Internet of Things in the Enterprise as a Production Process Control System

Michal Trziszka(✉)

Faculty of Engineering and Management, Poznan University of Technology, Strzelecka 11, 60-846 Poznan, Poland
michal.trziszka@put.poznan.pl

Abstract. Internet of Things (IoT), which is based on objects and devices equipped with sensors, differs from the traditional concept of the Internet based on data servers connected to users' access terminals. In the IoT concept, first of all, the transfer of data between objects is important, and interaction with humans is based on immediate needs and demands. Forecasts indicate that in 2020, over 70% of enterprises will invest in technical infrastructure and build an Internet of Things platform for their organizations. This year, 50 billion devices will be connected to the network around the world. The use of modern technologies contributes to the improvement of processes in the enterprise, and the equipment of production equipment with sensors allows better control of their operation. The Internet of Things, along with artificial intelligence and 5G technology, is transforming the economy and seems to be an inevitable process that is associated with a large increase in automation. It will significantly increase the system's vulnerability to cyber-attacks until security measures are included in new hardware and software, and security personnel will be increased accordingly to monitor new services and methods. Automated security monitoring will be crucial. However, an enterprise using this technology should secure access to the global Internet network in several ways to become independent of the possibility of failure outside its area of operation. The Internet of Things generates a lot of data, so it is crucial to ensure that they are securely transmitted and stored. The use of big data analytics to optimize the production process will not fulfill its function when the same sensor connections to the cloud are used by cybercriminals to paralyze production or the functioning of the enterprise. Systems previously inaccessible via the Internet suddenly become visible throughout the entire world network. Whether we manage to secure the Internet of Things against attacks will depend on whether it turns out to be the optimal solution. Technical security and cyber security are closely related. As a result of the research, the article presents not only the most common mistakes in data security policies made by enterprises, but also presents selected options for increasing the protection of corporate data.

Keywords: Systems engineering · Cloud computing management · Internet of Things · IoT · Industry 4.0 · Industrial Internet of Things · IIoT

B. Mrugalska et al. (Eds.): AHFE 2020, AISC 1216, pp. 56–62, 2020.
https://doi.org/10.1007/978-3-030-51981-0_7

1 Introduction

The growing importance of the Internet of Things is inextricably linked to the development of information and communication technologies [1]. The article proposes the use of this technology to collect information on the state of the manufacturing process in order to optimize decisions controlling this process. Acquisition of data on the state of machines and tools as well as technological process parameters and results, both qualitative and quantitative, will allow control of production and control of the entire production process [2]. The concept of resource management of tools and instrumentation using the Internet of Things gives both high functionality and reduced diagnostic costs. An increase in automation can, however, increase the vulnerability of the system to attacks. Therefore, safety monitoring is necessary in the production process [2]. In the concept of the Internet of Things, first of all, the transfer of data between objects is important, and control is exercised from the level of the mobile application.

2 The Internet of Things Is Growing in Importance

The Internet of Things provides tools for improving and controlling production processes, but also for reducing costs and monitoring. The connection of the device network ensures direct integration of the physical world with computer systems, which translates into increased accuracy and performance. Thanks to IoT, the barrier related to the lack of communication range and the speed of information transfer disappears [3].

The Internet of Things systems consist of such elements as:

- data collection - edge devices are key elements of the IoT system. These are primarily sensors that collect environmental information and end devices;
- wireless communication - depending on the application, among others from WPAN, WLAN, WMAN and WWAN;
- network gateways - provide communication between edge devices. They also perform various other functions, e.g. protocol translation, data processing and device security;
- cloud computing - is a combination of a data warehouse and a system that allows calculations, data processing and reporting. It also enables - what is important in remote work - flexible access to data via the Internet [4].

Thanks to these solutions, numerous installations can be located in remote places of the earth globe, therefore there is no permanent and reliable Internet connection. The possibilities may be limited to data collection in recording equipment and then transferred on storage media. However, thanks to appropriate technologies, long-distance communication can be maintained without using the Internet or IP addresses. One such example is Thingstream [5] - a long-range network built on the basis of USSD (Unstructured Supplementary Service Data) and LoRaWAN (Low Power Area Network) messages allowing IoT devices to communicate over distances up to several dozen kilometers with gates that connect to standard IP networks.

It is forecast that by the end of 2020, over 70% of enterprises will invest in technical infrastructure and build the Internet of Things platform for their organizations [Przemysl-40.pl]. This year, 50 billion devices will be connected to the network around the world.

3 Change in Production Management and the Industrial Internet of Things

The implementation of systems that can exchange data with each other and operate in a partially or completely autonomous way enables the architecture of the production management system to be changed. Over the years, the layered structure of production systems has dominated the manufacturing industry. As a result of introducing technological innovations, there is a change in the architecture of the production management system and a transition from linear production processes to the network of device connections and non-linear processes [6]. To achieve them, it is necessary to ensure a high level of autonomy of system components and the possibility of distributed decision making based on the current state of production.

