Cybersecurity in complex operations: a post-drilling approach foroil and gas wells

R.A. Perdomo[1], N. I. Serdyuk[2]

[1]Oil and Gas Drilling Department, Oil and Gas Faculty, Ukhta State Technical University, Russia
[2]Department of Modern Well Drilling Technologies, Faculty of Exploration Technology and Development, Russian State Geological Exploration University, Russia

Abstract: Many companies are now working to converge business models and engineering processes with the technologies of the fourth industrial revolution. The automation of industrial processes together with the implementationof infrastructure,makes it possible to interconnect people and performance indicators in real-time, reducing the decision-making time and time in the marketplace. This provides companies with unprecedented opportunities to create and capture value while rethinking business models but brings vulnerabilities and risks that must be properly assessed and mitigated. New malicious third parties are emerging and directly threaten the efforts of companies. The purpose of this article is to enumerate the possible attackers (vectors) and to define the possible areas where they can attack companies (surfaces), illustratingwith the example of drilling operations in the oil and gas industry, in order to provide discussion points about what new competencies technicians need to develop to face these emerging threats.

1 Introduction

The Fourth Industrial Revolution (4IR) is characterized by the fusion of the digital, biological, and physical worlds [1], which represents new ways of technology that are coming intothe service of societies. The 4IR is characterized by emerging technological advances and solutions in several fields [2], including but not limited to robotics, artificial intelligence, nanotechnology, quantum computing, the Internet of Things (IoT), 3D printing, and autonomous vehicles to name a few.

Astrategy of people and technology integration processes will allow oil and gas (O&G) companies to break out of traditional energy demand and price curves and capture new value in three main areas:

- Costs: Eliminating redundancies and run-time delays will dramatically improve productivity and further reduce CAPEX, OPEX, and inventories as a result of improved collaboration and sharing within the network.
- Diversity: The modularity of the network will facilitate the application of existing skills in a more diverse energy portfolio, for example, the application of offshore production capabilities to offshore mining.

- Results: The development of more result-oriented business models, e.g.,new partnerships and entries into the retail, banking, and consumer goods markets, will allow such outcomes to be achieved in transportation and heating, notjust infuelinputs.

However, there are a number of challenges to implementing a 4IR strategy [3]. Today, the same questions and concerns are recurring in forums and discussions in the O&G industry, as potentials of digital integration applications in operations are identified.

1. How to implement digital strategies throughout upstream operations?
2. How to integrate different upstream operations to guarantee interoperability?
3. How to turn a mature O&G field into a digital field?
4. How to generate a digital twin of the O&G field with operations running at different levels of technological maturity?
5. How toidentify potential securityvulnerabilities within the industrial automation processes?
6. How to securely integrate industrial networks with commercial networks in the cloud?
7. What are the challenges of putting sensitive information in the cloud?
8. How to integrate industrial cybersecurity solutions in industrial infrastructure?
9. How to implement cybersecurity models into old and legacy industrial infrastructure?
10. What skills and competencies must the company's personnel develop to be able to deal with the adoption of these technologies?

These questions, as well asmany others, have become meaningful when applying concepts that allow breaking the paradigms of siloed work and applying integrated operations concepts. A growing number of companies in the O&G sector are seeking to structure integrated operations applications [4] to introduce technologies of the 4IR into their business models and engineering processes.Digitization in the petroleum industry has allowed new opportunities to increase efficiency and reduce costs, but the convergence of both operating (OT) and information (IT) technology has exposed companies to a whole new set of threats. Some new cyber-threats, which didn't even exist a few years ago, can now come from many directions, including internal actors seeking to sabotage or delay drilling operations, outsiders seeking to cause brand damage, and external parties, such as activist groups. Specialist reports show thatthe cyber-maturity of theO&G industry is relatively low.

The purpose of this article is to identify how the adoption of 4IR technologies will expand the tasksof the O&G industry as a whole and the professionals working in it. Based on the facts, we will identifythe possible malicious agents (vectors) and the possible areas under attack (surfaces).As an example, we structured drilling operations, using them as a baseline scenario to explain possible attack vectors and surfaceson industrial targets.The contribution of this study stems from the hypothesis of how to outline a Competence Management System (CMS) that prepares technical professionals (PTPs) to face the new realities and concerns related to cyber-threats.

