DOI: 10.38146/BSZ-AJIA.2025.v73.SI1.pp183-197

Cybersecurity of Operational Technology in Critical Infrastructures

Péter Hunorfi
PhD Candidate
Óbuda University,
Doctoral School of Safety and Security Sciences
hunorfi.peter@phd.uni-obuda.hu

Tibor Farkas
Dr. habil, Associate Professor
Vice Dean for Education
Óbuda University,
Donát Bánki Faculty of Mechanical and Safety Engineering
farkas.tibor@bgk.uni-obuda.hu

Abstract

Aim: The aim of this study is to present the relationship between critical infrastructures and operational technology (OT) and to explore the cybersecurity challenges arising from the integration of IT and OT systems. The central research question is: What are the main vulnerabilities that emerge in critical infrastructures due to the interconnection of OT and IT systems, and what defense strategies can mitigate these risks?

Methodology: The research adopts an interdisciplinary approach that combines theoretical-logical analysis, literature review, case study analysis, and the examination of practical examples. The following hypotheses were investigated:
H1: The convergence of IT and OT systems results in an increased attack surface, as OT systems become vulnerable through IT networks.
H2: The security mechanisms applied in critical infrastructures do not always meet the specific security requirements of OT, increasing system vulnerabilities.
H3: Proper segmentation strategies and the establishment of controlled communication channels between IT and OT networks can reduce the risk of cyberattacks.
The research also includes comparative analyses examining security measures applied in industrial and critical infrastructure settings. To gain a deeper understanding of the cybersecurity challenges of OT systems, industry reports and case studies were also analysed.

Findings: The protection of operational technology systems in critical infrastructures is crucial for maintaining social and economic stability. The digitalization

The manuscript was submitted in English. Received: 19 January 2025. Revised: 16 February 2025. Accepted: 18 February 2025.

of OT systems and their increasing integration with IT systems create new cybersecurity challenges that require a complex and multi-layered approach to address. The study highlights that proper segmentation and secure interconnection of IT and OT systems are key to effectively managing cyber threats.
Value: This research provides a comprehensive overview of the cybersecurity challenges associated with operational technology, with a particular focus on critical infrastructures. It offers valuable guidance for developing defense strategies from both scientific and practical perspectives, supporting the secure integration of IT and OT systems.

Keywords: Critical Infrastructure, Operational Technology, Cyber Defense, Hacker Attack, Industrial Control Systems (ICS), Insider Threats, SCADA

Introduction

The fundamental pillars of the functioning of modern societies and economies are critical infrastructures, which provide essential services such as, among others, the uninterrupted operation of energy supply, financial systems, water supply, communication, transportation, healthcare, and public safety (Haig et al., 2009). These infrastructures are of paramount importance, as their disruption or malfunction - even at a certain level - can have severe consequences for the lives of individuals and nations.

Critical infrastructures are particularly vulnerable to natural disasters, cyberattacks, and other potential threats. Therefore, national and economic actors must devote special attention to their protection and sustainability (Muha, 2007). For instance, preserving energy supply requires the safe application of modern technologies, risk analysis, and the development and enforcement of preventive security measures (Répás & Dalicsek, 2015). Decentralized energy production, the use of renewable energy sources, the development of energy storage technologies, and smart grids (Vijayapriya & Kothari, 2011) not only enhance sustainability but also contribute to increasing the resilience of systems from a security perspective. In the field of critical infrastructure protection, legal regulation (Act LXXXIV of 2024 on the Resilience of Critical Entities), the establishment of standards (Hunorfi, 2024), the development of audit systems, and international cooperation are essential, as global threats - such as climate change and cybersecurity attacks - pose cross-border problems and challenges.

