Düzce University
Journal of Science & Technology

Research Article

Industry 4.0 and Cybersecurity at Automobile Manufacturing in Smart Factories

Cevat ÖZARPA [a], İsa AVCI [b,*]

[a] *Department of Mechanical Engineering, Faculty of Engineering, Karabuk University, Karabuk, TURKEY*
[b] *Department of Computer Engineering, Faculty of Engineering, Karabuk University, Karabuk, TURKEY*
* *Corresponding author's e-mail address: isaavci@karabuk.edu.tr*

DOI: 10.29130/dubited.1027236

ABSTRACT

The automotive industry in smart factories is constantly developing depending on technology. Depending on the developing technology, security problems come to the fore. Industry 4.0 and cyber security are widely used in automotive sector applications as well as in all areas of our lives. These applications pose security threats to automotive users and drivers. Attacks on vehicle software, especially by autonomous vehicle users, endanger passengers and vehicle safety. It should take the necessary precautions to be protected against cyber-attacks and be equipped to solve the problem. The rapid change of technology in smart factories and with industry 4.0 brings new security vulnerabilities and new cyber attacks. The hostility arising from inter-sectoral competition has lost its value compared to previous periods and has left its authority to cyberattacks, threats, and damaging moves against system security. Industry 4.0 is also known as the Industrial Revolution Industry, which covers a specific production technology and the interests of many groups, and exchanges data without human use and innovative system. With this industrial revolution, which also plays an active role in the establishment of a smart factory, more useful work examples are obtained as it ensures that each data is collected and analyzed in the best way in the production area. In this study, cyber attacks in the automotive industry and cyber threats in automobile factories are examined. In addition, layered protection has been proposed by investigating how to take precautions against these attacks and threats.

Anahtar Kelimeler: *Cybersecurity, Cyber-attacks, Industry 4.0, Smart factories.*

Akıllı Fabrikalardaki Otomobil İmalatında Endüstri 4.0 ve Siber Güvenlik

ÖZ

Akıllı fabrikalardaki otomotiv sektörü, teknolojiye bağlı olarak sürekli gelişmektedir. Buna bağlı olarak güvenlik sorunları ön plana çıkmaktadır. Endüstri 4.0 ve siber güvenlik hayatımızın her alanında olduğu gibi otomotiv sektörü uygulamalarında da yaygın olarak kullanılmaktadır. Bu uygulamalar, otomotiv kullanıcıları ve sürücüleri için güvenlik tehditleri oluşturur. Özellikle otonom araç kullanıcıları tarafından araç yazılımlarına yönelik saldırılar, yolcuları ve araç güvenliğini tehlikeye atıyor. Siber saldırılara karşı korunmak için gerekli önlemler alınmalı ve sorunları çözebilecek donanımlara sahip olunmalıdır. Akıllı fabrikalarda ve endüstri 4.0 ile teknolojinin hızlı değişimi, yeni güvenlik açıklarını ve yeni siber saldırıları beraberinde getirmektedir. Sektörler arası rekabetten kaynaklanan siber saldırılar, tehditler ve sistem güvenliğine yönelik zarar verici sorunlar yaşanmaktadır. Endüstri 4.0, belirli bir üretim teknolojisini ve birçok grubun ilgi alanlarını kapsayan, insan kullanımı ve yenilikçi sistem olmadan veri alışverişi yapan Sanayi Devrimi Endüstrisi olarak da bilinir. Akıllı fabrikanın kurulmasında da etkin rol oynayan bu sanayi devrimi ile üretim alanında her bir verinin en iyi şekilde

Received: 22/11/2021, Revised: 15/05/2022, Accepted: 20/05/2022

toplanıp analiz edilmesini sağladığı için daha faydalı çalışma örnekleri elde edilmektedir. Bu çalışmada otomotiv endüstrisindeki siber saldırılar ve otomobil fabrikalarındaki siber tehditler incelenmiştir. Ayrıca bu saldırı ve tehditlere karşı nasıl önlem alınacağı araştırılarak katmanlı bir güvenlik koruması önerilmiştir.

