International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A General View of Industry 4.0 Revolution from Cybersecurity Perspective

Ahmet Efe*[1], Abdullah Isik[2]

Submitted: 01/12/2019 Accepted: 16/03/2020

Abstract: The broad network and high-level data sharing that comes with Industry 4.0 will rapidly increase the companies' cyber security demands due to its vulnerabilities and new emerging threats. Therefore, large corporations need a risk management system and security strategy tailored to its safety needs and is committed to improving operational security and protection so that their operations and earnings are not adversely affected. In order to protect products, data and intellectual property against unauthorized and unauthorized persons, companies must absolutely take cyber security measures and continuously improve existing security systems to comply with Industry 4.0 requirements. This paper aims to address which type of problems enterprises should handle against cyber-attacks and illustrate how governments take precaution and refer this issue at their policy documents in the era of industry 4.0. The digitalization of production has paved the way for an ever-increasing existence of concepts such as Big Data, Cloud Computing, 3-D Printing, Augmented Reality, and Internet of Things in production. With the emergence of these concepts, the need for cyber security is also becoming crucial. This paper underlines many issues from the literature survey and comprehensive risk analysis by comparing modern history of ICT (Information and Communication Technology) and future smart factories. Some problems are also addressed with different case studies for possible solutions.

Keywords: *industry 4.0, cybersecurity, e-government, IoT, Smart cities*

1. Introduction

Continuous innovations and new technologies have changed manufacturing processes from industry-driven to information-driven. Adoption of ICT technologies at manufacturing industry has pioneered an enormous change at developing, manufacturing and all the logistic process activities. Productivity bottlenecks are surpassed through the rapid diffusion of Internet. All these evolvements played a big role while blurring the boundaries between the real and virtual environments. Digitalization of manufacturing industry-oriented developments at process, methods and technologies are collected under the Industry 4.0 [1].

The digitalization of production processes has paved the way for an ever-increasing existence of concepts such as Big Data, Cloud Computing, 3-D Printing, Augmented Reality, and Internet of Things in production. With the emergence of these concepts, the need for cyber security arose, which is also main key concern will be addressed at this study. Policies to be formed and cooperation mechanisms to be established between enterprises, institutions and countries are very important in terms of the effective management of the process and creation of positive reflections on social welfare.

When we look at the definition of Industry 4.0, data sharing as automation is most effectively used in production and industry as an innovative technology. Technologies and systems have to interact in Industry 4.0 which is including machine learning, IOT, cloud computing, enhanced robotics, data analysis. The wide network and high-level data sharing that comes with Industry 4.0 will rapidly increase the companies' cyber security requirements. Industry 4.0 and cyber security need to be intertwined and dependent with each other. Therefore, large companies need a comprehensive risk management system and security strategy tailored to cyber assurance needs. Companies must ensure that their production and automation systems are much more effective in terms of operational safety and systems protection so that their earnings are not adversely affected.

With the widespread adoption of digitalization, IOT, industry 4.0, hackers of diverse motivations are setting much more intense cyber-attacks to get business opportunities, ransoms or other financial or political goals. To solve this problem, with the 4th Industrial Revolution, large companies are looking for solutions to reduce the risk of cyber threats. If no action is taken against the cyber-attacks, Industry 4.0 may have devastating consequences for companies operating in the field.

At the same time, it is also important to use open source solutions in this area in order to make industrial systems more secure from a cyber security standpoint. Especially when using SCADA systems, it is necessary to protect the critical data which can be generated during the operation of these systems integrated with IoT devices. At this point, standard determination studies for M2M (Machine to Machine) systems are being made. The coding and implementation of these standards need to be developed both as open source, especially as embedded software.

It is known that the tools of cyber security are carrying some concealed sort of counter-weaponry. The developers of these products collect information from the product. Some make it clear, and the majority makes it secret. The Huawei incident with USA and some western countries are based on this risk. Naturally, in the case of national interests, the devices used in the Industry 4.0 field will be likely to become "weapons" of hardware and software products imported from abroad. A separate R & D work on cyber security in response to this risk is a vital issue and it would be very helpful to expand incentives for national product development / use. Cyber-attacks can create a devastating impact on Industry 4.0 if measures are not taken. Intelligent production systems, data sharing, and viruses that can disrupt large data networks can have very bad effects on companies' production facilities and therefore national economies.

2. Research problem

There are huge risks for the internet of 4 billion people, 25 billion

[1] *Dr., CISA, CRISC, PMP, Ankara Development Agency, Turkey ORCID: 0000-0002-2691-7517*
[2] *Department of Computer Eng., Ankara Yildirim Beyazit University, Turkey; ORCID: 0000-0002-8344-025X*
** Corresponding Author: Email: icsiacag@gmail.com*

devices will talk to each other and industry 4.0 period. The next industrial revolution will change the way of trade in a destructive way. 7 days 24 hours for this period we are at the beginning. Now, cyber hackers have access to all the information of the factory when we have a single thing, and we have to read the next period, for example, there are 55 thousand energy transfer stations in the US. In the next 10-15 years we will gradually lose the environmental control, four walls will be eliminated; pirates can be prevented if investments continue in this area. Nearly 60 percent of the people or organizations are attacked by hackers working on new methods today, who cannot be determined.

There will be more need for cyber security analysts in the coming period, because the internet of objects is a difficult phenomenon to protect. Not only the institution, but also cyber spies for security gaps in the supply chain will work on new methods. Today, companies are making significant investments to become more secure. The security measures taken in the energy sectors are a standard today, but there are not enough guidelines and resources available for the future.

In 2015, two thirds of industrial companies in Germany were attacked by cyber-attacks. Data theft, industrial espionage and sabotage attempts have left companies in a difficult position. 16 percent of data theft of competing companies, 14 percent of the corporate secrets of the network that sells and sells, 6 percent of the secret services have done. The biggest danger is the company's employees. 65 percent of the data theft of the company's active or former staff was found to be responsible [9].

It is not always necessary to search for confidential information leakage. For example, the company's passwords in a forgotten mobile phone can easily get hands in or watching porn movies in the company's control center can make it easier to infiltrate the company's computer network. Malicious computer programs are most commonly spread through porn sites. Therefore, the greatest danger in terms of security is caused by man. Average hackers try to hack systems but expert hackers are hacking human first with spear fishing attacks. Companies should not overlook the human factor in security-related issues, but they should keep their staff, outsiders, marketing officers, subcontractors and repairers under control.

