Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi
Yıl: 2025 Cilt-Sayı: 18(1) ss: 378–391

Academic Review of Economics and Administrative Sciences
Year: 2025 Vol-Issue: 18(1) pp: 378–391

https://dergipark.org.tr/tr/pub/ohuiibf

Araştırma Makalesi
Research Article

ISSN: 2564-6931
DOI: 10.25287/ohuiibf.1558269
Geliş Tarihi / Received: 30.09.2024
Kabul Tarihi / Accepted: 03.01.2025
Yayın Tarihi / Published: 31.01.2025

CYBER INFRASTRUCTURE GUIDE: IT/OT INTEGRATION

Mustafa Bilgehan İMAMOĞLU [1]

Abstract

Innovations in information and communication technologies have led to complex and dangerous security problems. Industries face financial and reputational losses due to inadequate applications in the field of cybersecurity. This situation increases the importance of industrial cybersecurity, which tries to protect industrial systems from cyber threats and attacks. Industrial cybersecurity is responsible for the protection of operational technologies and industrial control systems used in various branches of the industry, focusing on the continuity of business and the security of processes. It ensures the uninterrupted and secure operation of infrastructure and processes by minimizing cyber risks that may harm business and processes. Continuously evolving types of cyberattacks pose serious risks to industrial business and processes. Traditional protection methods are not sufficient to reduce these risks. Instead, industries should develop existing cybersecurity measures and integrate information technologies with operational technologies. In this way, initiative-taking measures can be taken before a cyberattack occurs, and uninterrupted business operations can be ensured. In addition, data obtained from operational technologies should be handled with up-to-date approaches. In this context, this study aims to serve as a guide for the integration of information technologies and operational technologies in industries against rapidly evolving cyber risks and to raise awareness about the necessary qualifications and standards they need to maintain. Thanks to this roadmap, sectors will be able to predict risks in advance and create an uninterrupted and secure business model.

Keywords ***:*** *Cybersecurity, Industry, Deep Learning, Information Technology, Organizational Technology*

Jel Classification ***:*** *Z19.*

[1] Dr. Öğr. Üyesi, Karadeniz Teknik Üniversitesi, bilgehan@ktu.edu.tr, ORCID: 0000-0002-3496-2959

***Atıf/Citation (APA 6)*:**
İmamoğlu, M. B. (2025). Cyber infrastructure guide: IT/OT integration. *Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 18*(1), 378–391. http://doi.org/10.25287/ohuiibf.1558269.

SİBER ALTYAPI KILAVUZU: IT/OT ENTEGRASYONU

Öz

Bilgi ve iletişim teknolojilerindeki yenilikler daha karmaşık ve tehlikeli güvenlik sorunlarını ortaya çıkarmıştır. Bu mağduriyetin bir parçası olan endüstriler, siber güvenlik alanındaki yetersiz uygulamalar nedeniyle maddi ve manevi kayıplarla yüzleşmektedir. Bu durum altyapı ve endüstriyel sistemleri siber tehdit ve saldırılardan korumaya odaklanan endüstriyel siber güvenlik alanının önemini arttırmaktadır. Çeşitli endüstri dallarında kullanılan operasyonel teknolojiler ve endüstriyel kontrol sistemlerinin korunmasını kapsayan endüstriyel siber güvenlik iş ve süreçlere odaklanmaktadır. Prosesleri kesintiye uğratabilecek, tehlikelere neden olabilecek siber riskleri minimize ederek kritik altyapı ve süreçlerin güvenli bir şekilde kesintisiz çalışmasını sağlamaktadır. Her gün evrim geçiren siber saldırı türleri endüstrileri iş ve süreçlerini ciddi risklerle yüzleştirmektedir. Bu risklerin minimalize edilmesi için geleneksel koruma yöntemleri yeterli gelmemektedir. Bunun yerine endüstrilerin güncel siber güvenlik önlemlerini değiştirerek bilgi teknolojileri ile operasyonel teknolojilerini entegre etmelidir. Böylelikle siber saldırı gerçekleşmeden önlem alınabilecek ve kesintisiz bir iş süreci sağlanabilecektir. Bunun yanı sıra operasyonel teknolojilerden elde edilen veriler güncel yaklaşımlarla ele alınmalıdır. Bu bağlamda çalışma, hızla gelişen siber risklere karşı endüstrilere bilgi teknolojileri ile operasyonel teknolojilerinin entegrasyonun sağlanmasına yönelik bir kılavuz olmayı ve sahip olması gereken nitelik ve standartlar konusunda farkındalık yaratmayı amaçlamaktadır. Sağlanan bu yol haritası ile endüstriler riskleri öngörerek kesintisiz ve güvenli bir iş modeli oluşturabileceklerdir.

Anahtar Kelimeler ***:*** *Siber Güvenlik, Endüstri, Derin Öğrenme, Bilgi Teknolojisi, Organizasyonel Teknoloji*

Jel Sınıflandırılması ***:*** *Z19.*

INTRODUCTION

The development of digital industrial technology has led to the emergence of targets such as smart factories and digital transformation for industries. All these advances related to big data improve communication between digital and physical environments by enabling the development of human and machine interactive systems. In addition to their positive aspects, these developments have also brought cyber threats (Ervural and Ervural, 2017). Cybersecurity, which is on the agenda of the whole world, has also deeply affected industries. For this reason, industries need to raise awareness about industrial cybersecurity to keep their existing systems safe and develop them.

In today's conditions, where conventional security measures are inadequate and cyber threats are becoming more complex every day, many industries see the supply of security-oriented IT products as meaningless or consider them an unnecessary cost. However, this approach leads to the growth of deficiencies in the security infrastructure and to businesses becoming vulnerable to cyberattacks. The security vulnerabilities caused by this deficiency have caused unexpected stops in industrial production processes, loss of critical data, disruptions in production lines, and serious financial losses. At the same time, it also causes moral grievances such as the loss of customer trust and damage to brand reputation.

