2024 International Conference “ROBOTICS & MEHATRONICS”
29 – 30 October, 2024, Sofia, Bulgaria

Some aspects of cybersecurity in Industry 4.0

Ivan Gaidarski
Unmanned Robotic Systems Lab
Institute of Robotics "St. Ap. and Gospeller Matthew"
Bulgarian Academy of Sciences
Sofia, Bulgaria
ivangaidarski@ir.bas.bg

Abstract
Technical progress brings four Industrial Revolutions - first one defined by the steam engine, the second with the electricity. The third is a result of adoption of electronic computing machines and communications, the Internet and the associated mass digitalization. The fourth is result of technological and scientific breakthroughs - artificial intelligence, big data, cloud, Internet of Things, Cyber-physical systems. In Industry 4.0 manufacturing facilities are integrated with the Internet of Things and the Internet of Services. CPS integrate sensing, control, communication, computational and physical interaction. CPS integrates roduction processes with vertical business processes, with result operational technology. Industry 4.0 merges OT with IT. The diversity of technologies brings enormous challenges for the security. In Industry 4.0 there is increased importance of System availability and Safety, compared to the traditional information security enterprise, where the focus is on confidentiality, integrity and availability (CIA). From a technological point of view, OT challenges the traditional IS paradigm with new elements - industrial control system (ICS) and IoT devices. Ensuring their security is critical to the security of the entire OT.

Keywords— Industry, Internet of Things, IoT, Internet of Services, IoS, Cyber-physical systems, CPS, operational technology, OT

I. INTRODUCTION

At the end of the 18th century, thanks to the revolution in industrial production, a qualitative transition from agrarian-based to industrial-based societies took place. With this comes the economic development of these societies and the associated increase in people's living standards. Rapid industrialization allows us to talk about Industrial Revolution. Depending on the achievements of technical progress, we can talk about several stages in industrialization. The First Industrial Revolution was associated with the invention of the steam engine, and the Second was associated with the discovery and widespread adoption of electricity. The third industrial revolution is associated with the introduction of electronics, electronic computing machines, electronic communications, the Internet and the associated mass digitalization. A characteristic feature is the rapid development of digital services and the related importance of information, its collection, processing, use, analysis and storage. During the Third Industrial Revolution, a transition from purely industrial production to the production of services is actually taking place. In turn, they require a new kind of resources - high degrees of qualification, innovative thinking and creativity. This, in turn, leads to an increase in the role of education and science in general, and the prerequisites are created to talk about an information society and a digital economy. The advent of mass automation and robotization together with digitalization lead to a qualitative change in industrial production. A new phase of technological development is coming and we have the reason to announce the arrival of a new stage in the industry - the Fourth Industrial Revolution or Industry 4.0. It is characterized by technological and scientific breakthroughs such as artificial intelligence (AI), big data, cloud services, Internet of Things (IoT), Cyber-physical systems (CPS), automated design and production systems, autonomous vehicles, nanotechnology, new materials etc. New Internet technologies enable the connection of multiple industrial systems, creating a new type of production facilities "Smart Factories". They are characterized by a high level of autonomy through the use of automated systems and robots, with maximally reduced labour force participation. Along with the advantages, new digital technologies bring enormous challenges to data security, digital infrastructure, industrial systems and production facilities. In this article, we consider some aspects in the security of the elements of Industry 4.0 [1].

II. WHAT IS INDUSTRY 4.0.

Industry 4.0 refers to the Fourth industrial revolution where manufacturing facilities are integrated with the Internet of Things (IoT) and the Internet of Services (IoS). This new form of industrial production builds on the first three stages characterized mainly by mechanization, electricity and information technology.

One of the new concepts related to Industry 4.0 is Cyber-physical systems (CPS). These are systems that integrate sensing, control, communication, computational and physical interactions. A typical CPS usually consists of a group of agents—sensors, actuators, control processing units, and communication devices—that are networked. They can form intelligent production facilities, infrastructure and supply chains built by connecting machines, equipment, warehouses and logistics centers communicating with each other. CPS ensures the integration of production processes with vertical business processes - delivery, logistics and sales, which we will call operational technology (OT) [10]. This enables smart factories to manage and control the entire life cycle of the production process - from the supply chain to the final products and services. Thus, in practice, with Industry 4.0, operational technology (OT) merges with information technology (IT).