2 Integrated operations in the 4th industrial revolution

Integrated operations (IOs) refers to the integration of organizations, disciplines, work processes, people, information, and communications technologies to make smarter, more collaborative decisions focused on increasing productivity and reducing costs. This means offering technology-driven solutions as an advantage thatallows companies toleverage limited resources, enabling the implementation of new technology applications such as Digital Oil Field (DOF), Industrial Internet of Things (IIoT), or the Digital Twin, using

online data and information transfer to efficiently and effectively maximize productivity and assetvalue throughout the life cycle of the production chain (upstream for our case).

To achieve effective implementation of IOs, the O&G industry must perform two processes in parallel, a process of conversion from analog (physical world) to digital (virtual world), i.e. Digitization. Another process, called Digitalization, which corresponds to the use of digital technologies and digitized data to improve the way the work is done, transforms the way clients and companies engage and interact, and creates new (digital) revenue streams. Digitization enables organizations to optimize processes internally in the physical world (e.g., process automation, paper minimization) and leads to cost reduction and productivity improvement. In contrast, Digitalization is a strategy or process that goes beyond the application of technology and involves a deeper and more fundamental change in the entire business model and the evolution of work because it integrates culture and work processes with technology.

With the adoption of the technologyof the 4IR and the application of IOs in the sector, O&G companies are rethinking their business models, business processes, and moving towards new job descriptions that will enable them to achieve the four driving forces of the transformation:

1. Innovation beyond the barrel - moving to the concept of energy suppliers
2. Digitization of products and services
3. Capacity to compete as an ecosystem
4. Digital platform.

On thepositive side, the adoption of the 4IR and OIs in the O&G sector is enabling a host of new opportunities that offer increased efficiency and reduced costs. Figure 1 illustrates the definition of the concept of integrated operations in O&G.

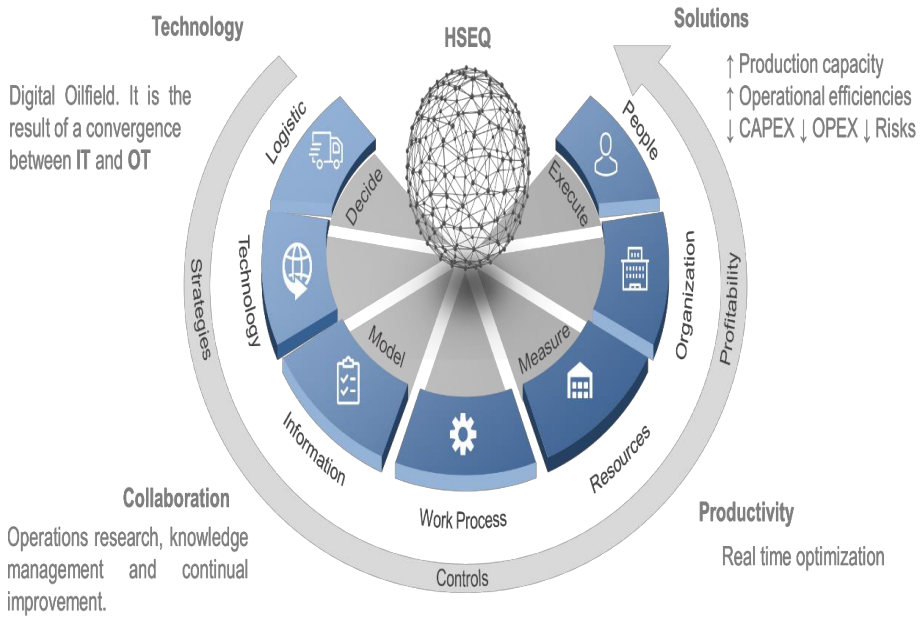

Fig. 1. Defining the concept of integrated operations (IO) in O&G.