Industrial cybersecurity is of significant importance in this context and has become an indispensable element for the sustainability of businesses. Providing a robust and secure infrastructure that will help industries progress and achieve their goals is a critical requirement in today's competitive market. With the support of this infrastructure, revision and optimization of business processes will be a major step for the successful realization of digital transformation. In this way, businesses will not only be protected against current threats but will also adapt to future technological developments and gain a competitive advantage.

This study aims to raise awareness about cybersecurity in industries. Examples are given of what industries will face if they do not have a cybersecurity infrastructure, and what they will achieve if they do. The study aims to contribute to industrial development with the method in which Information Technologies (IT) and Organizational Technologies (OT) are integrated.

I. CYBERSECURITY

With the development of information and communication technologies, cybersecurity has become an important concept in the last 10 years. Cybersecurity includes a series of measures and applications that aim to protect critical systems and sensitive information, which are of vital importance today, from digital attacks. These measures, also called IT security, are developed to cope with threats against internal or external network-connected systems and applications of the organization (IBM, 2023). In today's conditions, the number of users facing cybersecurity problems is increasing, and this situation also worries individuals and companies. Sensitive information of institutions and companies can be used by hackers for fraud or blackmail. Every organization wants to take precautions to ensure the integrity and confidentiality of their data against these crimes, which can cause great material and moral damage. Because cyberattacks carry the risk of not only losing confidential data but also losing the reputation of the companies (Bendovschi, 2015).

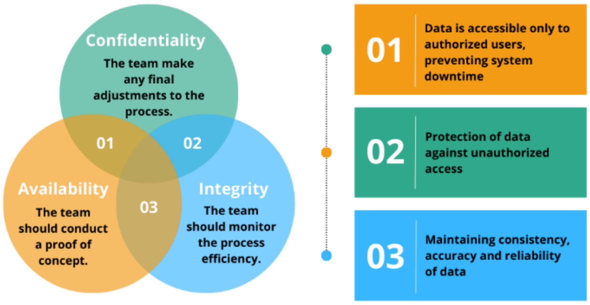
Today, the internet infrastructure is growing rapidly, and this digital environment, which has emerged with many new technologies, is taking humanity to a different dimension. However, while the protection of private information is inversely proportional to technological developments, this situation causes cybercrimes to increase day by day. Most of both commercial and individual transactions are conducted using online tools. Therefore, expertise is important to ensure the necessary security while performing transactions. Internet banking, e-commerce, cloud services, mobile phones, and other advanced technological processes should include high-security controls. Indeed, all technological tools included in these transactions hold critical and sensitive information about users. For this reason, ensuring the security of the tools and protecting sensitive data by improving cybersecurity and sustainability of infrastructures must be the priorities of every organization (Kumar and Panchanatham, 2015; Kalakuntla et al., 2019).

I.I. Cybersecurity and Components

Cyberattacks are deliberate attacks on the information and communication infrastructures of the targeted element. To prevent these attacks, information must be protected and secured. Therefore, regardless of whether the information is in a physical or electronic environment, it must be protected against unauthorized access and actions. In addition to technical measures, administrative and physical measures must also be taken to ensure the security of information. For example, using strong encryption methods and protecting systems with firewalls and antivirus software are technically important. At the same time, training and raising awareness of employees about cybersecurity, creating security policies, and conducting regular security audits are also among the administrative measures. In this way, comprehensive protection against unauthorized access and actions to information can be provided.

In this context, the basic elements used to ensure information security consist of the components known as the CIA Triad shown in Figure 1: "Confidentiality," "Integrity," and "Availability." These components represent the goals of information security (Alemdar, 2020).

Figure 1: CIA Triad


Confidentiality
The team make any final adjustments to the process.
01
02
Availability
The team should conduct a proof of concept.
03
Integrity
The team should monitor the process efficiency.
01
Data is accessible only to authorized users, preventing system downtime
02
Protection of data against unauthorized access
03
Maintaining consistency, accuracy and reliability of data

Source: Nikander et al., 2020

Confidentiality, which is one of the basic components of information security and therefore cybersecurity, covers the protection of data from unauthorized access. In this context, some measures such as encryption, authorization, and authentication are taken. The second component, integrity, refers to the data not being subject to unauthorized changes and being stored correctly. Finally, accessibility is the situation where only authorized users can access data when necessary. Backup and resilient system designs are used to ensure accessibility. In addition to these three components, there are many complementary elements. These can be listed as network security, physical security, application security, malware protection, identity and access management, emergency management, training, and awareness (John Justin and Manimurugan, 2012). Thanks to these elements, the effective operation of the basic components is achieved.

I.II. Industrial Cybersecurity

Cyberthreats are spread across a wide range of industries. Cybersecurity issues are an important issue for all industries, and companies need to protect themselves by taking security measures. Especially with the increase in industrial internet of things (IIoT) applications, infrastructure systems have become interconnected, and potential cybersecurity risks have increased. Organizations are required to ensure their internal security to continue their development. Despite this, many companies lack the resources to take adequate internal security measures (Conklin, 2016).

The security vulnerabilities that emerge vary at the technical and organizational levels. Critical issues such as the use of weak encryption algorithms, incomplete or untimely application of security patches, the use of old or outdated software and hardware, and inadequate network security are among the technical vulnerabilities (Ukwandu, 2022). The interconnected structure of IIoT devices creates a security area that is difficult to control as the number of these devices increases rapidly. The fact that many devices do not have sufficient security standards makes these systems vulnerable to external threats. Smart sensors, gateways, and other critical components that can be targeted by cyber attackers carry risks such as unauthorized access, data manipulation, and system deactivation (de Azambuja et al., 2023).

