International Journal of Modern Manufacturing Technologies
ISSN 2067–3604, Vol. XIV, No. 3 / 2022
https://doi.org/ 10.54684/ijmmt.2022.14.3.233

CYBERSECURITY STRATEGIES IN INDUSTRY 4.0

Gabriel Raicu[1], Alexandra Raicu[2]

[1]Constanta Maritime University, Faculty of Navigation and Naval Transport,
104 Mircea cel Batran Street, 900663 Constanta, Romania
[2]Constanta Maritime University, Faculty of Naval Electromechanics, Department of General Engineering Sciences,
104 Mircea cel Batrân Street, 900663, Constanta, Romania

Corresponding author: Alexandra Raicu, alexandra.raicu@cmu-edu.eu

Abstract: Cybersecurity is now the one of the highest important part of the Industry 4.0 and to all the design and manufacturing companies. This paper presents new cybersecurity strategies in Industry 4.0, where current vulnerabilities and exploitation processes, possible attack vectors, attack, compromise, and performance indicators should be considered. Also, cyber risk in product lifecycle management is a very important aspect. This revealed authentication issues, unsecured communications, default deployment issues, susceptibility to physical attacks. For example, a successful cyberattack could bring subtle changes to the control parameters of a robot or of a manufacturing process. This can further change the robot's operating mode in an almost undetectable way, but instead alters the efficiency and integrity of the final product. By monitoring these behaviours, cataloguing indicators, and inspecting potential risks, we can determine how an attacker gains access to the network and predict the intent they had. We need well-trained staff in any enterprise to drastically reduce the risk of cyberattacks. For this reason, appropriate measures must be taken to solve these problems, and one of these is cybersecurity education. It is necessary to implement appropriate policies and risk reduction plans in the product lifecycle management to prevent possible cyber-attacks.
Key words: Industry 4.0, secure by design, cybersecurity, vulnerabilities, attack vectors.

1. INTRODUCTION

In recent years, there has been a major change in approach to the concept of cybersecurity, which must be ensured on a mandatory basis at the level of a complete industrial chain from the perspective of the Smart Factory. European projects encourage the use of Information and Communication Technology (ICT) in the context of the product lifecycle management (PLM) and the achievement of digitalisation, thus taking industry and production to a new world known as Industry 4.0, or what we can say now Industry X.0. Industrialization 4.0 represents the use of cyber-physical systems, Internet of Things (IoT), Cloud Computing, Artificial Intelligence (AI), Blockchain Technologies, 5G Mobile telecommunications networks, Advanced automation, and 3D printing.

To keep up with the trend of the market, it is necessary to introduce advanced prototype design and production architectures capable of providing opportunities for long-term development and research. In the last five years, there has been a major change in approach from a conceptual point of view in terms of cybersecurity that needs to be ensured at the level of a complete industrial chain from the perspective of Smart Factory.

At present, cybersecurity risks have reached a worrying level, beyond the classic risk threshold and sensitive data leaks, leading to complex threats that can disrupt an entire company and / or industry, managing a supply chain or even, at the governmental level, affecting the functioning of a state. Thus, the losses due to cyber security incidents can reach billions of euros and affect companies in any field of activity with significant repercussions in the economy of a country.

In recent years and especially since many activities are online, several vulnerabilities have been highlighted following multi-criteria analysis. No prior knowledge of tools or malware is required. A critical initiative for defending networks is the "zero-trust" concept.

This study addresses cybersecurity strategies in Industry 4.0, considered the most technologically important issue, as presented in the Global Economic Forum's Global Risk Report for 2020, [1].

2. CYBERSECURITY IN THE CONTEXT OF INDUSTRY 4.0

Cybersecurity is a global, broader concept that refers to the protection of all electronic equipment, software components, data and information in a particular area called the target system. Cybersecurity is a concept that includes computer security and extends to the area of mobile equipment, smart equipment and information

used by them. The information flow managed by these systems also refers to data that is not only processed using computers but represents communications, images, online recordings, including data processed by third-party software products.