3 Describing vulnerabilities in the upstream – surface of attack

We will introduce the concept of Operational Technology (OT), defining it as the hardware and software that detects or causes a change in the physical world through direct monitoring and/or control of equipment, goods, processes, and industrial infrastructure. The term has been established to differentiate between technologies, functions, and applications of traditional computer systems and the environment of industrial control systems. The biggest challenge for the implementation of IO is the triangulation of three complementary aspects:1) integration of information systems (ITs), and operational and industrial systems (OTs); 2) convergence of business indicators with the continuous engineering processes improvement so that they can be evaluated in parallel, and 3) centralization of data and information in cyberspace to ensure data extraction and analysis. These three aspects haveled to an increase inthe number of threatsused by third-party attackers.

The OT is used to monitor and control physical processes in industry. The OT function isto collect process data (temperature, pressure, valve position, tank level, human operators) and directly control electrical, mechanical, hydraulic, or pneumatic actuators within a company or organization.

In a modern single-platform OT system, data communication and cross-layer integration are necessary for automationof drilling [5]. Figure 2 shows key threats and consequences that result from the intrusion of a malicious third party into an O&G interconnected infrastructure.

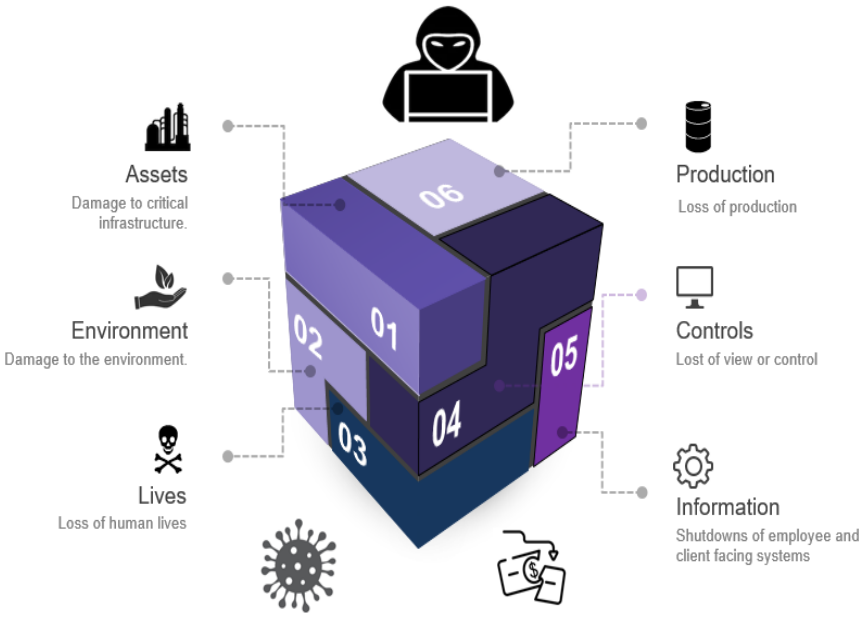

Fig. 2. Key threats caused by intruders (malicious third parties) in O&G operations.

4 Cyberspace and cybersecurity

It is necessary to give our adapted definition of cyberspace; here we will define it as a virtual space determined by connecting people, equipment, devices, and sensors through networksor virtual ecosystems to have real-time information about the efficiency of engineering processes and business model metrics. For this virtual space to come to life, it

requires interconnected computers (computer systems and networks). Cyberspace creates different environments to those of the analogous world (physical / traditional) and creates some threats that did not exist just a few years ago, and we will call them cyberthreats, which refer to anything that has the potential to cause serious damage to a computer system or networks. By their nature, these cyberthreats can now come from many actors and directions, including disgruntled insiders seeking to cause sabotage; competitors seeking to cause brand damage; and outside parties, such as activist groups seeking to damage or limit operations, among many others.

A high-level cybersecurity means understanding your systems and processes, the capabilities and limitations of your personnel, as well as a thoroug assessmentof your threat landscape [6]. In other words, the owners of the systems, whether industrial OT or IT, must fully understand that there will always be new technologies to enhance the company's ability to compete and new threats from external agents to counteract.

