Internet of Things and Cloud Computing
2023; 11(1): 1-17
http://www.sciencepublishinggroup.com/j/iotcc
doi: 10.11648/j.iotcc.20231101.11
ISSN: 2376-7715 (Print); ISSN: 2376-7731 (Online)

Analysis on Cybersecurity Control and Monitoring Techniques in Industrial IoT: Industrial Control Systems

Boye Aziboledia Frederick, Onate Egerton Taylor

Department of Computer Science, Rivers State University, Port Harcourt, Nigeria

Email address:
bayelsaforprogress2022@gmail.com (Boye Aziboledia Frederick), taylor.onate@ust.edu.ng (Onate Egerton Taylor)

To cite this article:
Boye Aziboledia Frederick, Onate Egerton Taylor. Analysis on Cybersecurity Control and Monitoring Techniques in Industrial IoT: Industrial Control Systems. *Internet of Things and Cloud Computing*. Vol. 11, No. 1, 2023, pp. 1-17. doi: 10.11648/j.iotcc.20231101.11

Received: March 4, 2023; **Accepted**: July 7, 2023; **Published**: November 9, 2023

Abstract: The paper focuses on the analysis on cybersecurity monitoring and control potentials in industrial IoT systems (ICSs, SCADA etc.). The Industrial Internet of Thing as part of IoT technology has provided an opportunity to build powerful industrial control systems and its applications with IIoT devices, especially in the manufacturing, oil and gas, chemical industry etc. These integrated IoT/IIoT systems needs cybersecurity monitoring and control due the present and unrelented cyberattacks on these systems. We explore in detailed 5 (five) techniques that aids cybersecurity monitoring and control in industrial IoT and other related industries. In this paper, we carried reviewed on past and recent events on cyberthreats and cyberattacks research literatures in industrial IoT systems (ICS, SCADA etc.) and other industries, which were used as research materials. In conclusion, the paper outlined industrial control system (ICS) incident response, defensible architecture, ICS network visibility monitoring, secure remote access, and risk-based vulnerability management that can create an efficient and effective cybersecurity techniques in industrial IoT systems. Inconclusion, we discover new ideas, applications, monitoring and best practices with critical control measures that will benefit other industries when deployed.

Keywords: Industrial IoT, Cyber-Attack, Cyber Threats, SCADA, Industrial Control Systems, Oil and Gas

1. Introduction

The oil and gas industry are usually [8], divided into three major sectors: upstream, midstream, and downstream, with the upstream sometimes known as the exploration and production (E&P) sector, the midstream provides the vital link between the far-flung petroleum producing areas and the population center's where most consumers are located, whereas the downstream includes oil refineries, petrochemical plants, natural gas distribution companies etc. and a cyber-attack at facility can occur at any point across the three major stages of oil and gas operations: upstream, midstream, or downstream [40].

The description of the oil & gas industry as a multibillion-dollar industry that has a history of conflict [5]. With deployment of modern technology and development, both the corporate aspects and technical aspects of the oil & gas industry have become heavily reliant on the cyber domain. Many organizations are losing so many data, fund, and resources as discussed [6] to unauthorized persons with great depths of breaking through any data, knowledge, programs, strategy, and tools protecting them. Also, in related development [5] said there is significant evidence of protracted, insidious espionage carried out by a state actor within the cyber realm. Oil and gas facilities are a major target for extremists to cause economic damage and project their influence as well [14], they believed that 'cyberattack can have highly negative impacts on energy delivery systems (EDS). The study obtained reflect that from central control room operators to rig managers, executives are making decisions that would impact all areas of the industry as regards to cybersecurity [9], taking risks in a balanced way to be profitable and managing compliance of regulations keeping up with technological advances continually present in the energy industry.

The author [1] describe the oil and gas industry as a tech and asset-heavy sector. but incorrect measurements and even tiny mistakes in this field result in billions of dollars in losses and, sometimes, tragic events like Deepwater Horizon or [3] Piper Alpha, Phillips Pasadena, Exxon Valdez in 2014 report by Willis Group, a multinational risk adviser and insurance firm in 2014, could indeed be caused by a cyber-attack, and that is why in every business and at every corporation size, [9] cyber risk is a base level exposure that every industry must confront and should be seen with the same significance as a company's personnel, liability or property's risks. The oil and gas [12] might not seem like an industry that hackers would target. But they do-and the cybersecurity risks rise with every new data-based link between rigs, refineries, and headquarters, so it becomes imperative that the oil and gas industry need protection against its infrastructures. Over the years, [13] there have been many cyber security attacks on the offshore oil and gas sectors, including the tilting of oil and gas rigs, malwares-infected-platforms, industrial control systems been hacked, and so, modern day interconnected world is very vulnerable to cyber-attacks and industries are taking more and more countermeasures than ever to safeguard their systems and data.

In this study, the researcher employed theoretical approach or model which is a logical exploration of a system of beliefs and assumptions as explored by [4]. This type of research includes theorizing, defining and analysisng how the oil and gas industry has been affected by cyber-attacks and its enhancement using the potentials of IIoT technology in monitoring systems in the oil and gas industry. The author [6] dwell on theoretical analysis or an approach using the quality of qualitative research to achieve results by stating the practical suggestions which on this paper means outlining the theoretical analysis of cyber-attacks and the possible IIoT improves monitoring systems in the oil and gas industry.

Although [16] Industrial IoT as an industry 4.0 is growing exponentially and leverages many of the same technologies as IoT and applies them to the complex needs of industrial environments. [9] most of the times it's not economically viable or technically possible for a company to be 100% secure from external threats, there are some important tools and improvements that can reduce or transfer these risks in an acceptable level. [11] Industrial IoT becomes a transformative manufacturing strategy that helps to improve productivity, quality, safety and delivery in an industry and manufacturers are increasing uses of IIoT solutions to enhance their analytics functionalities, to track assets and to upgrade their control rooms. [15] revealed that Industrial IoT is being shaped by many participants from the energy, healthcare, manufacturing, transportation, and public sectors, each with complex and fast-changing architectures, like the Reference Architecture for Industrial Internet Systems (RAII). which defines the Industrial Internet Systems and specifies an Industrial Internet Architecture Framework to aid in the development, documentation, and communication of the Industrial Internet Reference Architecture (IIRA) [15].

According to [10] bridging the gap between the digital and physical worlds, the industrial internet of things (IIoT) is ushering in a new era of efficiency, growth, and information by giving companies clear line of sight to critical assets and manufacturing processes. [7], IIoT is particularly important due to progressing computerisation of hardware resources leading to development of a virtualised model of autonomous real-time production management. The authors in [15] reveals industrial Internet of thing (IIoT), embodies the convergence of the global industrial ecosystem, advanced computing and manufacturing, pervasive sensing, and ubiquitous network connectivity. Industrial IoT solutions [27] like Sensata's Cynergy3 monitoring of termination temperatures enables the use of dashboards and real time alarms to predict potential failures up to three months in advance.

2. Literature Review

2.1. Cybersecurity Monitoring and Control Techniques in Industrial IoT: ICSs, SCADA etc.

The industrial world [24] of oil and gas involves critical processes and machinery for the exploration, extraction, refining, transporting, and marketing petroleum products. The industry 4.0 movement [23] is driving innovation in manufacturing through the application of digital technologies, leading to solid performance improvements. Using Industrial IoT technology, [16], the interconnection of these intelligent industrial devices with control and management platforms, collectively improve the operational efficiency and productivity of industrial systems and Improved [38] production efficiency and long-term viability are two key benefits of the Industrial IoT's.

As we explore on the possible Industrial IoT improved monitoring systems over the phenomenon of cyber-attacks in the oil and gas industry, we should not forget as revealed [5] that automation via SCADA/ICS has been an integral part of the oil and gas industry's past and will be even more so in the future. The authors [16] describing Industrial IoT as a group of technologies that collect and transmit data within traditionally isolated industrial devices found in SCADA systems and other ICS that monitor and control industrial critical infrastructure that includes factories, power plants, water systems, ports, and other industrial facilities etc.

From study, [17] reveals that oil production offshore is usually in remote locations, requiring remote access (monitoring) and control, and this can be achieved by integrating ICPS, Supervisory, Control and Data Acquisition (SCADA) systems, and Industrial IoT technologies. A comprehensive framework for risk assessment [13] of cyber damages in the absence of any and built a taxonomy of possible cyber catastrophe scenarios was established to review 'the state of the art in cybersecurity risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. Today's attack surfaces as reveals [37] are getting wider due to the steep increase in remote connectivity to ICS, and attackers know how to take advantage of nearly every security malfunction to gain confidential intelligence about ICS equipment that the victims use on their production floors.

Figure 1 below represent the Industrial IoT architecture, [62], where network interconnection layer takes care of network interconnection and end-to-end data flow, the network is the foundation to interconnect industrial systems and promote the transmission and seamless integration of industrial data. The platform layer executes information fusion, intelligent optimization and decision-making and the application layer analyzes and models the data information stored in the platform layer and forms the required information [63].