Keywords: *Siber güvenlik, Siber saldırılar, Endüstri 4.0, Akıllı fabrikalar.*

I. INTRODUCTION

With industry 4.0, the rapid transition to industry 5.0 all over the world has started in recent years. This development changes depending on the technologies. In particular, industry 5.0 is considered a smart society, and developments in the field of artificial intelligence are also taken into account. With the information itself increasingly feeling like a power factor, thinking shapes our perceptions, our research methods, and going significant changes in our lifestyle in many different areas [1]. However, making it a portable technology, producing and using autonomous vehicles is a beneficial innovation. It brings cyber threats, security vulnerabilities, cyber-attacks, and accessing and deactivating personal and system software. Since the personal sharing of data by individuals on social platforms disables their security, individuals should be made aware of and trained in cybersecurity. The same situation here applies to factories and autonomous vehicle users. The competitiveness of manufacturing enterprises in local and global markets is essential for private sector-based economies. With the changing conditions in the world and Turkey, "industrialization" has ceased to be the main objective, and now it has become the main objective to increase competitiveness [2]. Employees should receive the necessary cyber training, and a cybersecurity committee should be established. Security vulnerabilities should be identified, and complete security should be ensured so that autonomous vehicle users do not suffer any cyber attacks during their journey and that hackers do not control the vehicle. The automotive sector affects the economy by creating a multiplier effect for Turkey, as in many countries. This is why; digitalization in the industry should be followed closely. More efficient and customized production should be possible [3]. Unauthorized access to data, hijacking and controlling software is termed theft. Those who commit cybercrimes are considered guilty by law and are punished. The cyberattack area is an area that attracts attention and studies in the changing world of technologies.

Many technological developments in this field have been achieved within the scope of research. The development of industry 4.0, especially in smart factories, is a remarkable feature. Especially in Germany, the concept of cyber security systems and the Internet of Things have become an important area in automotive production in smart factories [4]. The main purpose of Industry 4.0 can be expressed as the needs of advanced industrialized countries, with the digitalization of the industry, to significantly increase the competitiveness of the manufacturing industry and to eliminate the competitive advantage of developing countries in this area. Intense trade relations with the EU and other European countries, especially the manufacturing industry sector, industrial investments of these countries in our country, our investment goods, and technology imports from these countries have brought digitalization in the sector to our country's agenda[5]. Although Industry 4.0 seems to have emerged based on production, similar to other industrial revolutions in the past, it is estimated that its possible effects will not be only in this area. Digitalization and the systems it supports affect all business functions, from production to marketing. Moreover, this process seems to affect a much wider area, not just at the enterprise level. Examples of macro-level issues such as growth, employment, education, investment climate, and entrepreneurship can be given [6]. In the information age, where data privacy and our information are the most valuable, being cyber-attacked indicates the collapse of the security system.

The industrial revolution, defined as Industry 4.0, has been replaced by smart factories in recent years [7]. Industry 4.0 is to continue production with robots that interact with each other, control the environment with sensors, analyze the data it collects, and find and meet needs. It also aims for more capable, safer, faster, and less wasteful production. However, Industry 4.0 examines cyber systems in smart factories using disassembled structures, controlling the cooperation between objects and people.

In an inter-sectoral competitive environment, it is necessary to include Industry 4.0 in their work and plan to maintain their strength and maintain their existence for the future. Smart factories can be developed in the production process and organization, software, hardware, and mechanical structure [8]. The factory, which has a strong, flexible, and agile production suitable for production, becomes possible. In this study, industry 4.0 and cyber security in automobile production in smart factories are examined [9]. Right now the industry is turning the physical world of real things into "virtual replicas". This transformation is a core element of industry 4.0, and industry 5.0 is becoming more and more popular due to the high requirements of end-users for the personalization of the purchased product [10]. However, institutions need to be ready in terms of infrastructure to make the transition to this. This transition implies the penetration of artificial intelligence into human life to increase human capabilities [11]. When industry 4.0 and cyber security are evaluated in terms of efficiency in smart factories and automobile manufacturing facilities, advanced analytical techniques in predictive maintenance programs can prevent machine errors encountered [12]. In addition, disruptions, problems, and job losses that may occur in cyber security, designing systems with the following technology, and using secure models provide advantages in terms of efficiency. Efficiency is achieved by preventing job loss, using innovations in technology, reducing maintenance errors, using automation systems, and establishing smart factories. In addition, some companies will be able to establish factories that continue production without employees. In these factories, a workforce will be needed and employees will work more efficiently [13].

This study aims to reveal the technology dependency for automotive production, industry 4.0, and later versions, especially in smart factories. These technologies are aimed at automating production, especially in the fields of IoT, 5G, AI, and cloud computing. However, according to these developing technologies, security vulnerabilities and cyber security threats should be investigated and necessary precautions should be taken. In this study, the ISA-99 PERA (Purdue Enterprise Reference Architecture) model, which is also a layered model, consists of the end-user layer, protection layer, and smart factory equipment layers. There are certain protection methods in each layer and there is separate equipment specific to each layer. In this study, a general evaluation has been made by researching industry 4.0 and cybersecurity in automobile manufacturing in smart factories. First of all, the industrial revolution, cybersecurity, the internet of things in automobile manufacturing, cyber-attacks, and precautions against cyber-attacks are explained.