Organizational vulnerabilities are mostly caused by the human factor. Weak or inadequate security policies, low levels of cybersecurity awareness of personnel, and a lack of regular inspection of security processes are important factors that increase risks. Inadequate resources allocated to cybersecurity training can cause employees to become vulnerable to social engineering attacks. Such vulnerabilities can cause severe damage not only to data breaches and operational disruptions but also to the reputation of companies (Benias and Markopoulos, 2017). In addition, especially for small and medium-sized enterprises, resource insufficiency weakens the ability to detect security vulnerabilities and defend against attacks. As a result, technological developments cause an increase in companies' cybersecurity problems. This leads to serious consequences that threaten operational continuity and financial and reputational losses (Clim et al., 2023).

Therefore, ensuring industrial cybersecurity has become a critical requirement for companies. Now, identifying and eliminating security vulnerabilities, establishing an infrastructure resistant to cyber threats, and ensuring operational continuity are essential to prevent financial and reputational losses. In addition to keeping their technical infrastructures up-to-date and secure, companies should invest in comprehensive training programs that will increase employees' cybersecurity awareness. In addition, it is necessary to implement strict security policies, conduct regular risk assessments, and develop emergency response plans to minimize cyber risks (Lipnicki et al., 2018). Based on all of this, ensuring effective industrial cybersecurity has become an essential requirement for companies to achieve sustainable growth and maintain their competitiveness.

However, the industrial cybersecurity market is growing day by day. The main purpose of this market is to protect production and supply chains against unauthorized access, manipulation, and interruptions. In this context, industrial cybersecurity goes beyond conventional data security and addresses risks to production and industrial infrastructures. In this way, both such risks will be minimized, and a design-oriented security approach will be adopted by maximizing the security of the infrastructures while they are still in the design phase. In today's industries, strategies that integrate IT, IIOT, and OT are needed due to the inadequacy of function-oriented cybersecurity applications. In summary, companies should adopt a more comprehensive and holistic perspective to protect their assets, effectively run their processes, and ensure their development (Murray et al., 2017; Gruyter, 2021).

Figure 2: IT/OT Integration Success Pyramid

Source: Cigref (2019).

Operational activities are the existential reason for an industry. Operations have been supported and gained efficiency with developing technologies. Indeed, increasing cyber threats have required the integration of operational technologies with information technologies. Only with this method will they be able to protect their digital assets and identities, which are the first step of the pyramid seen in Figure 2. If the security of the entire technological infrastructure is ensured, the data will be accurate, consistent, integrated, and strong enough to support digitalization. Thanks to this data, it will be possible to progress with strong steps to each step of the pyramid and achieve business goals.

II. CYBERSECURITY AND INDUSTRIAL DEVELOPMENTS

Industrial developments have been following each other rapidly for years. This series, which started with the invention of the steam engine, continued with Industry 1.0, 2.0, 3.0, and 4.0. Developments in the production line in these processes have resulted in technology and automation that allow many manual tasks to be conducted automatically. The focus of Industry 4.0, which we are currently in, is smart factories. Smart factories are automated production facilities that integrate technologies such as the internet of things (IoT), artificial intelligence (AI), and robotics to optimize operations using advanced technology and increase efficiency, productivity, and quality in production facilities. These facilities aim to collect, analyze, and optimize processes through smarter and connected systems (Soori et al., 2023; Güdek, 2023). Figure 3 shows some digital tools used in Industry 4.0.

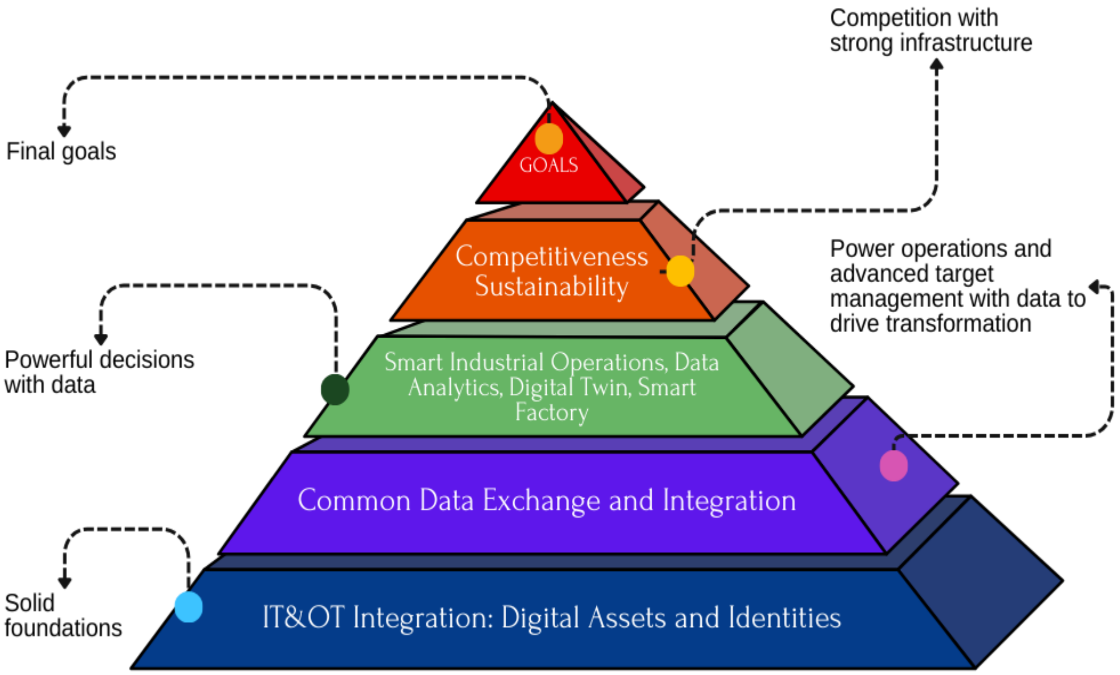
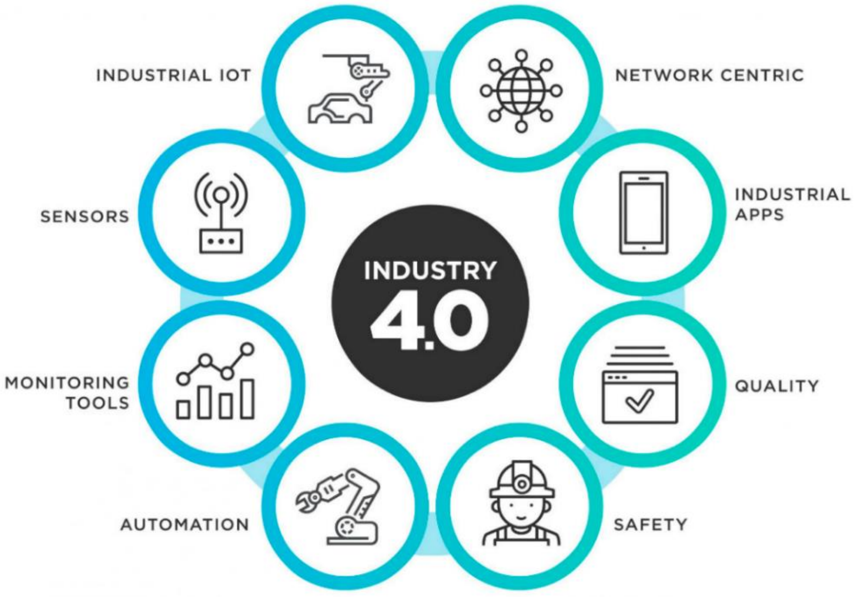