Industry 4.0 envisages not only the construction of smart factories, but also the production of smart products. The

ACKNOWLEDGE THE FINANCIAL SUPPORT OF THE PROJECT WITH ADMINISTRATIVE CONTRACT № КР-06-Н57/8 FROM 16.11.2021. - FUNDED BY THE "COMPETITION FOR FUNDING BASIC RESEARCH - 2021." FROM THE RESEARCH SCIENCES FUND, BULGARIA.

miniaturization of RFID tags allows smart products to have embedded intelligence so that they can be identified, located, and know what they are, what their condition is, where they were made, and where they are intended.

In essence, Industry 4.0 can be defined as:

1. Industry 4.0 represents a transition of the manufacturing industry to digital transformation. We have a merger of the physical and digital worlds that provides fundamentally new opportunities.
2. By using the latest technological advances and the fusion of operational and information technologies, Industry 4.0 provides a new approach to the production of goods.
3. Managing the entire process along the value chain, Industry 4.0 ensures the increase in the efficiency of production and industrial processes, through their automation and digitalization. The goal is to provide new, products and services with better quality [2].

The emergence of Industry 4.0 is determined by the latest technological achievements:

- Explosive growth in the volumes of data collected and generated, the development of cloud services covering increasing computing power for rent and data storage space.
- Advance of wide-ranging cross-platform network connectivity enabling communication between core production elements.
- New advanced capabilities for performing analysis of large volumes of data in real time. These capabilities provide rapid feedback and increase the efficiency of production, logistics and sales processes.
- Development and mass penetration of fast industrial WAN networks with low power consumption. They provide new levels of data processing necessary for production and logistics operations.
- Mass penetration of miniature RFID tags, allowing manufactured products to acquire a kind of intelligence - smart products.
- Entering interactive systems with augmented reality, leading to new levels of human-machine interaction.
- Improving robotic manufacturing and increasing their autonomy with the development of AI.
- Technological breakthroughs in the field of 3D printing, enabling rapid prototyping. and finished products.

There are four main characteristics of Industry 4.0:

1. **Vertical integration of industrial systems.** For the autonomous operation of smart industrial systems, it is necessary for them to communicate with each other. For this purpose Cyber-physical systems (CPS) are connected in communication networks. CPS ensure the rapid response to various variables - insufficient stock of materials, breakdowns and defects in machines, unforeseen delays, changes in the demanded quantities. Vertical integration includes both smart factories, as well as logistics and trade systems.
2. **Horizontal integration of the value chain.** In addition to the production of products, their logistics, marketing, sales and service are needed. These are the elements of value chains. At the heart of Industry 4.0 is the unification of industrial production and services, as well as the continuous addition of new business models and improvement of existing ones. The globalization of the market leads to the need to ensure compliance with various requirements - regulatory, local laws, requirements related to consumer requirements, as well as safety rules.
3. **Covering the entire life cycle of production and services.** Industry 4.0 focuses on ensuring quality through the unification of physical products and services. This requires the tracking and servicing of the full product life cycle, from production to retirement and recycling. In addition to the product itself, it is necessary to monitor customer satisfaction, provide service services to support the product, as well as recycling services at the end of its life cycle.
4. **Speeding up production.** In addition to the above-mentioned features of Industry 4.0, it also focuses on improving existing technologies and, accordingly, speeding up the production of products. By collecting data from every stage of production and providing fast feedback, bottlenecks such as material and production resource depletion, downtime due to breakdowns and the depletion of the life of production assets are minimized [3,4].

Industry 4.0 integrates existing and emerging technologies related to the production of physical products combined with various services, both physical interaction and purely virtual, such as cloud services providing computing power and data storage mechanisms. Technological, integration, logistics and business are needed to implement this integration. processes:

- Big Data and Analytics;
- Industrial Internet of Things (IoT);
- Autonomous Robots;
- Horizontal and Vertical System Integration;
- The Cloud;
- Additive Manufacturing;
- Augmented Reality;
- Simulation.

The diversity of technologies and processes, part of Industry 4.0 brings enormous challenges for the security of data, systems and last but not least the people involved in the process. Due to the fact that all elements of I4.0 have network connectivity and access to the global network, we will look at some cyber security challenges in Industry 4.0 [4].

III. New challenges to cybersecurity

Cybersecurity can be defined as a series of actions and processes undertaken to ensure information security in networked resources. It also refers to offline resources that can be accessed from the network. Traditional IT cybersecurity is based on the CIA triad. The main elements of which are Confidentiality, Integrity and Availability, ensuring the preservation of confidentiality, integrity and availability of information throughout its life cycle in information and communication systems.