II. REVOLUTION OF THE INDUSTRIAL AND SMART FACTORIES

The industrial revolution generally consists of four periods. These industries are 1.0, 2.0, 3.0, and 4.0. Industry 4.0 is known as the latest industrial revolution. The industrial revolution that has developed up to this time consists of these four periods. With the industrial revolutions, many understandings of production have changed, new rules have begun to be applied, and decisions have been made by looking at the development levels of countries and their industrialization levels. Industrialization can be defined as the transformation of nature parallel to human needs.

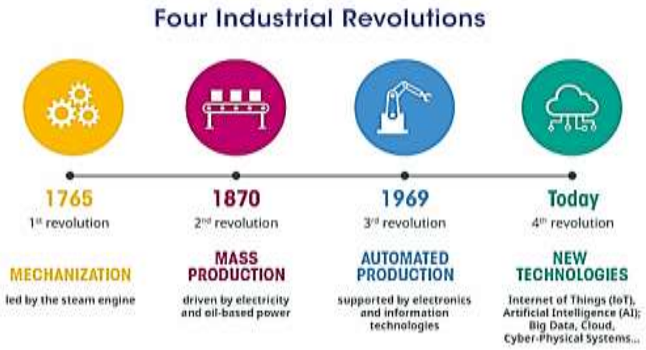
Four Industrial Revolutions
1765
1st revolution
MECHANIZATION
led by the steam engine
1870
2nd revolution
MASS PRODUCTION
driven by electricity and oil-based power
1969
3rd revolution
AUTOMATED PRODUCTION
supported by electronics and information technologies
Today
4th revolution
NEW TECHNOLOGIES
Internet of Things (IoT), Artificial Intelligence (AI); Big Data, Cloud, Cyber-Physical Systems...

Figure 1. *Industrial revolutions.*

A. INDUSTRY 1.0

At the end of the 18th century, the first mechanical weaving was made in 1784. In this period, the 1st Industrial period, mechanical production facilities working with water and steam power were established. In steam machines, the pressure was obtained by heating water and creating steam. With the use of steam, most human-powered movements were eliminated. Great convenience was provided. Considering the vehicle manufacturing factories established in this period, we would need intensive labor and a labor force. The process of completing the production line took a long time. This industrial revolution has enabled the increase of capital accumulation in Europe and the United States of America and the increase in welfare in these societies [14].

B. INDUSTRY 2.0

At the beginning of the 20th century, the first production line of Cincinnati slaughterhouses was established in 1870. It has become possible to start mass production based on work sharing, taking into account electrical energy. In this period, the 2nd Industrial Revolution, considerable efficiency was achieved from the energy and time allocated to the workforce. Steel production increased, and thanks to this, fantastic acceleration and profit began to be gained from trade. Toyota made progress on this production line and left its competitors behind. The telegraph, the telephone, was invented. This revolution came to an end at the end of the 1973 oil crisis. In addition, the change in the energy sources and raw materials used and the advancement of technology day by day are the cornerstones of the Second Industrial Revolution [15].

C. INDUSTRY 3.0

In 1969, the third industrial revolution entered. In the production stages, analog systems have been replaced by digital systems. The first microprocessor is put on the market. The development of 3D printers has advanced and has begun to be used in automobile manufacturing. Growth and progress have been observed in production.

D. INDUSTRY 4.0

Although it is a new concept, Industry 4.0 applications are becoming increasingly widespread and are starting to show their effects, especially in production processes [16]. It is the industrial revolution that we have recently put into practice and continue to work on. This revolution, is aimed to work on autonomous machines and virtual platforms. Cyber-physical systems and the internet of things have been tried to be implemented. Communication and production are integrated between devices without human influence. Compared to other revolutions, a more efficient and advantageous production has been achieved. Industry 4.0 was the main topic of the World Economic Forum held in Davos. How a small smart factory would work has been implemented for the first time. In this industrial revolution, remarkable innovations in manufacturing and manufacturing use were developed. Developing and innovating the production line for the needs of the consumption group has made progress possible. However, the fourth industrial revolution is in its infancy, to communicate with each other all the actors involved in industrial production, access all data, and prepare the ground to create high-added value through this data. 3. Industrial Revolution determines which computer hardware, software, networks, and the rapid development of digital technology and integration, just as it transformed the agrarian revolution or after the industrial revolution, society, and the economy. Information technology and the widespread use of cyber-physical system automation have reached a new data processing stage and connected the dynamic value chain [17]. Regional, economic, technological, and commodity flows affect the course of the world and shape its future; Sensors and industrial chains beyond a single company have been created by linking the production means and information technology [18].

Figure 2. *Industry 4.0 [18].*

E. INDUSTRY 4.0 COMPONENTS

Industry 4.0 components are the internet of things, artificial intelligence, big data, 5G technology, renewable energy, autonomous robots, cybersecurity, manufacturing of objects, simulation, system integration, additive manufacturing, and augmented reality.