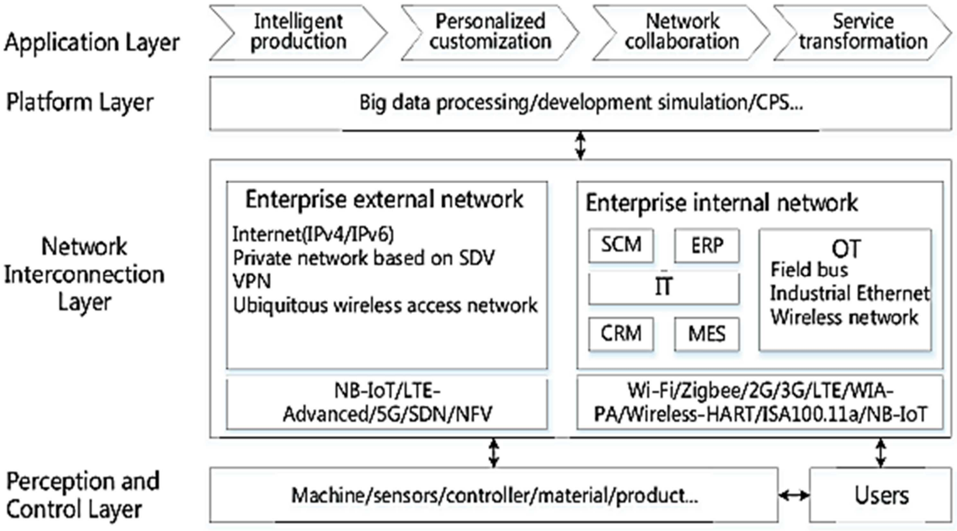

Application Layer
Intelligent production
Personalized customization
Network collaboration
Service transformation
Platform Layer
Big data processing/development simulation/CPS...
Network Interconnection Layer
Enterprise external network
Internet(IPv4/IPv6)
Private network based on SDV
VPN
Ubiquitous wireless access network
NB-IoT/LTE-Advanced/5G/SDN/NFV
Enterprise internal network
SCM
ERP
IT
CRM
MES
OT
Field bus
Industrial Ethernet
Wireless network
Wi-Fi/Zigbee/2G/3G/LTE/WIA-PA/Wireless-HART/ISA100.11a/NB-IoT
Perception and Control Layer
Machine/sensors/controller/material/product...
Users

Figure 1. *Architecture of the Industrial Internet [63].*

It was discovered [62] that Industrial control requires real-time, low delay, high reliability, and security of network communication. As the data sensed in the physical processes are reflected on the Internet, control strategies need to be taken by the cyber world and transferred into the physical devices. The technology [33] improve automation, flawless monitoring of resources, increased efficiency, lessened safety risks, avoiding oil spills, and other business-related incidents. Considering among IoT devices for oil and gas supply chain [1], drones, and robots play an important role also, enabled efficient site exploration, ongoing data gathering, and 3D mapping of landfills and can withstand hard conditions regular for drill sites.

2.2. The FASTEN Suite

Below is an Industrial IoT architecture for decision support in manufacturing system [23], is composed by a Decision-Support Framework called FASTEN Suite Tool, which is backed by an Open Industrial IoT platform that ensures a clean bi-directional integration among the system components.

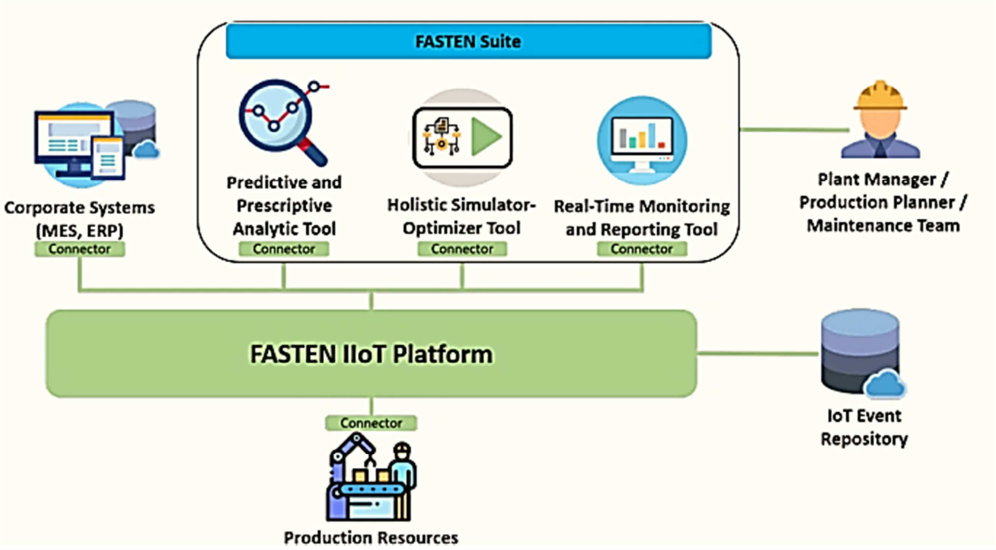

FASTEN Suite
Corporate Systems (MES, ERP)
Connector
Predictive and Prescriptive Analytic Tool
Connector
Holistic Simulator-Optimizer Tool
Connector
Real-Time Monitoring and Reporting Tool
Connector
Plant Manager / Production Planner / Maintenance Team
FASTEN IIoT Platform
IoT Event Repository
Connector
Production Resources

Figure 2. *Industrial IoT based architecture for decision support system [1].*

Thus, the FASTEN Suite as shown in figure 2 is presented as a solution to enhance real-time support material for decision-making on shop floor and help managers to deal with unexpected events and evaluate production scenarios. Also, it was revealed [34] that Industry 4.0, which is enabled by the integration of cloud technologies and cyber systems, a wide range of sensors are being installed around the industrial operational situation and tackled.

From their studies [25], for instance reveals a consolidated general requirement of a device management system for IIoT, comprises of security, maintenance, monitoring and configuration. So, the Device Management enables remote management, provisioning and authentication, configuration, and control, monitoring and diagnostics, software updates and maintenance. At its essence, [26] IIoT uses advances in sensing, communications, cloud, and computing technologies to help you (a) reduce costly unplanned downtime by providing an early indication of pending failure. The managers of Operational Technology (OT) perceive [33] the Industrial Internet of Things (IIoT) as beneficent for asset monitoring whereas the information technology (IT) leadership is much concerned about the security threats raised due to the increased IoT connectivity.

2.3. Yo-i Thingswise Industrial Data OS (iDOS)

Below is a system design based on the Yo-i Thingswise Industrial Data OS (iDOS), [35] an Industrial Internet Platform embedded with a digital twin framework, purposely designed, in reference to Industrial Internet Reference Architecture, for supporting digital transformation of industrial operational management.

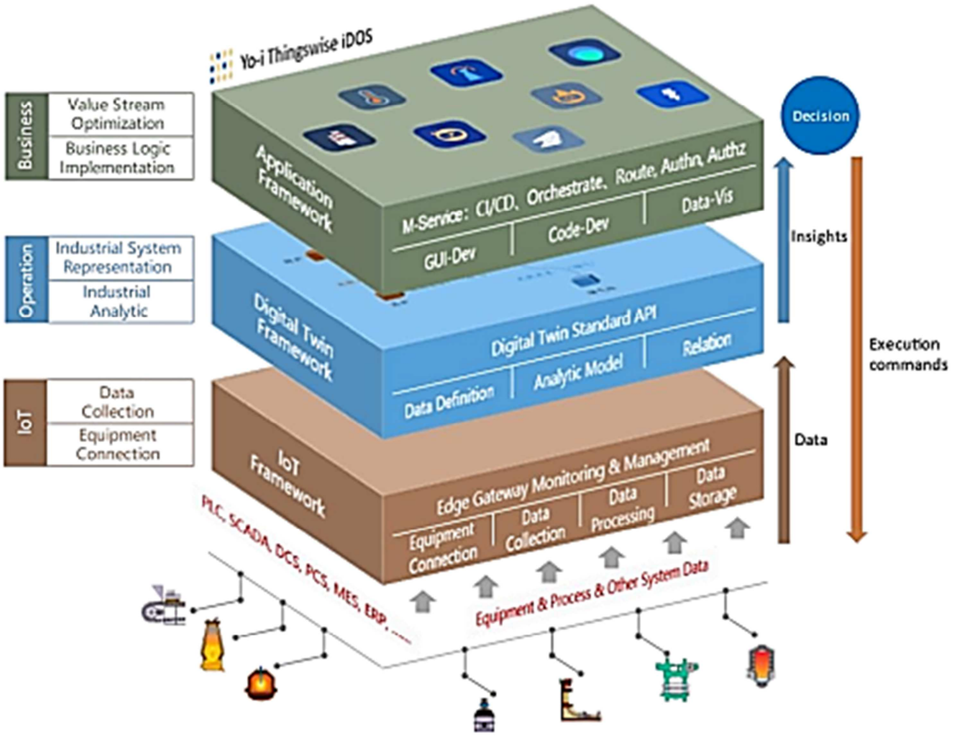


Figure 3. *Yo-i Thingswise iDOS platform functional architecture [36].*

2.4. The Nozomi-Industrial Defender Solution

According to the author [67], Nozomi-Industrial Defender Solution is targeted at complex industrial control system (ICS) environments to protect availability and safety of these systems, while also simplifying compliance requirements.

Figure 4. *The Nozomi-Industrial Defender solution [68].*

The followings are facts about this cybersecurity technique that operators of industry be familiar with are, this technique automatically collects, normalizes, and reports changes in the OT environment, regardless of vendor or location and, users can create asset baseline configurations that change detection engine compares with actual asset configuration data including ports and services, users, software, and firewall rules [67]. It supports vulnerability assessment, endpoint protection, traffic analysis capabilities, and more accurate diagnostics of in-progress threats and anomalies, including identifying compromised hosts with malware, rogue applications, unauthorized USB drives, and suspicious user activity [67].

2.5. GigaOm Radar Report for Industrial IoT Security

In its recently released GigaOm Radar Report for Industrial IoT Security as reported [43], the prominent technology-focused analyst firm placed OTORIO squarely in the inner leader's circle on its "Radar" of IIoT security vendors.

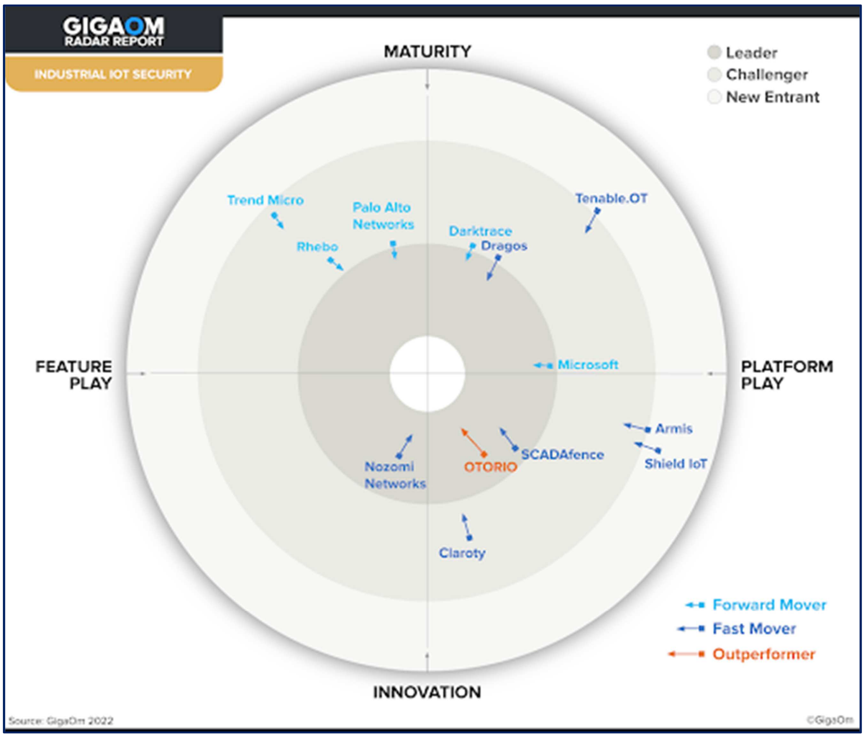


Figure 5. *GigaOm Radar Report for Industrial IoT Security.*

The above cybersecurity techniques [38], GigaOm Radar Report for Industrial IoT security will perform better in Industrial IoT security with the main aim of protecting operational technology from cyber-attack. Penetration testing has long been a technique used by organizations to find vulnerabilities in their systems and applications, enabling them to improve practical security outcomes, satisfy customer requests for third-party attestation, support M&A due diligence activity, and meet regulatory requirements. The value derived from penetration testing is significant, illuminating previously unknown weaknesses and granting security teams the ability to shore up defenses [38].

