

GRZEGORZ PILARSKI*

Akademia Sztuki Wojennej, Warszawa, Polska

KAROLINA MIKUSEK*

Akademia Sztuki Wojennej, Warszawa, Polska

CYBER THREATS TO OT SYSTEMS IN THE ENERGY INDUSTRY



ABSTRACT: In today's economy, we can see a modern direction of action including the concept of technological and organizational transformation of enterprises, known as Industry 4.0. Significant changes are also taking place in the energy industry, where modifications in the use of infrastructure, systems of operational technology (OT) are noticeable. The aim of the article is to present the threats in the field of cyberattacks that can be carried out on this infrastructure within the mentioned sector.

KEYWORDS: cyberspace, cybersecurity, cyber threats, energy industry, national security, operational technologies systems (OT),

INTRODUCTION



One of the main components characterizing the power and international status of states is the economy. Through the proper management of goods and the provision of services crucial to national interests, companies can be directly involved in the development of the country and building economic potential. Among the components relating to the economy, in addition to

* **ptk dr hab. inż. Grzegorz Pilarski**, War Studies University, Warsaw, Poland

 <https://orcid.org/0000-0001-9728-2611>  g.pilarski@akademia.mil.pl

Copyright (c) 2023 Grzegorz Pilarski, Karolina Mikusek. This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

* **Karolina Mikusek**, War Studies University, Warsaw, Poland

 <https://orcid.org/0009-0006-1645-7605>  karolina.mikusek@interia.pl

Copyright (c) 2023 Grzegorz Pilarski, Karolina Mikusek. This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

agriculture and services, industry deserves special attention. Understood as material production based on the acquisition of natural resources and obtaining products by mechanical means¹, it is an important issue relating to the proper functioning of the state. Industry has undergone frequent changes and evolutions over the centuries. Starting from the industrial revolution of the eighteenth century, ending with the current changes taking place within the so-called Industry 4.0, it is possible to see the progress of civilization and innovation in many aspects of human life.

Facilities provided as part of industrial development would not be possible without the process of mechanization, and recently the introduction of system solutions based on information technology and robotics. Owing to the potential of these measures, enterprises achieve greater profits while ensuring the effectiveness of services and the quality of manufactured goods. However, this does not mean that there are no risks associated with the use of operational technology (OT), especially in a cybersecurity context. Currently, the use of cyberspace² in industry is a very important element, thus it is justified to periodically identify threats in relation to OT systems.

Taking into account the above-mentioned issues, the main aim of this article is the analysis of cyber threats related to the use of operating systems in the energy industry. The authors formulated the research problem in the form of the following question: what threats in cyberspace affect the functioning of OT operating systems in the energy industry?

As part of the research on literature and Internet resources, attention was paid to the aspect of Industry 4.0 and the related development of industry, the use of operational technology in the energy industry and cyber threats that may occur within this sector.

Although the aim of the article is to identify the threats awaiting for us in the cyberspace in the energy industry, the authors of this publication do not intend to scare people but to raise

¹ Słownik języka polskiego PWN, entry: przemysł (industry). <https://sjp.pwn.pl/slowniki/przemys%C5%82.html> (access: 20.01.2023).

² Cyberspace - in Poland the definition of cyberspace was presented in the amendment to the Act of 30th August 2011 on the state of war and the competencies of the Commander-in-chief and the rules governing his subordination to the constitutional bodies of the Republic of Poland. In accordance with the document cyberspace is defined as "a space of processing and exchanging information created by the ICT systems, as defined in Article 3 point 3 of the Act of 17 February 2005 on the informatization of entities performing public tasks (OJ No. 64, item 565, as amended), together with links between them and the relations with users; in accordance with Article 2 paragraph 1b of the Act of 29 August 2002 on martial law and the powers of the Supreme Commander of the Armed Forces as well as the Commander's subordination to the constitutional authorities of the Republic of Poland (OJ No. 156, item 1301, as amended), Article 2 paragraph 1a of the Act of 21 June 2002 on the state of emergency (OJ No. 113, item 985, as amended) and Article 3 paragraph 1 point 4 of the Act of 18 April 2002 on the state of natural disaster (OJ No. 62, item 558, as amended)".

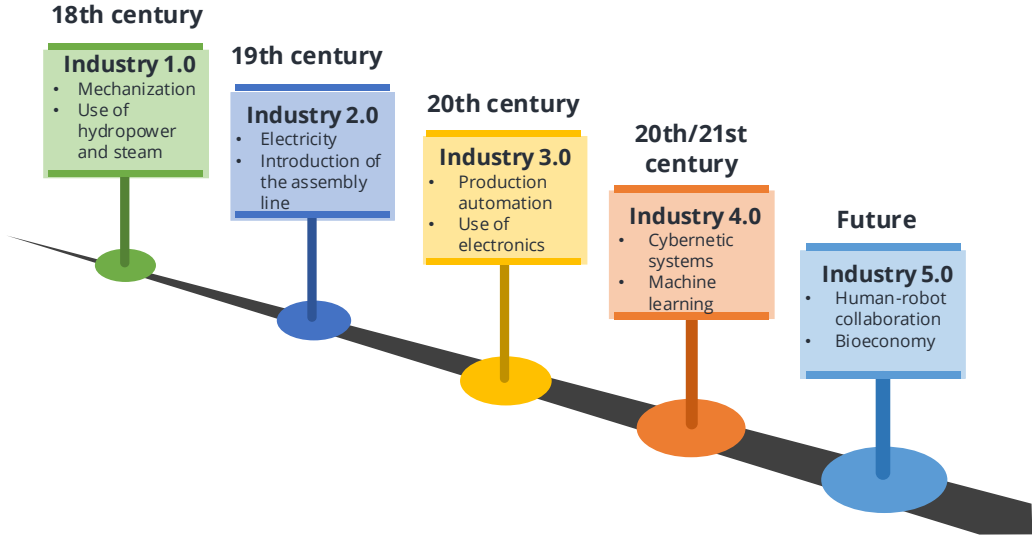
awareness of the key threats to which we may be exposed when using cyberspace. In the opinion of the authors, this is a very important aspect, because nowadays a very important task in the field of cybersecurity, or perhaps in other words in the field of counteracting cybercrime, is to raise the awareness of all of us who use cyberspace on a daily basis.