When we talk about industrial production and online services with high requirements for the continuity and consistency of the production processes, in addition to the traditional CIA concepts, it is mandatory to add additional ones - Reliability, Interoperability, Accountability and Assurance.

Reliability is defined as the probability a system is functioning accurately for a length period of time [8,9]. Interoperability refers to the ability of different components and systems to interact and exchange data in a way that is reliable, secure, and efficient. Accountability reflects the requirement for unique identification and accountability of an asset. It provides deterrence, isolation, intrusion detection and prevention, and loss recovery. Assurance is defined as the degree of confidence that the security needs of a system are satisfied [10].

Traditional enterprise IT Security and cyber security in particular can be represented by the conceptual model of Fig.1

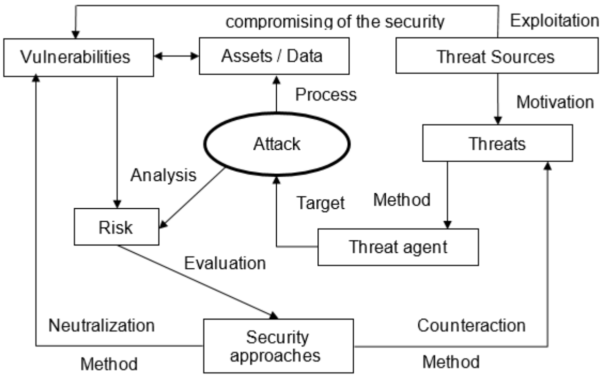

Fig. 1. Conceptual model of Information Security

The typical concepts making up a conceptual model are Vulnerability, Attack, Threat Source, Threat Agent, Motivation, etc. IT Security in Industry 4.0 can also be defined and presented with them. In Industry 4.0, we have several specific features of the environment and the used technologies. We will look at security in manufacturing process, which is distinguished by some features. Here, instead of traditional Information Security, we have operational technology (OT), which expands IT with additional processes and corresponding requirements. For example, with OT we have an increased importance of System availability and Safety, compared to the traditional information security enterprise, where the focus is on confidentiality, integrity and availability (CIA). The most important principle in OT is Safety. It plays a rather secondary role in traditional enterprise IT security, where the CIA is the priority, but in OT, failure to comply can be catastrophic for employee safety. OTs operate in an industrial work environment that requires specific work rules and equipment. IT employees servicing IT systems need special training and equipment. Compliance with the rules for safety in the specific work environment is a priority and serious training is required. The emphasis is on physical and behavioural security, as well as on the specifics of the technology used.

In an industrial environment, System Availability is also a priority. In industrial OT it is unacceptable to interrupt the production process, while in traditional IT it is a completely normal process that does not affect normal work. In general, OT cannot use traditional testing and servicing tools and processes that require disruption to IT processes - for example, stopping services, testing new systems in a live environment, and even rebooting servers.

From a technological point of view, at OT we have technologies that are not characteristic of the traditional IT environment. Such, for example, are industrial control system (ICS) and IoT devices [5,6,7].

The ICS environment is very different from the IT enterprise. ICS includes control systems, programmable logic controller (PLC), industrial networks and personnel responsible for operational and production tasks. Traditionally, IT includes the information systems, applications, people, and networks required to manage information technology. While IT networks have traditional security mechanisms such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) or data loss prevention systems (DLP), in OT they cannot be applied to the overall environment and sometimes cannot be used at all. Other mechanisms such as network isolation and segmentation can be implemented, but they cannot solve all challenges.

Typical industrial OT networks differ significantly from traditional IT, for example, they use both IP-compliant and non-IP-compliant protocols for machine-to-machine (M2M) communication and programmable logic controllers (PLC). In OT, a case-by-case approach must be taken in order to assess in which segments traditional protection measures may be used and in which must be used specific ones. It is also necessary to carry out a risk assessment to assess which elements need to be protected, with what resources, people and time. In any case, compliance with the principles of Safety and System Availability is a priority.

In addition to security measures, we also have differences in testing and maintenance tools. Some of the traditional tools and technologies are simply not designed for an OT environment because they rely on system brakes or greater than acceptable downtime and can hurt performance. Therefore, analysis and troubleshooting tools and their method of operation should be carefully analyzed before being used in OT and ICS environments.