On broad acceptation, the core of Industry 4.0 is the Smart Factory concept, which operates from cyber-physical systems (physical components that receive virtual commands) and innovative industrial robots simultaneously connected to the real environment. Cyber-Physical Systems (CPS) provides, by definition, the direct coupling of digital technology to physical reality, being used in industry through the implementation of intelligent production lines and efficient production systems, which also include management of material stocks, creation of customized products. Equipment in a manufacturing line is interconnected in a system and makes intelligent decisions (without human intervention), where objects communicate with each other in the so-called Internet of Things (IoT), or, on a larger scale, talking about the Industrial Internet of Things (IIoT). Figure 1 highlights the main components of Industry 4.0, cloud computing, Big Data and data analysis in robotics, the Internet of Things, with Cybersecurity as interconnected approach [2].

Fig. 1. Industry 4.0 Components: Cybersecurity, Big Data and Analytics, 5G, Artificial Intelligence, Robotics, Cloud computing and High-performance computing, Internet of Things, Cyber-physical systems, Additive Manufacturing
Source: European Court of Auditors.

The smart factory brings with its new security challenges. Smart Factory is part of a larger ecosystem and needs to be connected to more systems at once. As Industry 4.0 becomes more innovative, it becomes a more attractive target for attackers where they could move along a production network, oscillating in their malicious activities between IT (Information Technology) and OT (Operational Technology). Without a proper cybersecurity measure, attackers can take advantage from a broad list of a systemic threats in the case of Smart Factory concept:

- Industrial espionage,
- Intellectual property theft, personal data, and privacy,
- Leakage of information on technological advantages, patents, etc.,
- Production sabotage,
- Cyber terrorism.

All mentioned threats are based on common cybersecurity challenges facing Industry 4.0 era:

- Every device connected to the Internet poses a potential risk.
- Complex production systems such as Industrial Control Systems have vulnerabilities that make them particularly sensitive to cyber-attacks.
- Industry 4.0 connects previously isolated systems, which tremendously increase the attack surface.
- Updates are partial because the systems are very complex and different in their nature of interactions.
- Production has less regulated compliance standards than other sectors.
- Visibility is low for separate systems and isolated environments.
- Thus, to develop a successful smart factory, with protection against cyber threats, it must:
- Adopt a risk-based approach to security, linking business criticality to security strategy.
- Maintains an accurate inventory of all OT assets in real time.
- Combines the best IT and OT technologies as an integrated part of the security strategy.
- Identify and fix outdated systems, vulnerabilities, and poorly secured files.
- Highlight security issues when introducing new systems to the network.
- Always remain vigilant to detect potential threats with real-time vulnerability assessments and risk prioritization.
- Ensures that technology vendors and connected equipment manufacturers are committed to constantly conducting security patches and audits.

3. CYBERSECURITY STRATEGIES IN THE CASE OF COLLABORATIVE INDUSTRIAL ROBOTS

Cybersecurity risks are developing faster with the evolution and implementation of new digital technologies.

The Global Economic Forum's Global Risk Report for 2020 emphasized the impact of cybersecurity, as a main technological issue, to ensure effectiveness of cybersecurity in the case of collaborative robots.

3.1 Current vulnerabilities and exploitation procedures in the case of collaborative robots

From cybersecurity point of view, the tendency for cybercriminals to become more focused on IoT devices, will further increases the global cyber risk.

To ensure the security of the operation, a series of limitations are applied in the operation of the robots, such as:

• Limitation of force and power: to reduce the pressure exerted by the robot in the direction of movement in the event of a collision between the robot and the operator.

• Impulse limitation: to reduce transient energy and impact forces in the event of a collision between the robot and the operator by reducing the speed of the robot.

• Limit the orientation of the work tool: to reduce the risk associated with certain areas and features of the tool and the workpiece (for example, to avoid sharpening the edges of the work tool toward the operator).

• Speed limitation: to ensure that the robot arm operates at a low speed.

• Safety limits: to restrict the robot's workspace by forcing it to remain in a predefined safety zone.