Ensuring the continuous operation of energy supply and other critical infrastructures is not only a technical and economic challenge, but also a societal

and political responsibility. Close cooperation among stakeholders - governments, companies, scientific institutions, and civil organizations - is essential for effective protection. Establishing the long-term security of critical infrastructures requires strategic planning that takes into account future challenges and technological advancements. The application of artificial intelligence and data-driven (big data) analysis enables improved monitoring of systems in cyberspace and the prediction of potential issues, thereby minimizing the risk of unexpected failures.

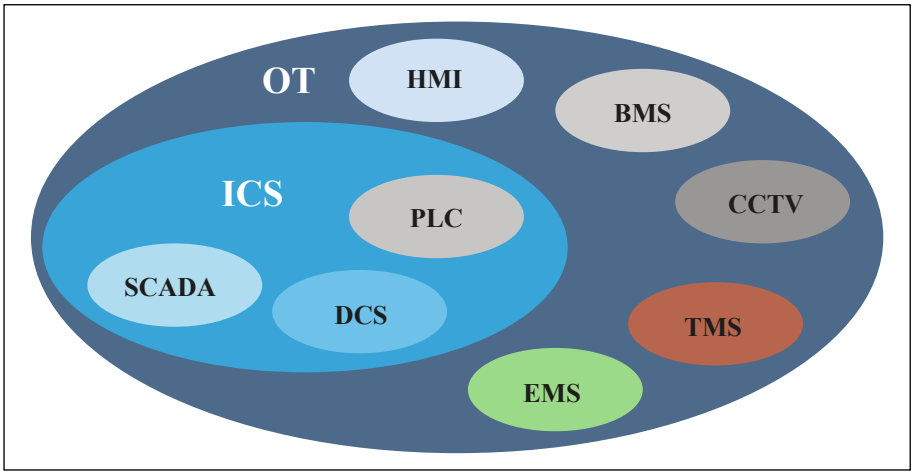
It is important to emphasize that the protection of critical infrastructures does not only involve strengthening physical systems, but must also extend to countering attacks in cyberspace. Due to the vulnerability of increasingly complex digital networks, the continuous development of cybersecurity systems and the training of experts are indispensable. Information sharing and real-time communication among the relevant organizations can play a crucial role in the rapid and effective management of a crisis situation.

Overall, it is clearly evident that preserving the security of critical infrastructures is of fundamental importance for the stability and development of nations. Therefore, it must be prioritized at social, economic, and political levels alike, in order to elevate the resilience and adaptability of these systems to the highest possible level—thus ensuring the well-being of both present and future societies. The aim of this publication is, on the one hand, to provide a comprehensive exploration of the relationship between OT cybersecurity and critical infrastructures, and on the other hand, to formulate practical recommendations for defense strategies.

What is Operational Technology (OT)?

From a technical perspective, critical infrastructures are built upon the foundations of operational technology, as these systems are responsible for their control and automation. Operational technology comprises the combination of hardware and software that directly controls, monitors, and manages physical devices and processes. While Information Technology (IT) primarily deals with data management, OT exerts a direct influence on the physical world. Operational technology (see Figure 1) includes, among others, industrial control systems such as Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), and Distributed Control Systems (DCS). These technologies are essential for the uninterrupted functioning of various sectors, including energy, water supply, transportation, and manufacturing.

Figure 1.
Overview of OT systems



ICS: Industrial Control System
SCADA: Supervisory Control and Data Acquisition
DCS: Distributed Control System
PLC: Programmable Logic Controller
EMS: Energy Management System
TMS: Transportation Management System
BMS: Building Management System
CCTV: Closed-Circuit Television
HMI: Human Machine Interface
Note. Figure created by the author.