Specifically, at this point, there is a need to compensate for the lack of monitoring. It is evident that only a quarter of companies train their staff members and companies have stated that they suffered a great deal from data theft. Reducing the risk will be the most difficult task of the coming years. As well as the transfer of computer applications and data to cloud storage, switching to mobile applications for mobile phones or tablets can increase the danger.

As operating systems, computers and electronic platforms are very different; 'integrated solution' pathways are being sought in information technologies. If the security program is standardized on all tools, from mobile phones to computers and machines, it is stated that both the danger will decrease and the cost will decrease. However, in order to do this, companies that benefit from information technologies need to reach a certain size. Therefore, it is estimated that the competition in the internet security branch will be heated. Few of the companies preparing solutions for data security are expected to survive.

3. Development in Industries and Revolutionary Phases

Revolutions are processes that are directly related to human life. For this reason, revolutions appear to be radical changes in the lives of communities, institutions and institutions, which lead to radical changes or innovations, reshaping, or sudden changes in a certain field. Revolutions can emerge in every field from daily living social and cultural fields to industrial production areas and can deeply affect these environments. If you go from the definition of revolution, it is seen that the revolutions sometimes progress inwardly with a certain evolutionary process. For example, the transition from the first industrial revolution to the second industrial revolution was not sudden. If we look at the process of the development of industrial revolutions from the perspective of history, after these two revolutions have lived together for some time, then the first industrial revolution begins to disappear and the actors of the second industrial revolution take its place. However, when we look at the human revolution, for example, the French Revolution; took place in a much shorter period and led to sudden and radical changes.

The world is discussing a new industrial revolution, defined by the Germans' Industrial 4.0 statement at Hannover 2011 Fair, and is trying to take various precautions by estimating the consequences of this revolution. But the best way to understand the revolutions is to know the processes and history of the revolutions. Four major revolutions have taken place in the field of production in the history of the world, one in agriculture and the other three in industry. Let's first look at these revolutions briefly:

3.1. First Industrial Revolution or Industry 1.0

This industrialization process, which lasts from the beginning of the 1700s to the end of the 1800s, is the main source of iron raw material and carp is the main energy source. The most fundamental and distinctive feature of this period is the emergence of large factories, which are the result of widespread use of machinery [25]. As a result of the increase in the number of factories in Europe, the European society has moved from agriculture to labor to produce in factories. In this period, Britain has provided economic superiority over the other states thanks to its rich coal deposits. The Fig 1. Depicts certain phases of industrial revolutions.

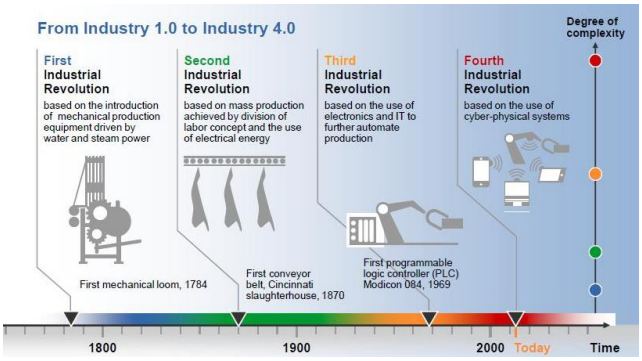

Figure 1. Depiction of Industrial Revolutions [28]

In 1712, Thomas Newcomen developed a new type of steam machine. The piston of this machine was operated by a chain with a lever and the lever by connecting to a water tumbler. At the top of the piston cylinder, the cold-water vapor sent into the cylinder was condensed so that the atmospheric pressure rises up to the water when the piston applies downward force. By repairing one of the Newcomen machines that had been damaged over time, James Watt developed this machine and turned it into a two-room and a valve. One of these rooms was designed to be always hot and the other cold. In 1781 Watt further improved the machine by adding new mechanical components. At this point, the steam engine became available to the industrial sector. The use of steam machines in weaving looms is regarded as the first industrial revolution, which is a process of integrating each other in such a way as to complement the various stages of the production process. This change which started in the textile industry spread rapidly to other industrial branches, especially to the chemical industry. In the first stage of the industrial revolution, the combination of steam, coal, and iron has opened the "railway age" with its significant political, economic, and social

consequences. Coal has not only provided power to vehicles moving in the railway, but railroads have also taken coal to places that are too far away and cannot be moved. Thus, factories with coal-working machines in Europe have grown up and spread to the farthest reaches. The widespread railway network has led to the widespread use of this revolution, and Industry 1.0,

3.2. Second Industrial Revolution or Industry 2.0

The second industrial revolution came about by the use of electricity in production systems and the control of electrical power on assembly lines. The industry has improved further by using steam, coal and iron as well as steel, electricity, petroleum and chemicals in the production process. The Second Industrial Revolution, which dates back to the beginning of the 20th century, triggered the use of oil-based and internal combustion engines. Other developments, such as telephone, radio, typewriter, cheap newspaper paper, have shaped communication and communication, while the development of steel production, railway transport and trade has accelerated in place of iron production, which dominated the first industrial revolution. The spread of the highway network played an important role in the spread of economic efficiency created by this revolution. Industry 2.0 is defined as serial production through mechanization of production and transportation of the produced goods to the consumption centers by road network as well as by railway [14].

3.3. Third Industrial Revolution or Industry 3.0

In the 1970s, microprocessor-based, programmable logic circuits were developed to transfer the information from sensors to business components within a program framework. Automation of the production system has been realized by using this developed system in production systems. This development reduced the human contribution in production and minimized the error. Thus, from the beginning of the 1970s to the present day a new industrial revolution began. In this period, the use of computers, the spread of smartphones and the internet has affected and shaped production in every way. Developments in communication and transportation, trade and industry are globalized. Industry 3.0 is defined as the reduction of human labor in production and the automation of production. We can say that each industrial revolution leads to a further reduction in the need for human labor according to the previous production system in production [13].

From the 1970s to the present, the Third Industrial Revolution was dominant. After the Second World War, automation of production was provided with the development of electronics, information and communication technologies. As a result of the development of programmable logic controller PLCs, automation in production has begun to move forward. The Mechanism of the First Industrial Revolution was defined as the serialization of the Second Industrial Revolution, while the Third Industrial Revolution was defined as the automation and digitization of the production. In this period, the development and production of science such as computers, microelectronics, fiber optics, lasers, telecommunication, nuclear, biotechnology and biogenetics affected the direction and form of development.