3.2. Possible attack vectors for universal robots

Cyber intrusion on UR3 universal robots: the initial infection is achieved by exploiting two vulnerabilities through one of the following two attack vectors:

1. Remote access through adjacent networks: RVD # 672 (**CVE-2018-10633**) allows an adjacent network attacker to easily enter the control box. Alternatively, RVD # 6 allows an adjacent attacker to exploit by overriding the buffer in the TCP ModBus UR3 service and executing commands as root [3].

2. Physical USB ports in the tutorial: By exploiting **CVE-2019-196262** (not made public) an attacker can execute a code with root privileges by simply connecting an external USB Stick. This attack vector is probably the easiest to use given the exposure of the teaching set to most UR3 robots. Moreover, the same attack vector applies not only in the handheld set, but also in the control box that exposes the directly accessible internal USB ports [4].

Universal Robots - The Robot Controller for the Version CB2 series of robots. Vulnerability **CVE-2020-10265** reported by NIST, as in Figure 2 [5] and ALIAS ROBOTICS [6].

Lack of encryption, authentication, or authorization capabilities in MiR collaborative robots used in healthcare and industry, UR10, UR5, and UR3 in firmware versions 1.10.0, 1.11.0, 1.12.0, 1.12.1, and 1.13.0 [7].

Specific elements have been developed to illustrate robot-specific cyber vulnerabilities like the CVE code - used by MITRE, namely RVE (Robot Vulnerability Exploit).

4. DOBOT MAGICIAN LITE COLLABORATIVE COBOT CASE STUDY, WORKING HYPOTHESES

In this chapter we propose for analysis from cybersecurity point of view, an educational mini robot for the PLM laboratory of Constanta Maritime University, Dobot Magician Lite made by Shenzhen Yuejiang Technology, Figure 3 and 4. The technical documentation of the product can be found on the manufacturer's website [8].

