UDC 004.7 **doi: 10.26906/SUNZ.2024.4.114**

Murad Omarov[1], Vusala Muradova[2]

[1] Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
[2] Lankaran State University, Lankaran, Azerbaijan

CYBERSECURITY PROBLEMS IN THE OIL AND GAS INDUSTRY

Abstract. Due to the widespread use of digital and Internet technologies in all processes of the oil and gas industry's production cycle, cybersecurity is becoming an increasing threat. Therefore, today cybersecurity is becoming one of the priorities of technological development of oil and gas companies. The article provides a brief description of the digital transformations taking place in the oil and gas industry, analyzes the main new cybersecurity threats and provides information on cybersecurity incidents. The issue of developing new technologies based on deep learning for smart oil fields is considered.

Keywords: oil and gas industry; digital mining; OT; IoT; cybersecurity.

Introduction

Currently, the oil and gas industry is going through a transitional period accompanied by a number of serious problems, this transitional period is characterized by a sharp drop in oil prices on world markets and chaotic fluctuations, depletion of light oil reserves, expansion of the heavy oil phase (heavy oil due to both its density and complexity of production), characterized by deepening competition between the leading players in the industry (transnational oil companies, oil-producing countries).

One of the main characteristics of this transition period is the widespread use of intelligent information technologies throughout the entire production cycle. It should be noted that large multinational oil and gas companies now have special departments dealing with intelligent oil and gas field technologies. Such companies are Shell (“Smart Fields”), BP (“Field of the Future”), Chevron (“iFields”), as well as Saudi Aramco, Petrobras, Kuwait Oil and others. Oil and gas companies Optimization of various oil and gas production processes using technologies such as the Internet of Things (IoT), cloud technologies, Machine Learning (machine learning, algorithms that learn during data processing), high-performance computing (data processing). large amounts of data) are working on the development of methods [1, 2]. The application of these technologies allows finding new methods to improve the efficiency of oil and gas field development, increase oil recovery rates and reduce costs.

At the same time, the oil and gas industry is facing new threats due to the widespread use of digital technologies and increased dependence on cyber structures. Cyberattacks on oil and gas facilities can be targeted at a variety of purposes: cyberterrorism, industrial espionage, sabotage of operations, data theft, etc. Oil and gas companies are forced to take various measures to prevent the legal, operational and technical risks they face in cyberspace.

1. Classification of the oil and gas industry

The oil and gas industry has different sectors, which include crude oil production, refining and the retail distribution network. In the English-language literature, these sectors are referred to as Upstream, Midstream and Downstream, respectively.

Upstream - generally, organisations involved in exploration - includes oil and gas exploration and production. Oil and gas exploration includes prospecting, seismic surveying and drilling for the purpose of developing oil and gas fields. Upstream often includes the well, wellhead, completion and reservoir, while downstream includes production and processing.

Midstream - includes the transportation, processing and storage of oil. This usually includes gas processing plants, LNG plants, and oil and gas pipelines.

Downstream includes oil refining, petrochemicals and retail.

2. Exploitation technologies in the oil and gas industry

Along with IT technologies, industrial automation technologies are widely used in the oil and gas industry. The term “operational technology” is used to demonstrate the technological and functional differences between traditional IT systems and industrial control systems. Operational technologies are hardware and software used to monitor and change the physical state of a system.

Operational technologies include industrial automation and control systems such as SCADA (supervisory control and data acquisition systems), DCS (distributed control systems), PLC (programmable logic controller), open platform communication servers, devices, and analyzers.

Rational technologies are used to monitor and control physical processes in the oil and gas sector; the data obtained on process parameters are used to automate processes.

Automation is possible with the help of electrical, mechanical, hydraulic, pneumatic actuators and control valves.

The integration of IT and OT technologies is now increasing, and devices are connected to the corporate network and external networks [3]. Attackers who can easily connect to control devices can cause even more damage. It is not only about the damage caused by stopping the technological process, but also about the possibility of causing physical damage - for example, a fire or explosion may occur at oil refineries and petrochemical plants. This scale of cybersecurity risks brings them to the national level [4].

3. Key cybersecurity threats in the oil and gas industry

Analytical company DNV GL has compiled a list of the ten most pressing cybersecurity threats to companies operating on the Norwegian continental shelf [5]. Obviously, these threats can be applied to other oil and gas companies around the world:

1. Lack of awareness and training of employees in the field of cybersecurity
2. Remote work during operation and maintenance
3. Use of standard IT products with known gaps in the production environment
4. Limited cybersecurity culture among vendors, suppliers and contractors
5. Insufficient separation of data networks
6. Use of mobile and storage devices, including smartphones
7. Data networks between land and sea facilities
8. Data centre premises, offices, etc. inadequate physical security
9. Sensitive software
10. Outdated and unusable management systems at enterprises

These gaps in cybersecurity can be overcome with a risk-based approach [6]. An international survey of 1,100 professionals conducted by DNV GL found that while companies are actively managing their information security, only just over half (58%) have adopted a specific management strategy and only 27% have set specific goals.

