer from near or far.

4.2 Trust concerns for O&G

4.2.1 Security concern for O&G

Security concerns may be classified in several ways based on different criteria. The big fear is attacks, which can come from a variety of sources: individuals or organizations, internal or external, or a combination of both. Our classifications for security concerns are as follows:

(1) Cyber fears

Petroleum firms are increasingly digitizing systems and integrating new technology to boost efficiency and profitability. This puts firms at risk of cyberattacks that aim to extort money, disrupt business processes, capture intellectual property, and capture employee personal information. Cyber-attack classification in the study of Mahmoud et al. [23] is: assaults such as replay, misdirection, and denial of service (DoS).

Attacks in the O&G sector aim to compromise the operation area [24]. The majority of attacks jeopardize security features. By overloading the connected device with requests, denial of service (DoS) attacks jeopardize system availability by blocking legitimate requests and jamming communication channels [25].

Researchers and specialists in the oil and gas industry illustrated the impact of utilizing protocol networks and systems, such as SCADA, PLC, and RTU, and highlighted their susceptibility to this sector [26, 27]. the concern about hardware and software and untrusted computing platforms [28, 29]. The fears of hardware trojans and attacks on plants within operational bounds. Another concern is the use of unsecured MODBUS/TCP protocols for equipment operation by regional SCADA systems, which lacking encryption and network separation. Another critical aspect of security is staff awareness. The primary attack methods in this field seem to be information spoofing and email phishing.

(2) Safety fears

The CPS's capacity to guarantee that there won't be any disastrous effects on stakeholders' lives, health, property, or data, as well as the natural environment, is a key component of safety. Process companies must prioritize safety, and IEC 61508 is widely recognized as a fundamental safety standard that cuts across all sectors of the economy.

Extraction of gas and oil can be hazardous. Long hours, challenging working conditions, and complicated machinery that can malfunction and seriously hurt bystanders are all necessary. Therefore, the businesses need to put strong safety management and monitoring procedures in place.

The activities of the energy sector have a direct impact on

the environment, giving rise to concerns about oil spills, solid and hazardous waste, greenhouse gas emissions, and climate change.

Incidents involving oil leaks happen during the offshore petroleum industry's exploration and transportation phases. The concern with oil spills is that they greatly contaminate the ocean, which leads to a host of negative effects on the ecology and economy [30].

(3) Piracy fears

Piracy is geographically associated [31], and it is driven by a variety of circumstances, including an unstable political climate, weak government, impoverishment, an underdeveloped economy, and the capacity to reward to thrive [32]. The Gulf of Guinea had developed as a major location for piracy and attacks on offshore installations by 2007 [33]. Piracy on Africa's east coast has also had an impact on the offshore petroleum business.

(4) Terrorism fears

Oil-producing countries are vulnerable to terrorism because they are crucial objectives for terrorists who may strike oil installations to have a greater impact and harm powerful countries' outside interests. It uses statistics on terrorist occurrences and oil revenue [34].

4.2.2 Trustworthiness concern for oil and gas

The trust concerns are interconnected with functional concerns and share two attributes (performance and dependability), as mentioned in the previous section. As with human concerns, it shares security and safety attributes. The additional attributes that are specified for trust quality are usability and correctness. To specify the fears, we have to identify the stockholders and the interactors with the entire system of oil and gas. Figure 2 presents the stockholder use case diagram for oil and gas.

The usability that is related to human concerns and fears is how all activities in all phases, such as production, transportation, and refinery, achieve their functional objectives effectively.

4.3 Functional concerns for O&G

A vast number of devices, including sensors and actuators, are embedded in an industrial cyber physical system to increase the execution of supervision and tracking in real-time [1].

Remote multi-sensing technology is employed during oil exploration and transportation for emerging services. By allowing the underwater simulation of an offshore petroleum CPS, it can be used for identifying leaks [35].

The fear is the unfunctionality of sensors and actuators that are dedicated to sensing leaks and spills.