Developments in communication and transportation, trade and industry have globalized. One of the most important developments in this process was the rapid depletion of world resources and the coming of the concept of sustainability. The coal, water and steam power in the First Industrial Revolution as energy source; In the Second Industrial Revolution, oil and electricity were at the forefront. But in the Third Industrial Revolution, renewable energy sources such as the sun and the wind became more important with the irreproducible sources and environmental concerns. All these developments not only made innovations that were not possible before, but also the effects of factors such as cyber-physical systems, the internet of objects and services, the Fourth Industrial Revolution started. In the Second Industrial Revolution, oil and electricity were at the forefront. But in the Third Industrial Revolution, renewable energy sources such as the sun and the wind became more important with the irreproducible sources and environmental concerns. All these developments not only made innovations that were not possible before, but also the effects of factors such as cyber-physical systems, the internet of objects and services, the Fourth Industrial Revolution started.

3.4. Fourth Industry Revolution or Industry 4.0

Although we are not a witness of the first three industrial revolutions, we can say that we are now witnesses because we are at the beginning of the Fourth Industrial Revolution. This revolution began with the 21st century and continues to rise above the digital revolution. In fact, if we consider that all of the machines and systems in the Fourth Industrial Revolution are composed of digits (0 and 1) and use digital objects, we can say that this age is "The Age of Digital Objects" [25].

The mechanical processes were accelerated by the software in the Third Industrial Revolution, and the speed with which the production was made by making very large calculations increased while contribution of human element is dramatically decreased by 4.0 revolution that uses AI, IoT and full-scale robotics of self-driving and unmanned vehicles. Developments in software and hardware technologies and internet technologies opened the way for objects that communicate, learn and react with each other [14].

4. Digitalization of Industry

At 18th and 19th centuries some occurrences such as adoption of innovative technologies to production and mechanization of the industry emerged by steam powered machines enabled increase of capital accumulation. Periodical developments belong that time is called as Industry Revolution. First Industrial Revolution (happened at United Kingdom) is stand for a radical transition from agricultural economy to manufacturing. Second phase of this radical transformation had started with establish of factories which were using electrical energy and making mass production. In the late of 1960s ICT systems are optimized for industrial processes and that helped automation of production. As of these times we are in the fourth phase of this revolution* and with IoT and other technologies there is no bond between cyber-physical systems.

The new generation of mobile internet technologies, the faster and more varied features of the Internet and the development of intelligent manufacturing robots through the development of devices connected to this global network form the basis of the Fourth Industrial Revolution. There are robots, smart readers (sensors), unmanned vehicles, etc., and other machines that we can identify as elements of each element and communicate over the internet.

Factors that are at the forefront of the Fourth Industrial Revolution and will shape the future of the revolution are:

Mobile Devices: The use of mobile devices, primarily mobile phones and tablets, is among the indispensable parts of life. In future, these devices will be used more and more in daily life. Especially applications that will manage many devices and systems remotely from the mobile phone will be developed and life will be made even easier. From here it can be predicted that the concept of mobile phones and mobile computers will become identical and that almost anything can be done with mobile phones without classical computers.

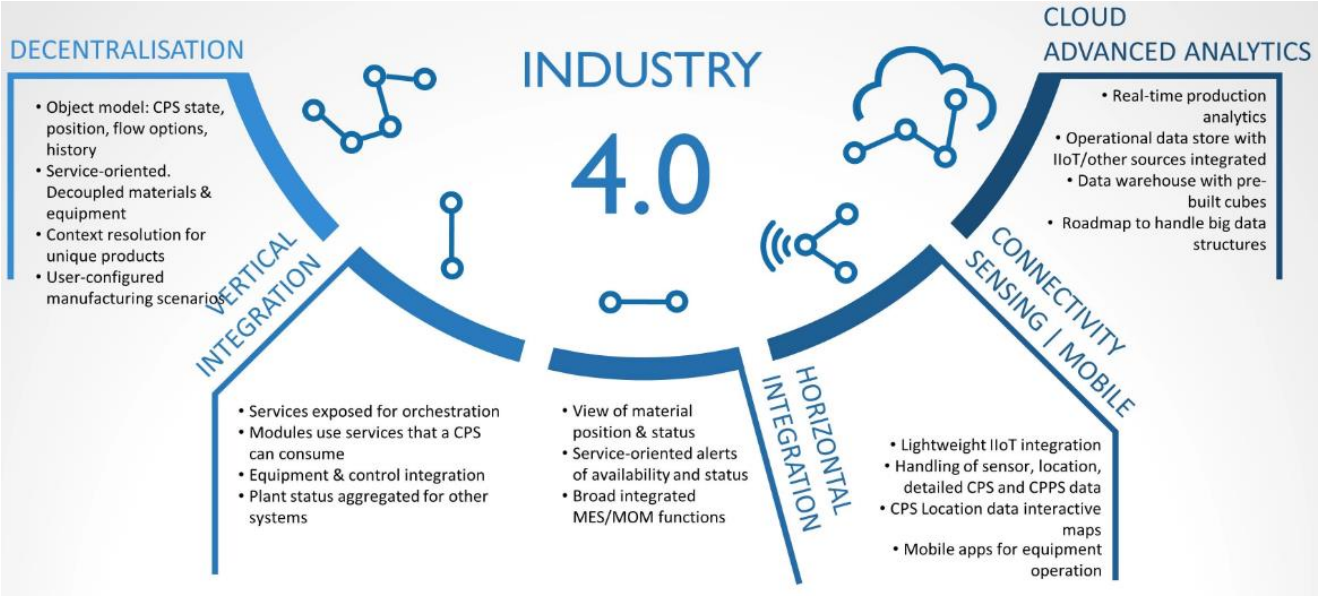

Figure 2. Industry 4.0 Template
(Source: https://www.myproductroadmap.com/products/industryfour006)

- **Networking and Internet Technologies:** It is very easy and fast to overcome the bottleneck of computer networks with IPv6 (6th Edition IP protocol), transferring faster and bigger data from one place to another. Moving video, audio and big data quickly and smoothly, especially over the internet and the network, will now become an acceptable event in the ordinary course of life. Almost every device in the world can be connected to the internet and be able to communicate via internet. If it is permissible, we will be a network society [9].

- **Cloud Computing Systems:** As the number of computing devices and systems used in human life increases, one of the biggest problems will be the problem of storing the data produced by these devices and systems. It will be necessary to solve this problem and to use cloud computing systems for storage of the data in a complete, robust, complete and reliable way. Especially when the data in the cloud is available at any time, and the fact that these data are never deleted or corrupted, it is of great value in terms of ease of use.