Note that IT and OT are created for different missions, so ownership and responsibility is fragmented across the organisation. The nature of new threats is related to attacks through IoT devices. The number of sensors, transmitters, and smart industrial systems connected to the network is growing rapidly, and hackers are finding new ways to connect to the network. The characteristic of IoT devices is that their computing power is low and it is difficult to build security systems on them, including mutual authentication and traffic encryption.

Another threat is caused by the increasing interdependence of systems, forming links in a single production chain. In [7], it is emphasised that a cyberattack on any element of the supply chain affects all other nodes.

4. Cybersecurity incidents in the oil and gas industry

The history of software incidents in the oil and gas industry goes back to the 1980s. In his book Into the Abyss, Thomas Reed, a senior US national security official, described how the US allowed SSRI to steal the codes for its pipeline monitoring programme from a Canadian company.

The malicious code embedded in this programme caused a massive explosion on the Trans-Siberian Pipeline in June 1982. The Trojan was activated during a pressure test on the pipeline, dramatically increasing the normal pressure and causing an explosion [8].

In the winter of 2002-2003, during a cyberattack on PDVSA (Petróleos de Venezuela, S.A.) systems, hackers managed to penetrate the SCADA system responsible for loading tankers at a marine terminal in eastern Venezuela. The hackers prevented the loading of the tanker for eight hours by deleting a programme in the PLC. The attackers' tactics were not perfect, and the problem was the relatively easy detection and restoration of the PLC programs from backups.

Here is a brief chronicle of the history of cybersecurity incidents that have occurred in the oil and gas industry.

2009 - A computerized monitoring system in Bayamon, Portugal, failed, causing an explosion of a tank filled with gasoline and a three-day fire.

2010 - The Stuxnet virus was used to take over industrial control systems around the world, including computers used to run oil refineries, pipelines, and power plants.

2012 - Saudi Aramco, the world's largest oil producer, became the victim of a large-scale cyberattack. The oil giant announced that 30,000 computers were infected with the virus. A group of hackers called Cutting Sword claimed responsibility for the attack on Saudi Aramco. They infected the company's systems with malware for political reasons [9,10].

2012 - Telvent, a provider of remote control and monitoring tools for the energy sector, suffered a breach of its internal firewall and security systems. According to Telvent, every Fortune 100 energy company uses its systems. The attackers stole files related to the SCADA project, a remote control tool that allows you to connect outdated IT equipment to Smart Grid technologies. Most likely, the hackers were trying to find holes in the software to directly attack energy companies, so they were looking for the source code.

2012 - Ugly Gorilla attacked more than two dozen American gas companies, stealing confidential data from gas pipeline companies.

2012 - The computer system of RasGas, the leading LNG exporter in Qatar, was infected with an unknown virus, which led to the company's closure for several days[11,12,13].

2012 - The popular Flame malware was used to spy on a company in the Middle East. The malicious program has the ability to record audio, screenshots, and user actions.

2014 - Hackers attacked about 300 different companies in the Norwegian oil and gas industry, including Statoil. The attack was carried out via email. When the email was opened, malware was downloaded and security holes were discovered.

2015 - It was discovered that online attackers were remotely controlling ATG (Automated Tank Gauges) devices used to measure gasoline levels at retail stations in the United States. The attackers could cut off the fuel supply to the ATGs.

2017 - Oil and gas companies were attacked by the global ransomware Petya [14–16].

5. Scada systems security standards

Companies turn to standards to ensure the security of their SCADA systems [6]. The ISA-99.02.01 standard, approved by the American National Standards Institute

(ANSI), is one such standard (Security for Industrial Automation and Control Systems). The standard defines seven key steps for establishing a cybersecurity management system (KMS) for SCADA and control systems.

The steps of ISA-99.02.01 fall into three main categories: risk analysis, risk management through KMS, and monitoring and improvement of KMS. The first category establishes milestones for both assessing the current security situation and determining what security objectives it wants to achieve.

The second category reflects the processes for defining security policy, security organisation and security awareness in the company, and provides recommendations for security measures to improve SCADA security. The key idea in this category is a concept known as defense in depth, where security solutions are carefully deployed at multiple levels to prevent cyber attacks.