The authors are aware that the research area is very broad and the article presents only selected issues in the field of cybersecurity in relation to systems of operational technology (OT) in the energy industry.

INDUSTRY 4.0 – THEORETICAL OUTLINE

When starting to consider OT systems in the energy sector, special attention should be paid to the aspect of development of the generally understood industry and the opportunities and challenges associated with the currently observed changes taking place within industry 4.0. In order for the best presentation of this issue, it is worth discussing the evolution of the issue in question over the centuries. This will make it possible to see the modernization activities taking place in the industry, as well as allow for further considerations. Taking into consideration the presented issue, it is necessary to refer to its individual stages, which are presented in the figure below.

Fig. 1.
The Industrial Revolution over the centuries



Source: Own elaboration based on J. Matuszak, Is Your Business Ready for Industry 5.0? <https://knowhow.distrelec.com/manufacturing/is-your-business-ready-for-industry-5-0/>, (access: 27.01.2023).

Before the Industrial Revolution, mankind used animals and its own physical power as productive power. Most of the buildings erected were made of wood, which became the main productive product³. The eighteenth century is identified with the period of the first changes taking place in industry. It was at the end of this century that production plants began to introduce mechanical devices powered by water or steam into their equipment. With the use of industrial machinery and new energy technologies, many companies recorded a significant increase in productivity and thus profits. Steel became a new manufacturing material, and the use of hard coal as a fuel accelerated the industrialization process.

In the following years, because of the introduction of the division of working time and mass production, another period of change called Industry 2.0 began, falling on the second half of the nineteenth century. The main source of power was electricity, and it became increasingly common practice to introduce science into production and industrial management. For this reason, in addition to technical progress in production, especially mass production, it was possible to observe progress in managerial activities⁴. Important events characteristic of the second industrial revolution are, among other things: the use of steam engines in ships, the development of air transport, as well as the production of goods on a mass scale⁵. Another revolution occurred in the 70s of the twentieth century. Taking into consideration the aforementioned changes, Industry 3.0 was a particularly important period of change not only in the sectors of the economy, but also in communication or the way new fossil fuels were used. It was then that crude oil began to gain in popularity. In addition, electronics and information systems were introduced into production methods⁶. The new approach to the way of managing the enterprise, based on the joint implementation of goals, as well as the globalization of relations in the economy are among other manifestations of this phenomenon.

Currently, we can see the next stage of changes taking place within Industry 4.0. Many entities decide to invest in the introduction of cloud solutions, Internet of Things infrastructure⁷

³ N. G. Pereira Carvalho, E. W. Cazarini, Industry 4.0 - What Is It?, [in:] J. H. Ortiz (ed.) „Industry 4.0. Current Status and Future Trends”, IntechOpen, Londyn 2020, p. 5.

⁴ K. A. Demir, H. Cicibaş, *The Next Industrial Revolution: Industry 5.0 and Discussions on Industry 4.0*, [in:] S. Gülseçen, et al. (ed.) „Industry 4.0 from the MIS Perspective”. (ed..) Peter Lang, 2019, p. 248.

⁵ N. G. Pereira Carvalho, E. W. Cazarini, *Industry 4.0 - What Is It?*, op. cit.

⁶ K. A. Demir, H. Cicibaş, *The Next Industrial Revolution (...)*, op. cit., p. 249.

⁷ „Internet of things (IoT) is a global infrastructure for the information society, enabling advanced services by

or miniaturization. In this way, it is possible to automate production, as well as adapt it to new technologies, which will evolve with the development of society and its requirements. By changing the previously used mechanical solutions to systems based on a combination of physical and cybernetic aspects, it is possible to make changes in the activities of enterprises without the need to supervise the processes taking place. Owing to this, the way of managing a given company is much simpler and more effective⁸.

Taking into consideration these issues, it is necessary to point out the numerous advantages of the solutions proposed under this matter in question. There is no doubt that with the introduction of technical and IT facilities to the sphere of production, it is possible to increase the number of goods acquired. Equally important, this issue allows companies to achieve impressive results, which affects their position on the market. Recognizing the development opportunities, other companies with a similar business profile will take all actions to achieve similar results. In this way, competitiveness will increase, and sectors of the economy will grow faster and faster. Another argument which indicates the opportunities resulting from the fourth industrial revolution is the improvement of the operational dynamics of enterprises. Despite the costs that entities have to bear in the context of purchasing new mechanisms and tools, in the long term the expenses incurred are inversely proportional to the profits obtained, which increases efficiency. The opportunities provided by new technologies also affect the quality of the products offered, which translates into customer satisfaction and an increase in the number of potential recipients⁹.