The scope of cybersecurity is to safeguard the activities of enterprises in the digital environment, such as integrity, privacy, intellectual property, security, and trust in digital infrastructure, generating both regulatory and collaborative framework to combat possible causes and identify possible effects.As an example, we can say that a vectorial attack through cyberspace (cause) onan enterprise implementing 4IR technologies mayaim to interrupt, disable, destroy, or maliciously control theenvironment or computer infrastructure, or destroy data integrity, or steal controlled information (effect). Meanwhile, a denial of service like acyber-attack (DoS attack) or a specific version of jamming will attempt to put a machine or network resource beyond the reach of users (clients – end-users), temporarily or indefinitely disrupting the services of a host connected to the Internet. A DoS attack is typically carried outby jamming or flooding the target machine or resource with superfluous requests or deactivationsin an attempt to overload systems and prevent some or all legitimate requests from executing.

It has been established that attacks against the OT infrastructure are primarily related tosecurity concerns, while attacks against the IT infrastructure are primarily related tosafety concerns [7].

It is worth asking then, why are we going to talk about cybersecurity in O&G: why can this sector be in the mind ofmalicious agents?

We must say about the O&G industry that

1. It is an attractive target vulnerable to cyber-attacks.
2. Its IT and OT environments are complex which results in a large attack surface.
3. It uses old and legacy systems.
4. A successful attack on it can have disastrous consequences.
5. There is a potential for significant financial benefit.

5 Attack vectors: cyber threats - who are the attackers?

Cybercrime willremain a major problemover the next few years. Between 2019 and 2023, it is estimated that approximately $5.2 trillion will be at risk l from cyber ttacksworldwide [8], posing an ongoing challenge to both businesses and investors. In fact, a 2019 Ernst & Young Global Limited (EY) security survey of 40 oil and gas industry found that 87 percent of respondents did not fully understand the implicationsof their new cyber protection policy and strategies [9]. The survey also showed that 63 percent of these companies did not thoroughly examine the financial impact of breaches despite suffering an attack that did not appear to be harmful [9].

In the same way, Deloitte mentioned that many O&G companies do not even mention "cyber" once in their 100+ page reports [7]. O&G cyber-security reports expose the

industry's cyber-maturity as relatively low [7]. Now let's briefly describe who the third-party attackermight be:

1. Nation-state actors are government-led and funded attackers organized to launch operations ranging from cyber espionage to intellectual property theft.
2. Cyberterrorist actors seek the opportunity to undermine the economic value of a country or economic sector, They have the potential to create a global impact.
3. Cybercriminals are individuals who use the Internet to commit various types of crimes. Seeking financial gain or crimeware-as-a-service (CaaS)
4. Activist actors perpetrate their attacks to promote a political agenda or social change.Hackers are individuals or groups that gain unauthorized access to websites by exploiting existing vulnerabilities.
5. Disloyal or malicious employees – Contractors, are often trusted employees of organizations and have access to critical systems and data, they represent a major threat to the well-being of the company.
6. Inadvertent Employee, sometimes people make mistakes or fall victim to common social engineering tactics, such as phishing, salesmanship, or pretexting.

Recent attacks on the O&G industry include the cyber spy group APT34, or OilRig, which posing as a Cambridge University researcher to send out LinkedIn invitations, spread malware on customers' systems in the UK [10].

The Triton/Trisis cyber-attack by the Xenotime threat group first targeted a Saudi petrochemical facility, shutting down industrial security systems, and then spread out to power companies in the United States and the Asia-Pacific region [10]. Cybercriminals have also used rescue programs to attack European oil and gas companies through phishing emails [10].

O&G companies' defense strategy begins with solid threat intelligence and knowledge of their systems. Every day, more than 60 potential offenses to Aramco's data center, the so-called EXPEC Computer Center (ECC) [10], are analyzed to ensure business continuity. The ECC is where the company performs its high-performance computing, including reservoir simulations and seismic processing [10].

The threat of cybersecurity becomes something beyond the nature of:

- The spread of the virus;
- Computer or data damage;
- Sealing data.