2.6. Third-Party Cybersecurity Services Across Product Lifecycle

Also, the cybersecurity services offered by CSA Group® combine well-established expertise in functional safety evaluation with a long history of working with emerging technologies [60]. The solutions are tailored to help customers identify potential issues early in the product design phase and implement security measures to mitigate potential cyber risk. The solutions are also comprehensive in that they address the responsibilities of each player in ICS. [60].

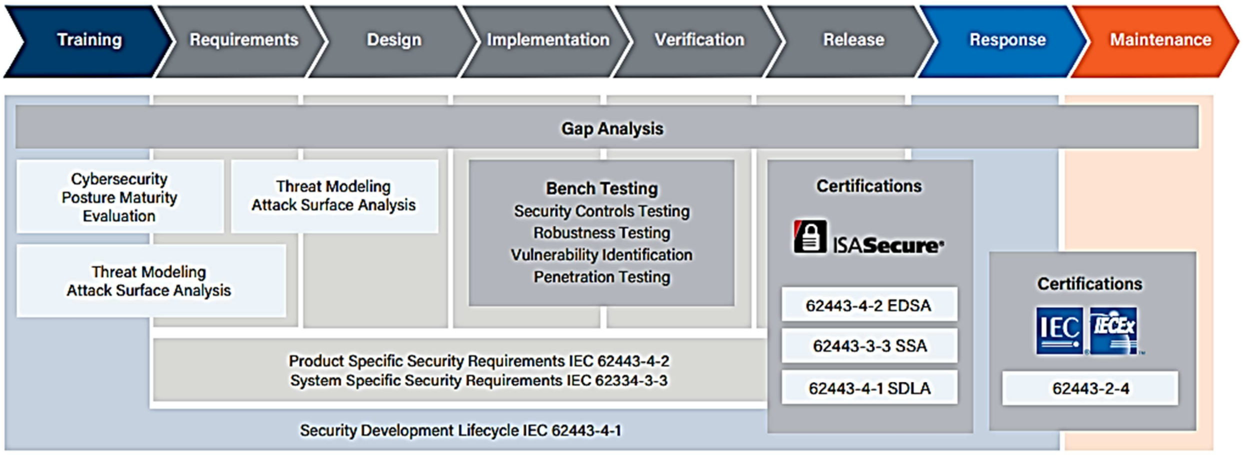

Training
Requirements
Design
Implementation
Verification
Release
Response
Maintenance
Gap Analysis
Cybersecurity Posture Maturity Evaluation
Threat Modeling Attack Surface Analysis
Threat Modeling Attack Surface Analysis
Bench Testing
Security Controls Testing
Robustness Testing
Vulnerability Identification
Penetration Testing
Certifications
ISASecure
62443-4-2 EDSA
62443-3-3 SSA
62443-4-1 SDLA
Certifications
IEC
IECEx
62443-2-4
Product Specific Security Requirements IEC 62443-4-2
System Specific Security Requirements IEC 62334-3-3
Security Development Lifecycle IEC 62443-4-1

Figure 6. *Third-Party Cybersecurity Services Across Product Lifecycle [61].*

The CSA Group's cybersecurity capabilities span the entire product lifecycle (Figure 6), and include:

(i) Gap Analysis: This service helps customers determine the overall areas of cybersecurity weakness in products or processes, as well as necessary improvements. [60].

(ii) Solution Provider Capability Assessment: An assessment of a set of cybersecurity related capabilities typically described in a plan or set of policies and procedures. This demonstrates that the vendor performing security services meets the IEC 62443-2-4 requirements while installing and /or integrating a control system at the customer plant [60].

(iii) Application of Solution Provider Capabilities Assessment: An assessment that security services providers use to install and/or integrate a control system, performed in compliance with IEC 62443- 2-4. [60].

(iv) Security Development Lifecycle Assurance (SDLA): This service helps customers stay ahead of potential security threats by addressing them early in the product lifecycle, before committing to production to ensure compliance with IEC 62443-4-1. [60].

(v) Embedded Device Security Assurance (EDSA): This service helps to provide third-party assurance on the security of embedded devices and its features, as well as the device supplier's development process, according to the requirements under IEC 62443-4-1 and 62443-4-2. [60].

(vi) Bench Testing: This includes testing against the Common Weakness Enumeration (CWE) database, product robustness and resilience against known cyber-attacks, as well as penetration testing, radio frequency testing, and source code analysis. [60].

2.7. Darktrace PREVENT/OT Product

Another [66] cybersecurity technique is the Darktrace PREVENT/OT product (figure 7). The approach deploys AI (artificial intelligence) to 'think like an attacker' to visualize pathways within IT and OT (operational technology) infrastructures that lead to critical infrastructure assets, empowering defenders to harden environments and stay steps ahead of the adversary [66].

Figure 7. *Darktrace PREVENT/OT product. [67].*

As shown in figure 7, Darktrace Prevent/OT Product [66] protects complex industrial environments against known and unknown attacks, using self-learning AI to discover and identify assets and detect subtle deviations that point to a cyber threat. Initially launched in 2015, Darktrace/OT DETECT and RESPOND is currently used by hundreds of critical infrastructure companies in utilities including electric, water, oil & gas, maritime, and transportation. Darktrace had in April last year joined with Zscaler, Okta, and Duo Security to extend its detection and autonomous response capabilities to zero trust technologies [66].

3. Cybersecurity Countermeasures Deployed in Industrial IoT: ICSs, SCADA etc.

Our increasing dependence on technology and web-based communication has opened the door for cybersecurity threat, particularly in the oil and gas industry. Petroleum companies face significant threats as revealed [50]. Also, recent study conducted [42] cybersecurity firm Nozomi Networks and the SANS Institute identified the risks and threats impacting critical infrastructure and provides direction on managing ICS risk to maintain the safety and reliability of operations. It outlines how the industry responds to these incidents with greater preparedness and more willingness to budget for industrial control systems (ICS) cybersecurity. For more than 30 years, [33] organizations have had their hands full protecting their data, intellectual property, and Information Technology from cyber threats, securing the bits and bytes crucial for business continuity.

By looking closer at the infrastructure of an oil and gas company [30] and identifying threats that can disrupt operation, a company can seal off loopholes and improve their cybersecurity framework. All Industrial organizations as suggested [38] need to secure their revenue-generating operations from the rising threat of cyber-crime. Applying predictive risk avoidance approaches appear to be ideal for mapping potential. The contribution from [41] advised that any new product that is internet connected, must be reviewed for security vulnerabilities prior to release. It is part of the development life cycle and factors into the risk management process.

However, while operators' general perceptions towards the importance of cybersecurity is advancing over time, we [31] might never reach the point where every operation is completely safe and secure, simply because the bad actors are constantly moving and improving their techniques. Oil and gas sector leaders [2] will need to build cyber resilience into their organizations and partnerships to continue providing reliable, timely fuel deliveries to their customers in a future full of cyber threats.

As confirmed by [9] an important Ernest Young's survey with oil & gas industry's executives, IT Security starts to become an important threat from 2013 Top 10 Risks. Considering the productivity enhancements, the risks involved to have a network digitally controlled in an unauthorized mode are highly significant and since oil and gas facilities are part of the energy chain o of a country and plays an important role in political aspects, it turns to be one of the primary targets for cyber-attacks and [40], Protection against cyber-attacks is essential to the worldwide economy.

It was reveals that [42], the industrial cybersecurity sector in 2022 continued to face adversarial attacks in critical infrastructure networks that illustrated knowledge of control system components, industrial protocols, and engineering operations. Fighting these attacks requires a different set of security skills, technologies, processes, and methods to manage the different risks and risk surfaces, setting industrial control systems (ICS) apart from traditional IT enterprise networks. But [51], currently, securing offshore oil platforms against cyberattack is based on industry standard and the assumption of cybersecurity measures into current security regulation rather than independent federal or state regulations. A study also [37] revealed that there three main cyber security concerns for the oil & gas industry are stemming from digital transformations and organizations should recognize and approach them diligently.

(1). Remote access communication combined with lack of security awareness.

(2). On- and off-shore connections and

(3). Vulnerable software, outdated systems, and lack of cybersecurity budget [37].

Although the business is about barrels, not bytes. [12] the industry's remote operations and complex data structure provide a natural defense. But with motives of hackers fast evolving—from cyberterrorism to industry espionage to disrupting operations to stealing field data—and companies increasingly basing daily operations on connected technology, risks are rising fast, along with the stakes.

According to [39], the countermeasures deployed in oil and gas industrial control platforms are a result of intensive cyber security assessments and audits that cover a wide area including physical security, environmental security, policies and procedures, safety on and offshore, host-based security, network security, etc.

(i) Cyber Security Training and Awareness: Almost 80% of cyber security attacks are related to incidents offshore reflect human error. This is due to a lack of awareness training which is one of the biggest challenges or vulnerabilities faced by the industry [39].

(ii) Unclear/Lack of Cyber Security Policies and Procedures: The process of establishing a clear, straight forward, and self-explanatory policy for cyber security can take a tremendous effort but the importance and the results of cyber security policy are worthwhile. Unclear cyber security policies are equal to none as it misleads the management and the employees about how the countermeasures are to be implemented [41].