Despite the benefits of changes related to Industry 4.0, it is also worth mentioning the possibility of difficulties and disadvantages of the implemented solutions. The aforementioned high costs of purchasing appropriate installations are also associated with providing employees with training and courses related to operation and knowledge of technical aspects, sometimes necessary to be repeated due to the update and development of technology. Another important aspect is also the adaptation of the objectives of the acquired tools to the mission

interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”. Cit, for: K. K. Patel, S. M Patel, *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges*, [in:] „International Journal of Engineering Science and Computing”, Pearl Media Publications Pvt Ltd, 2016, Vol. 6, No. 5, p. 6123.

⁸ United Nations Industrial Development Organization, *Industry 4.0. Opportunities and Challenges of the New Industrial Revolution for Developing Countries and Economies in Transition. Panel discussion*, UNIDO 2017, p. 4.

⁹ G. Immerman, *Industry 4.0 Advantages and Disadvantages*. <https://www.machinemetrics.com/blog/industry-4-0-advantages-and-disadvantages/>, (access: 27.01.2023).

of the company. A very common step taken by companies is the involvement of numerous entities in the process of introducing and personalizing mechanisms. Sometimes, for technical reasons, the production of the proposed tools may be limited or stopped altogether. This involves the need to acquire new solutions, which translates into the generation of additional costs. An indispensable element of new technologies, especially those based on cloud solutions and access to the Internet, are numerous threats. They involve cyber attacks, production stoppage or data theft¹⁰.

Referring to the predictions related to the possibility of further development of industry, Industry 5.0 should be mentioned. Despite the fact that this concept refers to issues that are difficult to predict, and even more problematic to determine in the subject literature, one can find attempts to formulate the main goal of the fifth industrial revolution. According to the researchers, it will be based on three main areas¹¹:

- human-centric approach – a change in the current approach to the way of understanding technology and its capabilities, the identification of new solutions as the main condition for ensuring efficient production and sustainable development will be replaced by focus on the needs of man and the benefits brought by the manufacturing process;
- sustainability – changes taking place as part of the climate crisis, as well as the growing importance of ecology will be a condition for the introduction of new ways of obtaining goods; recycling, re-use for products, reducing electricity consumption and reducing greenhouse gas emissions will be the main points of new business strategies;
- resilience in industrial production – the effects of the COVID-19 pandemic have affected all aspects of human life, including industry; staff shortages and the resulting production downtime have contributed to the economic problems of many countries; Therefore, it is necessary to introduce changes regarding manufacturing processes and protection of infrastructure elements particularly important for the proper functioning of the company.

¹⁰ Ch. Taylor, *Industry 4.0 – the pros and cons of the new industrial revolution*. <https://www.advancedengineeringuk.com/2022/01/21/industry-4-pros-cons/>, (access: 27.01.2023).

¹¹ European Commission, *Towards a sustainable, human-centric and resilient European industry*, European Union, 2021, pp. 13-14.

As can be seen, the process of changes taking place in industry has been going on invariably since the mid-eighteenth century. Along with subsequent revolutions, the industrialization of human activity is becoming an increasingly modern process, enriched with new solutions and tools. The currently functioning Industry 4.0 is a transition from the mechanical nature of the activities of enterprises to activities based on modern technology and information systems. Further possibilities of industrial development, considered as part of the fifth industrial revolution, assume the development of existing technologies with issues related to the diversified mode of production, putting man at the center of the production process, as well as the method of preventing climate change.

OT (OPERATIONAL TECHNOLOGY) SYSTEMS IN THE ENERGY INDUSTRY

The opportunities offered by the Fourth Industrial Revolution are an important aspect of the activities of numerous sectors of the state's economy. The implementation and use of new technologies in the process of acquiring goods enables constant development of enterprises, as well as a number of other benefits that were indicated in the earlier part of the article. The main reason for the use of new technologies in industry is the need to ensure effective and dynamic provision of services. This is one of the main stimuli determining the actions of entities and planning their strategic activities in the coming years. For this reason, the use of industrial automation¹² is becoming an indispensable element of innovative business management. One of the key issues related to the aforementioned concept is operational technology (OT) systems, the characteristics and application possibilities of which will be discussed below.

Operational technology systems should be understood as a set of systems enabling programming activities, as well as mechanisms supervising or affecting the physical sphere. The main task of these devices is to analyze the environment of controlled machines, search for irregularities in their operation and take action to reduce undesirable activities. OT systems consist of numerous controls that work together. Among the examples of the application of the discussed issues, the following issues should be highlighted¹³:

¹² „Industrial automation is the use of control systems and sophisticated equipment in a production environment. This includes robots, various sensors, and computers; performing tasks that were previously done manually. These systems will operate without significant human intervention or oversight, improving the quality and repeatability of repetitive operations”. Cit. for: G. Koos, *The 4 Fundamentals of Industrial Automation*, Harwin, p. 3.