One of the major physical-level issues with these networked and embedded devices in ICPS is reliability. It is a strict prerequisite for dependable performance and an extended lifespan.

Oil production offshore, for example, is typically at remote sites that necessitate remote access and control. This is accomplished by combining ICPS, Supervisory Control and Data Acquisition (SCADA), and IIoT technologies. Any failure has an effect on the global functionality.

4.4 Business concerns

4.4.1 Fears supply and demand

Oil and gas enterprises are exposed to the risk of market and supply disruptions, especially as energy facilities need a substantial amount of capital and time to reach maximum capacity. Any disruption in the global supply of oil and gas (O&G) is a cause for concern since it impacts oil prices and, consequently, the worldwide economy [36]. It's also difficult to manage operations when prices are rising and falling. Other economic factors are also important, as financial crises can drain money regardless of price hazards.

4.4.2 Financial fears

Gas and oil are goods, and market prices are erratic. The cost of extracting and processing natural resources is a major factor in their price, in addition to the cost of the raw materials altogether.

Oil and gas firms must consequently hedge their risks by investing in options, futures, puts, and other financial instruments to lessen the chance that price volatility may cause the business to operate at a loss for extended periods of time.

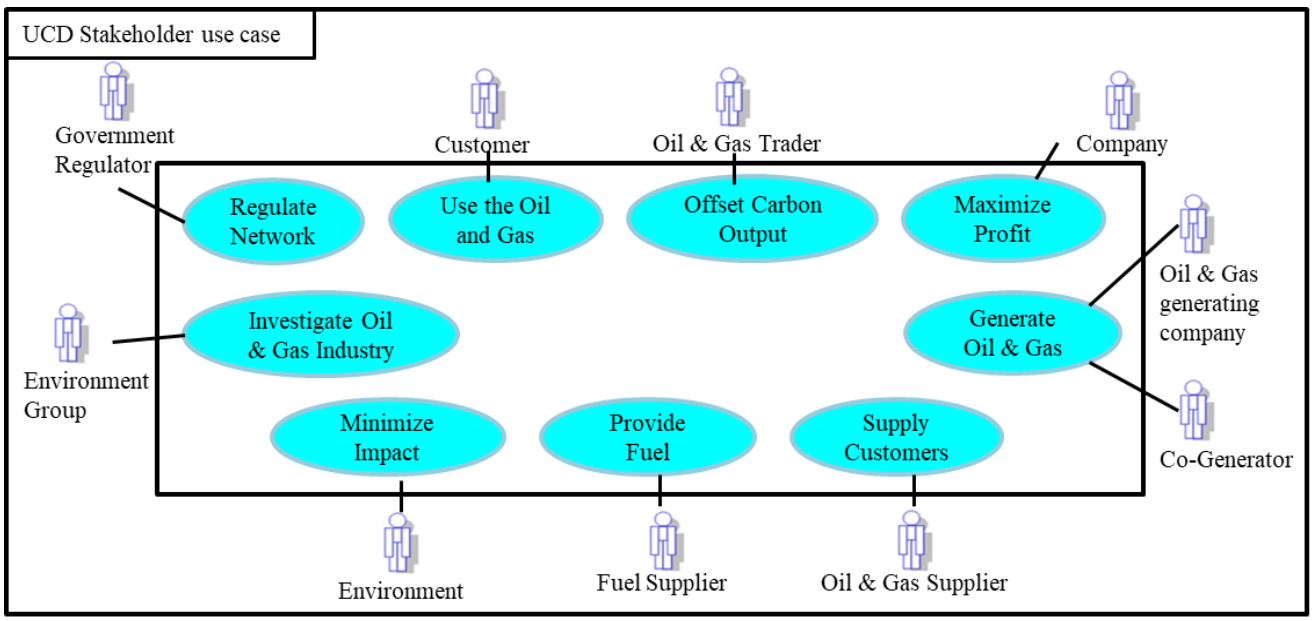

Figure 2. Stakeholders use case diagram

5. MITIGATION OF THREATS AND RISKS IN THE O&G INDUSTRY

5.1 Overview

Risk analysis and effective mitigation are not widely addressed in the literature. There are only reports, directives, and guidance, with no systematic and large collection of all pretentious threats and all kinds of risks in the petroleum industry. Stergiopoulos et al. [37] Stated that the O&G industry has not yet had a systematic method for mapping, cataloging, and categorizing cyber security threats. They also provided evidence that oil and gas OT infrastructure is susceptible to cyberattacks, as demonstrated by historical events. However, many surveys highlight the risks and the mitigation of those risks in different ways and with different targets, such as the study of Stergiopoulos et al. [37]. The weaknesses, possible dangers, and mitigation measures for CPS are detailed in the study of Alcaraz and Zeadally [38]. An experiment designed to find weaknesses in SCADA protocols was introduced by Sayegh et al. [39]. According to another survey, testbeds are usually used to demonstrate data acquisition for production and maintenance, as well as to establish security in energy systems [40]. Miller and Rowe [41] reviewed industrial systems by conducting real-world cyber-security incidents against SCADA systems and classifying the attacks, attack methods, and potential impact. A survey of vulnerabilities linked to ICS security, protocols (Modbus/TCP, DNP3, IEC 61850), and sensors/actuators was provided by Krotofil and Gollmann [42]. Security solutions were also suggested to mitigate these risks.