(iii) Outdated Industrial Control System: Advanced Persistent Threat (APT) – a type of attack, which is often described as stealthy, dangerous, and most importantly, often too successful. Such APTs directed towards a legacy Industrial Control System can cause huge damage in all aspects [39].

(iv) Inadequate Separation of Industrial and IT Networks: Any cyber-attacks on such systems [39], may lead to an eventual shutdown of the whole system. The internet access on an offshore platform for operational as well as leisure purpose sees a lot of threats and often comes with the increased risk of facing a cyber-attack therefore, [39] the growing use of Remote access from the IT domain to the OT comes with a certain risk, when not properly monitored and controlled becomes an easy target for cyber criminals.

(v) Too little Network Security Measures- On- and Offshore: The choice of implementing security measures depends on the type and the architecture of the Industrial Control System. The security measures also depend on the maturity of the company's security program. The security program [39] reflects the cyber security strategy of the company in response to the various threats and it should be an integral part of a company's daily operational business. That is the reason oil & gas industry needs cybersecurity more than ever [18], due to the ongoing digitalization of IT/OT convergence. Cybercriminals exploit the expanded connectivity to infiltrate systems and introduce malware to disrupt operations in ICS/OT environments. There is this [29] recommendation that ICS/OT security should not just cover traditional control systems but also modern systems that relate to critical operations. It also recommended that ICS/OT security should assess the current risk, including the system, threats, and impact. It was revealed [32] that to create a secure network, control engineers and plant managers must work together with the IT department and the technology they use. CYE's leading IT cybersecurity solution, Hyver™, provides full visibility of attack routes in enterprise networks, translating technical risks into business risks by correlating asset value, severity of vulnerabilities, and threat-actor activity. The technology delivers proactive risk management that grants visibility and simplified cybersecurity management over all OT and IoT assets, and IT devices in the operational network, correlating multiple security events into focused insights, and prioritizing risks by their impact on operational processes.

Figure 1 shows the EY global information security survey from 2016-2017 that reveals the Cyber threats faced by O&G sector as compared to other industrial sectors [22].

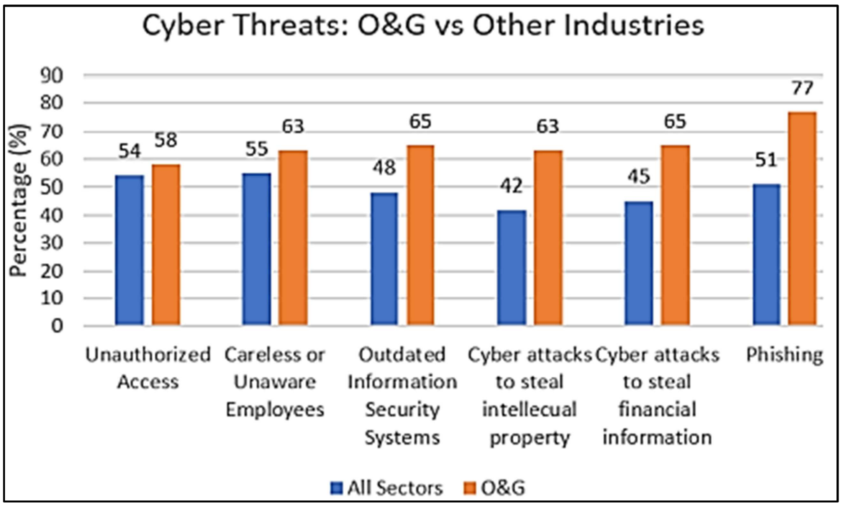


Figure 8. *Cyber threats faced by O&G sector as compared to other industrial sectors. Source: EY Global Information Security Survey 2016-17.*

As a possible solution at [31] global research and advisory firm Gartner came up with the idea of a "Soc (Security Operations Centre) triad". As Moles explains: "So these are the three technologies that you should use to give yourself maximum visibility in any corporate or enterprise environment. First is a sim tool, something that captures logs and correlates them and corroborates with other tools looking for threats. The second is an EDR, an endpoint tool that deploys agents on PCs and servers. And [31] the third part of the SOC triad is NDR – network detection response, looking into network traffic. Another useful piece of advice he offers operators is tracking what the ransomware is doing once in the system, instead of trying to stop ransomware running on the endpoint. OTORIO [38], recommends early preparation and taking proactive measures via penetration tests, incident response drills and even increased intelligence and detection, where Managers will also be responsible for OT cybersecurity and OT threat intelligence. If the federal government does not take stronger action to secure the country's oil rigs a cyberattack on an American oil rig—that cripples its functions and causes fatalities, supply disruption, and millions of dollars of damage—is not only probable, but a near certainty.

Mechanisms to ensure cybersecurity need development, whether it is industry standard or government regulations. Their study in industrial cyber [51], suggest that when building an ICS resiliency program in the industry or OT environment, start by asking the basic questions:

(i) Do I know what I need to protect (Asset inventory Management)

(ii) What are the holes in my protection and defense (vulnerability management)

(iii)Can I see if someone breach out OT environment (Monitoring) and

(iv)Can I get them out (Response) be added. [51].

4. Cyber Threats and Attacks in Industrial IoT: ICSs, SCADA etc.

Reports clearly indicate that attacks [63] on ICS in the oil & gas sector can have adverse effects to wide geopolitical areas and multiple countries. Even worse, the severity of some security incidents is likely to exacerbate due to cascading failures introduced by dependencies of other CI on the O&G infrastructure [63], so they attack to computational systems target to insert malware that executes [59]. In recent years, industries have witnessed or experienced the latter. Recognizing the different rankings of security issues between IT and OT can help us understand the multiple points of attack in an ICS, system.

Many documented attacks that affected downstream operations, administration and/or business processes, are also indirectly or directly connected with midstream and upstream systems, like in the case of Chevron back in 1992, when a malicious former employee hacked the warning controls of the management systems and reconfigured them to crash, eventually leading to an environmental pollution around the area of Richmond, California [65]. Some types and examples of ICS attacks include:

During the early 2000s, we witnessed attacks on infrastructures that had limited damage because back then systems remain on manual and were not connected to wide networks.

One example of this was the attack on Ukraine's power grid in 2015. The attackers planned their assault over many months, first doing reconnaissance to study the networks and steal operator credentials, then launching a synchronized attack against operating systems, which left about 225,000 customers without power temporarily [59].

Discovered in late 2017, Triton is a malware attack that targets safety instrumented systems and can shut down operations, masking the safety functions, or even triggering unsafe operations. While these attacks are carried out by highly sophisticated hackers, acknowledging, and addressing these common security gaps can go a long way in mitigating the risk of successful hacks [59].

Because industrial cybersecurity has caused the insurance industry fits for years [49]. A cyber expert [55], revealed that the industrial control system (ICS)/operational technology

(OT) security community is seeing attacks that go beyond traditional attacks on enterprise networks. Adversaries in critical infrastructure networks have illustrated knowledge of control system components, industrial protocols, and engineering operations.

From the previously observed impactful attacks [72], such as CRASHOVERRIDE1 in the electric sector, human machine interface hijacking through remote access in water management, and ICS-specific ransomware3 in the manufacturing and energy sectors, to the more recent Incontroller/PIPEDREAM4 advanced scalable attack framework targeting multiple ICS sectors, ICS/OT attacks are more disruptive with the possibility of physically destructive capabilities [72].

Threat intelligence supports the fact that industrial security defenders across all sectors must address new challenges and face serious threats [48]. This brings us to the understanding that both ICS endpoint and network visibility are critical for any ICS defense program, for all ICS sectors. As in [47], revealed that cyber-attacks on critical infrastructure can target technologies, processes, networks, services, systems, and facilities essential to public safety, health, and economic activities.

From the new study, 83% of firms that manage critical infrastructure suffered a cyberattacks in 2021. There are several threats as revealed [30] that oil and gas companies should be aware of. The biggest threat to the industry is those that have a direct negative impact on the production of their end products.

The first documented attack with effects purely on downstream operations was back in 2001, when a US-company owned gas plant suffered an attack from one of its suppliers. The supplier hacked three of the company's computers and caused a gas provision outage to homes and businesses in a European country, to create a distraction and cover up an error they had caused [63].

Furthermore, Allianz experts, cyber threats are the biggest change in the 2014 Risk Barometer from Allianz comparing with the year before, increasing up to rank 8th from 15th. [9]. One of the main aims cyber threats toward the O&G industry [40], targets including both IT and OT environments. [38] added that OT, IT, and IoT are rapidly converging. All three domains are under increasing threats that steal vital information, halt production, and even put human lives at risk. The Oil and Gas's upstream, midstream, and downstream lifecycles [36] are complex and have plenty of opportunities for threat actors to cause harm. Most of the others top 10 risks [9] identified are closely interconnected with a potential cumulative effect together with this threat.

So, most of the best understood attacks against the oil industry are [37] initial attempts to break into the corporate networks of oil companies. With in-depth research, [30] the expert team at Trend Micro identified the following threats that can compromise oil and gas companies. So, where OT assets used to be isolated from the IT part of the business, they are now converged with it [38] and the cyber attackers are noticing. Their lateral movements now enable them to jump from the shipping department to the factory floor and, once there, onto sensors, machines, and entire industrial networks, disrupting production and holding enormous production facilities to ransom.

The figure below reflects the most Targeted Industries (Global). As cybersecurity threats grow in scope, [50] suggest that owners and operators must proactively secure critical industrial controls and systems.