Faced with fierce competition and production optimization, production plants are striving to increase efficiency and minimize downtime. Production managers today can use the Industrial Internet of Things (IIoT) - or interchangeably referred to as Industry 4.0 [7] - and data generated by networked devices, increasing the "intelligence" of production lines. It assumes the integration of people and machines controlled digitally with the Internet and information technologies [8]. First of all, Industry 4.0 is identified primarily with the digitization of production systems, using more and more applications:

- data management - Big Data - data acquisition and analysis,
- automation - a combination of traditional manufacturing methods with artificial intelligence,
- communication using broadband links to tie the value chain,
- digital communication with clients - greater share of the final recipient in shaping the product or service [8].

As follows from the above, the concept of Industry 4.0 means the unification of the real world of production machines with the virtual world of information technology and the Internet. Materials produced or used for production can not only be identified, but also have the ability to communicate with each other. People, machines and IT systems automatically exchange information within various IT systems operating within an enterprise. Thanks to the system, employees have access to any useful information, at any time, from anywhere, which in turn not only affects the optimization of work, but also allows you to quickly respond to customer expectations by modifying the product.

In the next stage of technological development, value networks will be created in which IT systems and production lines of machine manufacturers and their suppliers will automatically exchange data with each other. This will result in the production being moved to a higher level of the production model.

An important feature of effective digitization strategies is the avoidance of "silos" [9], i.e. situations where individual departments or business units implement digital transformation without cooperating with others and in isolation from the broader perspective of the entire organization. Meanwhile, the implementation of the Industry 4.0 concept requires a coherent approach, agreeing digital standards and implementation methods at the level of the entire enterprise or capital group.

Thanks to the use of artificial intelligence in the production process, without the participation of planners and direct supervisors, optimal decisions are made regarding the order of implementation and selection of resources for individual technological activities of production. For this reason, production and maintenance managers have the greatest benefits from using IIoT. Through mobile solutions, they themselves can choose the type of data available for remote production control, and the system independently manages the work of employees and machines, taking into account in real time all changes regarding the state of these resources and the current situation of the production process. In case of any deviations from the standard assumptions, the system immediately introduces corrections and performs additional optimizations [10]. Each employee, after reporting to the system, is immediately ordered to perform the optimal technological operation at the time of its release. In this way, we obtain production control with the maximum use of the available working time of employees and machines. Various devices are used to interact with the system: tablets, smartphones, machine controller displays, industrial and office computers. Through them, the system transmits autonomously decisions taken and enables the introduction of additional reports and information. The system also enables the collection and use of data in decision-making mechanisms directly from machines and devices, as well as direct, independent control of machines and robots in processes that can be implemented without human intervention. This production management is optimization of production in real time. Production planning and resource management is done not through production scheduling, but through an intelligent decision-making mechanism.

Maintenance services also benefit from the use of IIoT, as repairs and inspections of devices are carried out more and more often remotely. "In the event of a failure, a specialist logs into the machine's system, performs diagnostics, and on this basis indicates which element has been damaged and how to repair it. In addition, if the system is equipped with 3D glasses, it can lead the mechanic "by the hand" at the machine. The system will tell you when to inspect and which parts need to be replaced. Traction batteries connected to the Internet generate information on how to use the forklift and battery consumption. The system will also prompt you when to take it out of service and send it for regeneration [10].

When discussing the operation of the IIoT system, it should be emphasized that it is not intended to create enterprises in which people are replaced by robots. Technological development is to make the enterprise a better place to work. People are the most important link in the company's operation, and thanks to new solutions they will receive even greater technological support to improve comfort and streamline their work.

4 Cybersecurity of the Industrial Internet of Things

The Industrial Internet of Things generates a lot of data, so you need to ensure cybersecurity in production. Systems previously inaccessible, closed within a single enterprise, through the Internet suddenly become visible in the entire world network. Cyber security and technical security are closely related. IIoT systems are built of a huge number of different types of connected devices that are potentially new points of unauthorized access, which causes that aspects related to ensuring an adequate level of their security become key. Uncontrolled surveillance of people, activity of hackers and taking control of devices are the most important dangers which, together with the development of the Industrial Internet of Things, will become real threats to the safety of users. The vulnerabilities are found in a number of devices, and hackers can easily get passwords to access them with administrator privileges, and then modify their system software to suit criminal purposes. Many devices that enable reading of the data contained therein using contactless technology are susceptible to illegal copying of content without the knowledge of its owner in order to perform unauthorized transactions [11].

Rot and Bartosz Blaicke cite the results of the SANS Institute research, which identified the greatest risks associated with IIoT [12], which include:

- problems with object software update;
- using the facilities as the least secure network entry points;
- DoS (Denial of Service) attacks, which, for example in the case of power grid infrastructure or medical devices, can lead to serious consequences;
- unauthorized modifications of device operating parameters;
- user errors and accidental modifications that can lead to unpredictable consequences for the entire system of connected devices.