6 Types of attacks

When systems or networks are in use, we are exposed to a sniffing or snooping attack also known as an eavesdropping attack, which is thetheft of information transmitted over a network by a computer or another device connectedto the network.Phishing and Malware are the two most common types of attacks in the oil industry [11]. Here we will briefly describe them and include Denial of service attacks (DoS) and Drive-by-downloads attacks (including snooping and downloading).

1. Phishing & Social Engineering: = Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, disguising itself as a trusted entity in electronic communication. Typically carried out via email or instant messaging, it often directs users to enter personal information on a fake website that matches the look and feel of the legitimate site.
2. Denial-of-Service: DoS attacks harm companies by flooding target web servers with requests, preventing their regular users from connecting. This means website downtime,

disappointed customers, reputational damage, and can even result in lost data and compensation payments.

3. Drive-by-downloads: unlike many other types of cyberattacks, you don't have to open an email attachment or download anything to get infected. A download can exploit an operating system, web browser, or application that has vulnerabilities (due to lack of security updates). It can be transmitted when you simply view an email, a pop-up window, or a website. We also can include here Snooping attacks which involve an intruder listening to traffic between two machines on the network, in most cases downloading this information to his/her computer.

4. Malware: short for malicious software, is a type of software that can be installed on a computer without the computer owner's permission. Different types of malicious software can damage computers, such as viruses and Trojans. The term also includes other intentionally harmful programs, such as spyware and rescue software.

- Bloatware is a process by which successive versions of a computer program become significantly slower, use more memory, disk space, or processing power, or have higher hardware requirements than the previous version.
- Spyware is unwanted software that infiltrates your computing device, stealing your Internet usage data and sensitive information.
- A virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its code.
- A worm is a self-replicating malware that duplicates itself to spread to uninfected computers. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing down or stopping other tasks.
- A Trojan is any malware that deceives users about its true intent.
- Ransomware is a type of malware. It restricts access to the computer system, infects it or the data it stores (often using encryption techniques), and requires payment of a ransom to the malware's creator(s). You pay for the encryption to be removed – one of the most famous is the renowned "Wannacry."

7 A post-drilling approachfor oil and gas drilling operations

This studyargues thatattack surfaces in today's drilling OT system operatingin remote environments under the premise are susceptible to malicious third partyinfiltrations. A cause-effect analysis of possible vector attackshas been conducted. The contribution of this studystems from the hypothesis of how to outline a Competence Management System (CMS) that prepares privacy technology professionals (PTPs) to face the new realities and concerns related withcyberthreats.

When defining an architecture or attack surface, it is possible to highlight the system it affects and the type of impact it causes.

Examples of operational technology include

- PLC= Programmable Logic Controller;
- SCADA= Supervisory Control And Data Acquisition;
- DCS = Distributed Control System;
- ICS = Industrial Control System;
- Computerized numerical control (CNC) systems, including computerized machine tools;
- Energy monitoring systems, safety, and protection of the built environment;
- HMI = Human Machine Interface.

Cyber Threats:what canhappen?

Four main categories of cyber threats in drilling operations have been analyzed.

1. Threats on drilling rigs can be physical or virtual depending on the form of the attack.Physical threat - spying examples, air attacks - impact (loss of an oil platform, oil spills, blowouts, explosions) – virtual threat - examples total or partial loss of control in sensors, false display (spoofing attack), response delay (jamming in wireless networks or positioning systems) or selective delay attack
2. Threats related with third-parties in control of operations in critical systems: the power system (generators); the hoisting system (drawworks clutches and brakes); the rotary system (top drive and control panel); and the circulation system (pumps and lines). Causing potential delays in the well control system and choke line (blowout prevention system)
3. Threats related with data alteration of sensor measurement readings (data diddling) by unauthorized modification of sensor data, or software installed on the rig's system master controllers, including deletion of operating range files in integrated drilling systems, machine control systems, control room, cabin, and panels. Signal-synthesis attack, generating and sending out false signals to make the receiver believe to be at a different position (MWD). Relaying attack (wormhole attack) - relaying the signals received at the wanted spoofing depth D^1 to the receiver at the actual depth D (Wireline, L/MWD)
4. Threats related with downloading and spreading of viruses and worms, Stuxnet- type specially designed to sabotage industrial equipment and damage systems. Alteration and destruction of information and data collected during drilling activities. Alteration and destruction of backups, interconnected systems, networks, and facilities.