- **Data Mining on the Big Data :** Big data is the result of automated procedures that accumulated the size of data that cannot easily be handled without automated software and machine assistance. Accelerating the flow of life with each passing day will make it more compulsory to obtain more data and to make sure that the obtained data can be accessed safely anywhere. Especially the acquisition, processing and presentation of data in large structures such as e-government will require intensive effort. In this direction, the processing of the obtained data will further enhance the importance of the specifically requested data mining. Identification of the data in the desired properties and examination of these data will be one of the most important aspects of data mining. [15]

- **Artificial Intelligence and Industrial Robots:** The use of robots that will increase rapidly in other fields of industry and industry will open the way for robots to communicate with each other and will make direct contribution to production. In this direction, robots with artificial intelligence will communicate with each other using artificial intelligence and they will be involved in every stage of production. Considering the developing situations and needs, it is obvious that the robots will come to the forefront in every field of production thanks to various artificial intelligence practices in the future. Advanced decision-making algorithms running in the cloud transmit real-time analysis to factory production and IT systems. At this point, there is a risk of infiltrating this communication if firewall-like security checks are not applied for the exchange of information. When competing companies acquire supply chain data, they can see the company's information and pricing information. It can even copy the products with essential data by accessing the technical data of the designs.

- **Three-Dimensional Printers:** Contrary to classical printers, three-dimensional printers will allow any industrial product in life to be produced in a very short time. Even today, three-dimensional drawings of many purchased product parts are supplied with the product. With these drawings, spare parts can be produced and parts can be changed as desired. Three-dimensional printers will further increase the use of the human beings to further their dreams and surprise them. 3D printers are widely used in industry. Ford produced many parts in the process of development of Mustang 2017 in America using 3D printers. Because it is possible to produce production at a lower cost. The importance of these printers is increasing day by day for the production of prototypes and spare parts. In this sense, it can be said that printers carry the trade secrets of the companies digitally. If protection mechanisms such as data encryption techniques are not used in3-D printers, there is a risk of trade secrets being stolen.

- **RFID (Radio Frequency Identification technologies)** are used in the internal logistic processes where robots working together with automatic forklifts convey raw materials from trucks to production and there is a risk of disrupting the supply chain with DoS (denial of service) attacks against these frequencies.

- **The use of sensors** in industrial automation and control systems has reached a high level. Sensors automatically generate a maintenance work order on critical issues such as maintenance time of the equipment. Hackers can interfere with the SIEM and security systems to give false alarms to minimize the risk of hackers, and even can attempt to interfere with or stop the operation of robots to halt a smart factory completely.

The concept of Industry 4.0 includes technologies of many disciplines and makes extensive use of artificial intelligence, robotics, Internet-of-Things (IoT) technology, automation, sensors, simulation, data collection systems and networks. These systems make possible the establishment of efficient, collaborative and sustainable industrial production [2]. The third industrial

revolution has its origins in the late sixties, when computers, automation and distributed control pushed ahead mass production and control in Industry. Until then, ICS (Information Communication Security) consisted of the discrete disciplines due to the fact that micro-controllers did not yet exist [3].

Discrete disciplines of ICS systems can be classified with 3 systems: Process Control Systems (PCS), Discrete Control Systems (DCS), SCADA. PCS used mechanical pneumatic for logic, DCS used relays and SCADA (Supervisory Control and Data Acquisition) systems used transistors and radio.

The smart factories, which are emerged after the new industry revolution, include technological devices which are linked each other by internet. These linked devices monitor all the production chain and make operational decision by own.

4.1. ICS Networks

Industrial communication system(s) is one of the main components for automation of today's modern production system. Acquisition and analysis of production process data is ensured by ICS. To operate and maintain a facility continuously system must have ability of monitoring remotely and show any error instantly. Today's many ICS are available for manufacturers to ensure communication of processes. These ICSs are called as industrial network or area navigation route communication systems also. There are many ICSs are available: WorldFIP, DAA, Interbus, PROFIBUS, P-Net.

Sensor, engine, PLC, microprocessor type systems are controlled by DAA or other similar ICSs. Many automation systems, data acquiring systems, smart buildings, and robotic systems can be giving as an example where ICSs are used.

ICSs can be a problematic about security for manufacturing facilities. If malicious software affected a computer, then it can also have a backdoor for the system to access and control remotely. Malicious software using backdoors can't be found easily. For instance; attacker install the malicious software and can stop all the manufacturing and logistic processes. He/she can reach the production and capacity data and manipulate them. The worst-case scenario is he/she can create physical damage.

Industrial robots get the orders through embedded systems which are connected with PLCs mostly. These PLCs are connected to internet directly. Any attacker who hacked into system can destroy production line and all networks.

According to the IBM's recent research certain sectors charm attacks because of the data, information, files, etc. they have. These are [6]:

- ICT
- Finance services
- Trade
- Health
- Manufacturing industry

The attacks against ICSs are doubled in 2016. Most happened attacks -against these five sectors- are database and operating system related penetrations. 71 percent of these attacks happened in manufacturing sector and the main reason for that many systems within the sector are weak and not in accordance with standards. The second most popular attack mechanism in manufacturing was "Abuse Existing Functionality," which accounted for about 7 percent of all attacks detected. Many of these attacks involved flooding a target system with numerous requests, to create a state of denial of service. "Collect and Analyze Information" was in position number three at 6 percent [7].

In the beginning of the 1990s cyber security is not the first concern for power stations or facilities. However total amount of edges increases each day and that also increase threat possibility for ICSs. Nigam also collected the reason of attacks under four heading [8]:

1. Devices in many plants are not updating weekly or monthly and they run for weeks or months without any security updates or anti-virus tools.

2. Many controllers used in ICS networks were designed in their period when cyber security was not a concern. As a result it can be easily infect by malicious network traffic or high volumes of normal traffic.

3. There are many way to bypass existing cyber-security measures. For example; personal laptops carried in of facilities and USB sticks used among multiple computers, without being properly checked for malicious software.

4. There is still no physical or virtual isolation at all between unrelated networks.

4.2. Smart factories

Smart factories are the heart of the new industrial revolution, the Industry 4.0. Advanced software enables smart machines to communicate with each other and make decisions. Artificial intelligence applications, robots and 3D printers change the shape of production and the way people work. But industry 4.0 also brings with it a number of risks and forces companies to take measures in terms of privacy and security measures.

In general, we can specify risks in two main categories, namely privacy and cyber security risk. These risks can occur in all processes in the factories from the production stage to the shipment.