The Network and Information Security Directive (NISD), which came into force in the European Union in May 2018, ensures that energy companies' network and information systems meet minimum cybersecurity standards. The UK National Cyber Security Centre has developed detailed guidance on the requirements for compliance with this Directive.

The directive refers to operators of ‘essential services’, which will apply to many energy companies. Along with electricity producers and transmitters, and oil and gas producers and distributors

the companies involved are also covered by this Directive. The Directive requires Member States to introduce ‘appropriate policies and regulatory measures to achieve and maintain a high level of security of network and information systems’, as well as an obligation to report incidents. The Directive provides for ‘effective, proportionate and impartial’ sanctions for non-compliance with the relevant standards and failure to report incidents.

6. Security issues at the layers in IoT architecture

The technical solutions used by companies in the oil and gas value chain are known as the Internet of Things (IoT). The IoT is a dynamic, large-scale environment where things are connected to a network and transmit data through software, sensors, and receivers [19]. IoT involves the collection, analysis, and action of data created by a network of objects and machines. An IoT device is a computer, laptop, smartphone, tablet, etc. with Internet access. In addition to these devices, it also includes Internet access for other traditional “unintelligent” devices and things. All events occurring in the environment can be monitored with the help of numerous small-sized receiving devices (sensors) using wireless technology. However, storing big data collected from sensors requires storage with a large capacity.

As you know, IoT can aggregate and analyze constantly changing data, which is necessary for making decisions driven by it. In the current industrial environment, oil and gas companies handle data the same way they handle hydrocarbons; data needs to be generated, transmitted, stored, and processed. With the development of IoT strategies, oil and gas enterprises are trying to capitalize on the era of “digital transformation”.

In today's digital era, information can often flow from the mine to the operational process network, then to the corporate network, and finally to the end user, and vice versa. This also includes trojans, malware, ransomware, viruses, etc. means that such cyber threats exist. People move from the Internet to the corporate network, from the corporate network to the ERP network, and from there to the industrial network. The conclusion from this point is very critical - if there are cyberattacks on oil and gas organizations, the consequences will be very serious.

Areas of application of IoT

The scope of the IoT concept is very broad. For example, the oil and gas industry, environmental monitoring, smart homes, smart transportation management, e-medicine, etc. can be widely used in various fields. As an example, it can be noted that as a result of the integration of the industrial concept and the IoT concept, intelligent devices involved in production processes will achieve minimization of human error, real-time evaluation by decision support systems. processing. This will lead to improved production quality, reduced financial costs by ensuring optimal use of resources and the production of competitive products.

1) Industrial IoT devices [20]: The use of existing industrial automation systems together with IoT devices has many important advantages:

- Smart devices with IoT functions can control the production process and minimize operator intervention by creating automatic communication with each other over the network;
- Recovery/protection measures against predictable failures can be implemented by preliminarily identifying possible errors;
- Shortage of raw materials to produce products of plants or companies can be ensured in a timely manner by determining in advance;
- Control issues at plants or companies can be carried out from anywhere in the world. Thus, information about the production process and malfunctions that have occurred is available from anywhere via a network connection.

The architecture of the Internet of Things.

Data collected from receiving devices/sensors placed on objects in the fields is continuously transmitted to the monitoring and control center via RFID or any wireless transmission medium, which is monitored online in real time. By functionality, the IoT architecture is divided into the following levels (Table 1)/

The application of existing data security solutions to the IoT concept requires transmission environments that are not secure at a serious level, are dynamic and large-scale, have a large number of devices of different origins, etc. is not considered effective for reasons such as Given that large amounts of data contain sensitive information during transmission, it becomes necessary to ensure data security. In general, the IoT has an architecture consisting of the following layers [21]: the receiver (perception) layer, the network layer, and the

application layer. Since the processes performed at different levels of the IoT architecture differ, security issues also differ by level. Security issues in the IoT concept require a different approach at each of these levels. Thus, in Fig. 1, the security issues in the IoT architecture are described as follows:

Table 1 – **IoT Architecture**

IoT architecture in layers	Levels Characteristics
Program layer	Integrated layer with existing hardware (RFID, sensors, actuators, etc.) to acquire physical environment data
Network layer	The layer that ensures the interaction of sensors and receiving devices with each other and the transmission of data over the network via a wired or wireless network.
Receiver layer	Interface layer (SCADA, DCS, etc.), which provides methods of interaction with the user and other programs.