5.2 Some mitigation directives and reports

One recommended best practice is the European Parliament and Council's directive (EU) 2016/1148, which is about "concerning measures for a high common level of security of network and information systems across the Union" [43]. Furthermore, the European Union released a regulation on cyber security certification for information and communications technology [44] 2019/881 of the European Parliament and of the Council.

Other important documents include the European Parliament's 2012/18/EU directive (SEVEZO-III) [45], which underlines fundamental principles for dealing with threats and repercussions from many types of situations, including cyber-attacks on industrial systems.

Some key reports also place a strong emphasis on the digitalization of the oil and gas sector, as well as the use of IoT and smart meters to automate monitoring and control. [46] Provides an illustration of the current global picture, including notable cases, their repercussions, general hurdles, and some mitigation measures, Deloitte [47], and PWC [48], and concentrating explicitly on the O&G sector. Assessing vulnerability to prioritize cyber investments was advocated by Deloitte [47].

For industrial control system (ICS) security, the National Institute of Standards and Technology (NIST) detailed in the study by Stouffer et al. [49] how firms should establish and implement an ICS security program and ICS security plans. It outlined how programs should be aligned with and integrated with current programs, policies, and expertise of IT security. It is frequently recommended to create particular requirements for ICS technology and its surroundings. It is also advised that businesses evaluate and revise their ICS security policies and processes periodically to account for modifications to norms, laws, practices, technology, and facility security requirements.

5.3 Some mitigation strategies

5.3.1 Mitigation for human fears

According to the majority of statistics, operator error on the part of the human or illegal operation causes mishaps. As a result, the petroleum sector ought to enhance employee training and take part in a range of promotion, assessment, and outreach initiatives.

5.3.2 Mitigation for safety fears

It is strongly advised that the O&G industry adhere to standards. In order to make the approaches understandable to design engineers, they illustrate IEC61508 compliance in OIL and GAS applications, with a particular emphasis on steam turbines, and provide a methodology for reliability analysis of complex safety instrumented systems [50].

Marzooq and Rashid's study [51] explored strategies for increasing awareness of safety-related concerns and shown how people's consciousness and behaviors greatly influence their safety, actions, and ability to manage hazards at work.

5.3.3 Mitigation for security fears

Security and privacy, intrusion and anomaly detection, and malware mitigation are proposed by Chen et al. [5]. Organizations should implement strict authentication and authorization procedures for all program units and all employees to reduce the risk of authorized access.