Competition with strong infrastructure
Final goals
GOALS
Competitiveness Sustainability
Power operations and advanced target management with data to drive transformation
Powerful decisions with data
Smart Industrial Operations, Data Analytics, Digital Twin, Smart Factory
Common Data Exchange and Integration
Solid foundations
IT&OT Integration: Digital Assets and Identities

Figure 3: Digital Tools of Industry 4.0



Source: Intelegain Technologies, 2022

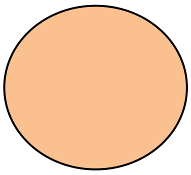
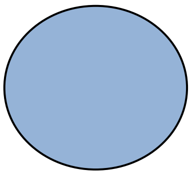
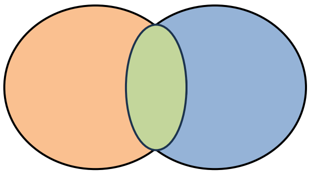
With Industry 4.0, a cyber-physical infrastructure has been created in the world to which a different machine can be connected for the operation to run more effectively. Different types of big data have caused an increase in cyber problems. Attacks, especially on smart factories, can cause severe damage to the production line, products, customers, and employees (Casalicchio, 2021). In addition to maintaining the digital security of sub-temperature IT hardware with firmware updates, authorized access must be physically prevented. While DMZ and VLAN methods can provide solutions for limiting digital freedom to critical IT infrastructures, these digital measures can be passively suppressed by attackers with unauthorized physical access to the relevant switching devices. For this reason, physical access to environments where critical infrastructure is located must be protected with biometric identification methods and authorization controls (Conklin, 2016; Paes, 2020).

One of the industrial cybersecurity vulnerabilities is that critical hardware is vulnerable to unauthorized physical access. It is important to protect the IT devices used by authorized users against viruses and other malicious attackers with anti-X (antivirus, antispyware, etc.) products. In addition to software solutions, limiting physical connections to the IT devices used by these users is also among the precautions that must be taken (Clim et al., 2023). An external data source should not be connected to a network device with high authority. Intrusion Detection and Intrusion Prevention systems are among the products used to ensure industrial security while protecting the end user and detecting and preventing malicious traffic in the network environment.

The sustainability of industrial devices can be ensured with hardware and software compatibility. Industrial security can be disrupted by a software update that will cause the hardware to operate differently than expected. For this reason, the firmware versions running on the hardware must be under control, and unauthorized persons must be prevented from updating the firmware. In cases where access to critical systems from outside the organization is required, methods that provide security and authentication, such as VPN (Virtual Private Network), must be used. In network topologies that do not require restriction of rule-based access, lack authentication for access to the internal network, and do not have configured source IP restrictions, it is inevitable for attackers to access and damage critical systems after seizing a device on the corporate network (Zhang et al., 2004; Dalmazo et al., 2021; Sahay et al., 2021).

In addition to providing a strong infrastructure in the organization, IT and OT collaboration has a supporting and strengthening role in business processes. Data collected through sensors or devices and processed in various software can be used for different purposes. The results obtained from this data can be helpful in decision-making, an order, or an alarm for a different business process (Tian and Hu, 2019). All of these can be fulfilled thanks to the intersection set given in Figure 4 and help with digital transformation.

Figure 4: Information Technologies & Organizational Technologies

Information Technologies	
	Critical infrastructure required for data processing Systems that serve as corporate information repositories; Making data available to business applications and their users
Organizational Technologies	
	Networking of devices and software used in industrial, manufacturing, and process control systems Supports specialized hardware that captures and transmits data and enables industrial equipment to perform specific tasks
Information Technologies & Organizational Technologies	
	Combining two separate networks and sharing the data each collects and distributes Establishing two teams that work independently to pool their resources and expertise

Source: Bigelor ve Lutkevich (2021).