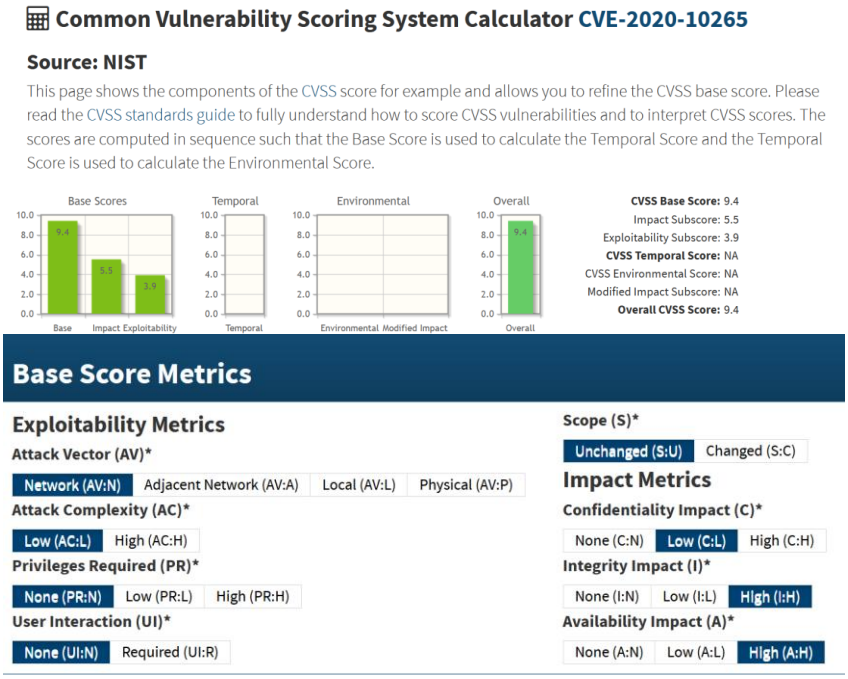

Fig. 2. Vulnerability NIST code CVE-2020-10265, Source: NIST

Fig. 3. Cobot analyzed, Source: Shenzhen, Yuejiang Technology

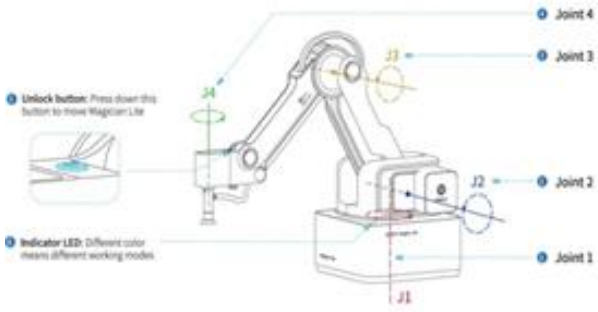

Fig. 4. Cobot joints, Source: Shenzhen Yuejiang Technology.

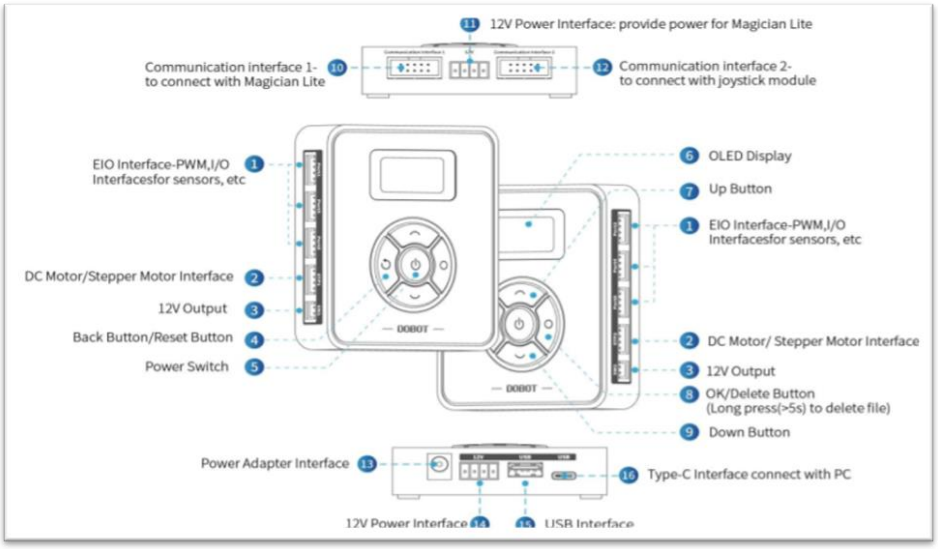

Fig. 5. Cobot interfaces, Source: Shenzhen Yuejiang Technology

The software used for command and control for Magician Lite, Dobot Studio, allows you to perform many functions such as programming, writing, and drawing, graphic design, positioning/manipulating objects.

We can consider two working hypotheses:

1. Attacks focused on vulnerabilities of the robot's communication system operating/programming/management technology (attack on the network/computer system used for programming activity, exploitation of vulnerable third-party software libraries and taking over communications access to controllers);

2. Alteration of basic functionalities that can be considered as physical sabotage, the consequences being major: modification of the dynamic parameters of an industrial robot arm to damage the production line, stock of products, to damage the machine itself or to generate a risk of physical security on human operators.

4.1 Attack and compromise indicators for the Dobot Magician Lite

Figure 5 shows the interfaces of the educational collaborative cobot Dobot Magician Lite.

Five simulated attack indicators presented below have been identified together with their effects:

1. Modifying the controller parameters

A successful cyber-attack could make subtle changes to a robot's control parameters. This can subtly change the way the robot operates, in an almost undetectable way, but instead changes the efficiency and integrity of the product – with the same effect as classical Low and Slow attack.

Effects: Defective product, non-compliant, reduced economic efficiency

2. Changing the calibration parameters

A successful cyber-attack could alter the robot's calibration parameters, causing it to move unexpectedly or deviate from the standard working path.

Effects: Robot damage and/or injury to human operators.

3. Modification of production logic

A successful cyber-attack could introduce minor, almost imperceptible changes, leading to variable product quality or random blocking of the assembly line.

Effects: products with inconsistent quality.