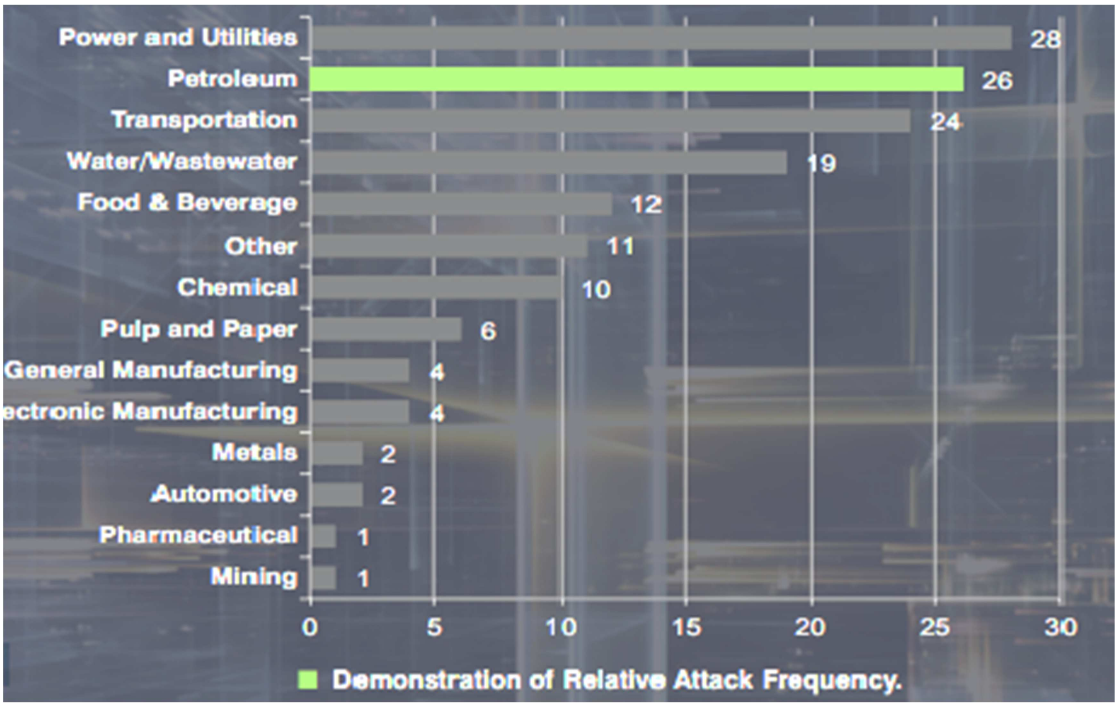


Figure 9. *Repository of Industrial Security Incidents/Security Incidents Org. [51]*

According to industrial cybersecurity and cyber risk management company OTORIO, [38] the number of industrial ransomware attacks is rising fast, and with it the average payout. It is important therefore to have an in-depth at cyberattacks than can disrupt oil and gas companies [30] because they affect operations and profit in a major way.

The Global Risk Management Survey from [9], Aon Risk Solutions identified cyber risks as the 8th position within the North America market but 18th in a worldwide range. The main reason for this position in a global perspective is that cyber risks are currently still underestimated by the companies in general since it's frequently seen as difficult to measure or transfer.

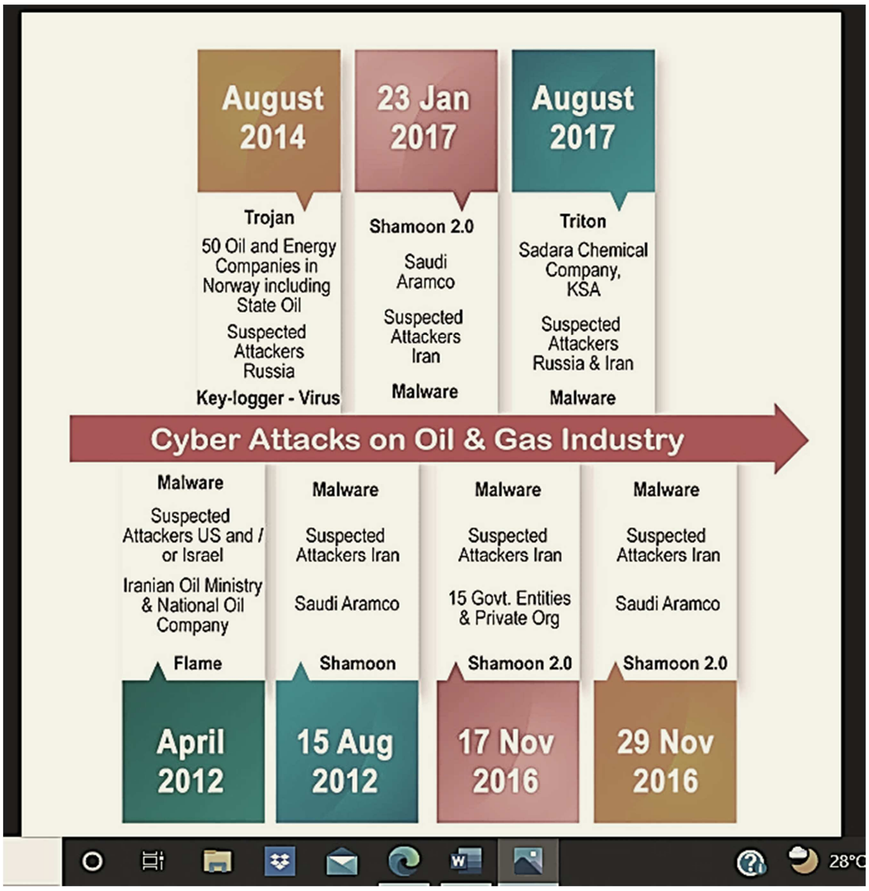
The research [32] reflects that 82 percent of oil and gas industry respondents, organizations have seen an increase in successful cyberattacks over the past 12 months. The study, conducted by Dimensional Research in November 2015, included more than 150 IT professionals in the energy, utilities, and oil and gas industries.

For years back [12, 19], cyber attackers have targeted crude oil and natural gas (O&G) companies, with attacks growing in frequency, sophistication, and impact as the industry employs ever more connected technology. Bur globally, [9] estimated that cyber-attacks against oil and gas. infrastructure will cost energy companies close to $1.9 billion by 2018. The British government estimates cyber-attacks already cost UK oil and gas companies around $672 million a year. Trend Micro survey also found that oil and gas companies have experienced disruptions with their supply due to cyberattacks [30]. On average, the disruption lasted six days. The financial damage amounts to approximately $3.3 million.

In 2008, the Japan Oil, Gas and Metals Corporation (JOGMEC) server was compromised by SQL injection (2008) [66]. Computers that accessed the falsified website were redirected to a server set up by the attackers for information theft.

Again in 2008, state-sponsored cyber actor successfully compromised servers of the Baku-Tbilisi-Cheycan pipeline. Attack exploited Internet connections or wireless networks for access to camera network. Attack caused temporary disruption in pipeline transfers using over-pressurization [74].

According to the research [5] The Middle East has scene perhaps the most evidence and variety of cyber conflict of all. While staying away from events which do not directly relate to the oil industry, a series of sabotage incidents using cyber as the medium are examined as shown below in figure 10.



Cyber Attacks on Oil & Gas Industry

August 2014
Trojan
50 Oil and Energy Companies in Norway including State Oil
Suspected Attackers Russia
Key-logger - Virus

23 Jan 2017
Shamoon 2.0
Saudi Aramco
Suspected Attackers Iran
Malware

August 2017
Triton
Sadara Chemical Company, KSA
Suspected Attackers Russia & Iran
Malware

April 2012
Flame
Iranian Oil Ministry & National Oil Company
Suspected Attackers US and / or Israel
Malware

15 Aug 2012
Shamoon
Saudi Aramco
Suspected Attackers Iran
Malware

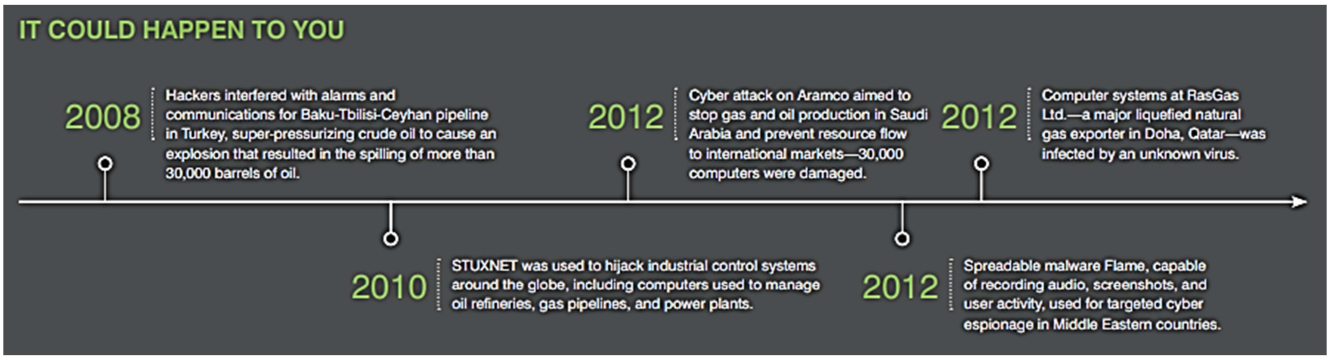
17 Nov 2016
Shamoon 2.0
15 Govt. Entities & Private Org
Suspected Attackers Iran
Malware

29 Nov 2016
Shamoon 2.0
Saudi Aramco
Suspected Attackers Iran
Malware

Figure 10. *Cyber-attacks on Oil and Gas Industry between 2012 and 2017.*

Symantec, the author [5] observed a group it refers to as the Elderwood gang operating a concerted campaign against a variety of industries including an undisclosed oil and gas company. Symantec also asserts that these are the same hackers who operated in the "Aurora" campaign against Google in 2009.

Like In 2010, the research [50] STUXNET shocked the industry as the first computer worm to attack SCADA systems. A year later, a derivative—DUQU— was specialized for cyber espionage. Today, oil and gas stakeholders face more advanced threats, such as DUQU 2.0 and Flame. As cybersecurity threats grow in scope, owners and operators must proactively secure critical industrial controls and systems. The figure below Just shows few incidents that happened between 2008 and 2012.



Hackers interfered with alarms and communications for Baku-Tbilisi-Ceyhan pipeline in Turkey, super-pressurizing crude oil to cause an explosion that resulted in the spilling of more than 30,000 barrels of oil.

STUXNET was used to hijack industrial control systems around the globe, including computers used to manage oil refineries, gas pipelines, and power plants.

Cyber attack on Aramco aimed to stop gas and oil production in Saudi Arabia and prevent resource flow to international markets—30,000 computers were damaged.

Spreadable malware Flame, capable of recording audio, screenshots, and user activity, used for targeted cyber espionage in Middle Eastern countries.

Computer systems at RasGas Ltd.—a major liquefied natural gas exporter in Doha, Qatar—was infected by an unknown virus.