According to Figure 4, which shows the relationship between IT and OT and their intersections, IT includes the critical infrastructure required for data processing and the systems that serve as corporate information repositories, and these systems make data available to business applications and their users. OT covers the network of devices and software used in industrial, manufacturing, and process control systems and supports specialized hardware that captures and transmits data and enables industrial equipment to perform specific tasks (Murray et al., 2017). The intersection with IT/OT is aimed at combining two different networks, creating two teams that work independently to share the data that each collect and distributes and brings together their resources and expertise.

Generally, IT deals with enterprise information management, data processing and business applications. OT deals with the control and management of industrial processes. Leveraging the collaboration and advantages of IT and OT enables the opportunities that data can provide to be used effectively in business and industrial processes. Thus, it creates data management and analysis opportunities by offering a holistic approach (Kamal et al., 2016; Lipnicki et al., 2018).

It is very important to develop strategies for the efficient and effective use of data in industrial processes and the optimization of processes. First of all, strong security protocols are needed in IT and OT areas to reduce cybersecurity risks (Paes, 2020). In order to ensure IT and OT collaboration, people from different areas of expertise need to work together. For this reason, teams need to be able to replace each other and have knowledge about their work areas. In this context, it is critical for the organization to provide the necessary training to its personnel. In this way, a strong organizational structure can be created and personnel from different units can replace each other. In addition, the collaboration of these two systems requires a complex organizational chart and management process. Various mechanisms should be created, and investments should be made to effectively manage and monitor these processes (Giannelli and Picone, 2022).

III. DEEP LEARNING-BASED THREAT DETECTION

By processing the data obtained from these technologies correctly and effectively, it is possible to use OT effectively to ensure industrial cybersecurity. We use OT systems to monitor production processes, evaluate equipment performance, and report on overall business status. However, using this data only for static reporting can lead to missing important silver security opportunities. Today, it is possible to process OT data with a more proactive and analytical approach with the use of advanced machine learning (ML) and deep learning (DL) techniques. These methods extract meaningful models and insights from the data, allowing both the detection of existing vulnerabilities and the prevention of potential problems in advance.

Machine learning and deep learning algorithms show superior performance in analyzing large data sets from OT systems and detecting anomalies. For example, time series-oriented algorithms such as recurrent neural networks (RNN) and long short-term memory (LSTM) can detect energy consumption, temperature changes, and anomalies in production processes in real time (Koay et al., 2023). These models learn from the reactions of the data over time, detect deviations, and alert operators to a security breach or system failure.

The integration of IT methods with OT combines the powerful data processing capabilities of IT with the field data of OT. For example, an IT-OT system can detect vulnerabilities in both physical and digital processes and create defense mechanisms (Cigref, 2019). Such an approach not only solves current problems but also helps to take measures to prevent future threats.

Especially with Industry 4.0, the rise of IoT devices, advanced sensors, and smart factories has caused OT systems to become more complex and interconnected. However, this increases cybersecurity threats and offers new ways to prevent them. For example, an LSTM-based model used in a power plant can detect sudden changes in energy production and predict a possible attack or equipment failure (Visconti et al., 2024). From this point on, analyzing data from OT systems using machine learning and deep learning techniques is one of the important elements of industrial cybersecurity strategies. The integration of IT and OT plays an important role both in closing existing security gaps and in creating a defense mechanism against future threats.

Figure 5: Roadmap for Deep Learning-Based Anomaly Detection

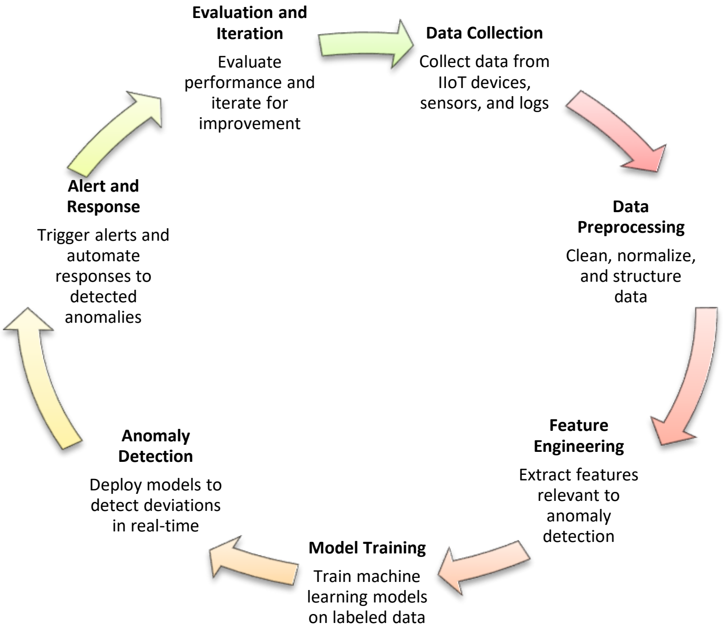

Evaluation and Iteration
Evaluate performance and iterate for improvement
Data Collection
Collect data from IIoT devices, sensors, and logs
Data Preprocessing
Clean, normalize, and structure data
Feature Engineering
Extract features relevant to anomaly detection
Model Training
Train machine learning models on labeled data
Anomaly Detection
Deploy models to detect deviations in real-time
Alert and Response
Trigger alerts and automate responses to detected anomalies

Figure 5 provides a roadmap for deep learning-based anomaly detection. According to this systematic, vulnerabilities will be proactively identified precautions will be taken, and the security of enterprises will be increased.

The first stage, data collection, is the collection of data from IT and OT systems, which forms the basis of deep learning models. For example, in a smart factory, a comprehensive data set can be created by combining temperature, pressure, and energy consumption data from sensors with network traffic logs. This approach allows the determination of the normal behavior profiles of the system. In the second stage, incomplete or erroneous data are cleaned, normalized, and transformed to make the collected data suitable for analysis. Synchronizing and scaling the data from different sensors to a common period increases the accuracy of the model. The third stage is featuring engineering. At this stage, the effectiveness of DL models extracting meaningful features from the data set is determined. If we consider energy consumption, performing trend analysis of temperature changes and sudden increases can help in the early detection of potential abnormal situations.