Cyber-physical systems are enabler of the productivity and development for not only manufacturing but also other sectors, such as; health or agriculture. Rate of these developments will rise with launch of products to the market. Even though we can't forecast what will be next, there is a common view about the factories will be smarter. Today's advance level automated factories include some components, tools, containers used on shipments, machines, etc. and within Industry 4.0, all these systems will be equipped sensors and communication systems. Hence, speed, productivity and quality will increase. Smart factories will be helpful for having idea about product at pre-production because of the virtual reality, simulation and other technologies.

Smart factories are one of the pivot points for Industry 4.0. Advance level software help factory machines to communicate with each other and make decision. Artificial intelligence, robots and 3D printer also will change how blue collars work. However, within the Industry 4.0 cyber security is also a factor that smart factories must deal with it (Figure 2).

Real-time decision-making programs which run at the cloud send real time analyses to factory's manufacturing system and main IT system. Through this communication process if there isn't any security check, it's possible an attacker can easily hack into the system. It's used RFID technology for robots which can work with automatic forklifts at in-door logistic activities. RFID is a technology use radio frequency and it's possible that supply chain can be interrupted by attackers with DoS attacks. Data also can be stolen from 3D printers which they can have important product model data.

Thanks to intelligent, autonomous technologies, Industry 4.0 seeks to make the digital world relate to physical movements in order to mobilize intelligent worlds and enable improved production. Today, industrial control systems that are permanently connected via TCP / IP and Ethernet are a common aspect, such as the use of standardized wireless systems. All these protocols should provide the maturity and reliability requested by the newly developed and analyzed Industry 4.0. Incorporating known communication capabilities into control systems provides many benefits, but making them more visible makes them vulnerable to specific risks.

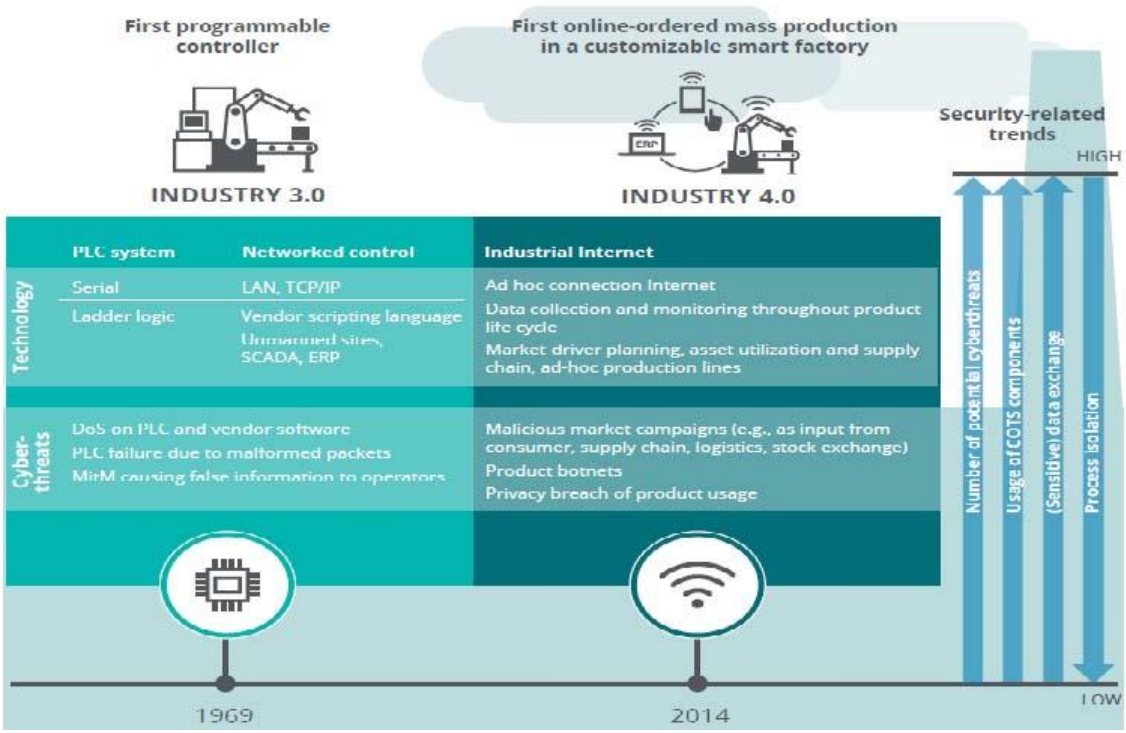

Figure 3.

For this reason, Industry 4.0 creates a wide range of attack possibilities, while at the same time placing systems in a much more threatening position.

As threat vectors expand radically with the advent of Industry 4.0, new risks must be considered and addressed. Simply put, the difficulty of implementing a safe, vigilant and resistant cyber risk strategy is different at the point of Industry 4.0. When supply chains, factories, customers and operations are interconnected, the risks posed by cyber threats are broadening even more potentially and even more.

However, it is important that we can balance our focus between the external threat environment and the real and often ignored cyber risks created by businesses that are increasingly tactical, innovative, transforming, modernizing or otherwise mimicking intelligent, connected technologies.

In the era of industrial internet (IIoT), there are some precautions you need to take into consideration to protect your factory from cyber-attacks:

- Systemic information is closed to the outside,
- To admit that the defense of physical security is from building blocks,
- To base the acquired system on a holistic approach,
- There is no defense of the disturbance, no external threats have to be taken into account at all times,
- Taking security precautions against insiders.

4.3. Standards Required for Industry 4.0

There are numerous IEC/ISO standards that may be related with the Industry 4.0 applications and structure. Here is the depiction of related standards. The most important ones of cyber security are demonstrated in yellow (Figure 4).

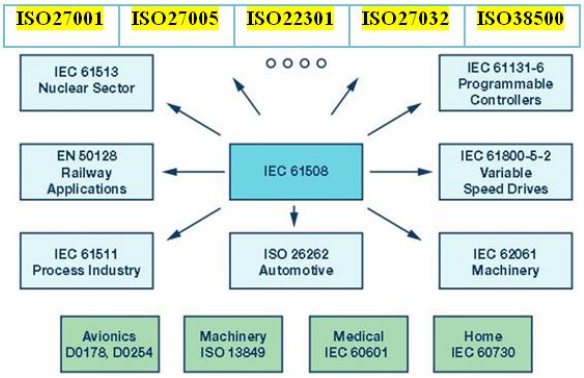

Figure 4. IEC 61508 and its related environment

Source: Modified from

https://www.analog.com/en/technical-articles/functional-safety-and-industry-4.0.html

As far as IEC 61508 is concerned, this life cycle applies to all electrical and programmable aspects of the safety-related equipment. Therefore, if a safety-related system contains an E/PE element then the Standard applies to all the elements of system, including mechanical and pneumatic equipment. There is no reason, however, why it should not also be used in respect of "other technologies" where they are used to provide risk reduction. For that reason, the Gas Industry document IGEM/SR/15 is entitled "Integrity of safety-related systems in the gas industry" in order to include all technologies. Below a diagram that depicts application of 61508 standard to Industry 4.0. It is seen that it does not specify cyber security for Industry 4.0 but rather it covers general security and safety. Therefore, recommend that the ones in the yellow are to be integrated for the Industry 4.0.