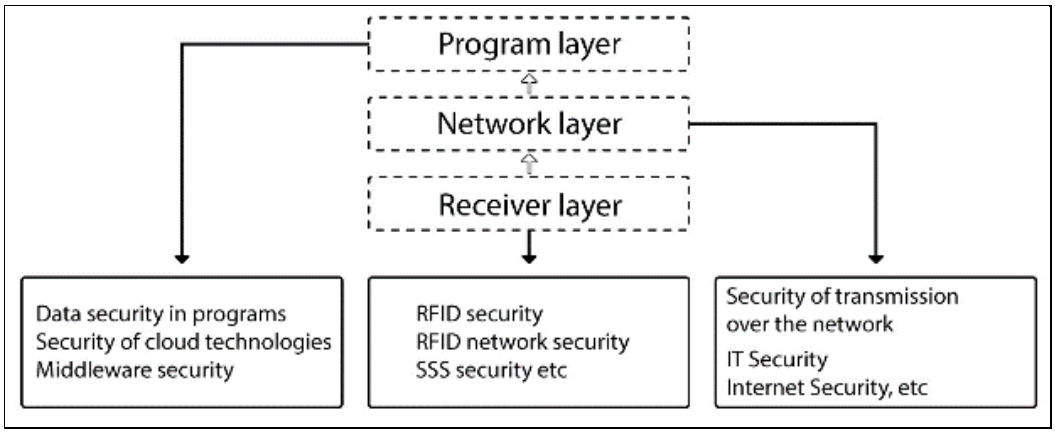

Fig. 1. Security issues at the layers of IoT architecture

A. Program layer. The program layer is the lowest layer in the IoT architecture. Typically, the memory and processing capacities of sensors/receivers are not at an adequate level.

Security issues at this level include ensuring the physical security of sensor devices and the security of data collection. Security systems are difficult to install here, and sensor data must be protected in terms of completeness, availability, and confidentiality. Additionally, attacks from the external network environment, such as DoS attacks, pose new security challenges. RFID includes security issues such as information leakage, replication attacks, data tracking, counterfeiting, cloning attacks, and man-in-the-middle attacks [21].

B. Network layer. The implementation of existing communication security mechanisms at this layer is complex and difficult. Verification of the authenticity of the data provided by the user (subject) - authentication and identification of the subject by unique information previously recorded in the system - identification is one of the methods of preventing unauthorized access. It is the basis of a security mechanism where confidentiality and integrity are equally important. In addition, distributed denial of service attacks is a common attack method in the network, especially in the Internet of Things, as this attack method is more relevant, an approach should be developed to solve against distributed denial of service attacks.

C. Receiver layer. The receiver layer is the highest layer in the IoT architecture and imposes different security requirements for different application environments.

In general, security concerns at the receiver level include tracking and external intrusions. In addition to being responsible for processes such as transmission control and traffic management, this layer also includes responsibilities for securing the applications used to collect data by sending requests, converting data into an understandable, relevant form.

For example, data sharing at the receiver layer can create issues such as data privacy, access control, and disclosure.

The completeness and reliability of sensor data is becoming a major research area [21]. Another key issue in sensors is to ensure objectivity, which is one of the main challenges. It is necessary to apply mechanisms to protect the privacy of people and objects in the physical environment. People are often unaware of the sensors/receivers around them. For this reason, it is necessary to adopt rules to protect human rights

Conclusions

The oil and gas industry is one of the industries most exposed to cyberattacks, with serious potential economic and national security implications.

Therefore, cybersecurity is an extremely important issue for the oil and gas industry, and cybersecurity

measures must keep pace with the speed of digitalisation of oil and gas operations.

Different sectors of the oil and gas industry naturally have different levels of risk and require different cybersecurity strategies. It is necessary to address the cybersecurity of mines, oil and gas transportation and processing, environmental processes, and the entire range of activities in the industry. On the other hand, it is necessary to adopt laws and regulations related to the physical environment in the environment that surrounds us.

Therefore, there is a need to overcome the contradictions and improve the security of the IoT concept as a relevant and new field of research.