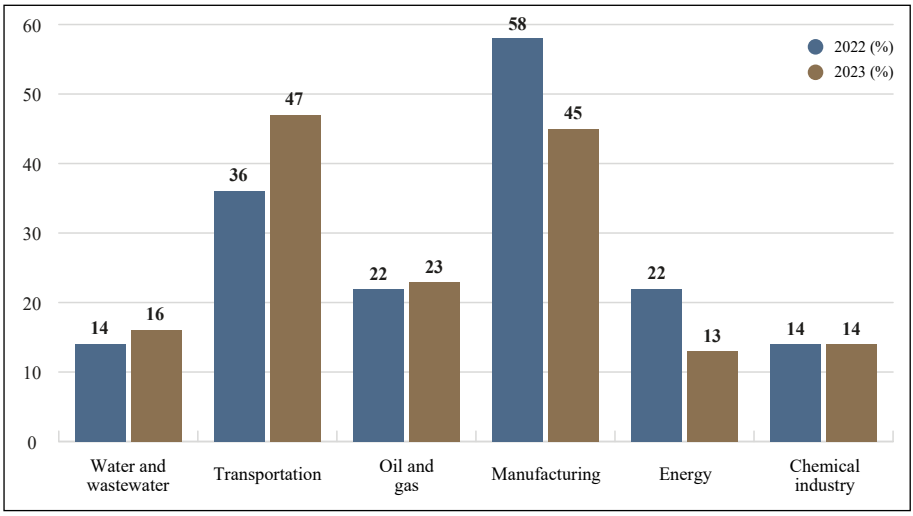
Operational technology enables the automated and efficient functioning of critical infrastructures, ensuring the rapid and reliable provision of essential services. In the energy sector, for example, supervisory control systems collect real-time data on the status of the network and intervene immediately, if necessary, to eliminate disruptions. Another advantage of operational technology is real-time monitoring and control, which allows operators to respond quickly to faults or threats. This is particularly important in sectors where delays can result in severe social and economic damage. OT systems are directly integrated with physical components such as valves, motors, and pumps, which they monitor and control. This integration ensures the precise and secure operation of complex processes. However, OT systems also present challenges, as many of them are outdated or were not originally designed to withstand modern cybersecurity threats. Their integration with IT systems and increasing internet connectivity have heightened their vulnerability, allowing attackers to potentially

gain control and cause disruptions via cyberattacks. To ensure security, the modernization and maintenance of OT systems are of paramount importance, including the implementation of cybersecurity measures such as network segmentation and the deployment of intrusion detection systems.

The growing risk of cyber threats

OT systems were traditionally operated as closed, isolated networks. However, with the advancement of Industry 4.0 (Hearn et al., 2023) and digitalization, they are increasingly integrated with IT systems. While this integration enhances efficiency and flexibility, it also significantly increases the risk of cyber threats. Hackers, state-sponsored groups, and even malicious insiders now view these systems as high-value targets, as successful disruptions can have severe consequences for both the economy and society. The growing issues related to network segmentation (see Figure 2) mainly stem from the digitalization of industrial systems and the inherent security weaknesses of complex infrastructures, which are often difficult to align with modern security principles. In parallel, attackers are employing increasingly sophisticated methods, while investments in security and the implementation of proper segmentation policies are often lacking. A shortage of resources, lack of expertise, and competing business priorities further exacerbate the situation, increasing the likelihood of vulnerabilities being exploited. According to observations by Dragos in 2023, approximately 70% of incidents related to OT systems originated from the IT environment (Dragos, 2024). As a key preventive measure, network segmentation and the separation of IT and OT systems into distinct domains are strongly recommended.

2. Figure
Reports containing segmentation deficiencies



Note. Figure created by the authors based on Dragos reports.

The protection of OT systems involves numerous unique challenges. Below are some of the key issues:

a) Legacy systems: many OT systems are based on decades-old technologies that were not designed to address today's cybersecurity threats. These systems are often difficult to upgrade or modernize without disrupting operations.
b) Closed systems: OT systems frequently use proprietary protocols and closed architectures, which complicates the implementation of standard cybersecurity tools and methods. Applying security patches or updates can also be more difficult, as any changes may impact process stability.
c) Continuous operation: in OT environments, availability and uninterrupted processes are of paramount importance. In certain industries, such as energy supply, downtime can result in serious economic and societal consequences. As a result, applying security updates or patches is often a time-consuming and high-risk endeavour.
d) Diverging priorities: the management and protection of OT systems require a different approach than IT systems. While IT primarily focuses on data security, access control, and encryption, the primary goal in OT is ensuring the continuous and reliable operation of physical systems.