¹³ K. Stouffer et al., *Guide to Operational Technology (OT) Security*, NIST 2022, p. 3.

- Systems responsible for the supervision of technological and production processes (e.g. SCADA) (Supervisory Control And Data Acquisition);
- Systems related to the control and illustration of production processes (e.g. DCS) Distributed Control System;
- Controllers enabling control of machines and tools (e.g. PLC) (programmable logic controller);
- Systems for building automation (e.g. BAS/BMS - Building Automation Systems, Building Management Systems);
- Access control systems (e.g. PACS) Physical Access Control System;
- The Internet of Things used in industry (IIoT).

The current changes taking place within Industry 4.0 assume a shift in the current division between operational and information technology (IT). Both types of systems are often considered in terms of separately functioning areas, operating in parallel in the industrial space. Each of them has separate tools with the help of which it is possible to achieve the correct effects of the work of individual mechanisms, as well as to ensure supervision of the processes taking place within these systems. Companies often decide to separate the operational part from the information part by using the systems responsible for the supervision of technological and production processes. However, the transfer of information technology to the operating environment is becoming an increasingly common practice, which is to ensure an increase in the efficiency of acquired goods and improve the profitability of enterprises¹⁴.

With regard to the benefits of combining the two systems, a number of opportunities related to the development of enterprises should be pointed out. In this context, the following aspects are important: production automation, the ability to obtain information on changes taking place in a given environment and send it to other devices or applications, as well as faster response in the event of a system failure. In addition, the economic aspect of reducing the costs associated with possible repairs and production stoppages are another benefit of the discussed issue¹⁵. Taking into consideration the difficulties associated with the introduction of IT solutions into the operational sphere, it is necessary to refer to the technological requirements of

¹⁴ U. Schälling, *Bridging the gap between IT and OT systems*. <https://www.power-grid.com/td/bridging-the-gap-between-it-and-ot-systems/#gref>, (access: 30.01.2023).

¹⁵ J.-E. Ambroise, *IT/OT Convergence: Benefits, Challenges, and Examples*. <https://www.emnify.com/iot-glossary/it-ot-convergence#chapter-2-1>, (access: 30.01.2023).

individual tools¹⁶, as well as the differences in the way both systems function. Issues related to communication protocols, resource constraints and the possibility of support in the management process are further examples of the challenges associated with the integration of OT and IT systems¹⁷.

The opportunities provided by operational technology are part of many sectors of the economy. As for the industry, the use of OT systems in the energy industry deserves special attention. Taking into consideration the specified systems included in the operational technology, it is possible to find their application in the energy industry. In the case of tools responsible for supervision and monitoring, it is worth mentioning the SCADA system. Within the energy industry, the technology used in the transport and supply of electricity focuses, among other things on¹⁸:

- Energy Management System (EMS) – understood in technological terms, a product that sometimes uses the possibilities of cloud computing. Its main task is to acquire, store and manage information related to consumption and energy expenditure¹⁹;
- Transmission Management Systems (TMS) – a set of programming equipment enabling supervision and management of transmission systems, an additional advantage of the system is to establish a pattern of emergency development²⁰;
- Advanced Distribution Management Systems (ADMS) – a system providing assistance in the decision-making process, which involves supervising and administering the electricity distribution system without compromising the quality of services provided; the architecture is also responsible for ensuring the safety of field workers and the reliability of the tools used²¹.

Referring to systems providing supervision and imaging of production processes in the energy industry, it is worth mentioning distributed control systems Distribution Management System

¹⁶ M. Stępień, *Bezpieczeństwo: działy OT i IT – razem, czy oddzielnie?* <https://seqred.pl/bezpieczenstwo-ot-it-razem-czy-oddzielnie/>, (access 30.01.2023).

¹⁷ K. Stouffer et al., *Guide to Operational Technology (...)*, op. cit., pp. 24-26.

¹⁸ ARC Advisory Group, *SCADA Systems for Electric Power Industry*. <https://www.arcweb.com/market-studies/scada-systems-electric-power-industry> (access: 31.01.2023).

¹⁹ C. Delas, *What is an Energy Management System (EMS)?* <https://www.metron.energy/blog/ems-energy-management-system-definition/> (access: 31.01.2023).

²⁰ Energy Knowledge Base, *Transmission management system (TMS)*.

<https://www.energyknowledgebase.com/topics/transmission-management-system-tms.asp> (access: 31.01.2023).

²¹ L. Rousse, T. Crawford, *Advanced Distribution Management Systems. How to choose the right solution to improve your utility's safety, reliability, asset protection and quality of service*, Capgemini, 2012, p. 4.

(DMS). The system consists of technical and electronic tools responsible for coordinating the mechanisms or systems. All DMS components are arranged in the power plant in the form of computers, sensors and controllers, which acquire and collect data on the processes taking place. This solution is used in local networks, including the ability to supervise the actions taken using servers and operating stations²².

Considering the controllers used in power plants, it is worth referring to programmable logic controllers (PLCs). In the process of generating electricity, sensors responsible for supervising mechanisms and the correct acquisition of production goods transport the obtained information to PLC sensors, which analyze the obtained data and take action to improve production capabilities. These activities focus inter alia on transmitting a signal to hydraulic tools and appropriate regulation of their work depending on the needs²³.