To secure processes, border devices such as industrial sensors are used, but also security solutions such as video monitoring and access control are used, whose primary function is to constantly provide security and protection in production facilities. Data from access control systems in combination with images from cameras guarantee that only authorized persons will have access to the facility. Vision as a medium begins to be used in the production process also for other tasks, e.g. machine vision, in which the image recorded by cameras is used to detect defects, operate robots or automatically drive vehicles in the factory [13]. Sensors can also be used to monitor the process and trigger alarms in hard to reach areas of industrial installations. They also facilitate remote repairs, and help reduce production losses [14].

The implementation of solutions in the area of the Industrial Internet of Things requires cooperation with third companies and various technology providers who gain access to information within and sensitive data. This raises concerns about the security of owned know-how - especially when the implementation is to include cloud technologies and remote access to production systems.

Security should be seen as a basic function of the IoT world. It is a prerequisite for the development of the Internet of Things. However, without certifying IoT products, an adequate level of security cannot be guaranteed.

5 Conclusion

As the research shows, in the coming years, the amount of autonomous traffic generated on the Internet via the Internet of Things will exceed the amount of traffic generated by users [13]. An example is e-mail, where nearly 90% of messages on the network are generated by vending machines. In its assumptions, the Internet of Things allows almost unlimited connection and communication of any device within the production system, enables the creation of a coherent architecture that provides the data necessary to implement improvements and flexibly shape the final product. On the other hand, such a sharp increase in traffic and the number of devices connected to the network will translate directly into the scale and type of security threats. Already today, for example, the largest networks (botnets), and used to attack other systems, and sometimes entire countries, are built using IoT devices.

According to the presented data, the Internet of Things is a process that manufacturers cannot ignore. IoT is forecast to connect as many as 28 billion devices in 2020. Devices are increasingly equipped with an Internet connection and are changing into elements of IoT systems - for devices related to home furnishings, to complex production lines, increasing their "intelligence". The new generation IIoT production processes are based on a combination of communication technologies, software and sensors. Their task is to connect the digital, virtual and real world of production from design and product development through production to maintenance and service. The Industrial Internet of Things means using the potential of several new technologies simultaneously, including IoT, AI, big data, cloud computing, augmented reality. Benefits include a definite improvement in the workflow, a change in the production management system that allows achieving a very economical and highly efficient system, reduction of downtime and service times and costs, improvement of quality, increase of productivity and identification of threats in real time.

References

1. Website information: https://www.postscapes.com/internet-of-things-market-size. Accessed 28 Nov 2019
2. Website information: https://mfiles.pl/pl/index.php/Internet_rzeczy. 28 Nov 2019
3. Website information: https://www.juniper.net/us/en/. 3 Dec 2019
4. Website information: http://przemysl-40.pl/index.php/2018/05/08/iot-hub-internet-rzeczy/. 30 Nov 2019
5. Website information: https://thingstream.io/. 30 Nov 2019
6. Owerczuk, M.: Przemysł 4.0 PL Szansa czy zagrożenie dla rozwoju innowacyjnej gospodarki? Boston Consulting Group (2016)
7. Wittbrodt, P., Łapuńka, I.: Przemysł 4.0 – wyzwanie współczesnych przedsiębiorstw produkcyjnych. http://ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2017/T2/t2_793.pdf. Accessed 8 Dec 2019
8. Woliński, B.: Koncepcja "Industry 4.0" jako strategia reindustrializacji i wdrożenia procesów produkcyjnych kolejnej generacji, Studia Ekonomiczne. Zeszyty Naukowe nr 308/2016 (2016)

9. Website information: http://przemysl-40.pl/index.php/2018/02/08/od-industry-4-0-do-smart-factory-czesc-3/. Accessed 9 Dec 2019
10. Kucia, G., Skowronek, G.: Mobilne sterowanie fabryką. Menedżer w erze IoT, Production Manager nr 9/2017 (2017)
11. Kobyliński, A.: Internet przedmiotów: szanse i zagrożenia, Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług 2014, nr 112, t. 1, s. 101–109 (2014)
12. Rot, A., Blaicke, B.: Bezpieczeństwo Internetu Rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych. Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie Nr 26 (2017)
13. Website information: https://www.digitalpoland.org/assets/publications/iot-w-polskiej-gospodarce/iot-w-polskiej-gospodarce-raport.pdf. Accessed 9 Dec 2019
14. Lipski, J.: Internet rzeczy w zastosowaniu do sterowania produkcją. [w:] Knosala R. (red.) Innowacje w zarządzaniu i inżynierii produkcji, t. 2, Polskie Towarzystwo Zrządza-nia Produkcją, Opole (2015)