Adversaries targeting critical infrastructure from a cybersecurity perspective

Critical infrastructures may be targeted by various types of adversaries, each with different motivations and objectives. These attackers can be external or internal actors pursuing economic, political, ideological, or even technological goals. The methods and aims of such attacks vary widely, ranging from espionage and data theft to the deliberate disruption of system operations. The increasing digitalization of infrastructures and the integration of technological systems further expand the attack surface, the exploitation of which can lead to severe consequences.

Nation-states

State-sponsored attacks represent one of the most significant categories of cyber threats targeting critical infrastructures. These attacks are often carried out by actors with substantial resources and specialized expertise. Their objectives may include espionage aimed at acquiring sensitive information, disrupting or disabling operations, or exerting political and economic pressure.

A well-known example is the 2010 Stuxnet attack, which targeted Iranian uranium enrichment facilities. Another noteworthy case of a successful state-sponsored cyberattack was the 2015 power outage in Ukraine, executed by Russian-affiliated hackers. Investigations identified the presence of the malicious software BlackEnergy in the systems of three service providers, along with the KillDisk malware, which was used to delete essential operational files. These viruses infiltrated the systems through targeted phishing attacks, known as spear phishing. As a result of the attack, approximately 225,000 households were left without electricity (URL1; Müller, 2016).

Criminal groups specializing in cyberattacks

Organized criminal groups are another of the most common actors in cybercrime. Their primary goal is financial gain, which they pursue through ransomware, phishing, or other illegal activities. These groups are particularly dangerous because they use highly specialized tools and techniques and often operate under a 'Crime-as-a-Service' (CaaS) model.

One of the most well-known examples of a ransomware incident targeting critical infrastructure is the 2021 attack on Colonial Pipeline. The attackers - identified as the hacker group DarkSide - successfully compromised the IT systems

of Colonial Pipeline, forcing the company to shut down its entire fuel pipeline operation. This pipeline supplies approximately 45% of the East Coast's fuel in the United States, and its shutdown had immediate economic and societal consequences, including panic buying and fuel shortages. The main target of the attack was the company's billing system, which the group disrupted to prevent transaction processing. To contain the threat, the Colonial Pipeline leadership decided to isolate their IT systems from OT networks, thereby preventing the ransomware from spreading to the operational technologies essential for pipeline operations. To restore functionality, the company paid the attackers $4.4 million in Bitcoin (Insurica, 2021).

Hacktivists

Hacktivists are individuals or groups who carry out cyberattacks driven by ideological, political, or social motives. These attacks are often intended to draw public attention, but they can also cause significant damage. Common tactics include website defacement, distributed denial-of-service (DDoS) attacks, and the public release of confidential data.

A notable 2023 example of hacktivist activity targeting critical infrastructure involved the hacker groups CyberAv3ngers and Team Insane Pakistan, who claimed responsibility for a series of actions against Israeli infrastructure. According to their statements, they disrupted the operations of Israeli railway systems, which play a vital role in the country's freight and passenger transportation. They also reportedly attacked the power grid of an Israeli city, resulting in blackouts that severely impacted the population and the operation of local services. Furthermore, they targeted a hydroelectric facility in Israel—critical for energy supply and infrastructure maintenance—claiming to have successfully disrupted its operations (Dragos, 2024).

Insiders (internal personnel)

Insiders - employees working within administrative functions or infrastructure systems - also represent a significant cybersecurity threat. Their actions, whether intentional or negligent, can lead to serious breaches of security. Insider threats may include deliberate data theft or sabotage, as well as careless data handling or the use of weak passwords.