There are different approaches in the model training stage. Although ML models have been used frequently in literature, current studies show that DL models are more successful and faster in abnormal situation detection. DL models are trained to detect and distinguish between normal and abnormal situations (Pang et al., 2021; Pang et al., 2022; Abdalgawad et al., 2022). Long Short-Term Memory (LSTM) and Recurrent Neural Networks (RNN) are effective in detecting abnormal situations in temporal datasets (Munir et al., 2019; Lindemann et al., 2021; Ullah and Mahmoud, 2022). The model trained for anomaly detection analyzes the dataset and determines abnormal situations and deviations. For example, if an excessive temperature increase is detected in a chemical plant, the system automatically starts the cooling process and can convert the abnormal situation to a normal situation. When a production line is considered, there may be unexpected stops or performance drops in the processes. These can be marked as abnormal by the model. Automatic warning systems are activated against the detected anomalies and the necessary mechanisms are worked for precautions. Finally, evaluation and improvement are carried out systematically, and the performance of the model is regularly evaluated, and updates are made when necessary. This continuous improvement process increases the resilience of the system against new threats.

DL-based threat detection systems provide an effective solution to manage the complexities brought about by IT and OT integration. These systems both create proactive defense mechanisms against cyber threats and ensure that business processes continue uninterrupted and secure. Thus, the operational efficiency of businesses is increased.

DISCUSSION AND SUGGESTIONS

As a result, organizations must ensure industrial security in digital and connected production environments that are evolving in parallel with Industry 4.0. With the proliferation of smart factories and connected systems, security concerns in business and processes have increased. This has put basic security elements such as data confidentiality, integrity, and availability at risk. The resulting risks have rendered traditional security measures inadequate and required companies to develop more sophisticated and holistic security strategies.

To create an effective and efficient security management system, companies must develop strong protection mechanisms against cyber threats in both digital and physical environments. To increase the difficulty of attackers to overcome obstacles, multi-layered control and monitoring systems and defense-in-depth strategies must be implemented (Rahman, 2020). These strategies should cover not only technological measures but also the human factor. Increasing employees' awareness of cybersecurity, eliminating skill deficiencies, and implementing continuous training programs will help minimize human-related security vulnerabilities.

In addition, to fully ensure cybersecurity across the organization, security measures must be integrated horizontally and vertically into all operations. Strengthening collaboration between IT and OT teams will allow systems to be managed with a holistic approach and will make it easier to detect and eliminate security vulnerabilities. Ensuring transparency of technological assets and processes, increasing collaboration between teams and processes, and reducing resistance to change will enable companies to achieve a more flexible and resilient structure.

In this context, to ensure industrial cybersecurity, companies need to constantly review and update their security policies and conduct regular risk assessments. Based on this, it is of great importance to develop emergency response plans. In addition, it is very important to implement security standards throughout the supply chain and evaluate relationships with third parties from a security perspective to increase the overall level of security.

Ensuring industrial security is not only the protection of existing businesses and processes but also an ideal method for capturing future growth and innovation opportunities. Companies will be able to maintain their competitive advantage and succeed in new value chains with an infrastructure that is resistant to cyber threats. Therefore, industrial security is not only a technical requirement but also a strategic priority and should be integrated into every layer of the organization.

As a result, to ensure industrial security, top management should first lead and increase the cyber security awareness of its personnel. To this end, it should organize training programs for personnel consistently. It should use up-to-date technology and software in its systems in the business. It should carry out all processes in effective cooperation between IT and OT teams. It should create an infrastructure that is resistant to attacks by implementing innovative defense strategies and multi-layered security measures.

To respond quickly to cybersecurity attacks in emergencies, response plans should be developed and tested regularly. Security policies should be established, audited, and strictly enforced. Asset and inventory management of all digital and physical assets and the security of these inventories should be ensured. Supply chain security must be prioritized, and relationships with third parties must be managed from a security perspective.

Cyberthreat intelligence must be monitored, and proactive measures must be taken against threats by investing in new technologies. Compliance and compliance with standards must be ensured, communication between departments must be strengthened, and disconnected teams and processes must be integrated. Employees' adaptation to new systems and processes must be supported with change management strategies, and business continuity must be protected with regular backup and data recovery plans. Physical security measures must be taken, and continuous improvement and monitoring processes must be implemented. Thanks to these holistic approaches, companies will become more resilient to cyber threats and will be able to effectively ensure industrial security.

The use of innovative technologies in the field of cybersecurity is very important to developing more effective defense mechanisms against cyberthreats. To get fast and accurate results in attack and threat detection, it is necessary to adopt newly developed models by leaving aside traditional methods. While traditional approaches use the data obtained from OT devices to monitor the current situation and create reports, the strategic potential of this data is ignored. This data is obtained from OT devices and can be used as an effective source for attack, threat, and anomaly detection with advanced analysis methods. Thus, vulnerabilities can be detected and prevented before they occur. Although there are limited studies on deep learning-based anomaly detection systems in the literature, current findings show that these methods provide more successful results compared to traditional approaches. Thanks to their ability to process complex and large data sets, DL algorithms have provided significant improvements in the field of anomaly detection. A defense mechanism can be created in industrial systems with deep learning models such as autoencoder, LSTM, and RNN (Pang et al., 2020; Ma et al., 2021; Arshad et al., 2022). There are still challenges such as data requirements, explainability, and cost for these models. Despite all these disadvantages, important steps are being taken to develop more effective, faster, and more versatile anomaly detection systems. In this context, the expansion of deep learning methods to support future applications in industrial cybersecurity has a critical potential.

