Analysis and Prospects for Ensuring the Cybersecurity of Industrial Robots

Sabyrzhan K. Atanov[1], Kymbat Z. Seilkhanova[1], Yerzhan N. Seitkulov[1] and Shadi A. Aljawarneh[2]

[1] *L.N. Gumilyov Eurasian National University, 2 Satpayev St., Astana, 010008, Kazakhstan*
[2] *Jordan University of Science and Technology, Irbid, 22110, Jordan*

Abstract

Ensuring a high level of cybersecurity for industrial robots is of fundamental importance given their key role in automating industrial processes. Vulnerabilities in robotic systems can lead to serious consequences, including production downtime, data loss, and even threats to workers and the environment. Cybersecurity problems for industrial robots are caused not only by insufficient software protection but also by their physical integration into industrial networks. In this article, we will look at real-life examples of vulnerabilities in robotic systems that can have serious consequences, including the possibility of unauthorized access, potential impact on physical processes in a production environment, and so on. The authors propose several ways to strengthen the cybersecurity of industrial robots in the future.

Keywords

Cybersecurity, industrial robots, industrial automation

1. Introduction

Cybersecurity for industrial robots is an extremely important aspect of the field of industrial automation. It plays a key role in ensuring the safety of the work environment and equipment, as well as protecting the enterprise's confidential data and intellectual property [1]. Maintaining strong cybersecurity helps prevent potential threats to production and ensures business continuity. In addition, compliance with safety standards and legal requirements is important both from a legal liability perspective and to maintaining a good company reputation.

According to [2], robotics is rapidly developing using the Internet of Things (IoT), increasingly applying the concept of the Internet of Everything (IoE). This development combines robotic systems with wireless networks, sensors, cloud platforms, open-source software, other devices and artificial intelligence. This process increases the complexity of robot development and emphasizes the importance of ensuring robot safety.

Therefore, in this article, we will consider industrial robots as IoT devices, which allows us to assume that these devices can be attacked by “traditional” hacking methods.

DTESI 2023: Proceedings of the 8th International Conference on Digital Technologies in Education, Science and Industry, December 06–07, 2023, Almaty, Kazakhstan

atanov5@mail.ru (S. Atanov); kimakowi@gmail.com (S. Seilkhanova); yerzhan.seitkulov@gmail.com (Ye. Seitkulov); saaljawarneh@just.edu.jo (Sh. Aljawarneh)
0000-0003-2115-7130 (S. Atanov); 0009-0001-4994-2491 (S. Seilkhanova); 0000-0002-5172-8339 (Y. Seitkulov); 0000-0003-3972-5300 (Sh.Aljawarneh)

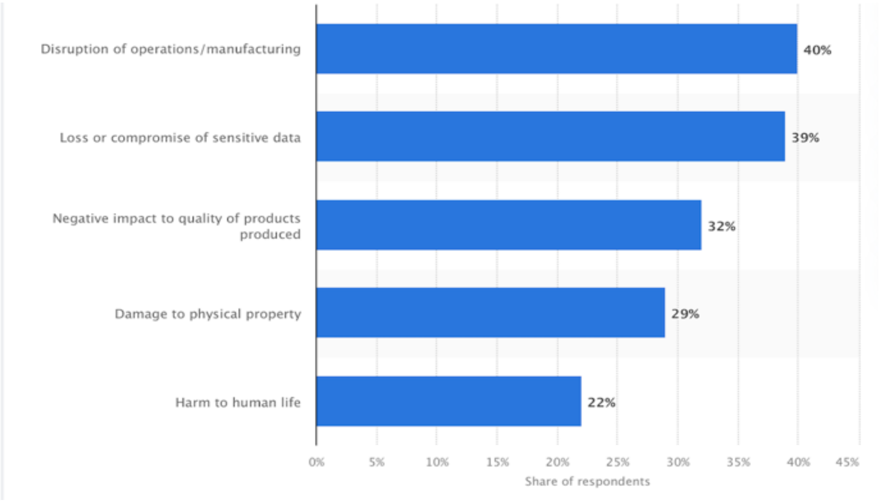


Figure 1: The expected results of global cyber-attacks on automation/robotics systems in 2017 [4]

In addition, over the past decades, industrial automation has been developed without, in fact, paying due attention to safety aspects as we can see in Figure 1. This has led to the fact that there is now a significant amount of equipment in industrial plants that have structural flaws that can be exploited by hackers and cybercriminals [9]. In this article, we will analyze the vulnerabilities characteristic of industrial automation systems and provide recommendations for improving the current situation in this area.

2. Vulnerabilities in industrial robots

In modern conditions, most robots and automated systems are controlled either by human operators directly or using hardware and software systems operating in remote control mode.

Robot security covers two important aspects: information security and control security. Information security focuses primarily on areas related to data encryption, transmission, and subsequent decryption. Device management security focuses on possible attacks aimed at changing the dynamic characteristics of a given system [12].

The [6] study examined the technical details and weaknesses of eight of the most popular industrial programming environments and confirmed that without proper data validation, industrial automation programs can express common vulnerabilities found in applications written in general-purpose languages.