In the case of the use of the Internet of Things architecture in the energy sector, it is necessary to mention the possibilities that this solution provides to energy companies. One of them is to reduce electricity consumption by individual customers and enterprises. The use of advanced media monitors allows you to adjust the temperature depending on external conditions, as well as the needs of users. Owing to this, energy consumers can make changes, and thus minimize the costs associated with the use of electricity. Another example of the application of IoT is the use of certificates and sensors responsible for predicting failures, as well as early notification of energy system administrators. An additional convenience is the ability to create scenarios that in the future can improve the process of detecting threats. An important aspect of the use of the Internet of Things in the energy industry is finding places where security is insufficient. Paying attention to the fact that transmission systems and networks are extensive, and it takes a long time to detect gaps in them, it is necessary to use IoT solutions in the form of operational repair devices²⁴.

As can be seen, the use of operational technology in the energy sector has a wide range of applications. Thanks to the ability to analyze data, detect errors and prevent the effects of failures, OT is one of the main components of the energy infrastructure. The ability to adapt IT

²² Alexander S. Gillis, *Distributed control system (DCS)*, <https://www.techtarget.com/whatis/definition/distributed-control-system>, (access: 31.01.2023).

²³ A. Taylor, J. R. Parish, *Career Opportunities in the Energy Industry*, Infobase Publishing, New York 2008, p. 78.

²⁴ S. Rawat, *5 Uses of IoT In Energy Sector*. <https://www.analyticssteps.com/blogs/5-uses-iot-energy-sector>, (access: 31.01.2023).

systems to the operating environment presents both innovation and a number of challenges. Despite this, operational technology is used both as part of supervisory and control processes, as well as detecting possible threats and counteracting them in numerous entities of the energy industry.

CYBER THREATS TO OT SYSTEMS

As part of industrial activities, many entities are responsible for a number of decisions, the effects of which can have a significant impact on the proper operation of enterprises. These activities may be subject to the risk of hazards that may contribute to stopping the distribution and production of goods. Therefore, this also means the possibility of incurring both financial and image losses. Reference should also be made to the fact that those responsible for the proper operation of systems and machines cannot foresee all the destructive events that may occur during the operation of these tools. For this reason, it is so important to check for the possibility of security holes, which are referred to as vulnerabilities. Thanks to finding and appropriate response to the defects, it is possible to minimize the risks. Taking into consideration the fact that the energy industry is based on operational technology, it is worth presenting and characterizing vulnerabilities and discussing the likely effects of their occurrence.

When reviewing vulnerabilities associated with the use of OT systems in the energy industry, it is important to refer to elements of OT systems that may negatively affect the way they operate. According to the OT ICEFALL report, the legacy of "insecure by design" and its implications for certifications and risk management, developed by Forescout Technologies, this issue can be divided into the following categories²⁵:

- a breach of authentication – the most common type of vulnerability involves unauthorized access by third parties to confidential or protected data. The most common factors that increase the occurrence of this vulnerability are: reusing the same passwords, not changing passwords recurringly, or using easy-to-crack

²⁵ Forescout, *OT ICEFALL. The legacy of "insecure by design" and its implications for certifications and risk management*, Forescout 2022, p. 14.

passwords (e.g. admin, password), and lack of appropriate password security (e.g. saving login credentials on cards and placing them in a prominent place)²⁶;

- manipulating system software/configurations/files – the attacker's main goal is to modify the settings in such a way as to manipulate data in the system, as well as manage applications or affect their functioning²⁷. Achieving these assumptions is possible by acquiring critical functions that do not have adequate authorization and authentication security, as well as do not ensure the integrity of resources²⁸. In this respect, it is also possible to point to the manipulation of the logic of the data used, thanks to which the attacker can change them and, consequently, create a completely different set of data²⁹;
- denial of service attack (DoS) – A service ban occurs when a user is unable to access resources to which they have gained access³⁰. The attacker obtains the ability to disable the device, as well as prevent access by authorized persons to certain functions³¹;
- authentication bypass – Many applications, platforms, and devices require users to provide login information. This is to ensure that only people who have the right to do so gain access. Unfortunately, it is possible to bypass authentication mechanisms, which creates another vulnerability. In this respect, the main factors that allow hackers to do so are: lack of data protection by administrators, lack of change of the default password by users, or the appearance of files in the application without authentication security³².

²⁶ SailPoint, *How Compromised Credentials Lead to Data Breaches*. <https://www.sailpoint.com/identity-library/how-compromised-credentials-lead-to-data-breaches/>, (access: 03.02.2023).

²⁷ Owasp, *Setting Manipulation*. https://owasp.org/www-community/attacks/Setting_Manipulation (access: 03.02.2023).

²⁸ Forescout, *OT ICEFALL. The legacy (...)*, op. cit., p. 8.

²⁹ UNext, *Data Manipulation: Definition, Purpose, Examples*. <https://www.jigsawacademy.com/blogs/data-science/data-manipulation/>, (access: 03.02.2023).

³⁰ B. Kiprin, *What is "denial of service"?* <https://crashtest-security.com/denial-of-service-attack/>, (access: 03.02.2023).

³¹ Forescout, *OT ICEFALL. The legacy (...)*, op. cit., p. 8.

³² The SecMaster, *What Is Authentication Bypass Vulnerability? How To Prevent It?* <https://theseckmaster.com/what-is-authentication-bypass-vulnerability-how-to-prevent-it/> (access: 03.02.2023).