A notable case occurred in 2000 involving an attack on the wastewater treatment system of Maroochy Shire, Australia. A disgruntled former employee gained unauthorized access to the facility's telemetry system, which was controlled

by SCADA systems (Slay & Miller, 2007). He repeatedly disrupted the operation of sewage pumps, resulting in untreated wastewater being discharged into nearby rivers and parks, causing significant ecological and public health damage. This incident was one of the first documented cases of a critical infrastructure OT system being deliberately manipulated, and it contributed to the global advancement of cybersecurity protocols for SCADA systems used in critical infrastructures.

Individual hackers and so-called ethical hackers

While individual hackers act with malicious intent, ethical hackers often assist in identifying vulnerabilities. However, when a hacker crosses the line between good intentions and accidental or deliberate damage (grey hat hacker), they can pose a significant threat.

In 2021, the Oldsmar water treatment system was subjected to a cyberattack when an intruder used TeamViewer remote access software to increase the dosage of sodium hydroxide (NaOH) added to the water (Cervini et al., 2022). The attack was quickly detected by an on-site operator, who restored the values to normal, preventing the water quality from exceeding permissible limits. The incident highlighted the vulnerabilities of remote access tools and OT systems, as well as the need for increased transparency, improved segmentation, and stricter security measures to prevent similar incidents.

Terrorist groups

Terrorist organizations have also discovered the potential of cyber warfare. They increasingly use cyberspace for propaganda purposes, mobilizing supporters, and organizing attacks. Particularly threatening is their ability to incite panic and uncertainty through cyberattacks on critical infrastructures, as well as through data manipulation or destruction.

A prominent example highlighted in Dragos reports is the group known as Xenotime, which has been linked to terrorism-related activities (Dragos, 2024). This group is particularly known for targeting critical infrastructure, especially energy sector systems. Xenotime developed the Trisis malware, specifically designed to disrupt industrial safety systems known as Safety Instrumented Systems (SIS) (Geiger et al., 2020). These systems are vital for ensuring the safe operation of industrial processes. The intent of such attacks is often to disable these systems, which could lead to explosions or severe damage. In 2017, Trisis was deployed at a petrochemical facility in Saudi Arabia, where attackers

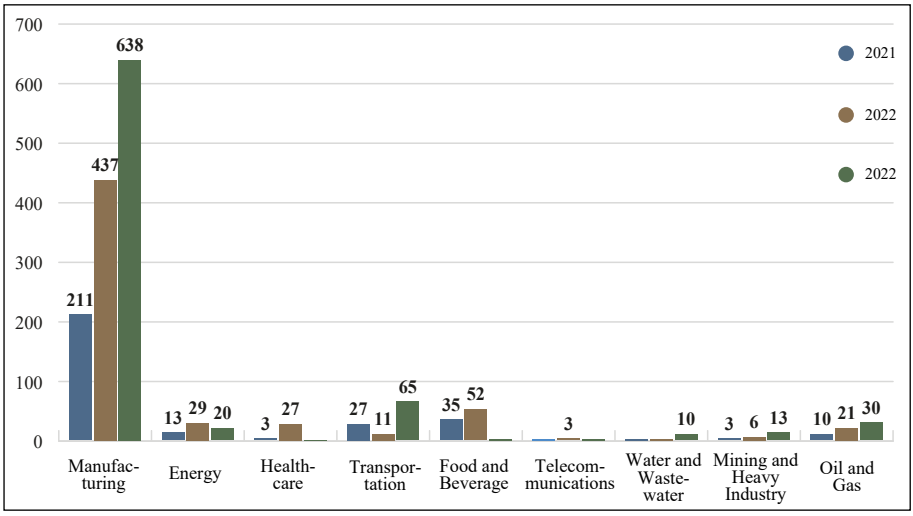
attempted to endanger operations by disabling the safety systems (Green, 2022). This incident demonstrated that Xenotime's objectives went beyond mere disruption, potentially aiming to endanger human lives as well.