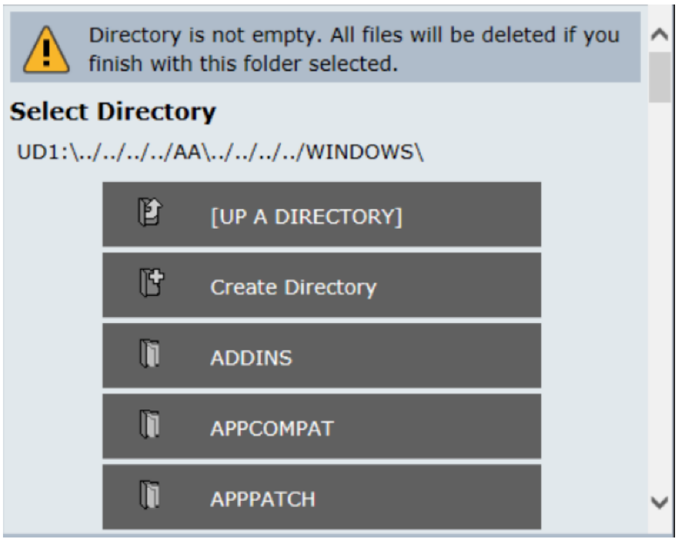
Another issue with legacy industrial automation programming languages, such as the Industrial Robots Programming Language (IRPL), is the lack of tools to identify unsafe patterns in the code. Unlike modern programming languages, legacy IRPL languages do not have tools available to automatically check code for potential vulnerabilities [6, 10].

Let's look at some examples and possible consequences of these applications, taking into account today's cybersecurity threats.

2.1. Data theft

Engineers use a computer-based development environment, often known as "offline programming" (OLP), to customize how robots behave offline. However, when using OLP with remote services enabled, engineers' computers become susceptible to remote attacks. These computers are sometimes located outside the enterprise's internal network, creating the risk of attacks on their computer equipment without access to the enterprise's main network.

Those types of vulnerabilities were discovered in the ROBOGUIDE-HandlingPRO simulator, which is true for version 9 Rev.ZD FANUC ROBOGUIDE-HandlingPRO and earlier versions [3].



Directory is not empty. All files will be deleted if you finish with this folder selected.

Select Directory

UD1:\../../../../AA\../../../../WINDOWS\

Figure 2: Resources of the Remote Unauthorized Access System, ROBOGUIDE-HandlingPRO [3]

Attackers can relatively easily gain access to the simulator on an engineer's computer through the web interface (Figure 2). Moreover, OLP was found to not provide adequate access control to computer resources, allowing remote attackers to exploit vulnerabilities such as security bypasses to gain unauthorized access to system resources [3,12]. It should also be noted that integrators who need to maintain robots in different plants often move potentially compromised computers from one location to another, which can increase the risk of negative consequences from attacks.

2.2. Substitution of commands at the network level

Spoofing industrial robot commands over a network is the process of changing or forging commands sent to the remote control of a robot via a network. The vulnerability occurs when the authentication and security mechanisms used to access the robot over the network are not sufficiently secure. If an attacker can bypass or replace authentication, he will gain access to control the robot. An attacker can intercept or modify commands sent to the robot. This may be done to change its behavior or cause unwanted behavior that may be hazardous to operators or the environment.

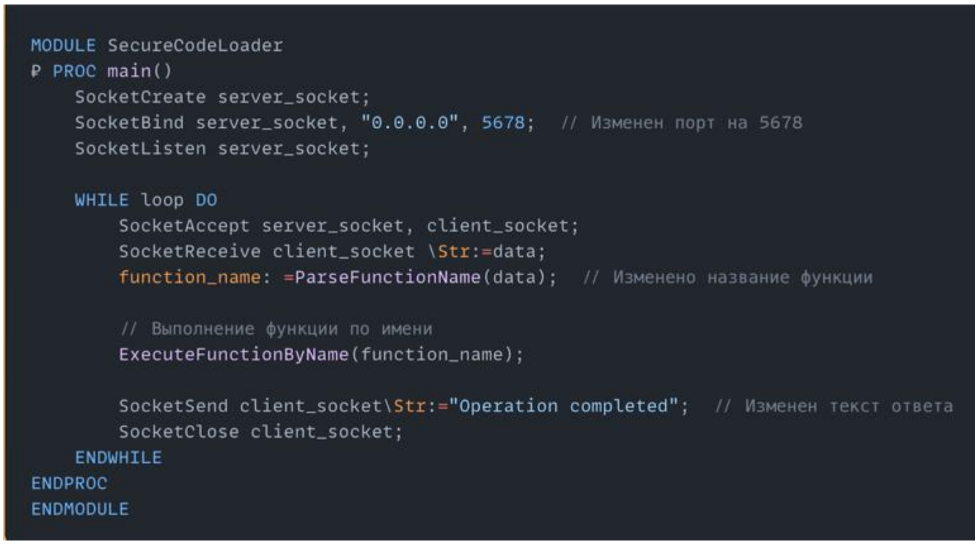
For example, according to [11], a study conducted on seven industrial robots from six different OEMs revealed the ability of malware known as CORMAND2 to bypass existing anomaly detection systems. These systems are typically designed to verify the authenticity of traffic data received through a SCADA system. SCADA (Supervisory Control and Data Acquisition) system is a comprehensive system used in industry and critical infrastructure to monitor, control and collect data about work processes.