OT environments are typically designed for a life span of 20 years. This means that in a modern factory there can be both the latest technologies and technologies 15-20 years old. Thus, technologies of different age and functionality are accumulated in an OT environment.

OT networks are heterogeneous, and can support several different network types, protocols and standards, for example Modbus, Ethernet/IP, Profibus and Profinet. Separately in them we also have a combination of different media and cabling standards, such as fiber optics, copper cables or wireless for Ethernet 10/100 Mbps or Gigabit Ethernet. The reason is that in order to maintain the equipment on daily basis, the latest technologies for a given period are used. In order to ensure compatibility and, above all, operability (61), OT systems relying on outdated technologies and components are adapted and new technologies are gradually introduced to replace the outdated ones. For example, some of the protocols in use such as Modbus are being upgraded with new versions capable of handling IP traffic. Another example is the emergence of new protocols such as the industrial version of Ethernet - Ethernet/IP (IP stands for Industrial Protocol) and Profinet providing new capabilities to industrial networks. The trend is a complete shift to IP and Ethernet protocols.

IoT devices, on the other hand, by definition, are devices capable of collecting information and at the same time are executive devices capable of controlling certain physical objects - for example, valves on pipelines or gas pipelines, actuators and thermostats for temperature control, etc. In effect, they dramatically expand the attack surface of known cyber security threats and carry the risk of additional security threats not inherent in traditional IT environments. Ensuring the security of the IoT is critical to the security of the entire OT environment. Here we are talking not only about loss or alteration of data, but also about possibilities for physical impact of assets from the OT environment, with all the risks and possible consequences of that.

IV. Conclusion

Due to the fact that Industry 4.0 is still only a concept, for the purposes of cyber security it is necessary to look for analogy with already existing and imposed in practice technologies, for example SCADA and C4ISR systems. They have some close characteristics to the Industry 4.0 from cyber security viewpoint, the most important of which is that they are Network Centric and they their connectivity to the Internet. Other common features are: traditional vulnerabilities, online connectivity, data communication, physical vulnerability, multiple communication interfaces, heterogeneous operating environment, OS and work environment.

Methods for protection against known threats, as well as new methods to detect brand new threats by analogy with these and existing environments and systems, are the subject of further research.

ACKNOWLEDGMENT

This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

References

[1] Thames, Lane & Schaefer, Dirk. (2017). Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges. DOI: 10.1007/978-3-319-50660-9_1.

[2] Mehnen, Jorn & He, Hongmei & Tedeschi, Stefano & Tapoglou, Nikolaos. (2017). Practical Security Aspects of the Internet of Things. 10.1007/978-3-319-50660-9_9.

[3] Gilchrist A., Industry 4.0: The Industrial Internet of Things, Apress Berkeley, CA, 28 June 2016, eBook ISBN 978-1-4842-2047-4, DOI https://doi.org/10.1007/978-1-4842-2047-4

[4] Mohammadi A, Plataniotis K., Secure State Estimation in Industrial Control Systems, Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop, CRC Press, 2016, DOI 10.1201/b19629-7

[5] Yang, Lei & Xue, Hao & Li, Fengjun. (2015). Privacy-preserving data sharing in Smart Grid systems. 2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014. 878-883. 10.1109/SmartGridComm.2014.7007759.

[6] Zhu, Quanyan & Wei, Dong & Ji, Kun. (2016). Hierarchical Architectures of Resilient Control Systems: Concepts, Metrics, and Design Principles. 10.1201/b19629-9.

[7] S. Misbahuddin, "Fault tolerant remote terminal units (RTUs) in SCADA systems," 2010 International Symposium on Collaborative Technologies and Systems, Chicago, IL, USA, 2010, pp. 440-446, doi: 10.1109/CTS.2010.5478479.

[8] Trividi, K. (1990, July). Reliability evaluation of fault tolerant systems. IEEE Transactions on Reliability, 44(4), 52–61

[9] Djambazova E., Achieving System Reliability Using Reliability Adjustment, In International Conference on Computer Systems and Technologies 2022 (CompSysTech ’22), June 17, 18, 2022, University of Ruse, Ruse, Bulgaria. ACM, New York, USA, ISBN: 978-1-4503-9644-8/22/06, DOI: https://doi.org/10.1145/3546118.3546129, SJR (Scopus): 0.23.

[10] US National Institute of Standards and Technology (NIST), NIST Internal Report (NISTIR) 5472 A Head Start on Assurance: Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness, USA, 1994