Some suggested methods for reducing the risks in ICS include adding firewalls to ICS interfaces to protect against a variety of concerns [52] and keeping an eye on the safeguarding environment that surrounds the systems is an important technique for supporting conventional network protection and authorization mechanisms, including the design and implementation of security.

5.3.4 Other mitigations

Stergiopoulos et al. [37] suggested more approaches that are used in the oil and gas industry to mitigate and control vulnerabilities. These include updated and patched field equipment, reliable procurement procedures, and measures against tampering. Securing the network and employing many technologies, including network segmentation, penetration testing, encryption, and internal auditing.

How can the identification of concerns help to mitigate risks and enhance the CPS' trustworthiness in the O&G industry?

The identification of potential risks that could affect user trust and the implementation of appropriate policies to reduce the threats play key roles in maintaining and monitoring system quality and trust characteristics.

In the study by Oudina et al. [53], a long-term mitigation security strategy for the oil and gas perimeter is described. is a holistic security approach that starts with the possible infrastructure configuration phase in the oil and gas zone. In the second stage, industrial new-generation firewalls are integrated with the petroleum SCADA and ICS systems. The last phase focused on establishing adherence to oil and gas standards, which can be very helpful in managing risks that are continuously increasing.

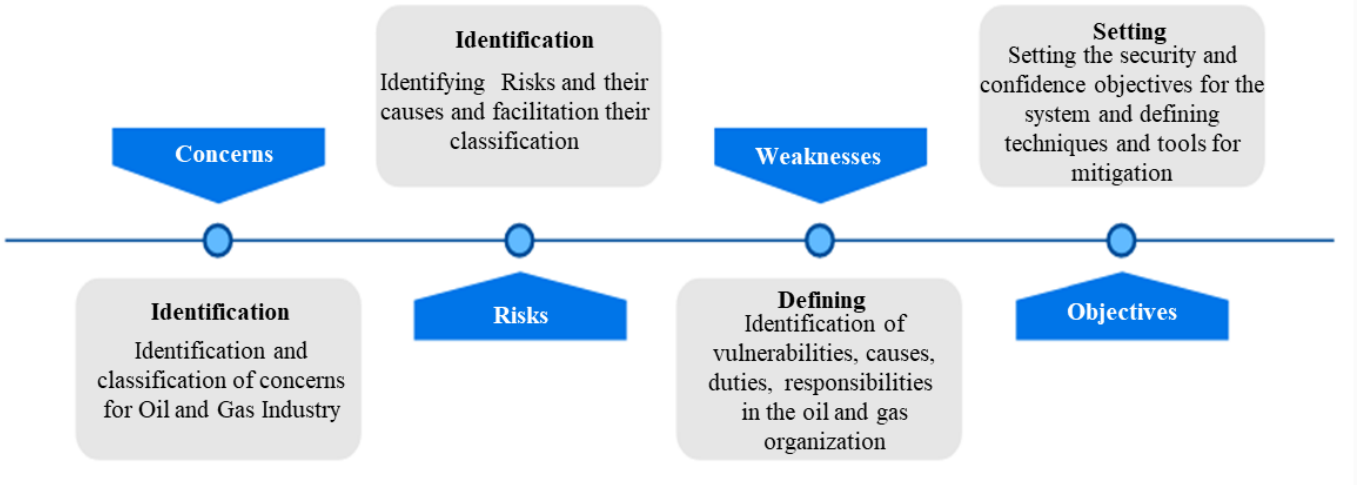

Figure 3. Initial Stage in the development of a general security and confidence plan

Experts in the field of oil and gas consider good practices in all phases of the development life cycle of oil and gas projects as a tool to lower risks. For this reason, the identification of concerns in this industry is a mandatory task for risk management as well as defense and mitigation strategies.