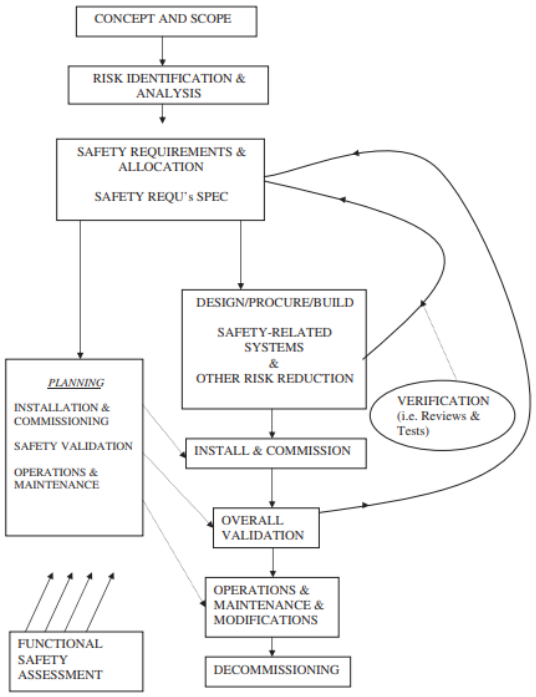

Figure 5. Security Life Cycle by 61508
(Source: ISO 61508)

5. Case Scenarios

While it's been guessed that there will be 20 billion things linked each other in 2020, it's inevitable that increasing number of IoT products and within the production period security will be key elements. Because; at previous years some systems designed without giving particular importance to security, were not successful against cyber-attacks: [9] [10] [11].

- One of the early attacks against ICSs was the Slammer worm, which happened in 2003. This malicious effected two monitoring system of nuclear facility at USA. Same year another malicious caused damage to railway transportation at USA stopped all transportation.

- In 2009, the French Navy was victim of the Conficker worm. Conficker used Windows vulnerability and the malicious infected vulnerable machines, self-update and download and install other malwares. Physical impact: Failure to download flight plans leading to grounded aircraft.

- In 2009, the Night Dragon virus hit oil, gas, and petrochemical companies such as Exxon, Shell, BP. The virus allowed the infected computers to be controlled remotely by attackers.

- In 2010, a computer worm Stuxnet was found at Iran's Natanz nuclear facility. It was spying on and reprogramming industrial systems. This virus intercepted and made changes to data to a PLC. Physical impact: Destroyed a fifth of nuclear centrifuges.

- In 2014, Havex was infected as trojanised SCADA software downloads from compromised vendor websites. It scanned the local network for servers that collect data from industrial equipment and sent collected data to a command and control server.

6. How governments and universities act on Cybersecurity at Industry?

As can be seen in the case of Germany, one of the biggest tasks in the Industry 4.0 process is to the governments. It is of great importance that such large transformations are carried out with the support of the state. Governments are accelerating the development of Industry 4.0 strategies and processes thanks to their investments and collaborations with universities, industry representatives, non-governmental organizations and think tanks.

The integration of the identified strategies at various points of the public, especially vocational and technical education is one of the responsibilities of the states. In particular, identifying strategies that support intensive R & D efforts and infrastructure support are also highlighted as a responsibility that governments should undertake in the Industry 4.0 transformation.

No transformation with a social, economic or administrative influence is realized by the encouragement of a single group or institution. For the transformation of the Industry 4.0, universities and research organizations have great responsibilities in the presence of formal strategies.

In line with the new employment opportunities that Industry 4.0 will bring, universities need to update their training programs. Adoption of multi-disciplinary approaches, especially in the field of science; It is important to create new educational programs in the field of mechatronics, which combine electrical, electronics, mechanical engineering and computer science.

At the same time, both universities and research institutions are expected to take a more active role in all areas, especially R & D, by following world-wide standards. In other words, it is not possible for Industry 4.0 to succeed as a merely academic or just commercial enterprise, so the triangle of academia-business-politics must be drawn.

In the Fourth Industrial Revolution, we cannot talk about security, which will be devices, systems and robots that communicate and communicate with each other in all areas of our lives. So, can this technological product and system work with hundred percent securities? I wish the answer was "yes". First, imagine a factory; Raw materials coming to the factory come with unmanned vehicles, are automatically lowered with robots, and raw materials are being processed in robotic looms. The size, color, and all other features of the product to be produced are programmed and the product becomes ready for sale. In this process, there will be minimum human power and maximum robot and computer power. These computers and robots will talk to each other with artificial intelligence and will produce within the framework of codes and codes determined at every moment of production. Well, to change these rules and codes, if it tries to disrupt and disable it? As a result, everything is connected to a network, wired or wireless, and it is an identity on the network. There is a malicious person leaking into this network that can turn the factory into a battlefield and cause irreparable damage.

Although implemented as a pilot yet, smart homes will be indispensable in the near future. We are talking about a digital house that produces its own electricity and water, refines and recycles waste to sewerage, and all devices and systems in the house can be managed over the internet. In the past, the modems used to connect to the internet are secure in cyberspace by putting the middle of the house in terms of security of information! It will not be possible to deploy such a safety criterion in such a house.

Technological devices and systems that facilitate human life can become the nightmare of humanity if adequate security measures are not taken. If you think, your house is hacked, the refrigerator's lids are opening and closing, the oven is working on its own, the washing machine is pumping out the wastewater, your TV is locked and the sound is blown up to the end and the shower taps are pouring out. In the Fourth Industrial Revolution, I think this is the simplest scenario for horror films.

We must be a country that thinks and plans cyber security to the finest detail, which produces technology instead of consuming and using technology, uses its own national system and codes while

producing. In particular, the incentives given to these field producers should be given for very high technological products from low and medium technological products and should be encouraged to produce high technological products. In these direction universities, technical high-tech industrialists should be developed a business association and necessary and sufficient incentives should be provided by the commissions to be created by any state that wants to produce technological products. A country can only declare its independence as long as it produces domestic, national technological products and provides them with domestic and national solutions for the safety of cyberspace.