Trends in attacks on critical infrastructures

Based on Dragos' ICS/OT cybersecurity reports from 2021, 2022, and 2023, it is evident that both the number and sophistication of attacks targeting OT systems have been increasing year by year (Dragos, 2024). Precise figures are difficult to determine, as many incidents are not publicly disclosed. It is in the fundamental interest of nations, companies, and organizations to keep certain information - particularly the occurrence and outcomes of attacks on critical infrastructure - confidential for security and economic reasons.

Nevertheless, data related to ransomware attacks are often accessible and help illustrate ongoing trends. Ransomware incidents have been steadily rising (see Figure 3), with 2023 witnessing nearly a 50% increase compared to 2022 figures.

Figure 3.
Sectoral breakdown of registered ransomware attacks between 2021 and 2023



Note. Figure created by the authors based on Dragos reports.

These attacks most frequently targeted the systems of manufacturing, the energy sector, transportation, healthcare, and the food industry, reflecting the financial motivation of the attackers. In addition, new threat groups emerged

each year, such as KOSTOVITE, ERYTHRITE, and PETROVITE in 2021, CHERNOVITE and BENTONITE in 2022, and GANANITE, LAURIONITE, and VOLTZITE in 2023. These groups are applying increasingly sophisticated techniques, such as the exploitation of industrial protocols and the development of modular attack frameworks. Geopolitical conflicts, such as the war between Russia and Ukraine or events in the Middle East, have played a significant role in the increase in attacks against OT systems. For example, the threat group named ELECTRUM targeted several Ukrainian critical infrastructures with destructive attacks.

Among the targets of the attacks, manufacturing remains the most frequently affected sector, as 70% of all ransomware attacks in 2023 were directed at it. Energy and water service providers are also prime targets, since their disruption can have a significant impact on the population and the economy. Among technological and vulnerability trends, a key finding is that in 2023, 80% of systems lacked proper OT network monitoring, which made it difficult to detect attacks. Network segmentation and the separation of IT/OT users also posed problems, as 54% of OT systems used identical authentication credentials for both environments. OT system vulnerabilities also became increasingly common. In 2023, 31% of the analysed vulnerabilities contained incorrect data, and in many cases, no alternative mitigation steps were available. New attack tools, such as PIPEDREAM, also emerged, elevating OT system attacks to a new level, as they are capable of targeting multiple industries and exploiting native industrial protocols. These trends clearly highlight the importance of OT system protection and the significant threat such attacks pose to critical infrastructures.

What can be done for defense?

Protecting critical infrastructures is vital importance, as these systems form the foundation of our societies' supply and service networks. The threats mentioned above can only be effectively countered with a complex and integrated defense strategy (Berzsenyi, 2014). Continuous improvement of cybersecurity and the forecasting of potential threats are essential for sustainable and secure operation. To effectively address OT cybersecurity challenges, comprehensive approaches are required.

The integration of IT and OT systems is inevitable, but it must be implemented securely and in a controlled manner. One key element of this is proper network segmentation, which does not mean complete isolation but enables secure and regulated communication between systems. While applying updates may

be difficult for older OT systems, regular security patches and vulnerability management are essential for maintaining cybersecurity (Nyári & Kerti, 2021).

Continuous monitoring of IT and OT systems, intrusion detection, and anomaly detection in networks are necessary to identify irregularities in a timely manner. Ongoing employee training and the enhancement of cybersecurity awareness are fundamentally important not only for protecting IT systems but also OT systems (Kerti, 2023). Employees must be aware of potential risks and follow proper procedures to ensure secure operations.

Applying the Zero Trust principle is increasingly necessary in OT networks as well, where every access attempt is continuously verified and monitored, regardless of whether it originates from an internal or external source.