Figure 11. *Source Parsons [15].*

Norway had the most [5] prolific series of cyber-attacks in the country's history in November 2011, As reported by Norway's National Security Agency (NSM), more than 10 firms were targeted by an advanced persistent threat using spear-fishing attacks, many of which were in the oil industry.

It's been patently obvious by the number of high profile large breaches that we've [31] seen since Aramco in 2012, The Shamoon virus attack [32], erased data in at least 30,000 of Aramco's corporate computers, and the objective of the attack was to stop the company's production, which represents more than 10 percent of world oil supply [31], the Lockheed Martin breach in 2011, before Aramco, so it's patently obvious you cannot keep a determined threat actor out.

In September 2012 Canadian energy company Telvent was infiltrated. [9] Telvent is responsible for supplying control programs and systems for over half of the oil and gas pipelines in North and Latin America. 14 The attacker's installed malware which they used to steal project files related to Telvent's OASyS SCADA product. According to security blogger Brian Krebbs, OASyS is "a product that helps energy firms mesh older IT assets with more advanced 'smart grid' technologies.

TRITON/TRISIS malware attacked Saudi oil Petro Rabigh in 2017 by the Xenotime hacking group. It modified behavior of Triconex Safety Instrumented System (SIS) from Schneider Electric [64].

Back in 2015, [19] hackers linked to Russia were able to turn off a power station in the country for hours and after an initial delay, electricity systems have been increasingly targeted this year.

Another attack happened during 2018 at the Energy Services Group (ESG) [65]. ESG handled customers' transactions for natural gas pipelines owned by several energy firms [52]. Customers during the ESG attack did not have access to transactions for a substantial amount of time. Attack stemmed probably from collateral damage from the unavailability of ESG systems led to gas outages, since at least five major energy companies had to disable operating processes [65].

The energy sector is no stranger to cyber-attacks [2]. The most personally disruptive incident in recent memory came in May 2021 with the ransomware attack that shut down a major U.S. oil and gas pipeline responsible for supplying nearly half of the East Coast's petroleum.

The December 2017 Triton attack on a petrochemical plant in Saudi Arabia, [37] that attempted to compromise Schneider Electric Triconex SIS *(*safety instrumented system) is often mentioned as one of the most devastating ICS malwares that could have caused unprecedented damage and risked human lives.

The report [37] reveals that the malware was able to pass through the OT network of the victim and manipulate the safety systems by reverse engineering Schneider Electric industrial protocol.

Furthermore, XENOTIME, [40] which targeted Triconex controllers to disrupt Saudi Arabian oil and gas facilities in 2017, has expanded its target list to include oil and gas companies in Europe, the U.S., Australia, and the Middle East; electric utilities in North America and the Asia-Pacific region; and devices beyond Triconex controllers.

Constella Intelligence's most recent [28] Telco Sector Exposure Report identified nearly 4,900 total breaches and leakages and more than 5.6 million records exposed from the 20 top telecommunications companies between January 2018 and September 2021.

In 2019, the LYCEUM hacking Group was known to mainly target Middle East oil and gas facilities [38]. Attacks relied on password spraying and spear phishing. Remote access Trojan used DNS and HTTP-based communication to provide remote access capability for executing arbitrary commands and additional modules and uploading files [38]. Attack compromised email accounts of employees and stole information and credentials.

Also, [40] As adversaries targeting ICS bolster their capabilities, they can more easily carry out destructive attacks that cause operational disruptions and environmental damage.

Dragos noted that there were several “activity groups” targeting oil and gas industry in 2019, including DYMALLOY is an aggressive and capable group that can achieve long-term and persistent access to IT and OT environments for intelligence collection and possible future disruption attacks [40].

The ransomware attack on the Colonial Pipeline in May 2021 [29] had a huge impact on the industry. In February 2022, it was also reported that European oil facilities hit by cyber-attack and forced to operate at limited capacity.

February 2022 [69] the Germany energy giant was attacked and saw its IT infrastructure destabilized. The result? A closure of more than 200 gas stations across Germany. As reported [74] the aerospace industry remains the highest and biggest threat industries with 195% increase in cyberattacks, then comes the chemical industries 92%, followed by automobile 53% and industrial goods and services organizations 24% ransomware cyberattacks from the second half of 2022.

5. Recent Cyberthreats and Cyberattacks in Other Industries

There are several different types of cyber-attacks and security threats on several industries outside oil and gas. More popular among cyber security threats are the Trojan Horses, Worms, Ransomware, DDoS, and Phishing scams etc. These types of threats can be very dangerous for the cyber system.

In July 2023, Shell confirms that employee personal information has been stolen after the Cl0p ransomware group leaked data allegedly stolen from the energy giant [73]. The Cl0p ransomware group exploited a zero-day vulnerability in the MOVEit managed file transfer (MFT) product to steal data from at least 130 organizations that had been using the solution. To date, at least 15 million individuals are believed to be impacted. Other major organizations that have been named by Cl0p and confirmed being affected by the recent MOVEit exploit include Siemens Energy, Schneider Electric, UCLA, and EY [73].

On recent threats and cyber-attacks in other industries other than oil and gas, in fact all critical infrastructure sectors as revealed [43], including energy, manufacturing, health and transportation sectors etc. mostly rely heavily on sophisticated technologies like instrumented and industrial control systems. also, added that because, these are all accessed, monitored, and controlled via the internet, which, in turn, makes them susceptible to hacking, malware attacks, and other malicious activities [43].

In 2011, several vulnerabilities on Microsoft Windows resulted in the Night Dragon attack on downstream infrastructures of oil, energy, and petrochemical companies around the globe, including Exxon Mobil Corp and BP Plc [63]. Although cyber threats and attacks can be traced from decades back, actors are becoming more active and popular in hacking.

With the research [70], In 2014, Marriott was breached and almost 340m guest records were exposed. This incident was undetected until September 2018 and led to a £14.4m fine from the UK Information Commissioner’s Office. In January 2020, Marriott was hacked again, affecting 5.2m guest records. [70]

Report by [68] revealed that the Media giant NewsCorp has disclosed that hackers were dwelling on its network for two years. The incident was detected in 2022; notification letters recently sent to affected individuals reveal that the attackers had initially gained access to the network in 2020. [68]

As in the research [46], T-Mobile disclosed a breach that affects 37 million customer accounts. The attacker was able to gain access to the information through an Application Programming Interface (API). The intruder first gained access to the data in late November 2022; T-Mobile learned of the breach on January 5, 2023.

From “Ref” [52], revealed that starting in March, Microsoft will block XLL files coming from the Internet in Office Excel. In its Microsoft 365 roadmap, Microsoft writes that it is making this change "to combat the increasing number of malware attacks in recent months. “It was revealed [46], Health sector breaches recently reported to the US Department HHS include a network disruption affecting more than 250,000 patients at Bay Bridge Administrators, a network intrusion affecting more than 60,000 patients at Circles of Care Providers, and a data exposure affecting more than 35,000 patients at the Elizabeth Hospice In a joint cybersecurity advisory, the Cybersecurity, and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Multi-State Information Sharing and Analysis Center (MS-ISAC) warn that threat actors used legitimate remote monitoring and management software to gain access to the networks of multiple federal civilian executive branch agencies [46].

Researchers from Akamai say that most Windows data centers have not patched systems against a critical spoofing vulnerability in CryptoAPI. CircleCI has disclosed that a laptop belonging to one of its engineers was compromised in mid-December. The attackers used data-stealing malware that allowed them to obtain elevated privileges within CircleCI’s system [52, 53].

With [55] plenty of hacks are motivated by politics rather than pure financial gain, and that’s certainly true of GiveSendGo’s breach in February 2022. GiveSendGo is a Christian fundraising site favored by Canadian truckers who drove across the country to protest against COVID rules. Political hackers stole and then published the information of 90,000 people who had donated money to the protestors (opens in new tab) and then redirected the fundraising page to another site that criticized the truckers – a classic DDoS (opens in new tab) attack. Some data was also sent to a group that publishes leaked data that usually comes from far-right groups. It’s a clear lesson that companies need top-notch security to ward off political attacks – because not all breaches are driven by financial gain [55].

According to News Corp is one of the biggest news organizations in the world [55], so it’s no surprise that hackers are eager to breach its security – and in February 2022, News Corp admitted server breaches way back in February 2020.

As in the research [55] At the end of 2021 and the start of 2022, appointment management business FlexBooker was hit by a vast attack that affected around three million of its users. Confidential data including ID information, drivers' licenses and passwords was stolen by the hackers and then offered for sale on popular hacking message boards, and many powerful users have left FlexBooker because of the breach [55].

In March 2022, Trend Micro researchers observed several alleged cyberattacks perpetrated by different groups [30]. It has now become important more than ever to identify potential threats that may disrupt oil and gas companies, especially in these times when tensions are high.

The Computing giant Microsoft is no stranger to cyberattacks, [55] and on March 20th 2022 the firm was targeted by a hacking collective called Lapsus$(opens in new tab). The hackers made off with some material from Microsoft, too, but by March 22nd Microsoft announced that they'd shut down the hacking attempt promptly and that only one account was compromise [55].

On the same page [55], PressReaders is Vancouver-based company and the world's largest online distributor of newspapers and magazines. In March 2022 an attack halted its publication of loads of top news titles – from big names like the New York Times to local papers and outlets.

PressReader hasn't said if any ransomware (opens in new tab) was involved in the attack, but the attack immediately followed the company's announcement that it would give users in Ukraine free access – so it could well be a political attack. The company was able to quickly restore its full publishing capability, but the three-day attack stopped people from accessing more than 7,000 news sources.

Furthermore, still on recent cyber-attacks, the "Ref"[55] added that the Block (formerly Twitter) owns this popular mobile payment tool (opens in new tab), and in April 2022 the firm acknowledged that a former employee had breached the service's servers. The culprit clearly had a significant axe to grind with the business. The hack involved customer names, stock trading information, account numbers and portfolio values alongside load of other sensitive financial information [55].

Also, Google platform certificates [67] used by original equipment manufacturers (OEMs) of Android handsets have been compromised (stolen) and used to validate malicious Android apps. But Google says that "OEM partners promptly implemented mitigation measures as soon as we reported the key compromise.