Table 1. *Industry 4.0 key components [19].*

Components	Explains
Smart factory, smart production, the future of production	Smarter, more flexible, and more dynamic factories. Machinery and equipment will be able to improve processes by making their own decisions.
Self-organization	In manufacturing, processes will become dynamic in all supply and production chains. A decentralized, self-regulating system will emerge.
New systems for the production of new products and services	Product and service development issues will generally be individualized.
Smart product	Products are embedded with sensors and chips that enable them to communicate with each other and with humans. While this makes products smart, it also introduces security and privacy risks.
New systems in distribution	Distribution and supply will become increasingly individual.
Cyber-physical systems	Production systems designed to follow human needs can be compatible with Siri, Cortana, and Google Now. A new interaction may occur between buyers and sellers.
Smart Cities	Smart cities are cities formed by using other sensor networks based on the combination of the internet, telecommunications network, broadcast network, wireless broadband networks, next-generation information technologies and networks, and accelerated development of the information-based economy.
Digital Sustainability	Sustainability and resource efficiency, smart cities, and smart factories are becoming increasingly central in design. Ethical rules must be followed in the use of private information. These factors form a basic framework for successful products across all systems.

With smart tools connecting to the internet and using networks, an environment suitable for threats is created. Malicious hackers who want to take advantage of this situation work against the system. All built-in systems, from road lines to traffic signs, from traffic lights to person and object detection methods, from accident warning systems to speed regulation systems, have an essential role in smart vehicles, which emerged as a result of researching the use of "Autopilot" application used in airplanes in land vehicles [20]. First of all, as much information as possible about the system to be attacked is collected [21].

F. SMART FACTORIES

The definition of smart factory has been defined differently by many academics and people working in this field [22], [23]. Park [24] defines the smart factory as a system that collects all information about production facilities in real-time over the internet, and as a network-based integrated production system that independently changes a production method, changes raw materials, and ultimately develops an optimized dynamic structure. Chen et al. [25] a smart factory is an intelligent production system that integrates communication processes, information processing processes, and control processes in production and services to meet the needs of manufacturing factories.

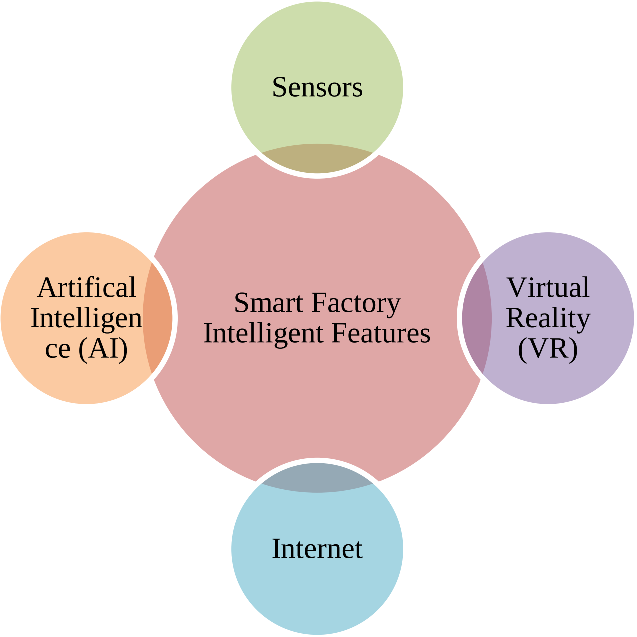
Sensors
Artifical Intelligence (AI)
Smart Factory Intelligent Features
Virtual Reality (VR)
Internet

Figure 3. *A smart factory intelligent features [26].*

G. AUTOMOTIVE INDUSTRY IN SMART FACTORIES

Automotive production in smart factories is possible only by integrating the smart production of automotive components. Especially for this situation, automatic technology, personnel, and innovation are required together with the developing technologies today. But this technology can be used for the Internet of Things, blockchain, cloud computing, and 5G. It will certainly redefine its solutions and improve design and communication possibilities.

III. CYBER-ATTACK METHODS AND MEASURES

A. CYBERATTACK METHODS IN THE AUTOMOTIVE INDUSTRY

In smart factories, there are cyber attacks and attack vectors that may occur depending on the technologies used in the automotive industry in general. Cyberattack methods are likely to experience the same methods in each component. These attacks occur in cyber attack components such as V2S, V2V, V2I, and V2N. The cyberattack methods that may occur in these components are shown in Table 2 [27].