Referring to the risk category of threats to OT systems, the following categories should be distinguished³³:

- human factor – employees of enterprises may not have adequate knowledge in the field of OT systems management, as well as the combination of operational and information technology; an additional issue is destructive activity considered in terms of random or intentional activity;
- technological factor – the ability to connect OT and IT systems increases the productivity and interoperability of operational technology, but it should be remembered that this can also cause the emergence of cyber security risks;
- process factors – the inability to provide adequate cyber security as well as the use of outdated software may affect the way systems function.

Given these issues, there are a number of opportunities to influence the cybersecurity of operating systems. In the case of the energy sector, it is worth mentioning the following risks:

- Use of malware – there are many forms of malware access to OT systems. One of them is the use of unsecured, often private data carriers in the form of disks and pen drives that have been infected with malware. Another possibility is the ingress of the software through the office network, directly connected to the Internet. By exploiting these methods, hackers use files or malicious code, enabling them to obtain important data and cause damage to the system and image of the company³⁴. An example of such a threat is the use of Industroyer software by the Russian Federation against a Ukrainian power plant in December 2016. In connection with the infection of the systems, the operation of the power plant was stopped, and consequently, the power supply in Kiev and its surroundings was interrupted³⁵.
- IoT-botnets – the use of IoT infrastructure in the form of numerous sensors enabling inter alia remote control or obtaining knowledge about the location of a given tool

³³ Cyber Security Agency of Singapore, *Cybersecurity Policy for Operational Technology: A Guide for Governments*, Access Partnership, 2020, p. 15.

³⁴ Nomios, *Top five OT security threats*. <https://www.nomios.com/news-blog/top-five-ot-security-threats/>, (access: 03.02.2023).

³⁵ BBC News, *Ukraine power cut 'was cyber-attack'*. <https://www.bbc.com/news/technology-38573074>, (access: 03.02.2023).

creates an opportunity for attackers. IoT botnets have turned out to be a popular solution in recent times³⁶. They use the connection of this technology to the Internet to infect systems with malware³⁷. The use of these methods may affect the possibility of manipulating the energy market through small fluctuations in the price or amount of energy made available³⁸.

- DDoS attacks - denial-of-service attacks based on numerous requests being made. Their number is so large that the attacked devices or systems are not able to perform appropriate procedures. Therefore, the network and the mechanisms that it supports stop working³⁹. An example of a DDoS attack against the energy industry is the attack carried out on the Lithuanian energy company Ignitis Group. Russian hackers from the Killnet group disrupted the digital services provided by the company and prevented customers from accessing the website⁴⁰.
- No network segmentation – many companies choose to connect operating systems to internal networks. Sometimes this solution is associated with a direct cyber threat, due to the lack of appropriate network security and the lack of separation of the network sphere for the operational technology. According to Kaspersky Lab's Industrial Control Systems Cyber Emergency Response Team report, in 2017 the energy sector was the most popular industrial environment in terms of the number of attacks carried out. The most common reason for this was inadequately constructed internal networks, which resulted in the detection of around 18,000 versions of malware⁴¹.
- Attacks on web applications – sensors used as part of operational technology and applications providing control of mechanisms are subject to numerous updates and changes. Actions are often taken to transfer them to the Internet sphere, which is

³⁶ Nomios, *Top five OT security threats*, op. cit.

³⁷ Trendmicro, *What is an IoT botnet?* <https://www.trendmicro.com/vinfo/us/security/definition/iot-botnet>, (access: 04.02.2023).

³⁸ L. H. Newman, *Hackers Could Use IoT Botnets to Manipulate Energy Markets*. <https://www.wired.com/story/hackers-iot-botnets-manipulate-energy-markets/>, (access: 04.02.2023).

³⁹ Bezpieczny Internet, *Co to jest DDoS? Na czym polega atak DDoS?* <https://bezpiecznyinternet.edu.pl/co-to-jest-ddos/>, (access: 04.02.2023).

⁴⁰ A. Meehan, *Lithuanian Energy Firm Disrupted by DDOS Attack*. <https://www.infosecurity-magazine.com/news/lithuanian-energy-ddos-attack/>, (access: 04.02.2023).

⁴¹ M. Bieńkowski, *Cyberbezpieczeństwo w przemyśle*, <https://automatykaonline.pl/Artykuly/Bezpieczenstwo/Cyberbezpieczenstwo-w-przemysle>, (access: 04.02.2023).

associated with an additional threat⁴². An example of such an event is the attack using the Suxnet Internet worm in 2010. The purpose of the destructive actions was Iran's uranium enrichment infrastructure. Due to manipulations carried out on the SCADA system and PLC controllers, the implementation of the planned activities was delayed⁴³.