It began in November of last year [69], when the Emotet malware was detected on Royal Mail servers. Early January 2023, Royal Mail was subject to a ransomware attack by an affiliate using LockBit Ransomware-as-a-Service (RaaS). This attack affected a distribution center near Belfast, Northern Ireland, where the printers began printing the ransomware gang's demands [69].

In a press release [58], a financial software firm ION Group was the victim of a ransomware attack on January 31 and February 2, 2023. The attack affected ION's Cleared Derivatives division. In a press release, ION wrote, "The incident is contained to a specific environment, all the affected servers are disconnected [58].

The SANS Institute revealed [68] on February 2023, the US Marshals Service (USMS) detected a cybersecurity incident involving ransomware and data exfiltration on one of its stand-alone systems. SANS report that "The affected system contains law enforcement sensitive information, including returns from legal process, administrative information, and personally identifiable information pertaining to subjects of USMS investigations, third parties, and certain USMS employees [68].

Finally, the Ref" [60] revealed in February 2023 that Password manager LastPass says that an attacker infiltrated a DevOps engineer's home computer and installed a keystroke logger. The infection allowed the attacker to access a decrypted corporate vault [60].

6. Cybersecurity Control and Best Practices for Industrial IoT (ICS, SCADA etc)

Responsibility for implementing ICS security controls has shifted this year (2022), with many organizations claiming the responsibility belongs to the owner or operator of the ICS (38%) or the engineering manager (36%) as revealed by survey [48]. Since, ICS attack groups have been observed "living off the land"; that is, abusing systems, features, and industry protocols native to industrial environments, turning control systems against themselves, Some examples of living off the land are an attacker gaining access to an HMI with legitimate operator access but then using the HMI commands against the process to, for example, open circuit breakers in the field in an electric substation or change the chemical mixture in a water treatment facility. No malware is used to cause the impact; rather, the adversaries are using built-in and legitimate engineering software, features, and/or ICS protocols to cause impacts [48]. Organizations should note, especially if they are part of critical infrastructure, that they have an obligation to ensure a safe operating environment for personnel and a duty to protect from harm the communities they operate in by ensuring appropriate investments in ICS cybersecurity. They must possess this as a priority. [55] The controls are intended to be outcome focused instead of prescriptive in nature. They are also intelligence-driven in that they have been chosen based on the analysis of recent compromises and attacks in industrial companies around the world. The survey by [55] revealed Five cybersecurity controls can be utilized together to create an efficient and effective industrial control system (ICS) or operational technology (OT) security program.

(i) Industrial Control System Incident Response: Operations-informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises are designed to reinforce risk scenarios and use cases tailored to the ICS environment.

(ii) Defensible Architecture: Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement.

(iii) Industrial Control System Network Visibility Monitoring: Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control.

(iv) Secure Remote Access: Identification and inventory of all remote access points and allowed destination environments, on-demand access, and MFA where possible, jump host environments to provide control and monitor points within secure segment. and

(v) Risk-Based Vulnerability Management: Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

Finally, according to ICS-CERT [59], revealed that overarching principles of ICS security are incorporated into various global standards and best practice frameworks. Specifically, the International Electrotechnical Commission (IEC), International Society of Automation (ISA), and National Institute of Standards and Technology (NIST) [59]. CSA GROUP in addition to [55] mentioned some elements of their recommended strategies and best practices for ICS cybersecurity which include:

(i) Developing security policies, procedures, training, and educational material.

(ii) Implementing a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.

(iii) Separating corporate and ICS networks.

(iv) Establishing separate authentication mechanisms and credentials for users of the ICS and corporate networks.

(v) Restricting physical access to ICS networks and devices.

(vi) Building redundancies in system components and networks.

(vii) Applying stronger controls to safety systems in the ICS to help ensure that they can properly deploy risk reduction measures against major accident hazards.

(viii) Designing critical systems for graceful degradation to prevent catastrophic cascading events.

The authoring agencies at [59] called upon network defenders to examine their current cybersecurity posture and apply recommended mitigations in this joint CSA. These include training users to recognize and report phishing attempts, enabling, and enforcing phishing-resistant multi-factor authentication, while also installing and regularly updating antivirus and antimalware software on all hosts [68].

Finally on best control measures to mitigate against cyber-attacks in the oil and gas ICS and other industries as revealed on March 2, 2023 [71], the White House released its National Cybersecurity Strategy, which rests on five pillars: Defending critical infrastructure, disrupting and dismantling threat actors to blunt their threat to national security and public safety, shaping market forces to boost security and resilience, Investing in a resilient future through “strategic investments and coordinated collaborative action:” and forging international partnerships to achieve common goals. The strategy’s initiatives include seeking to place responsibility for cybersecurity to manufacturers rather than end-users, imposing minimum security standards for critical infrastructure operators, Directing the Office of Management and Budget (OMB) to oversee technology modernization at federal civilian agencies [71].

Finally, we take the suggested cybersecurity control measures and best practices for oil and gas industrial control system, and other industries provide us new ideas and updates in the industry.

7. Methodology

Research methodology simply means a guide to research and how it is conducted and allows the reader to critically evaluate a study ‘s overall validity and reliability [44]., Research can be carried out in virtually every field of endeavours including Science, Engineering, Information and Communication Technology etc. [45]. This study commenced with an attentive review of cyber-crime’s happenings, with a review on cybersecurity specialized international literatures, including legal aspects, and analysis of the last years and this year major events in industrial IoT domain devices (SCADA, ICS etc.). The aim of the paper to have an overview of new cybersecurity monitoring and control techniques in industrial IoT ecosystem, to understand the means of operation and potential impact upon the industries, as well as the countermeasures and best practices deployed for control against industrial IoT systems attacks.

The analysis of cybersecurity monitoring and control techniques, throws more light also on their limitations and resources, clarify their pre- suppositions and consequences, relating to their potentialities to the twilight zone at the frontiers of knowledge [44]. The study also reveals recent threats and cyberattacks in industrial IoT systems. The action research types were employed as a most useful form of research method during this research work [44].

8. Conclusion

Our finding remains that cybersecurity in industrial IoT systems (ICS, SCADA etc.) needs defense daily to mitigate against various cyber actors and attacks as shown in figure 8 by the global cybersecurity alliance on monitoring cybersecurity performance (GCAMCP). Great development has been made in cybersecurity monitoring and control in industrial IoT ecosystem, especially on critical infrastructures based on physical and cyber-physical systems.

The study reveals improved cybersecurity monitoring and control techniques that can be deployed to mitigate against cyber-attacks in industrial IoT systems and other related industries. First, the FASTEN Suite (2.1) Industrial IoT based architecture was made for detection support systems, secondly, YO-i Thingwise industrial Data OS (iDOS) (2.2) is for supporting digital transformation of industrial operational management, Thirdly, the NOZOMI Industrial Defender Solution (2.3) support vulnerability assessment, endpoint protection, traffic analysis capabilities and many more, fourthly, GigaOM Radar Report is for industrial IoT security protecting OT from cyber-attacks (2.4), and then, the Third-Party Cybersecurity Services Across Product Lifecycle and Draktrace PREVENT/IoT Product (2.5) has been deployed in hundreds of critical infrastructures companies which boost their cyber safety capabilities and yet the chemical industries where industrial IoT technology is deployed experienced 92% ransomware cyberattacks in second half of 2022. With these analysis cybersecurity monitoring and control techniques in industrial IoT systems (ICSs, SCADA etc.), including other industries will be of help to researchers and academia's have new ideas on industrial IoT security monitoring and control techniques, and to carry out future research works development in this same domain.

References

[1] Digiteum Team (2021), IoT Revolution in the Oil and Gas Industry (Online).

[2] Siemen Energy (2020), Oil and Gas Companies Must Act Now on Cybersecurity, hbr.org/sponsored/2021/08/oil-and-gas-companies-must-act-now-on-cybersecurity.

[3] Trent J., (2016), Industrial-sized Cyber Attacks Threaten the Upstream Sector, SPE-0316-0042-JPT, nepetro.org/JPT/article-abstract/68/03/42/209373/Industrial-sized-Cyber-Attacks-Threaten-the?redirectedFrom=fulltext

[4] Thomas W. E, & David O. M., (2017), Theoretical Research in Research Methods for Cyber Security, www.sciencedirect.com/topics/computer-science/theoretical-research

[5] Jake K, Kristine W. E, Mary H, Tyler J, Kyle J, Brian L., (2013), An Analysis of cyber-Conflict and Within the Oil & Gas Industries, www.mandiant.com/apt1

[6] Cathy Cassell (Online), Manchester Business School, Theoretical approaches, Quality in Qualitative Research, www.methods.manchester.ac.uk/themes/theoretical-approaches/

[7] Jakub P., Grzegorz K., and Jerzy L., (2019), Key role and potential of Industrial Internet of Things (IIoT) in modern production monitoring applications, MATEC Web of Conferences 252, 09003. published by EDP Sciences.

[8] CS Makarand Lele (2018), Oil and Gas Industry, Publish by The Institute of Company Secretaries of India,

[9] Laudelino Soares, Rafael Souza (2020), Cyber Risks in The Oil & Gas Industry, Rio Oil & Gas Expo, and Conference 2014.

[10] Bill S & Mario C, Parker H (), Bridging the gap between the digital and physical plant, eHANDBOOK: IIoT, www.plantservices.com.

[11] Multan Singh Bhati (2018), Industrial Internet of Things (IIoT): A Literature Review, International Journal for Research in Engineering Application & Management (IJREAM), Vol-04, Issue-03.

[12] Anshu M, Andrew S. & Paul Z., (2017), Protecting the Connected Barrels, Cybersecurity for Upstream oil, and gas. jpt.spe.org/protecting-connected-barrels-cybersecurity-upstream-oil-and-gas.

[13] Essang ONUNTUEI (2018), Safety, Risk, And Reliability of Cyber Network in Oil and Gas Industry, PUPIL: *International Journal of Teaching, Education and Learning*, 2 (2), 81- 97.

[14] Helms J., Salazar B., Scheibel P., Engels M., & Reiger C., (2017). Safe Active Scanning for Energy Delivery Systems Final Report. Lawrence Livermore National Security https://doi.org/10.2172/1409972

[15] Robert A Martins, Graham John B, Bradford W. M., Jesus M., (2015). Industrial Internet Consortium. Industrial Internet Reference Architecture Technical Report, tech-arch.tr. 001 2015-06-04 Version 1.7.