Table 2. *Cyberattack methods in the automotive industry in smart factories [27], [28].*

Cyber Attack Components	Cyber Attack Methods
Vehicle-to-sensor cyberattacks (V2S)	1. Jamming attack 2. False data injection attack 3. GPS deception 4. Denial of Service attack (DoS)
Vehicle-to-vehicle cyberattacks (V2V)	1. Selfish attack 2. Modification cyber-attack 3. FDI attack 4. Eavesdropping 5. Blackhole cyber-attack 6. Gray hole attack 7. Wormhole attack 8. Denial of Service attack (DoS)
Vehicle-to-infrastructure cyber-attacks (V2I)	1. Attack replays 2. Referrer ad fraud 3. Privacy attacks 4. RSU spoofing 5. Duplicate address blocking (DAD)
Vehicular-to-network communications attacks (V2N)	1. At the roadside Wi-Fi access point (Wi-Fi AP) 2. DDoS 3. MiTM 4. Rogue attacks 5. Physical attacks 6. Eavesdropping 7. Jamming attack 8. Configuration attacks

B. CYBERATTACK INCIDENTS IN THE AUTOMOTIVE INDUSTRY

With the rapid development of smart factories and industry 4.0 concepts and the fact that everything is smart, cyber incidents occur due to cyber attacks that can be experienced. The cyber incidents experienced in the research and the root causes of these incidents are shown in Table 3 by year.

Table 3. *Cyber attack incidents in the automotive industry[29],[30].*

Year	Location	Cyber Incident	Cyber Incident Cause
2019	USA / Texas	An accident in a vehicle with autopilot on.	For the autopilot to be activated, there must be lanes on the road, and there is no lane line at the place where the accident occurred.

2018	Andes / Arizona	The car in automatic driver mode collides with a pedestrian.	He first perceived the pedestrian as an unknown object, then as a vehicle, and then as a bicycle. Although the system slowed down, the car hit the pedestrian.
2017	San Francisco	Car lane to the left. He started to change but suddenly went back to his first lane and collided with Nilsson.	The vehicle driving in autonomous mode stops changing lanes.
2016	California	The person inside the vehicle thinks that the bus will slow down, so it does not interfere with the vehicle's automatic driver system.	The test driver in his self-driving car takes control.

C. MEASURES AGAINST CYBER-ATTACKS IN THE AUTOMOTIVE INDUSTRY

Information and communication and the public that people nowadays become an indispensable part of daily life in various application services technology realizes the many organizations in both the private sector in cyberspace [31]. Evaluating cyber security vulnerabilities in big data has become much more critical today. Cybersecurity vulnerabilities in big data can be detected on Log IDS [32]. While technology provides convenience to people's lives, it also captures specific centers. Transactions made in the virtual environment make users' information easily accessible and processable. Hackers can use and sell the data they collect as they wish. As the cyber threat landscape changes, the measures must change as well. Developments in information and communication technology should be followed closely. In light of experience, a higher safety net should be created and constantly updated [33].

Table 4. *Measures against cyber-attacks in the automotive industry [34].*

Measures	Detailed Description
Keeping the firmware up to date	NVR, DVR, and IP software to keep up to date.
Using strong passwords	Password must be at least 8 characters. In addition, these characters consist of a combination of memorable characters, uppercase and lowercase letters, and numbers.
Changing passwords regularly	With regular password changes, your accessibility to your password will decrease.
Disabling UPNP	Your router or your modem will try to forward ports automatically. Typically, this is a method that facilitates the user's work. However, if you leave your system and automatically redirect ports by default credentials, you experience unwanted visitors.
Disable P2P	P2P is used to access a system remotely via a serial number. Your system's username, password, and serial number are also required, so it is unlikely that someone hacked into your system using P2P.
Disable SNMP	If you do not use SNMP as Disabled, you only need to do this temporarily for monitoring and testing if you are using SNMP.
Enable HTTPS / SSL	Make sure that you create an SSL HTTPS. This code takes advantage of all the communication from the communication service unit.
Change ONVIF Password	When you change the system's credentials, the software does not change the old IP Camera ONVIF password. The IP camera's firmware to the latest revision to update or ONVIF will need to change the password manually.
	Enabling your IP filter will prevent anyone other than the specified IP

	addresses from accessing the system.
Enable IP Filtering	A recording device is used to change between two video recordings of broadcast and multicast. Currently, there are no known issues involving posting a multi-point, but you should disable this feature if you do not use it.
Disabling Multicast	Be sure to change the HTTP and TCP ports.
Changing Default HTTP and TCP Ports	If you suspect someone is accessing your system without authorization, you can check the system logs. These logs will show from which IP addresses your system was accessed and from which it was accessed.
Check the log	POE ports on the back of the camera connected to the NVR should be isolated.
Connect IP Cameras to POE Ports on the Back of the NVR	You should avoid unauthorized physical access to your system.
Physically Locking the Device	If the cameras are connected to a recording device, you need not transmit ports for individual cameras; Simply forward the port you want to NVR.
Forward Only Ports You Need	In case of a violation of any of the accounts, have been collecting these passwords and security you do not want to try in video surveillance systems.
Use a Different Username and Password for IP Camera Security Management Software	If your system is configured for more than one user, checks must be made.
Limited Features of Guest Accounts	NVR and IP cameras on your network must have the same network as the overall computer network. This, of any visitor or an attacker, will prevent network access is necessary for the proper operation of the safety system.