REFERENCES

1. R.M. Alıquliyev, Y.N. İmamverdiyev, "Neft-qaz sənayesi üçün konseptual Big Data arxitekturası," İnformasiya texnologiyaları problemləri, №1, s.3–14, 2017.
2. R.M. Alıquliyev, Y.N. İmamverdiyev, "Neft-qaz sənayesi üçün Big Data strategiyası: Ümumi istiqamətlər," İnformasiya texnologiyaları problemləri, №2, s. 34–47, 2017.
3. F. Shaik, A. Abdullah, & S. Klein, Digital transformation in oil & gas - Cyber security and approach to safeguard your business. World Petroleum Congress. 2017.
4. B. Clayton, & A. Segal, Addressing cyber threats to oil and gas suppliers. Council on Foreign Relations, 2013.
5. Top 10 cybersecurity vulnerabilities for oil and gas // Pipeline &Gas Journal, vol. 243(2), February 2016.
6. P. A. Ralston, J. H. Graham, & J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," ISA transactions, vol. 46(4), pp. 583-594, 2007
7. M.A. Nasir, S. Sultan, S.Nefti-Meziani, & U. Manzoor, "Potential cyber-attacks against global oil supply chain," IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1-7, 2015.
8. E.J.Byres, "Cyber security and the pipeline control system," Pipeline & Gas Journal, pp.58-59, 2009.
9. C. Bronk, & E. Tikk-Ringas, "The cyber attack on Saudi Aramco," Survival, vol. 55(2), pp. 81-96, 2013.
10. İmamverdiyev Y.N. Big Data texnologiyalarının böyük perspektivləri və problemləri // İnformasiya cəmiyyəti problemləri, 2016, №1, s.23–34.
11. Alıquliyev R.M., İmamverdiyev Y.N., Abdullayeva F.C. Neft-qaz sənayesi üçün Big Data analitikanın cloud computing platformasında analytics-as-a-service kimi reallaşdırılması imkanlarının tədqiqi // İnformasiya texnologiyaları problemləri, 2016, №1, s.11–26.
12. Sangvai P. Impact of Big Data in oil and gas industry // Proc. of the 10th Biennial International Conference & Exposition, 2013, pp.439□440.
13. Saha B., Shah H., Seth S., Vijayaraghavan G., Murthy A., Curino C. Apache Tez: a unifying framework for modeling and building data processing applications // Proc. of the ACM SIGMOD International Conference on Management of Data, 2015, pp.1357□1369
14. Eissa H. Unleashing Industry 4.0 opportunities: Big data analytics in the midstream oil & gas sector / International Petroleum Technology Conference, 2020, 9 p. DOI: 10.2523/IPTC-19802-Abstract
15. Imamverdiyev Y. N. A conceptual model of digital twin for the oil and gas industry // Problems of Information Technology, 2020, No. 2, pp. 41-51.
16. Sennaar K. Artificial Intelligence in oil and gas – Comparing the applications of 5 oil giants. February 18, 2019. https://emerj.com/ai-sector-overviews/artificial-intelligence-in-oil-and-gas/
17. Abdullayeva F.D., Imamverdiyev Y.N. Development of oil production forecasting method based on Deep Learning // Statistics, Optimization and Information Computing, 2019, Vol. 7, pp. 826–839.
18. Fataliyev T., Mehdiyev S. Industry 4.0: The oil and gas sector security and personal data protection // International Journal of Engineering and Manufacturing, 2020, 10(2), pp. 1-14.
19. Temizel C., Canbaz C.H., Palabiyik Y., Putra D., Asena A., Ranjith R., Jongkittinarukorn K. A comprehensive review of smart/intelligent oilfield technologies and applications in the oil and gas industry / SPE Middle East Oil and Gas Show and Conference, 2019, 22 p. DOI: 10.2118/195095-MS.
20. Abdullayeva F.J. Multidisciplinary study of the problems of Big Data technologies in the oil and gas industry/ Alıguliyev R.M //International Journal of Oil, Gas and Coal Technology № 9 ,2018
21. A.V.Vijayalakshmi , Dr. L. Arockiam, "A Study on security issues and challenges In IoT", International Journal of Engineering Sciences & Management Research, 2016, vol.3, no.11, pp.34-43

Received (Надійшла) 15.09.2024
Accepted for publication (Прийнята до друку) 06.11.2024

Проблеми кібербезпеки в нафтогазовій галузі

Мурад Омаров, Вюсаля Мурадова

Анотація. Внаслідок широкого застосування цифрових та інтернет-технологій у всіх процесах виробничого циклу нафтогазової промисловості кібербезпека стає все більшою загрозою. Тому сьогодні кібербезпека стає одним із пріоритетів технологічного розвитку нафтогазових компаній. У статті подано короткий опис цифрових трансформацій, що відбуваються в нафтогазовій галузі, аналізуються основні нові загрози кібербезпеці та надається інформація про інциденти кібербезпеки. Розглядається питання щодо розробки нових технологій на основі глибокого навчання для інтелектуальних нафтових родовищ.

Ключові слова: нафтогазова промисловість; цифровий майнінг; OT; IoT; кібербезпека.