Classifying fears is the first step to understanding the risks surrounding the system, as well as the first step to identifying risks and their causes. Risk classification facilitates the identification of areas of vulnerability and their causes, as well as the definition of duties and responsibilities in the oil and gas organization. Assuming that this classification is thorough and aware of all immediate threats and all factors and aspects related to them directly or indirectly, following the previous steps, the stage of setting the security and confidence objectives for the system and the organization will occur. Then it is feasible to find the security spots that were previously deemed loopholes and weaknesses. The necessary security measures and strategies, as well as how to employ them, should be identified. Also, don't forget to provide essential supervision and learning for the human element involved in this task at this stage. Figure 3 displays our proposal as an initial and partial stage in the development of the general security and confidence plan for the oil and gas cyber system.

Trustworthiness can be ensured by constantly checking the system's characteristics, proper operation, and compliance with all requirements of those involved with it, as well as by constantly guarding against risks and implementing policies to mitigate and reduce expected and unexpected attacks. Furthermore, robust security measures requiring highly specialized scientific competencies must be implemented.

6. CONCLUSIONS

This study analyzes trust concerns by describing the whole range of trust concerns and requirements. The concerns are classified into human, business, functional, and trust, which include safety and security and trustworthy. Each concern class is a collection of qualities that may be related to one or more classes. The groups of trust properties should meet in the development of CPS to guarantee their trust quality. Also, the connectivity of the classified classes was demonstrated.

We extended the categorization of fears to the oil and gas sector. The properties of CPSs are influenced by this industrial environment. The environment may be hazardous and harmful. Long hours, hard working conditions, and complicated machinery can endanger humans. CPS should ensure trust characteristics such as safety to protect human life, security to safeguard data confidentiality, and availability to assure long-term system functionality.

The requirements are a translation of the concerns, and they are avoided and minimized by attaining the required CPS properties. Defining the concerns surrounding the cyber system in a critical industry, such as gas and oil, is an important key in the design of CPS from the start, as it aids in the development of safety, security, and trust characteristics throughout the design life cycle.

We consider that the identification of trust concerns and threat awareness, along with excellent practice in all phases of oil and gas development, are the pillars of the identification of security and trustworthiness objectives and a risk-mitigation plan. Recognizing anxieties and threats facilitates the use of suitable preventative measures and solutions for safety and security weaknesses for CPS and within its environment.

The development of petroleum cyber physical systems and maintaining their dependability and confidence within a secure oil and gas perimeter are challenging due to a variety of reasons, such as the increasing complexity of SCADA, ICS, and cyber physical systems (CPS); the intricate nature of the oil and gas industry; the increasing risk and attacks in that industry; the development of attack techniques and tools; and the difficulty of foreseeing unanticipated threats.

Our futur work will present a multi-level security method for the oil and gas perimeter. This method considers a trust architecture for petroleum cyber physical systems and a zero-trust strategy that encourages continual verification for offering sustainable security within the oil and gas zone. The goal is to thoroughly protect all components within the perimeter and protect access.