4. Change the status of the robot

A successful cyber-attack could alter your security settings. The security limits of a collaborative robot may be exceeded in a way that is difficult for the user to detect.

Effects: Injury to humans.
5. Changing the status of the robot perceived by the user
A successful cyber-attack could cause the robot to appear to be in a stable state while it is in an operational state. For example, the controller might display that the robot is turned off while operating without set security limits.
Effects: Injury to humans.

4.2 Dobot Magician Lite cobot performance indicator used as reference parameters

An indicative list of performance indicators is presented below:
• Duration of the activities cycle - Time required for programming, graphic design, positioning/ handling of parts, from order to launch.
• Yield - The number or percentage of parts that are programmed, graphically designed, positioned/ handled as specified.
• Rejections and/or returns from customers - the number or percentage of products returned due to quality issues or customer dissatisfaction.
• Manufacturing cost as a percentage of revenue - The percentage of revenue that the company spends on collaborative cobot activity.
• Downtime - The amount of time (often expressed as a percentage) in which the cobs in the manufacturing process are not available for production.

4.3 Eisenhower decision matrix

It is very important that the methods of addressing cyber security consider all aspects related to the particular importance of the operation of industrial robots.
The principle of Dwight Eisenhower was to use time effectively, not just efficiently: "What is important is seldom urgent and what is urgent is seldom important." In our case, the purpose of this decision matrix is to increase the level of security in the use of collaborative industrial robots [9].
A critical initiative for the defense of networks is the "zero-trust" concept. Zero confidence implies a set of security paradigms that cover the entire chain of activity of the use of industrial robots. Protection needs to be provided, especially at the resource level and less at the network level, given that certain services can be outsourced to the cloud.
We propose an additional contribution based on the customized Eisenhower matrix able to improve the effectiveness of cybersecurity measures in companies, in which tasks were organized on two criteria: urgency and importance, as you can see in the Figure 6.

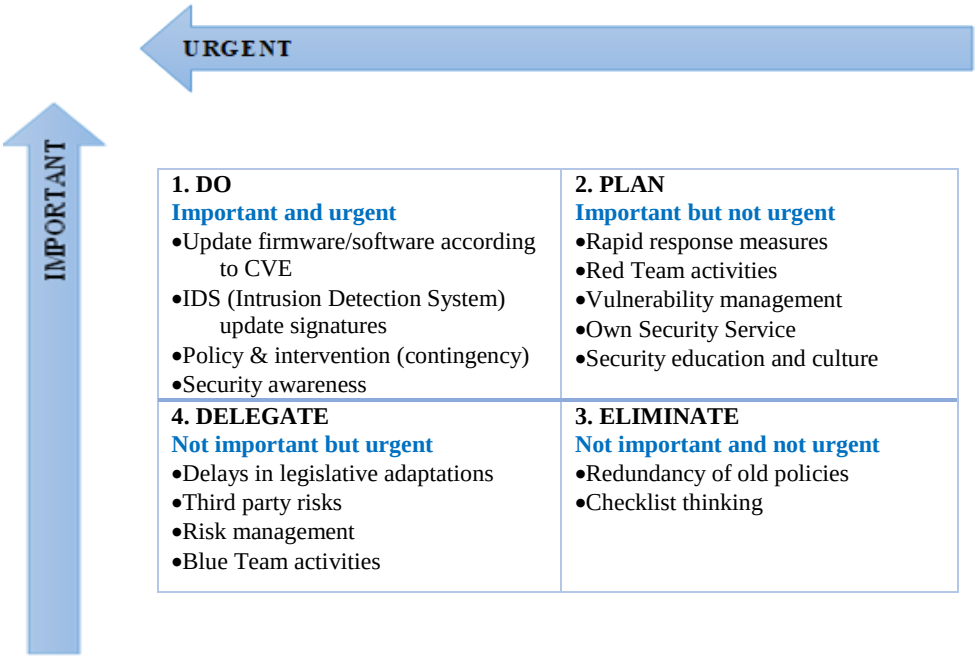

Fig. 6. Proposing an Eisenhower matrix
to improve the activity of collaborative robots