D. USING LAYERED MODEL AGAINST CYBER-ATTACK

All systems should be examined and a safe layered model should be created against cyber security vulnerabilities that may occur during the production of automobiles in smart factories and among the end-users. In this model, all systems are divided into layers and important protection devices such as firewalls are used between each layer. The most important feature in layered structures is the data flow between the layers and the protection of the equipment to be controlled against attacks. This protection is also aimed at ensuring sustainability in terms of production in smart factories and protecting corporate reputation. Disclosure of data has undesirable consequences for all companies. In particular, it becomes possible to sell the information of customers and employees stolen by the attackers for money. It is possible to make layered structures according to the ISA-99 PERA (Purdue Enterprise Reference Architecture) model to protect all systems [35]. Therefore, when a system is attacked, it becomes possible to prevent the attacker from accessing other systems. Although these layered structures are high in cost in the first installation phase, it is possible to compensate for this in the following years[36], [37].

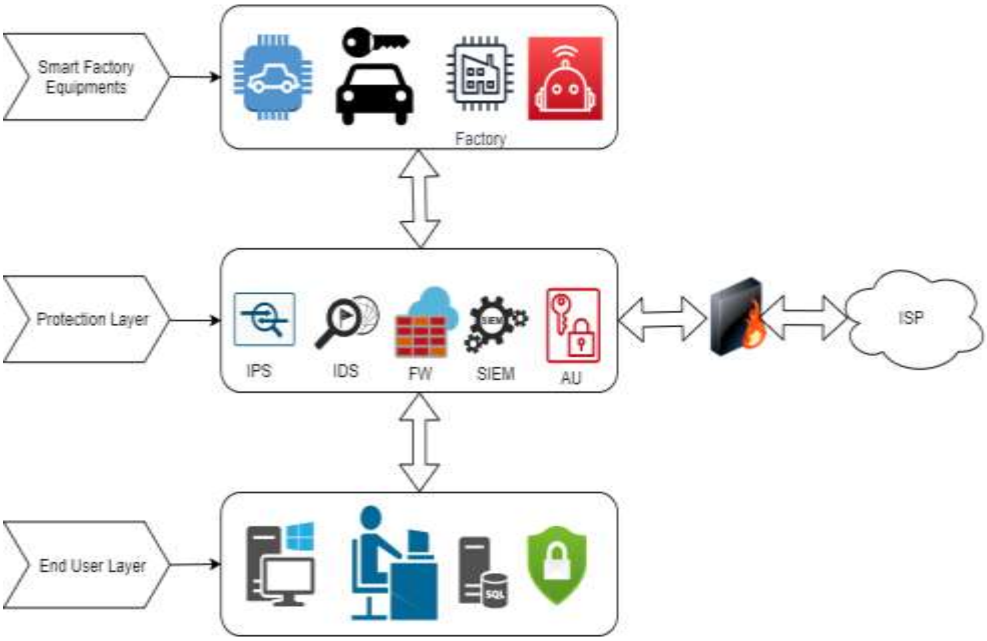

Figure 3. *Using layered model [35].*

The feature of using a layered structure is to protect other layers when there is weakness in one layer. In particular, software and hardware measures to be used between layers are expected to protect systems in terms of security. Each system installation may incur high costs in terms of initial installation, but these costs may decrease over the years. There is financial risk, security risk, strategic risk, compliance risk, and security risk in terms of applications made in smart factories. SCADA systems are used especially for the control of industrial equipment used in smart factories. When we exemplify the security weaknesses that may occur in these systems for automobile production, interruptions in automotive production, theft of information and projects, financial losses, and sabotage may become possible. For this reason, layered protection is important in terms of not interrupting production and sustainability. The most important feature of layered protection is that it is possible to prevent attackers from accessing other layers, depending on which layer the attack occurs.

IV. CONCLUSION AND DISCUSSION

Cyber security is of great importance in automobile production in smart factories. The production and increase in the automotive sector also increase the safe usage areas in this sector. In this study, Industry 4.0 and cyber security issues in automotive manufacturing are discussed and cyber attacks in the automotive sector and methods of protection from cyberattacks are mentioned. In Industry 4.0, the Fourth Industrial Revolution is assumed and businesses; move forward with their role of succeeding, creating value, creating strategy, competing, and changing the way it is implemented, which is still at the beginning of this subject. In this study, comprehensive and practical information is given to researchers who will work on this subject in the future. In this article, the automotive sector has been examined in terms of cyber security, and past cyber incidents in the automotive sector have been mentioned and should be adopted in some way. Increasing productivity in smart factory environments, that is, in the digital factory environment, is one of the greatest conveniences it provides. It is necessary to protect and filter from attacks. While providing network security with the help of the internet of things in smart factories, support should be sought when it is insufficient due to its complex structure. Production in smart factories should be protected against cyberattacks, especially with layered secure architectures. Layered models prevent an attacker from taking over entire systems. Therefore, smart factories need to be protected as a systemic whole. Industry 4.0 and cyber security were evaluated in terms of efficiency in automobile production facilities in smart factories. In future studies, efficiency analyzes can be put forward in production environments made according to industry 5.0 principles in smart factories. In addition, the reliability, sustainability of these systems, and the cost risks that may arise in case of a cyber attack can be calculated. This article describes cyber systems and attacks in smart factory manufacturing. It was also written to facilitate research in the literature. Societies developing with Industry 4.0 will use the gains of new technologies as an advantage over Industry 5.0. Therefore, this development will have both social and technological security in the future.