In terms of threats in the energy industry, the issue of cyberattacks attribution should also be mentioned. In this respect, we can encounter cyberattacks carried out by cybercriminal groups, which, due to their specificity, are referred to as Advanced Persistent Threat (APT). These groups use high-tech ICT attacks on political, economic, industrial, technical, and military targets. APT groups are often identified with specific countries, because there are indications that certain cybercriminal groups act on behalf of specific countries, carrying out pre-planned activities. Examples include groups referred to by the acronyms APT1 identified with China, or APT28 or APT29 identified with Russia⁴⁴. Of course, indicating affiliation to specific attribution entities is not easy and requires advanced investigative activities in cyberspace. The modus operandi of these actors varies, but it is possible to generalize and distinguish four main phases of the attack lifecycle carried out by these specialized cybercriminal groups: reconnaissance, initial infection, hijacking, and infiltration. An example of an APT entity characteristics may include the following information:

- suspected attribution – as a rule, groups of this type act on behalf of various organizations often identified with a specific country, e.g. APT 1 (People's Republic of China); APT 28 (Russia);
- target sector – specifying likely victims is often helpful in identifying who is behind a cyberattack, e.g. APT 40, although they have a global reach, they focus on the tourism industry and IT companies; APT 38s focus on financial institutions around the world;

⁴² Check Point Software Technologies, *Top 10 Critical Infrastructure and SCADA/ICS Cybersecurity Vulnerabilities And Threats*, Check Point Software Technologies, 2020, p. 1.

⁴³ M. Stepień, *Segmentacja sieci w ochronie przemysłowych systemów sterowania*. <https://seqred.pl/segmentacja-sieci-ot/>, (access: 04.02.2023).

⁴⁴ cf. G. Pilarski, *Cyberprzestrzeń : relacje w wojnie hybrydowej*, ASzWoj, Warsaw 2020, p. 69.

- description of the entity – this part of the analysis includes a description of the so-called TTP, i.e. how the entity has functioned so far and how it has carried out cyberattacks;
- related malware – identifying a set of malware is also helpful in attribution, indicating with a high probability which entity is associated with the analyzed cyberattack;
- attack vector – indicates the most frequently chosen means of conducting a cyberattack, e.g. a vulnerability in SCADA systems in the field of PLCs.

As can be seen, the security of operating systems in the energy sector is a key aspect. The exploitation of vulnerabilities in OT systems creates the possibility of disruptions that may affect the business activities of energy companies. Awareness of the occurrence of gaps in the applied solutions, as well as factors affecting the risk of negative events are an important issue in understanding and observing possible threats, as well as ways to counteract them.

CONCLUSION

The development of industry from the mid-eighteenth century to modern times brings many new solutions and technologies supporting human activity, as well as facilitating the process of acquiring goods and distributing services. This is particularly noticeable in the case of the current fourth industrial revolution. As part of it, among the new technologies supporting industrial activity, cloud solutions, artificial intelligence or the Internet of Things should be mentioned. The vision of Industry 5.0 is a combination and interpenetration of specified solutions based on human needs and changes taking place in climate issues. In this way, it will be possible to achieve greater efficiency and productivity.

Within Industry 4.0 there are many technical issues that together can be described as industrial automation. As part of it, OT systems operate that allow entrepreneurs to supervise mechanisms occurring in the physical sphere, as well as to detect vulnerabilities in systems and fix them. It is possible to connect operational tools with IT systems. This procedure has many benefits as well as drawback that should be considered by entrepreneurs before implementing this solution. Many OT variants can be used in the energy industry. These include inter alia SCADA and DMS systems, PLC controllers, as well as IoT infrastructure.

Despite the positive aspects associated with the facilities provided by operating systems, it is important to pay attention to the inherent aspect of the risks. A necessary step in this area is

to diagnose susceptibility and factors that increase the occurrence of negative scenarios. In terms of OT, attention should be paid to the human factor (lack of appropriate knowledge, erroneous or deliberate destructive action), the technological factor (lack of appropriate access and authentication security, as well as the possession of infected files or devices used for both private and employee purposes) and the process factor (lack of appropriate scenarios of conduct or system updates). Cyber threats that may emerge in the energy sector include malware attacks, DDoS attacks, the use of IoT botnets, lack of network segmentation and attacks on web applications.

Each entity, regardless of the characteristics of the actions taken, should have knowledge of the likelihood of destructive situations and the correct prevention of them. In this way, it will be possible to quickly detect threats and eliminate the effects of their occurrence. This will also affect the ability of companies to maintain productivity and efficiency.

REFERENCES LIST

LITERATURE

- Check Point Software Technologies, Top 10 Critical Infrastructure and SCADA/ICS Cybersecurity Vulnerabilities And Threats, Check Point Software Technologies, 2020.
- Cyber Security Agency of Singapore, Cybersecurity Policy for Operational Technology: A Guide for Governments, Access Partnership, 2020.
- Demir K. A., Cicibaş H., The Next Industrial Revolution: Industry 5.0 and Discussions on Industry 4.0, [in:] Gülseçen S., et al. (ed.) „Industry 4.0 from the MIS Perspective”, Peter Lang, 2019.
- Forescout, OT ICEFALL. The legacy of “insecure by design” and its implications for certifications and risk management, Forescout, 2022.
- European Commission, Towards a sustainable, human-centric and resilient European industry, European Union 2021.
- Koos G., The 4 Fundamentals of Industrial Automation, Harwin, 2022.
- Patel K. K., Patel S. M, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, [in:] „International Journal of Engineering Science and Computing”, Pearl Media Publications Pvt Ltd, 2016, Vol. 6, No. 5.
- Pereira Carvalho N. G., Cazarini E. W., Industry 4.0 - What Is It?, [in:] J. H. Ortiz (ed.) „Industry 4.0. Current Status and Future Trends”, IntechOpen, London 2020.
- Pilarski G., Cyberprzestrzeń : relacje w wojnie hybrydowej, ASzWoj, Warsaw 2020.
- Rousse L., Crawford T., Advanced Distribution Management Systems. How to choose the right solution to improve your utility’s safety, reliability, asset protection and quality of service, Capgemini, 2012.