5. CONCLUSIONS

In recent years, there has been a major change of approach to the concept of cybersecurity, which must be ensured at the level of a complete industrial chain from the perspective of Smart Factory. We need well-trained staff in every enterprise to drastically reduce the risk of cyber-attacks. Unfortunately, statistics show that a large part of cyber-attacks today are related to human error. For this reason, appropriate measures must be taken to address these issues, and one and very important of them is education.
Collaborative robots, 3D printers, AI, digitizing the entire life cycle of a product represent the future in

the automation industry, but only in the context of cybersecurity. Universal robotics or 3D printing products contain serious security vulnerabilities that could easily be exploited to hack and take control of the movements and operations of espionage equipment or to cause physical damage, with implicit harm to the human factor, thus becoming a threat. real danger on a large scale.

Recent studies have shown that collaborative robots can be exploited for cybersecurity and can later become dangerous. About 50 vulnerabilities have recently been discovered that can be exploited in widely used robots and their control software. Thus, these vulnerabilities could trigger a cyber-attack that remotely manipulates a robot to infiltrate other networks, spy on and steal information, and even cause physical damage. According to researchers, a pirated robot could be used in the long run to infiltrate and penetrate other networks or even other robots.

To increase security and prevent cyber-attack in Industry 4.0, steps must be taken such as:

• Monitoring and updating of software (operating system, web server, application server, database server, libraries, and related programs);
• Use of antivirus software, through recalibrated and Intrusion Detection System (IDS) and Active Web Firewall;
• Using complex passwords, even two-factor authentication, respectively 2FA authentication mechanisms (local password + Google Authenticator);
• Use of information only from official sources, websites, and e-mails from trusted sources;
• Always making backup copies of important data;
• Document security in addition to security measures, by ensuring OpenVPN interconnections;
• Connection encryption;
• Regular education and training of Smart Factory personnel and adoption of general Security policies;
• Carrying out procedures and schemes for different types of threats;
• Introduce additional security measures, such as biometric identity or smart cards;
• Implement the "secure by design" principle.

Ensuring a secure cyberspace in any context is the responsibility of both the state and the competent authorities, the private sector and civil society. For the development of the cybersecurity culture, the most important levers are education and research, public-private partnerships, and cooperation mechanisms at European level.

6. ACKNOWLEDGMENTS

The authors would like to reiterate in this way the technical and scientific support received in the research activity within the CYMAROP Project - Cybersecurity Maritime Operations Center for Research and Education and Autonomous Operations - developed within the partnership of Constanta Maritime University and GMB Computers.

7. REFERENCES

1. World Economic Forum, The Global Risks Report 2020, Available from: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf, Access on: 2022.
2. Digitising European Industry: an ambitious initiative whose success depends on the continued commitment of the EU, governments and businesses, Special Report, 2020, Available from: https://www.eca.europa.eu/, Access on: 2022.
3. National Institute of Standards and Technology, National Vulnerability database, Available from: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2018-10633&search_type=all, 2018, Access on: 2022.
4. National Institute of Standards and Technology, National Vulnerability database, Available from: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2019-19626&search_type=all, Access on: 2022.
5. NIST, Available from: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2020-10265&vector=AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H&version=3.1&source=NIST, Access on: 2022.
6. Alias Robotics, Available from: https://aliasrobotics.com/, Access on: 2022.
7. UR security case study - penetration testing, https://aliasrobotics.com/case-study-pentesting-ur.php, Access on: 2022.
8. Dobot web site, Available from: www.dobot.cc, Access on: 2022.
9. McKay, B., McKay, K., (2013). *The Eisenhower Decision Matrix: How to Distinguish between Urgent and Important Tasks and Make Real Progress in Your Life*, Available from: https://www.artofmanliness.com/articles/eisenhower-decision-matrix/.

Received: April 25, 2022 / Accepted: December 15, 2022 / Paper available online: December 20, 2022 © International Journal of Modern Manufacturing Technologies