V. REFERENCES

[1] F. Özdemirci, M. Torunlar, ‘Bilgi-değişim-siber güvenlik-bağımsızlık,’ *Bilgi Yönetimi*, c.1, s.1, ss.78-83, 2018.

[2] E. Çağlar, Türkiye'de yerelleşme ve rekabet gücü: Kümelenmeye dayalı politikalar ve organize sanayi bölgeleri, *Bölgesel Kalkınma ve Yönetişim Sempozyumu Kitabı,* TEPAV Yayını, Ankara, 2006, ss. 305-316.

[3] N. Gabaçlı, M. Uzunöz, “IV. Sanayi Devrimi: Endüstri 4.0 ve Otomotiv Sektörü,” *International Congress on Politic, Economic and Social Studies*, Ankara, Türkiye, 2017.

[4] K. C. Koca, “Industry 4.0: Chances and threats from the point of Turkey,” *Sosyoekonomi Journal*, vol. 26, no. 36, pp. 245-252, 2018.

[5] M. Lazoi, A. Corallo, “Cybersecurity for Industry 4.0 in the current literature: A reference framework,” *Computers in Industry*, vol. 103, pp. 97-110, 2018.

[6] X. Krasniqi, E. Hajrizi, “Use of IoT technology to drive the automotive industry from connected to fully autonomous vehicles,” *IFAC-Papers Online*, vol. 49, no. 29, pp. 269-274, 2016.

[7] A. C. Pereira, F. Romero, “A review of the meanings and the implications of the Industry 4.0 concept,” *Procedia Manufacturing*, vol. 13, pp. 1206-1214, 2017.

[8] E. Kamber, G. İ. S. Bolatan, “Endüstri 4.0 Türkiye Farkındalığı,” *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, vol. 11, no. 30, ss. 836-847, 2019.

[9] İ. Akben, İ. İ. Avşar, “Endüstri 4.0 ve Karanlık Üretim: Genel Bir Bakış,” *Türk Sosyal Bilimler Araştırmaları Dergisi*, vol. 3, no. 1, ss. 26-37, 2018.

[10] L. Monostori, B. Kadar, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, and K. Ueda, ‘Cyber-physical systems in manufacturing,’ *Corp Annals*, vol. 65, no.2, pp. 621-641, 2016.

[11] V. V. Martynov, D. N. Shavaleeva, A. A. Zaytseva, "Information Technology as the Basis for Transformation into a Digital Society and Industry 5.0," *2019 International Conference "Quality Management, Transport, and Information Security, Information Technologies" (IT&QM&IS),* 2019, pp. 539-543.

[12] O. Doğan ve N. Baloğlu, ‘Üniversite Öğrencilerinin Endüstri 4.0 Kavramsal Farkındalık Düzeyleri,’ *TÜBAV Bilim Dergisi*, c.13, s. 1, ss. 126-142, 2020.

[13] K. Atashgar, O. A. Zargarabadi, “Monitoring multivariate profile data in plastic parts manufacturing industries: An intelligent data processing,” *Journal of Industrial Information Integration*, vol. 8, pp. 38-48, 2017.

[14] M. A. Arıcıoğlu, B. Yiğitol, A. Yılmaz, “Endüstri 4.0 Üzerine Yöntem ve Literatür Çalışması: Türkiye'deki Lisansüstü Tez Çalışmaları,” *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, vol. 57, ss. 293-324, 2018.

[15] J. Hertin, K. Jacob, U. Pesch, and C. Pacchi, “The production and use of knowledge in regulatory impact assessment – An empirical analysis,” *Forest Policy and Economics*, vol. 11, Issues 5–6, pp. 413-421, 2009.

[16] Imascon, International Marmara Sciences Congress IMASCON 2020, *P. Book*, December 2020.

[17] C. Daban, “Siber Güvenlik ve Uluslararası Güvenlik İlişkisi,” *Cyberpolitik Journal*, vol. 1, no. 1, pp. 78-94, 2016.