Figure 3 summarizes the concerns of advanced automation. This includes cybersecurity strategies that companies (adopters) must recognize, as well as main threats and impacts, to be able to mitigate them.The latter may include

- Increasing pressure in a pipelines;
- Failures or errors in PLC and DCS;
- Changesof the parameter settings of the sensors in the field;
- Closer/Opening motorized valves;
- Causing denial service attack within the ICS;
- Increase/decrease of motor speeds of compressor units;
- Showing false HMI readings;
- Lack of reliability of SCADA systems in offshore O&G platforms.

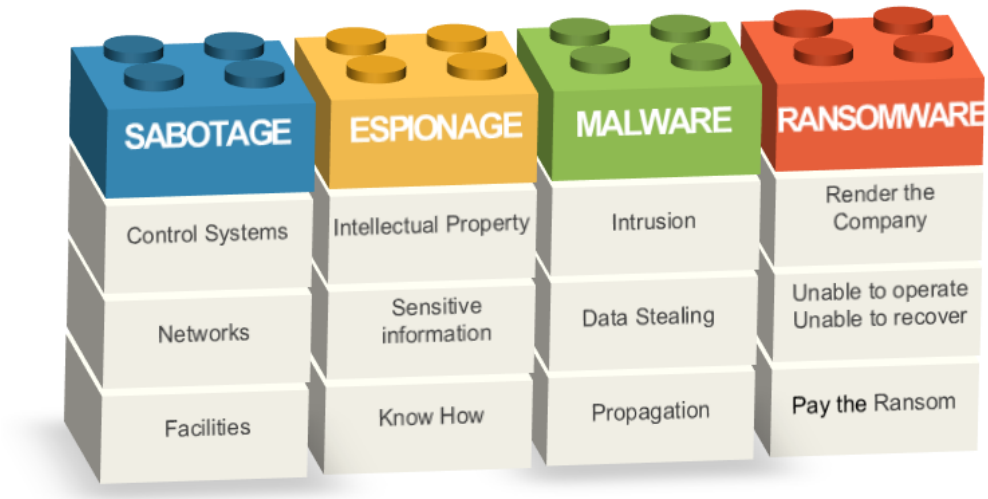

Fig. 3. The concerns of advanced automation that cybersecurity must deal with.

8 New threats – new competences

Multiple policy-makers and sectors have been recognizing the importance of nurturing and increasing a skilled workforce thatcan effectively work on identifying and quantifying risks associated with the automation of industrial systems and on mitigating those. Unfortunately, the speed of adoption of the 4IR technology by many industries overpasses the speed of training and preparation of the relevant professionalpool in organizations. This, coupled with the fact that the O&G industry has a ratherolderworkforce [2], maintains a negative view in many sectors of the public opinion [12], especially among digital natives. That entails that the O&G industry faces a major challenge never seen before: it must attract and retain new generations and create a skilled cybersecurity workforce to face the new challenges.

An overall diagnosis shows thatthe O&G industry has not paid much attention to strengthening cybersecurity skills [13] among its technical professionals (PTPs).Besides, many companies in the sector have not still recognized the importance of implementing this new force into their operations, and the resources allocated to this purpose remain quitelimited.The O&G sector has a shortage of cybersecurity skills and inadequate OT/IoT threat detection tools and processes.

To go further in the discussion, we propose to consider: "The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security" [14] as a document that provides methodological aspects establishing the new competencies and skills of the new workforce. Moving forward, what we want is to work on building a system of competencies based on roles and responsibilities. In the case of PTPs, the guidelines should refer to operational technology security and enterprise's applied security.