REFERENCES

[1] 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
[2] 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
[3] 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
[4] 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
[5] 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. In 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), IEEE, pp. 1-7. https://doi.org/10.1145/2966986.2980091
[6] Petersen, S., Doyle, P., Vatland, S., Aasland, C.S., Andersen, T.M., Sjong, D. (2007). Requirements, drivers and analysis of wireless sensor network solutions for the Oil & Gas industry. In 2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007), Patras, Greece, pp. 219-226. https://doi.org/10.1109/EFTA.2007.4416773
[7] Flouri, M., Karakosta, C., Doukas, H., Psarras, J. (2009). Review & analysis of oil & gas incidents related to the supply interruptions. In 2009 3rd International Conference on Energy and Environment (ICEE), IEEE, Malacca, Malaysia, pp. 171-176. https://doi.org/10.1109/ICEENVIRON.2009.5398652
[8] Sklet, S. (2005). Safety barriers on oil and gas platforms. Means to Prevent Hydrocarbon Releases. Doctoral theses at NTNU, Fakultet for Ingeniørvitenskap og Teknologi. http://hdl.handle.net/11250/241291.
[9] 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). https://doi.org/10.14569/IJACSA.2023.0140748
[10] Anwar, R.W., Ali, S. (2012). Trust based secure cyber physical systems. In Workshop Proceedings: Trustworthy Cyber-Physical Systems, Tech Report Series.
[11] Mohammadi, N.G. (2019). Trustworthy cyber-physical systems: A systematic framework towards design and evaluation of trust and trustworthiness. Springer Vieweg. https://doi.org/10.1007/978-3-658-27488-7
[12] Oudina, Z., Derdour, M., Boudour, R., Dib, A., Yakoubi, M.A. (2023). Trust cyber physical systems: Trust degree framework and evaluation. International Journal of Safety & Security Engineering, 13(2): 213-225. https://doi.org/10.18280/ijsse.130204
[13] Progoulakis, I., Nikitakos, N., Rohmeyer, P., Bunin, B., Dalaklis, D., Karamperidis, S. (2021). Perspectives on cyber security for offshore oil and gas assets. Journal of Marine Science and Engineering, 9(2): 112. https://doi.org/10.3390/jmse9020112
[14] Williamson, O.E. (1993). Calculativeness, trust, and economic organization. The Journal of Law and Economics, 36(Part 2): 453-486. https://doi.org/10.1086/467284
[15] IEEE (1990). IEEE Standard Glossary of Software Engineering Terminology. In IEEE Std 610.12-1990, 1-84. https://doi.org/10.1109/IEEESTD.1990.101064
[16] Achaw, O.W., Boateng, E.D. (2012). Safety practices in the oil and gas industries in Ghana. International Journal of Development and Sustainability, 1(2): 456-465.
[17] Motte, J., Alvarenga, R.A., Thybaut, J.W., Dewulf, J. (2021). Quantification of the global and regional impacts of gas flaring on human health via spatial differentiation. Environmental Pollution, 291: 118213. https://doi.org/10.1016/j.envpol.2021.118213
[18] Rodhi, N.N., Anwar, N., Wiguna, I.P.A. (2017). A review on risk factors in the project of oil and gas industry. IPTEK The Journal for Technology and Science, 28(3). http://doi.org/10.12962/j20882033.v28i3.3217
[19] 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
[20] Norazahar, N., Khan, F., Veitch, B., MacKinnon, S. (2014). Human and organizational factors assessment of the evacuation operation of BP deepwater horizon accident. Safety Science, 70: 41-49. https://doi.org/10.1016/j.ssci.2014.05.002
[21] Strand, G.O., Lundteigen, M.A. (2016). Human factors modelling in offshore drilling operations. Journal of Loss Prevention in the Process Industries, 43: 654-667. https://doi.org/10.1016/j.jlp.2016.06.013
[22] Ergai, A., Cohen, T., Sharp, J., Wiegmann, D., Gramopadhye, A., Shappell, S. (2016). Assessment of the human factors analysis and classification system (HFACS): Intra-rater and inter-rater reliability. Safety Science, 82: 393-398. https://doi.org/10.1016/j.ssci.2015.09.028
[23] 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
[24] Avanzini, G.B., Spessa, A. (2019). Cybersecurity verification approach for the oil & gas industry. In Offshore Mediterranean Conference and Exhibition OMC, Ravenna, Italy, pp. OMC-2019.
[25] 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), IEEE, Avignon, France, pp. 1-6. https://doi.org/10.1109/MoWNet.2017.8045959
[26] 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
[27] Kovacs, B. (2019). 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/, accessed on Nov. 5, 2023.
[28] 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