Stouffer K. et al., Guide to Operational Technology (OT) Security, NIST, 2022.

Taylor A., Parish J. R., Career Opportunities in the Energy Industry, Infobase Publishing, New York, 2008.

United Nations Industrial Development Organization, Industry 4.0. Opportunities and Challenges of the New Industrial Revolution for Developing Countries and Economies in Transition. Panel discussion, UNIDO, 2017.

SOURCES

Ambroise J. E., IT/OT Convergence: Benefits, Challenges, and Examples. <https://www.emnify.com/iot-glossary/it-ot-convergence#chapter-2-1>, (access: 30.01.2023).

BBC News, Ukraine power cut 'was cyber-attack'. <https://www.bbc.com/news/technology-38573074>, (access: 03.02.2023).

Bezpieczny Internet, Co to jest DDoS? Na czym polega atak DDoS? <https://bezpiecznyinternet.edu.pl/co-to-jest-ddos/>, (access: 04.02.2023).

Bieńkowski M., Cyberbezpieczeństwo w przemyśle, <https://automatykaonline.pl/Artykuly/Bezpieczenstwo/Cyberbezpieczenstwo-w-przemysle>, (access: 04.02.2023).

Delas C., What is an Energy Management System (EMS)? <https://www.metron.energy/blog/ems-energy-management-system-definition/>, (access: 31.01.2023).

Energy Knowledge Base, Transmission management system (TMS). <https://www.energyknowledgebase.com/topics/transmission-management-system-tms.asp> (access: 31.01.2023).

Gillis Alexander S., Distributed control system (DCS). <https://www.techtarget.com/whatis/definition/distributed-control-system>, (access: 31.01.2023).

Immerman G., Industry 4.0 Advantages and Disadvantages. <https://www.machinometrics.com/blog/industry-4-0-advantages-and-disadvantages>, (access: 27.01.2023).

Kiprin B., What is "denial of service"? <https://crashtest-security.com/denial-of-service-attack/>, (access: 03.02.2023).

Meehan A., Lithuanian Energy Firm Disrupted by DDOS Attack. <https://www.infosecurity-magazine.com/news/lithuanian-energy-ddos-attack/>, (access: 04.02.2023).

Newman L. H., Hackers Could Use IoT Botnets to Manipulate Energy Markets. <https://www.wired.com/story/hackers-iot-botnets-manipulate-energy-markets/>, (access: 04.02.2023)

Nomios, Top five OT security threats. <https://www.nomios.com/news-blog/top-five-ot-security-threats/>, (access: 03.02.2023).

Owasp, Setting Manipulation. https://owasp.org/www-community/attacks/Setting_Manipulation (access: 03.02.2023).

Rawat S., 5 Uses of IoT In Energy Sector. <https://www.analyticssteps.com/blogs/5-uses-iot-energy-sector>, (access: 31.01.2023).

RC Advisory Group, SCADA Systems for Electric Power Industry. <https://www.arcweb.com/market-studies/scada-systems-electric-power-industry> (access: 31.01.2023).

SailPoint, How Compromised Credentials Lead to Data Breaches. <https://www.sailpoint.com/identity-library/how-compromised-credentials-lead-to-data-breaches/>, (access: 03.02.2023).

Schälling U., Bridging the gap between IT and OT systems. <https://www.power-grid.com/td/bridging-the-gap-between-it-and-ot-systems/#gref>, (access: 30.01.2023).

Słownik języka polskiego PWN, entry: przemysł (industry). <https://sjp.pwn.pl/slowniki/przemysl%C5%82.html> (access: 20.01.2023).

Stępień M., Segmentacja sieci w ochronie przemysłowych systemów sterowania. <https://seqred.pl/segmentacja-sieci-ot/>, (access: 04.02.2023).

Stępień M., Bezpieczeństwo: działy OT i IT – razem, czy oddzielnie? <https://seqred.pl/bezpieczenstwo-ot-it-razem-czy-oddzielnie/>, (access: 30.01.2023).

Taylor Ch., Industry 4.0 – the pros and cons of the new industrial revolution. <https://www.advancedengineeringuk.com/2022/01/21/industry-4-pros-cons/>, (access: 27.01.2023).

The SecMaster, What Is Authentication Bypass Vulnerability? How To Prevent It? <https://thesecmaster.com/what-is-authentication-bypass-vulnerability-how-to-prevent-it/> (access: 03.02.2023).

Trendmicro, What is an IoT botnet? <https://www.trendmicro.com/vinfo/us/security/definition/iot-botnet>, (access: 04.02.2023).

UNext, Data Manipulation: Definition, Purpose, Examples. <https://www.jigsawacademy.com/blogs/data-science/data-manipulation/>, (access: 03.02.2023).

Contribution to the creation of the article: management of works, scientific editing, introduction, summary – GP; introduction, theoretical approach, research, summary – KM.



Copyright (c) 2023 2023 Grzegorz Pilarski, Karolina Mikusek



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.