For cyber security, we must first produce products that meet local and national needs, and while we produce these products, we must plan all the steps to ensure the safety of the cybercrime. In order to be a fully independent country in your future digital world, we must train our children already and take the necessary precautions to ensure that they receive adequate and good education in this area.

So those who want to be protected against attack must always be a few steps ahead of pirates. Here, large organizations like Siemens are developing comprehensive techniques to minimize their threat risks to their own companies and customers. These technologies are up to date and they always adapt to new visions in a stable way.

Safety precautions should not be confined to studying only the incoming threat, and strategies should be developed and taken against future threats. This is a very comprehensive view of security and is a permanent system that will be integrated into the whole life cycle of institutions' activities. So safety activities will be considered during development and engineering as well as during service and operation activities. By combining physical security, network security and system-software integrity to these users, it will provide comprehensive and permanent safety mechanisms.

Furthermore, the advanced interaction between the units identified in Siemens' safety portfolio is an important factor that will enable the problem to be solved. Safety solutions should work as a network operation between automation systems and the production centers. Fully integrated automation provides the efficiency of the simulated interaction and the fundamental safety, comprehensive protection of the production centers against the cyber eyes. In order to reduce risks and maintain production continuity with industrial safety services, frequent protection is provided and an advanced safety mentality is established with full safety from tiptoe.

As a result, there will be a great need to ensure critical pipeline systems and production lines that are critical to the growing cyber eyes, coupled with the connectivity and interaction protocols that come with Industry 4.0. Industry 4.0 and Cyber Safety are important for manufacturers. The reason for the importance of the cyber security issue is that it will be subject to destructive consequences if measures are not taken against data thieves, hackers and anticipated casinos. Therefore, they are trying to minimize and eliminate the security tactics and techniques developed by the big companies and the threats that may arise from the outside.

Many countries embraced cybersecurity at manufacturing sector as a government policy. For example; European Union (EU) aimed to provide confidence and security for online processes. About this matter, EU published a reference policy document, Cyber Security Strategy, in 2013.

According to digitalization research conducted by Minister of Science, Industry and Technology of Turkey, manufacturing enterprises have a concern about mostly data security and cyber risks. On the other hand Turkey also has published National Cyber Security policy documents and gave wide coverage to cyber risks which are possible can be regarded with Turkish manufacturing industry. It's mentioned at the document that increased rapid of digitalization of (Turkey) industry also affects the increase of cyber risks. These following actions will be taken by the ministry for risk management:

- Starting identification processes for manufacturing enterprises to determine their current condition about cyber security and risks,
- Raising awareness and competence among manufacturer SMEs for cyber security,
- Analyzing risks, risk rates and effects among factories and supply chains and take preventive precautions,
- Monitoring digitalized processes, testing all system periodically,
- Stimulating enterprises to recruit cyber security experts,
- Grant enterprises which provide service and product about cyber security area.

7. Recommendations

The sectors are changing and the concept of connectivity is central to this change. Expenditure on the Internet of Industrial Objects is expected to reach $ 500 billion globally by 2020. Cyber security will have a big role in this world, which is more connected with each other. Ensuring the correct implementation of security will be an important challenge for the industry. Epson's recent research into the effects of technology on key business areas[1]. In fact, 67 percent of Europe's manufacturing sector labor force believes cyber security is the biggest threat in the industry. This figure rises to 76 percent in management roles. To deal with the threat of cyber-attack will require businesses to adapt.

Changing perceptions

There is a common perception that many people fear that the future industrial transformation will lead to a spread of technology and a reduction in jobs. This view was not significantly supported by our research, which revealed that only 47 percent of European workers believe that they will disrupt the future roles of technology. Furthermore, there is no doubt that some of this deterioration will be due to the negative effects of cybercrime rather than the automated processes. In a US study by Deloitte, it was found that cybercrime affected more than 40% of manufacturing companies and 38% of them suffered losses exceeding $ 1 million. Industry should find a way to prevent threats such as plain text messages transmitted by encryption or networks to infiltrate vital systems and cause operational interruptions. It should be vigilant to reduce opportunities for disabling firewalls or stealing sensitive data. In an increasingly automated future, securing a robotic infrastructure against such tampering attempts will also become important. Education will also play a vital role in this.

Training of employees

The labor force in the manufacturing sector, which accounts for 15 percent of European GDP and has over 52 million direct or indirect jobs, has a refreshingly positive view of employment in the midst of such a period of uncertainty. 62 percent of the respondents believe that manufacturing works will develop with technology and technology will not replace manufacturing. Moreover, experts think that with the 74% of the top executives in Europe, rapid global change in manufacturing will increase local economies and employment prospects by technology. To inform workers about best practice, it is critical to help them understand security gaps

[1] Within the scope of the research carried out by FTI Consulting, the opinions of 17 industry experts were discussed and more than 7000 business leaders and employees working in various industrial sectors of Europe were asked.

and to inform them about the role that falls in reducing cybercrime. A known example comes from the US retail company Target. In this case, we see a huge amount of data being stolen from fraud by access to a simple email through a third-party vendor [16]. These are security issues that require employees to be trained to protect themselves.

Feeling the positive effect

Even if it is evident that the future manufacturing sector will have a devastating impact on jobs, perhaps the most important thing to focus our attention on is the cybercrime. By 2020, only the number of machines to machine will reach 12 billion [17]. This includes everything from digitalized energy distribution systems to robotic logistics technology. Securing these links will be a natural part of building a successful and interconnected future. A study by the European Network and Information Security Agency found that cybercrime could lead to a cost of 1.6 per cent of GDP for some countries [18]. In the light of all this information, it is quite a wise attitude that 67% of the workforce and 76% of the management are aware of the vital role cyber security will play in the future of manufacturing [19].

8. Conclusion

The revolution of Industry 4.0 is inevitable. Regardless of whether they open problems in terms of employment, or bring them growth in terms of development, these competencies must be won. Automation and automatization will be seen at the line stage in the producing sectors and in the sectors carrying / distributing these products.

Production sectors will produce products on the one hand, while automation, integration and automatization layers will be formed on top of the factory. These services will be as valuable as the product itself. The product, product information, production timer's information and other digital layers will become commercial value on their own.