[29] Jin, Y., Maniatakos, M., Makris, Y. (2012). Exposing vulnerabilities of untrusted computing platforms. In 2012 IEEE 30th International Conference on Computer Design (ICCD), IEEE, Montreal, QC, Canada, pp. 131-134. https://doi.org/10.1109/ICCD.2012.6378629
[30] Rink, K., Chen, C., Bilke, L., Liao, Z., Rinke, K., Frassl, M., Yue, T., 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
[31] Kamal-Deen, A. (2015). The anatomy of gulf of guinea piracy. Naval War College Review, 68(1): 93-118. https://www.jstor.org/stable/26397818.
[32] 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.
[33] Nincic, D. (2009). Maritime piracy: Implications for maritime energy security. Journal of Energy Security, 3(1).
[34] Lee, C.Y. (2018). Oil and terrorism: Uncovering the mechanisms. Journal of Conflict Resolution, 62(5): 903-928. https://doi.org/10.1177/0022002716673702
[35] Wang, Y., Chen, X., Wang, L. (2023). Cyber-physical oil spill monitoring and detection for offshore petroleum risk management service. Scientific Reports, 13(1): 4586. https://doi.org/10.1038/s41598-023-30311-w
[36] 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
[37] 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
[38] 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
[39] Sayegh, N., Chehab, A., Elhajj, I.H., Kayssi, A. (2013). Internal security attacks on SCADA systems. In 2013 Third International Conference on Communications and Information Technology (ICCIT), IEEE, Beirut, Lebanon, pp. 22-27. https://doi.org/10.1109/ICCITechnology.2013.6579516
[40] Oudina, Z., Derdour, M., Bouhamed, M.M. (2022). Testing cyber-physical production system: Test methods categorization and dataset. In 2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS), IEEE, Oum El Bouaghi, Algeria, pp. 1-8. https://doi.org/10.1109/PAIS56586.2022.9946868
[41] Miller, B., Rowe, D. (2012). A survey SCADA of and critical infrastructure incidents. In Proceedings of the 1st Annual Conference on Research in Information Technology, pp. 51-56. https://doi.org/10.1145/2380790.2380805
[42] Krotofil, M., Gollmann, D. (2013). Industrial control systems security: What is happening? In 2013 11th IEEE International Conference on Industrial Informatics (INDIN), Bochum, Germany, pp. 670-675. https://doi.org/10.1109/INDIN.2013.6622964
[43] Wilbrandt-Gotowicz, M. (2018). Numerous forms of actions of public administration authorities as illustrated by the requirement to implement directive (EU) 2016/1148 of the European parliament and council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the union. Opolskie Studia Administracyjno-Prawne, 16(1): 169. https://doi.org/10.25167/osap.1169
[44] European Union. (2019). Regulation (EU) 2019/881 of the European parliament and of the council of 17 April 2019 on ENISA (The European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881.
[45] Directive 2012/18/EU of the European Parliament and of the Council. (2012). Directive 2012/18/EU of the European parliament and of the council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing council directive 96/82/EC. Official Journal of the European Union. 197: 1-37. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:197:0001:0037:en:PDF.
[46] Souza, R. (2014). Cyber risks in the oil & gas industry. Rio Oil & Gas Expo and Conference, pp. 15-18.
[47] Deloitte. (2023). Protecting the connected barrels. Cybersecurity for Oil and Gas, A report by Deloitte Center for Energy Solutions, 2-17. https://www2.deloitte.com/content/dam/insights/us/articles/3960-connected-barrels/DUP_Protecting-the-connected-barrels.pdf.
[48] PWC, (2016), Turnaround and transformation in cybersecurity: Oil and gas. Key Findings from The Global State of Information Security. https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2016-oil%20and%20gas.pdf, accessed on Nov. 24, 2023.
[49] Stouffer, K., Falco, J., Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST Special Publication, 800(82): 16-16.
[50] 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
[51] 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/ijsse.130103
[52] Fabro, M., Gorski, E., Spiers, N., Diedrich, J., Kuipers, D. (2016). Recommended practice: Improving industrial control system cybersecurity with defense-in-depth strategies. DHS Industrial Control Systems Cyber Emergency Response Team.
[53] Oudina, Z., Dib, A., Yakoubi, M.A., Derdour, M. (2024). Comprehensive risk classification and mitigation in the

petroleum cyber-physical systems of the oil and gas industry. International Journal of Safety & Security Engineering, 14(1): https://doi.org/10.18280/ijsse.140110 99