[18] A. Çarkacıoğlu, “Kripto-para bitcoin, Sermaye piyasası kurulu araştırma dairesi araştırma raporu,” Sermaye Piyasası Kurulu Araştırma Dairesi, Türkiye, 2016.

[19] V. Roblek, M. Maja, and K. Alojz, “A complex view of industry 4.0.,” *Sage Open*, vol. 6, no. 2, 2016.

[20] H. Gökozan, M. Taştan, “Akıllı taşıtlar ve kontrol sistemleri,” *Mesleki Bilimler Dergisi*, c.7, s. 2, ss. 58-62, 2018.

[21] C. Özarpa, M. A. Aydın, İ. Avcı, ‘International Security Standards for Critical Oil, Gas, and Electricity Infrastructures in Smart Cities: A Survey Study,’ *Lecture Notes in Networks and Systems*, vol. 183, pp. 1167-1179, 2021.

[22] S. Park, Development of innovative strategies for the Korean manufacturing industry by use of the Connected Smart Factory (CSF). *Procedia Computer Science*, 91, pp. 744–750, 2016. https://doi.org/10.1016/j.procs.2016.07.067

[23] N. Bicocchi, G. Cabri, F. Mandreoli, & M. Mecella, Dynamic digital factories for agile supply chains: An architectural approach, *Journal of Industrial Information Integration*, 15, pp. 111–121, 2019. https://doi.org/10.1016/j.jii.2019.02.001.

[24] H. Cai, L. Xu, B. Xu, C. Xie, S. Qin, & L. Jiang, IoT-based configurable information service platform for product lifecycle management, *IEEE Transactions on Industrial Informatics*, 10(2), pp. 1558–1567, 2014.

[25] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee & B. Yin, Smart factory of Industry 4.0: Key technologies, application case, and challenges, *IEEE Access*, 6, pp. 6505–6519, 2017.

[26] M. Afrin, J. Jin, A. Rahman, Y. C. Tian, & A. Kulkarni, Multi-objective resource allocation for edge cloud-based robotic workflow in smart factory, *Future Generation Computer Systems*, 97, pp. 119–130, 2019.

[27] D. K. Nilsson & U. E. Larson, Conducting forensic investigations of cyber attacks on automobile in-vehicle networks, *International Journal of Digital Crime and Forensics (IJDCF)*, 1(2), pp. 28-41, 2009.

[28] A. Seetharaman, N. Patwa, V. Jadhav, A. S. Saravanan & D. Sangeeth, Impact of Factors Influencing Cyber Threats on Autonomous Vehicles, *Applied Artificial Intelligence*, 35(2), pp. 105-132, 2021.

[29] S. K. Khan, N. Shiwakoti, P. Stasinopoulos & Y. Chen, Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions, *Accident Analysis & Prevention*, 148, 105837, 2020.

[30] R. Bolz & R. Kriesten, Automotive Vulnerability Disclosure: Stakeholders, Opportunities, Challenges, *Journal of Cybersecurity and Privacy*, 1(2), pp. 274-288, 2021.

[31] C. Özarpa, S. A. Kara, İ. Avcı, Siber Güvenlik Savunma Hiyerarşisinde Yeni Bir Eğitim Modeli, *4.Uluslararası Eğitim ve Değerler Sempozyumu ISOEVA-2020*, Karabük, Türkiye, 2020, ss. 939-947.

[32] M. Koca, M. A. Aydın, A. Sertbaş, A. H. Zaim, 'A New Distributed Anomaly Detection Approach for Log IDS Management Based on Deep Learning,' *Turkish Journal of Electrical Engineering & Computer Sciences,* vol. 29, no. 5, pp. 2486-2501, 2021.

[33] İ. Avcı, C. Özarpa, M. A. Aydın, "A Survey of International Security Standards for Smart Grids, Industrial Control System and Critical Infrastructure," *12th International Exergy, Energy and Environment Symposium (IEEES-12)*, Doha, Qatar, 2020, pp. 421-424.

[34] M. Piccarozzi, B. Aquilani, and C. Gatti, "Industry 4.0 in management studies: A systematic literature review," S*ustainability*, vol. 10, no. 10, pp. 3821, 2018.

[35] ISA. (2021, 25 Ağustos) [Çevrimiçi]. Erişim: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99.

[36] A. M. Shaaban, E. Kristen, & C. Schmittner, Application of IEC 62443 for IoT components. In International Conference on Computer Safety, Reliability, and Security, 2018, pp. 214-223, *Springer, Cham.*

[37] S. Suarez-Fernandez de Miranda, F. Aguayo-González, J. Salguero-Gómez, & M. J. Ávila-Gutiérrez, Life cycle engineering 4.0: A proposal to conceive manufacturing systems for industry 4.0 centred on the human factor (DfHFinI4. 0), *Applied Sciences*, 10(13), pp. 4442, 2020.