Conclusion

Operational technology (OT) cybersecurity is one of the most critical and pressing areas of protecting critical infrastructures, holding exceptional importance not only from a technological perspective but also in terms of economic and social stability. The rapid development of global digitalization and automation is fundamentally transforming the operation of critical infrastructures while creating increasing vulnerabilities within such systems. Therefore, it is imperative to approach the protection of OT systems with an integrated, holistic perspective that takes into account information security, operational safety, and technological aspects.

The increasing integration of OT and IT systems comes with not only advantages but also new challenges. Traditionally isolated OT environments are opening up to IT infrastructures due to digitalization, which significantly heightens the risk of cyber threats. Therefore, it is crucial that the connections between different systems are established securely, and that IT solutions prioritize maintaining the continuity and stability of operational processes. Research findings show that the protective mechanisms employed in critical infrastructures often do not fully align with the specific security requirements of OT systems, leading to greater vulnerability.

Addressing the vulnerabilities of OT systems requires regular security audits and continuous employee training as critical steps. Recognizing and mitigating cybersecurity threats can only be effective if human resources and technological tools work together in harmony. Leveraging artificial intelligence and data-driven solutions provides an opportunity for systems to respond to threats in real-time, thereby reducing the risk of downtime and disruptions.

Improving OT system security requires long-term planning and international collaboration. Global threats - such as cyberterrorism or state-sponsored cyberattacks - present cross-border challenges that can only be addressed through close international cooperation. Based on analysed cases, proper network segmentation and controlled integration of IT and OT systems can significantly reduce the risk of cyberattacks, making widespread implementation of these solutions crucial. Tools such as standardized protocols and global cybersecurity guidelines play a vital role in increasing system resilience.

In summary, operational technology (OT) cybersecurity is not merely a technological challenge but also a broad societal, economic, and political endeavour that requires a careful balance between modernization and security. Only comprehensive, integrated strategies can ensure that these systems serve society effectively and safely. Accordingly, it is clear that international standards, such as IEC 62443 (Hauet, 2012) and ISO/IEC 27019, can contribute to making OT systems more secure, particularly in the case of industrial control systems. Additionally, the cooperation of national cybersecurity centres and the use of information-sharing platforms (such as ISACs) play a significant role in the rapid detection and mitigation of threats. It is evident, therefore, that future research must pay particular attention to the security aspects of next-generation technologies - such as artificial intelligence and machine learning - when integrating OT and IT systems. Furthermore, it is important to explore industry-specific cybersecurity challenges, where OT system vulnerabilities are especially critical.

References

Berzsenyi, D. (2014). Kiberbiztonsági analógiák és eltérések: A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése [Cybersecurity analogies and differences: A comparative analysis of cybersecurity strategies issued by the member countries of the Central European Cybersecurity Platform]. *Nemzet és Biztonság*, *7*(4), 110–138. https://folyoirat.ludovika.hu/index.php/neb/article/view/4097/3352

Cervini, J., Rubin, A., & Watkins, L. (2022). Don't drink the cyber: Extrapolating the possibilities of Oldsmar's water treatment cyberattack. *International Conference on Cyber Warfare and Security*, *17*(1), 19–25. https://doi.org/10.34190/iccws.17.1.29

Dragos. (2024). OT cybersecurity: The 2023 year in review. https://www.dragos.com/ot-cybersecurity-year-in-review/

Geiger, M., Bauer, J., Masuch, M., & Franke, J. (2020). An analysis of Black Energy 3, Crashoverride, and Trisis, three malware approaches targeting operational technology systems. In *Proceedings of the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1537–1543). IEEE. https://doi.org/10.1109/ETFA46521.2020.9212128

Green, M. (2022, April 19). Throwback attack: TRISIS malware mystifies industrial community. *Industrial Cybersecurity Pulse*. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-trisis-malware-mystifies-industrial-community/

Haig, Z., Hajnal, B., Kovács, L., Muha, L., & Sik, Z. N. (2009). A kritikus információs infrastruktúrák meghatározásának módszertana [Methodology for defining critical information infrastructures]. ENO Advisory Kft. https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf

Hauet, J.-P. (2012). ISA99/IEC 62443: A solution to cyber-security issues? Paper presented at the ISA Automation Conference. https://www.kbintelligence.com/Medias/PDF/ISA_Doha_hauet.pdf

Hearn, G., Williams, P., Rodrigues, J. H. P., & Laundon, M. (2023). Education and training for industry 4.0: A case study of a manufacturing ecosystem. *Education + Training*, *65*(8/9), 1070–1084. https://doi.org/10.1108/ET-10-2022-0407

Hunorfi, P. (2024). Az ISO/IEC 27001 szabvány elmélete és gyakorlati alkalmazása OT/ICS-rendszerek kiberbiztonsági jelentéseinek tükrében [Theory and practical application of the ISO/IEC 27001 standard in the context of cybersecurity reports of OT/ICS systems]. *Scientia et Securitas*, *5*(3), 323–332. https://doi.org/10.1556/112.2024.00228

Kerti, A. (2023). Az információbiztonsági tudatosság fejlesztésének tervezése [Planning the development of information security awareness]. In Tóth, A. (Szerk.), *Új típusú kihívások az infokommunikációban* (pp. 181–194). Dialóg Campus Kiadó.

Muha, L. (2007). A Magyar Köztársaság kritikus információs infrastruktúráinak védelme [Protection of the critical information infrastructures of the Republic of Hungary] [Master's thesis, Zrínyi Miklós Nemzetvédelmi Egyetem].

Müller, T. (2016). Kiberfenyegetések és kibervédelem [Cyber threats and cyber defense] (Infojegyzet 2016/44). Országgyűlés Hivatala Képviselői Információs Szolgálat. https://www.parlament.hu/documents/10181/595001/Infojegyzet_2016_44_kibervedelem.pdf

Nyári, N., & Kerti, A. (2021). A szoftverminőséggel kapcsolatos ISO szabványok áttekintése [Overview of ISO standards related to software quality]. *Biztonságtudományi Szemle*, *3*(2), 61–72. https://biztonsagtudomany.hu/index.php/btsz/article/view/284

Répás, S., & Dalicsek, I. (2015). Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében [Methodological issues of information security risk analysis for organizations operating critical infrastructure elements]. *Pro Publico Bono – Magyar Közigazgatás*, *3*(4), 22–33. https://folyoirat.ludovika.hu/index.php/ppbmk/article/view/2639

Slay, J., & Miller, M. (2007). Lessons learned from the Maroochy water breach. In E. Goetz & S. Shenoi (Eds.), *Critical infrastructure protection* (Vol. 253, pp. 73–82). Springer. https://doi.org/10.1007/978-0-387-75462-8_6

Vijayapriya, T., & Kothari, D. P. (2011). Smart grid: An overview. *Smart Grid and Renewable Energy*, *2*(4), 305–311. https://doi.org/10.4236/sgre.2011.24035

Online link in the article

URL1: *Cyber-Attack Against Ukrainian Critical Infrastructure (2015).* America`s Cyber Defence Agency. www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

Laws and Regulations

Act LXXXIV of 2024 on the Resilience of Critical Entities

Decree No. 234/2011 (XI. 10.) of the Government on the Implementation of Act CXXVIII of 2011 on Disaster Management and the Amendment of Certain Related Acts

Government Decision No. 1139/2013 (III. 21.) on Hungary's National Cybersecurity Strategy

Reference of the article according to APA regulation

Hunorfi, P., & Farkas, T. (2025). Cybersecurity of Operational Technology in Critical Infrastructures. *Belügyi Szemle*, *73*(SI1), 183–197. https://doi.org/10.38146/BSZ-AJIA.2025.v73.SI1.pp183-197

Statements

Conflict of interest

The authors have declared no conflict of interest.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Ethics

The data will be made available on request.

Corresponding author

The corresponding author of this article is Péter Hunorfi, who can be contacted at hunorfi.peter@phd.uni-obuda.hu.