We believe thatthis guide presents a first step for the construction of a Competency Management System (CPM) based on such areas as investigation; collection and operation; analysis; protection and defense; oversight and development, operation and maintenance; and securely provision.Of course, it will be necessary to break down each part of this guide to determine its application within industrial systems in O&G and its importance in the competency profiles of PTPs. For reasons of space, it is not possible to discuss these issues in detail in this article. But it is important to notethat in a future article we will explorethis topic in detail to continue to addelements to a discussion that is just beginning and that is becoming more and more important every day.

9 Conclusions

1. Cyber threats are real and can harm companies, affecting the safety and security of theiroperations; vulnerabilities, and risks must be properly assessed and mitigated.
2. New malicious third parties are emerging and directly threaten the efforts of the O&G sector to adopt the 4IR technology.
3. The O&G industry is an attractive target, vulnerable to cyber-attacks;IT and OT environments are complex, which results in a large attack surface.
4. Historically, O&G companies have not focused on cybersecurity.
5. The O&G industry has a perceived low level of cybersecurity maturity.
6. Drilling rigs are attack surfaces for multiple vector attacks. Some of the attack types that can be carried out were described.
7. There has been a lack of laws and regulations around cybersecurity in O&G, unlike in other industries.
8. The cyber defenses used in IT are not necessarily suitable for OT environments.

9. Operational technological systems require not only information technology but also engineering knowledge for their management and maintenance.

10. Professionalism shortage: IT and OT skills are hard to come by;a skilled cyber workforce is essential to keep pace with evolving threats.

11. It is necessary to outline a CMS that prepares PTPs to face the new realities and concerns related to cyber-threats.

References

1. N. Ndung'u, L. Signé *Capturing the fourth industrial revolution.A regional and national agenda, Africa growth initiative of Brookings*. (Washington D.C, USA, 2020).
2. S. Sumbal, E. Tsui Knowledge retention and an aging workforce in the oil and gas industry: a multi-perspective study, *Journal of Knowledge Management*, **21**, (2017).
3. T. Shu., T. Lee., et al An Overview of the Rising Challenges in Implementing Industry 4.0., *Int. J Sup. Chain. Mgt (IJSCM)*, **8**, (2019).
4. F. Bento, Complexity in the oil and gas industry: a study into exploration and exploitation in integrated operations. *J. of Open Innov*, **4** (11), Springer, London, UK. (2018).
5. H. Houmb, F. Iversen *Companies must look at cross-layer monitoring of rig automation systems, tie cybersecurity monitoring to overall situational awareness of the rig*. (Drilling contractor. Houston TX, USA, 2019).
6. J. M. Jorgensen, K. P. McSweeney Cyber Security - Understanding Your Threat Landscape. *Offshore Technology Conference* (2018)
7. Deloitte University Press, Protecting the connected barrels – Cybersecurity for upstream oil and gas – A report by Deloitte Center for Energy Solutions, New York, NY, USA (2017).
8. D. Antonucci *The Cyber Risk Handbook, creating and Measuring Effective Cybersecurity Capabilities*. (John Wiley & Sons, Inc., New Jersey, NJ, USA, 2017).
9. W. Williams, P. Ciepiela, P. Van Kessel, *Six cybersecurity issues for oil and gas companies*. (20th Global Information Security Survey, Ernst & Young, London, UK, 2019).
10. M. Zborowski As oil and gas data multiply, so do the Cybersecurity threats, *Journal of Petroleum Technology (JPT) – Society of Petroleum Engineers (SPE)*, (2019).
11. P. Ciepiela Digitization and cyber disruption in oil and gas, *EY EMEIA OT/IoT Security & Critical, Ernst& Young*, (2017).
12. S. Rassenfoss The challenge of the public perception, *Journal of Petroleum Technology (JPT) – Society of Petroleum Engineers (SPE)*, (2019).
13. K. Francis, W. Ginsberg The federal cybersecurity workforce: Background and congressional oversight issues for the departments of defense and homeland security. Congressional research service. CRS Report prepared for members and committee of Congress, Washington D.C, USA (2016).
14. F. Lobo, Upstream Oil & Gas cyber risk: insurance technical review. A joint rig committee report, International Underwriting Association (IUA), Insight Consensus Influence (ICI). London, UK (2018).