Industry 4.0 is the inevitable continuation of a natural development curve. Our people should not work in heavy jobs, dangerous jobs, and toxic work. This is true in terms of the development of humanity. In the mines, hot and toxic gases in the factory environment, heavy-duty warehouses, instead of human robots, machines are much more convenient to work. Do routine work every day, like retirement? No, you must also pass the algorithms instead. It will be much more valuable and efficient for these people to be involved in social affairs, in civilization, in culture and art.

Cybersecurity may not be first issue for enterprises in times gone; however, increased attacks with the new communication protocols, defending industrial systems will be one of the major issues. To ensure digital transformation at manufacturing industry safe and secure and make sustainable, cyber security infrastructure is a crucial for future factories. There will be a great need to protect critical industrial systems and production lines against potentially bulky pepper threats, along with the connectivity and communication protocols that come with Industry 4.0. The importance of cyber security is that it will be subject to devastating consequences if measures are not taken against data thieves, hackers and industrial casinos. Therefore, large organizations are trying to minimize or even eliminate threats and security strategies and techniques they have developed.

Concepts such as the digital evolution of the industry or the 4th Industrial Revolution urge us to think about the future and focus on "tomorrow". That being the case; we acknowledge that the failure to take the necessary steps in the right time towards the right direction shall cause great losses in the future.

As a result, it will be a great requirement to ensure the safety of critical second-generation systems and production lines against cyber-threats that will significantly increase with the connection and interaction protocols that come with Industry 4.0. Industry 4.0 and Cyber Security are very important for manufacturers. The reason for cyber security is that it is possible to face destructive consequences if data is not taken against data thieves, hackers and spies. For this reason, it tries to minimize and eliminate the threats that may arise from outside with the security tactics and techniques developed by the big companies.

References

[1] M. L. GYORFFI, «Digitising Industry (Industry 4.0) and Cybersecurity,» European Parliament, 2017.

[2] T. P. ve I. B., «Process Improvement Trends for Manufacturing Systems in Industry 4.0.,» Academic Journal of Manufacturing Engineering, 2016.

[3] N. Benias ve A. P. Markopoulos, «A review on the readiness level and cybersecurity challenges in Industry 4.0,» 2017.

[4] E. IRMAK ve İ. ERKEK, «Endüstriyel Kontrol Sistemleri ve SCADA Uygulamalarının Siber Güvenliği: Modbus TCP Protokolü Örneği,» Gazi Üniversitesi Fen Bilimleri Dergisi PART C: TASARIM VE TEKNOLOJİ, 2018.

[5] T. P. ve I. B., «Process Improvement Trends for Manufacturing Systems in Industry 4.0.,» Academic Journal of Manufacturing Engineering, 2016.

[6] IBM, «IBM X-Force Threat Intelligence Index,» 2017.

[7] N. Benias ve A. P. Markopoulos, «A review on the readiness level and cybersecurity challenges in Industry 4.0,» 2017.

[8] R. Nigam, «SCADA Attacks Over The Years,» [Blog] https://blog.fortinet.com/2015/02/12/known-scada-attacks-over-the-years , 2015.

[9] Deloitte, «Industry 4.0 and Cybersecurity, Managing risk in an age of connected production,» 2017.

[10] C. W. Ahmad-Reza Sadeghi ve M. Waidner, «Security and Privacy Challenges in Industrial Internet of Things,» IEEE, 2015.

[11] D. Aksoy, «Endüstriyel Sistemlere Yapılan Sanal Saldırıların İçyüzü,» http://www.globaltechmagazine.com/endustriyel-sistemlere-yapilan-sanal-saldirilarin-icyuzu/, 2015.

[12] E. Byres, «SCADA Security Basics: SCADA vs. ICS Terminology.,» https://www.tofinosecurity.com/blog/scada-security-basics-scada-vs-ics-terminology, 2012.

[13] Symantec, «Smarter Security for Manufacturing in the INDUSTRY 4.0 Era,» https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf, 2016 .

[14] GTAI, https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Brochures/Industries/industrie4.0-,» 2014.

[15] SCHWAB, Klaus, Dördüncü Sanayi Devrmi, Otpmist, 2016, s.15-17

[16] ÖZDOĞAN, Ogan, Endüstri 4.0 Dördüncü Sanayi Devrimi ve Endüstriyel Dönüşümün Anahtarları, Pusula Yayıncılık, 2017, s.27-29

[17] GREENGARD, Samuel, Nesnelerin İnterneti, Optimist, 2017, s.65-71

[18] Charlie Osborne, (2014) "How hackers stole millions of credit card records from Target" https://www.zdnet.com/article/how-hackers-stole-millions-of-credit-card-records-from-target/

[19] Thomas Barnett, (2016), "Updated Cisco VNI Complete Forecast Released Today" https://blogs.cisco.com/sp/updated-cisco-vni-complete-forecast-released-today-so-what

[20] ENISA, (2016), "Determining the real economic impact of cyber-incidents: A mission (almost) impossible" https://www.enisa.europa.eu/news/enisa-news/determining-the-real-economic-impact-of-cyber-incidents-a-mission-almost-

impossible
[21] EPSON, (2017) “Industry should focus on cyber security, not job insecurity”, https://epson.presspage.com/endustri-i-guvensizliine-deil-siber-guvenlie-odaklanmaldr/
[22] F. Turkey, Şubat 2017. Available: http://www.fortuneturkey.com/akilli-uretim-cagi-endustri-40-42841.
[23] World Economic Forum, «The Future of Jobs,» Switzerland, 2016.
[24] Vdare, 2016. Available: http://www.vdare.com/posts/davos-meeting-focuses-on-fourth-industrial-revolution-aka-automation.
[23] «Computer World,» 6 Ekim 2014. Available: https://www.computerworld.com/article/2691607/one-in-three-jobs-will-be-takenby-software-or-robots-by-2025.html.
[25] World Economic Forum, Ocak 2017. Available: https://www.weforum.org/agenda/2017/01/jobless-world-and-its-discontents.
[26] E. Bulut ve T. Akçacı, «Endüstri 4.0 ve İnovasyon Göstergeleri Kapsamında Türkiye Analizi,» 2017.
[27] World Economic Forum, «Towards a Reskilling Revolution,» Switzerland, 2018.
[28] Üç Ülke Evrensel Gelirde Öncü Olacak, 2017. Available: http://uzmanpara.milliyet.com.tr/haber-detay/gundem2/uc-ulke-evrensel-gelirde-oncu
[29] P. Chourasya, “What is Industry 4.0, Working Principles, Its Impact on Industries in India & rest of World” *Finance Adda*, 2019 https://www.financeadda.in/2019/01/what-is-industry-40-working-principles.html