[16] Mario A., et al., (2015), Industrial Internet of Things (IIoT), Opportunities, Risk, Mitigations.

[17] Abubakar Sadiq M., Philipp R., Pete B., Omer R., & Eirini A., (2022), Cybersecurity Challenges in The Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective.

[18] Cybersecurity Solutions for Oil & Gas, Your Partners in Oil & Gas Cybersecurity (Online), oxguardsolutions.com/oil-gas-cybersecurity/

[19] Gas (Online), Journal of Petroleum Technology, search.spe.org/i2kweb/SPE/doc/speorg: ED4F437D.

[20] Leo D., (2022), BBC (Online), UK helping Ukraine combat Russian cyber-attacks.

[21] DNV GL. Oil and gas forecast to 2050, 2017.

[22] Piotr Ciepiela (2016), Digitization and cyber disruption in oil and gas.

[23] Roberto V., Narciso C., João B., Symone A., & Flavio D., (2019), An IIoT-based architecture for decision support in the aeronautic industry, MATEC Web of Conferences 304, 04004, (http://creativecommons.org/licenses/by/4.0/).

[24] Mohammed Y. A., Wazir Z W., Gharibia M., Khurram., & Quratulain A, Wireless Sensor Networks in oil and gas industry: Recent advances, taxonomy, requirements, and open challenges.

[25] Ralf Luis de M, Luciana D, L, Tiago M. B, Luiz P. B., Alexandre G, Ludmilla B. W (2020), Industrial Internet of Things: Device Management Architecture Proposal, 2019 International Conference on Computational Science and Computational Intelligence (CSCI), OI 10.1109/CSCI49370.2019.00221

[26] Andy Zimmerman (), Plant Services, TECHNOLOGY REPORT: IIoT and Asset Monitoring, Putman Media, www. plantservices.com

[27] Martin Sime (2021), How IIoT Thermal Monitoring Solutions Can Increase Asset Lifetime and Prevent Fires on Solar Farms, www.sensata.com

[28] Centre for Cybersecurity (2022), 3 Ways to Protect your Organisation from Identity-Based Cyber-attack (Online),

[29] Kazuhisa T., (2022), Oil/Gas Cybersecurity: Halt Critical Operation Attacks, Compliance & Risks, www.trendmicro.com/en_us/research/22/c/oil-gas-cybersecurity-critical-operation-attacks.html

[30] Trend (2022), Cyber Security Review (2022),_Oil and Gas Cybersecurity: Industry Overview Part 1, Cyber Threats www.cybersecurity-review.com/news-august-2022/oil-and-gas-cybersecurity-industry-overview-part-1/

[31] Yoana C., (2021), Free Whitepaper, Preventing cyberattacks in the oil and gas industry,

[32] Technology (2019), Cyber security for oil and gas industry applications (Online).

[33] Wazir Z. K., & Muhammad K. K., (2019), Advance Persistent Threats Through Industrial IoT on Oil and Gas Industry, Global Foundation for Cyber Studies, and Research, ResearchGate.

[34] Shi-Wan Lin., Maxine Fu., Jin Zhou., Liu Zhenqi., Li Kun., Jia Yangkai & Isabella Li (2021), Digital Twin and IIoT in Optimizing Manufacturing Process and Quality Management, IIC Journal of Innovation.

[35] Kimberley W. (2018), 3 Cyber Threats to the Oil & Gas Industry, w.cs4ca.com/newsroom/feature/3-cyber-threats-to-the-oil-gas-industry/

[36] Cybersecurity for oil and gas industry, Cyberthreats protection, www.otorio.com/industries/oil-and-gas/, (Online).

[37] 2021 Cyber security Predictions: These two words should keep security experts at night (2020) (Online). The Industrial Cybercrime Impact Report - 2021 Predictions.

[38] Ashok S. (2019), Cyber Security Challenges in the Oil and Gas Industry- An Overview www.yokogawa.com/eu/blog/oil-gas/en/cyber-security-challenges/

[39] Asheesh Kumar., (2020), Energy & Utility, Defending the Oil and Gas Industry Against Cyber Threats, securityintelligence.com/posts/oil-gas-security/

[40] Nate T., (2021), AskWavesCybersecurityNews, How does a ransomware attack work?

[41] Cybersecurity risks in US critical infrastructure sector call for better skills, technologies, processes.

[42] Anna Ribeiro (2022), Testing environments assist S&T, CISA to safeguard transportation infrastructure, expand training tools.

[43] Fidelis I. U (2016), Fundamental of Research Methodology and Data Collection, Research Gate.

[44] Kenneth I. Nkuma-Udah (2020), ICT Research Methodology and Statistics, Published by National Open University of Nigeria.

[45] Haradhan K. M., (Online), Research Methodology, Chapter III, Aspects of Mathematical Economics, Social Choice, and Game Theory.

[46] George M (2021), 8 Cyber Attacks on Critical Infrastructure, Cybersecurity.

[47] Dean P (2022), The State of ICS/OT Cybersecurity in 2022 and Beyond, Analyst Program. A Survey.

[48] Pascal A, Tom S & Ian B (2023), Compelling need to Build ICS Resiliency across OT and ICS environments in 2023. Industrial Cyber News.

[49] J. Jeba Praba., (2016), Cyber Security and Threats, https://www.researchgate.net/publication/322466321, Vol. 3, Page No. 201, Research Gate.

[50] Jamie Crandal., (2019), Cybersecurity and Offshore Oil: The Next Big Threat, 4 OIL & GAS, NAT. RESOURCES & ENERGY J. 703, Vo l4 No 6.

[51] SANS NewsBites Vol. 25 Num. 08: VMware Software Needs Top Priority Patching; Microsoft Blocking XLLs is a Good Thing; One More Warning About Living Off the Land and Remote Access Attacks.

[52] SANS NewsBites Vol. 25 Num. 05: Many Lessons to Learn from CircleCI Breach Report; Patch Zoho ManageEngine Ahead of Exploit Code Release; Yet Another Password Manager Product (Norton) Breached.

[53] Cliff Glantz et el. (2021), Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (On), -C2M2) G.

[54] Mike J,. (2022), Top data breaches and cyber-attacks of 2022, Cybercrime is big business, and it's already rife in 2022 – we've highlighted ten top cases. www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022

[55] Robert M. L & Tim C., (2022), The Five ICS Cybersecurity Critical Controls, SAN Institute.

[56] SANS NewsBites Vol. 24 Num. 94: Rackspace Outage Emphasizes Need for Cloud Outage Workarounds; Check for Falsely Signed Malicious Android Apps; Isolate Baseboard Management Controllers from External Connectivity.

[57] SANS NewsBites Vol. 25 Num. 010: Check Enrollment Status on Your Managed Chromebooks; Another Ransomware Incidents Points Out Costs of Manual Workarounds; Vulnerabilities Found in Electric Vehicle Charger Protocols.

[58] CSA, protecting industrial control systems from advanced cyber threats, A comprehensive defense strategy that pairs cybersecurity and functional safety in every layer of the system. www.csagroup.org/wp, content/uploads/CSA_Group_Protecting_Industrial_Control_Systems_White_Paper_NA_English.pdf

[59] Steve Mustard (2022), Global Security Alliance, Industrial Cybersecurity Case Studies and Best Practices.

[60] Wei Qin, Siqi Chen, Mugen Peng (2020), Recent advances in Industrial Internet: insights and challenges, Digital Communications and Networks,

[61] George S, Dimitris G, and Evangelos L., (2020), Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns, https://creativecommons.org/licenses/by/4.0/.

[62] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, C. Glyer, "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure", FireEye Dec. 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers deploy-new-ics-attack-framework-triton.html. Accessed on Mar. 16, 2020.

[63] "Triton: Malware that aims to attack industrial safety systems", Symantec, Dec. 2017. [Online]. Available: https://symantecblogs.broadcom.com/blogs/threat-intelligence/triton-malware-ics. Accessed on Mar. 15, 2020.

[64] H. Kobayashi, K. Watanabe, T. Watanabe, and Y. Nagayasu., (2010), "Development of Information Security-Focused Incident Prevention Measures for Critical Information Infrastructure in Japan", Critical Information Infrastructures Security, LNCS, pp. 22–33.

[65] J. Robertson, M. Riley., (2020), "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," Bloomberg.com, Dec. 2014. [Online]. Available: https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar. Accessed on Mar. 15.

[66] Anna Rabeiro, (2023), New Darktrace PREVENT/OT will use AI to 'pre-empt' cyber-attacks on critical infrastructure.

[67] Anna Rabeiro (2023), DPRK hackers target critical infrastructure, exploit Log4Shell, SonicWall vulnerabilities. industrialcyber.co/ai/new-darktrace-prevent-ot-will-use-ai-to-pre-empt-cyber-attacks-on-critical infrastructure/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Industrial+Cyber+News&utm_campaign=Industrial+Cyber.

[68] SANS NewsBites Vol. 25 Num. 017: Is Bitmining Raising Your Electric Bill?; It's Time to Try High Fidelity Automated Attack Disruption Techniques; Password Manager Vendor LastPass Breached Was Caused By Engineer's Use of Reusable Passwords for Remote Access

[69] Mike Jennings (2022), Top data breaches and cyber-attacks of 2022, www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022. (Online).

[70] Patrick O'Connor, (2022), The biggest cyber-attacks in 2022, www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2022/. (Online).

[71] SANS NewsBites Vol. 25 Num. 018: US National Cybersecurity Emphasizes Need for Regulation; Enable GitHub Secret Scanning on All Libraries; Make Sure You Are Not Repeating Booking.com's OAuth Misconfiguration.

[72] SANS Survey (2023) - The State of ICS/OT Cybersecurity in 2022 and beyond, Nozomi Networks, www.bankinfosecurity.com/whitepapers/sans-survey-i-state-icsot-cybersecurity-in-2022-beyond-w-11610

[73] Eduard Kovacs (2023) Shell Confirms MOVEit-Related Breach After Ransomware Group Leaks Data, www.securityweek.com/shell-confirms-moveit-related-breach-after-ransomware-group-leaks-data/

[74] Chris Morgan (2023), The Top Cyber Threat to Manufacturing Industry in 1H, Reliaquest, ww.reliaquest.com/blog/cyber-threats-to-manufacturing-industry-1h-2023.