RESULT

IT and OT collaboration is very important in increasing the efficiency and speed of modern production processes in industrial systems. The integration that occurs with this collaboration brings many advantages. Thanks to this integration, data is collected and analyzed more quickly and efficiently. As a result of these analyses, meaningful insights and predictions are obtained. All of these also support the optimization of industrial processes. In this way, industries can protect their infrastructures not only against physical threats but also against digital threats and ensure business continuity. Operating IT and OT systems within a common security framework offer a different perspective. It provides a holistic approach against cybersecurity threats and thus strengthens the security and sustainability of industrial processes.

The application of DL models in intrusion detection offers a promising way to make sense of the data stream obtained from OT devices. DL algorithms that analyze large and complex data sets can detect anomalies accurately and quickly. Compared to traditional approaches, these methods create a more dynamic and proactive defense mechanism, allowing the detection of existing problems and the prevention of potential threats at an early stage. The applicability of deep learning in industrial systems has great potential to close existing vulnerabilities and increase resilience against future threats. Therefore, adopting deep learning-based systems supported by IT-OT collaboration can be considered a harbinger of a new era in industrial cybersecurity.

This study argues that IT and OT collaboration is necessary for ensuring industrial cybersecurity, while it states that IT would be more beneficial if it took advantage of advanced technologies. Therefore, for future studies, it calls on researchers to develop threat systems using DL algorithms from data obtained from OT devices. The next phase of this study will be an applied test of DL models for anomaly detection.

REFERENCES

Abdalgawad, N., Sajun, A., Kaddoura, Y., Zualkernan, I. A., and Aloul, F. (2022). "Generative Deep Learning to Detect Cyberattacks for the IoT-23 Dataset," in IEEE Access, vol. 10, pp. 6430-6441. doi: 10.1109/ACCESS.2021.3140015.

Alemdar, A. (2020). Bilgi Güvenliği ve Siber Güvenlik | Türkiye Siber Güvenlik Kümelenmesi. Erişim: https://www.defenceturk.net/bilgi-guvenligi-ve-siber-guvenlik-turkiye-siber-guvenlik-kumelenmesi

Arshad, K., Ali, R., Muneer, A., Aziz, I., Naseer, S., Khan, N., & Taib, S. (2022). Deep Reinforcement Learning for Anomaly Detection: A Systematic Review. *IEEE Access*, 10, 124017-124035. https://doi.org/10.1109/ACCESS.2022.3224023.

Bendovschi, A. (2015). *Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 28, 24–31.* doi:10.1016/s2212-5671(15)01077-1

Benias, N. and Markopoulos, A. P. (2017). "A review on the readiness level and cyber-security challenges in Industry 4.0," *South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Kastoria, Greece, 2017, pp. 1-5, doi: 10.23919/SEEDA-CECNSM.2017.8088234.

Bigelor, S. J. & Lutkevich, B. (2021). What is IT/OT convergence? Everything you need to know. Erişim: https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence

Casalicchio, E., & Gualandi, G. (2021). *ASiMOV: A self-protecting control application for the smart factory. Future Generation Computer Systems, 115, 213–235.* doi:10.1016/j.future.2020.09.003

Cigref (2019). IT/OT Convergence: A fruitful integration of information systems and operational systems. https://www.cigref.fr/wp/wp-content/uploads/2020/02/Cigref-IT-OT-Convergence-Fruitful-integration-information-operational-systems-December-2019-EN.pdf

Clim A, Toma A, Zota RD, Constantinescu R. (2023).The Need for Cybersecurity in Industrial Revolution and Smart Cities. Sensors. 23(1):120. https://doi.org/10.3390/s23010120

Conklin, W. A. (2016). "IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilienc," *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, pp. 2642-2647, doi: 10.1109/HICSS.2016.331.

Dalmazo, B., Marques, J., Costa, L., Bonfim, M., Carvalho, R., Silva, A., Fernandes, S., Bordim, J., Alchieri, E., Schaeffer-Filho, A., Gaspary, L., & Cordeiro, W. (2021). A systematic review on distributed denial of service attack defense mechanisms in programmable networks. *International Journal of Network Management*, 31. https://doi.org/10.1002/nem.2163.

de Azambuja, A.J.G.; Plesker, C.; Schützer, K.; Anderl, R.; Schleich, B.; Almeida, V.R. (2023) Artificial Intelligence-Based Cybersecurity in the Context of Industry 4.0—A Survey. *Electronics*, *12*, 1920. https://doi.org/10.3390/electronics12081920

Ervural, B. C., & Ervural, B. (2017). *Overview of Cybersecurity in the Industry 4.0 Era. Industry 4.0: Managing The Digital Transformation, 267–284.* doi:10.1007/978-3-319-57870-5_16

Giannelli C, Picone M. (2022). “Industrial IoT as IT and OT Convergence: Challenges and Opportunities”. *IoT*. 3(1):259-261. https://doi.org/10.3390/iot3010014

Gruyter, D. (2021). Industrielle Cybersicherheit: ein Wachstumsmarkt. *Zeitschrift für wirtschaftlichen Fabrikbetrieb*, *116*(12), 857-857. https://doi.org/10.1515/zwf-2021-1019

Güdek, B. (2023). Endüstriyel dönüşüm ve endüstri 5.0. Ömer Halisdemir Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi, 16(4), 1129-1142. https://doi.org/10.25287/ohuiibf.1331731

IBM (2023) Erişim: What is cybersecurity? https://www.ibm.com/topics/cybersecurity

Intelegain Technologies (2022). The Ultimate Guide to IoT-Driven Digital Transformation in Manufacturing. Available online: https://www.intelegain.com/the-ultimate-guide-to-iot-driven-digital-transformation-in-manufacturing/ (20.09.2024).

John Justin, M., & Manimurugan, S. (2012). A survey on various encryption techniques. *International Journal of Soft Computing and Engineering (IJSCE) ISSN*, *2231*, 2307.

Kalakuntla, R., Vanamala,A. & Kolipyaka,R.(2019).Cybersecurity. HOLISTICA – Journal of Business and Public Administration,10(2) 115-128. https://doi.org/10.2478/hjbpa-2019-0020

Kamal, S. Z., Al Mubarak, S. M., Scodova, B. D., Naik, P.. , Flichy, P.. , and G.. Coffin (2016). "IT and OT Convergence - Opportunities and Challenges." Paper presented at the SPE Intelligent Energy International Conference and Exhibition, Aberdeen, Scotland, UK. doi: https://doi.org/10.2118/181087-MS

Koay, A.M.Y., Ko, R.K.L., Hettema, H. *et al.* Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. *J Intell Inf Syst* **60**, 377–405 (2023). https://doi.org/10.1007/s10844-022-00753-1

Kumar, D. & Panchanatham, N. (2015). A case study on Cybersecurity in E-Governance. International Research Journal of Engineering and Technology (IRJET). 2(8), 272-275.

Lindemann, B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). A survey on anomaly detection for technical systems using LSTM networks. Computers in Industry, 131, 103498.

Lipnicki, P., Lewandowski D., Pareschi D., Pakos W. and Ragaini E. (2018). "Future of IoTSP – IT and OT Integration," *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, Barcelona, pp. 203-207, doi: 10.1109/FiCloud.2018.00037.

Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q., & Xiong, H. (2021). A Comprehensive Survey on Graph Anomaly Detection With Deep Learning. *IEEE Transactions on Knowledge and Data Engineering*, 35, 12012-12038. https://doi.org/10.1109/TKDE.2021.3118815.

Mining (WSDM '21). Association for Computing Machinery, New York, NY, USA, 1127–1130. https://doi.org/10.1145/3437963.3441659

Munir, M., Siddiqui, S., Dengel, A., & Ahmed, S. (2019). DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series. *IEEE Access*, 7, 1991-2005. https://doi.org/10.1109/ACCESS.2018.2886457.

Murray, G., Johnstone, M. N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. DOI: 10.4225/75/5a84f7b595b4e

Nikander, J., Manninen, O., & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communication networks. Computers and electronics in agriculture, 179, 105776.

Paes, R., Mazur D. C., Venne B. K. and Ostrzenski J. (2020). "A Guide to Securing Industrial Control Networks: Integrating IT and OT Systems," in *IEEE Industry Applications Magazine*, vol. 26, no. 2, pp. 47-53, March-April 2020, doi: 10.1109/MIAS.2019.2943630.

Pang, G., Shen, C., Cao, L., & Hengel, A. (2020). Deep Learning for Anomaly Detection. *ACM Computing Surveys (CSUR)*, 54, 1 - 38. https://doi.org/10.1145/3439950.

Pang, G. Cao, L., and Aggarwal, C. (2021). Deep Learning for Anomaly Detection: Challenges, Methods, and Opportunities. In Proceedings of the 14th ACM International Conference on Web Search and Data

Pang, G., Shen, C., Cao, L., and Hengel, A.V.D. (2022). Deep Learning for Anomaly Detection: A Review. ACM Comput. Surv. 54, 2. https://doi.org/10.1145/3439950

Sahay, R., Geethakumari, G., & Mitra, B. (2021). A holistic framework for prediction of routing attacks in IoT-LLNs. *The Journal of Supercomputing*, 78, 1409 - 1433. https://doi.org/10.1007/s11227-021-03922-1.

Soori, M., Arezoo, B. & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. Internet of Things and Cyber-Physical Systems. 3, 192-204. doi:10.1016/j.iotcps.2023.04.006

Tian, S. and Hu, Y. (2019). "The Role of OPC UA TSN in IT and OT Convergence," *2019 Chinese Automation Congress (CAC)*, Hangzhou, China, pp. 2272-2276, doi: 10.1109/CAC48633.2019.8996645.

Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information*, *13*, 146. https://doi.org/10.3390/info13030146

Ullah I. and Mahmoud, Q. H. (2022) "Design and Development of RNN Anomaly Detection Model for IoT Networks," in *IEEE Access*, vol. 10, pp. 62722-62750. doi: 10.1109/ACCESS.2022.3176317.

Visconti, P., Rausa, G., Del-Valle-Soto, C., Velázquez, R., Cafagna, D., & De Fazio, R. (2024). Machine Learning and IoT-Based Solutions in Industrial Applications for Smart Manufacturing: A Critical Review. *Future Internet*, *16*(11), 394. https://doi.org/10.3390/fi16110394

Zhang, Z., Zhang, Y.Q., Chu, X. & Li, B. (2004). An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN. Photonic Network Communications. 7, 213-225.

Etik Beyanı **:** *Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu yazarlar beyan eder. Aksi bir durumun tespiti halinde ÖHÜİİBF Dergisinin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazar(lar)ına aittir.*

Bu çalışmada kullanılan veriler, herkesin kullanımına açık şekilde paylaşıldığından ve etik kurul izni gerektiren araştırmalar içerisinde bulunmadığından etik kurul izni alınmamıştır.

Teşekkür (Varsa) **:** *Yayın sürecinde katkısı olan hakemlere ve editör kuruluna teşekkür ederiz.*

Ethics Statement **:** *The authors declare that ethical rules are followed in all preparation processes of this study. In case of detection of a contrary situation, ÖHÜİİBF Journal does not have any responsibility and all responsibility belongs to the author (s) of the study.*

Since the data used in this study is shared publicly and does not include research requiring ethics committee approval, ethics committee approval has not been obtained.

Acknowledgement **:** *We thank the referees and editorial board who contributed to the publishing process.*