The CORMAND2 attack is based on a Man-in-the-Middle (MITM) technique that establishes a new TCP connection between two victims using proxy solutions such as Mitmproxy and Burp Suite. However, these solutions do not apply to industrial robots, since the connection between the robot and SCADA is established and maintained throughout the entire system operation [11]. CORMAND2 overcomes this limitation by introducing the MITM attack and modifying the existing connection between the robot and SCADA without causing anomalies in the robot's movement that would be seen by the SCADA system, in the transmitted data packets, or in the TCP connection itself. This highlights the threat posed by data tampering in industrial systems and requires additional security measures to protect against such attacks.

A similar vulnerability was discovered in 2022 in KUKA.SystemSoftware (KSS), which is the robot controller operating system for most KUKA robot models. KUKA SystemSoftware V/KSS versions prior to 8.6.5 did not provide access controls for the specified interface. If access control is absent or disabled, reading and changing the robot's configuration can be performed without the need for authentication, solely based on access to TCP port 49003 at the network level (CVE-2022-2242l) [5].

2.3. Remote Code Execution vulnerability

RCE (Remote Code Execution) vulnerability is a serious vulnerability in a computer system or software that allows an attacker to execute remote code (often malicious) on the target system (Figure 3).



```
MODULE SecureCodeLoader
₽ PROC main()
    SocketCreate server_socket;
    SocketBind server_socket, "0.0.0.0", 5678;  // Изменен порт на 5678
    SocketListen server_socket;

    WHILE loop DO
        SocketAccept server_socket, client_socket;
        SocketReceive client_socket \Str:=data;
        function_name: =ParseFunctionName(data);  // Изменено название функции

        // Выполнение функции по имени
        ExecuteFunctionByName(function_name);

        SocketSend client_socket\Str:="Operation completed";  // Изменен текст ответа
        SocketClose client_socket;
    ENDWHILE
ENDPROC
ENDMODULE
```

Figure 3: Example code that implements the vulnerable logic

CISA [8] has reported this type of vulnerability that affects motion servers in robots and allows an attacker to execute arbitrary code. Motion servers are programs that run on robot controllers and are used to set up and control the motion of robots. The vulnerability is present in many OEM robots and is not associated with any specific vendor.

For example, ABB [7] reported in 2020 that the OPC server for the AC 800M contained a remote code execution vulnerability, CVE-2021-22284. An authenticated, low-privilege remote user who successfully exploited this vulnerability could insert and execute arbitrary code on a host running the AC800M OPC Server.

3. Discussion

As can be seen from the examples above, the sources of vulnerabilities in industrial robots represent a variety of threats that can compromise the safety and efficiency of robotic systems. These sources include network attacks, software bugs, insufficient security of network protocols, authentication problems, physical threats, and even social engineering [13]. All of these factors can contribute to vulnerabilities that attackers can use to gain access to and control robots, creating potential production and security risks.

To protect against such vulnerabilities, it is important to pay due attention to the cybersecurity of industrial robots.

To help protect against vulnerabilities and reduce risks, future projects should consider the following scientific principles and methods:

- Engineer safety from the start: Safety must be built into the robot design process from the very beginning. Consider potential threats and risks during the design and selection of components [15].

- Secure standards and protocols: Apply standards and protocols to ensure the safety of robots and their network interactions. This includes the use of encryption and authentication tools.
- Regular software updates: Implement mechanisms to regularly update robot software to fix vulnerabilities and improve security.
- Integration of monitoring and incident detection systems: Include monitoring and anomaly detection mechanisms in the robot system to quickly respond to possible attacks and incidents.
- Proactive testing and security analysis: Conduct regular testing of robots for vulnerabilities and weaknesses. This will help identify potential problems before they are used.
- Collaborate with Cybersecurity Experts: Involve cybersecurity experts in robot development and maintenance who can evaluate and improve system security.
- Physical Security: Ensure robots and their components are physically protected from unauthorized access.

Industrial automation remains insecure while traditional software developers have been grappling with the consequences of insecure programming for decades. With the accelerating convergence of information technology (IT) and operational technology (OT), the adoption of secure code development methodologies in industrial automation has become important [14]. Otherwise, serious industrial cyber incidents are possible in the coming years, with impacts in both the digital and physical worlds.

There is currently no globally standardized and mandatory cybersecurity certification for industrial robots. However, such certification may become relevant and necessary in the future, especially if the industry and customers begin to require it as a prerequisite for contracts and the implementation of robotic systems. It is important to note that not all industrial robots are equally vulnerable, and the need for mandatory certification may vary depending on the type of robot and the specific threats.

We propose for future research to implement security for manufacturing robots using lightweight cryptography and granite computing, which represents a promising research direction that could greatly impact the future of industrial automation.

Lightweight cryptography will enable secure communication and data storage in robots' limited computing resources. Granite computing involves performing calculations in a distributed environment with maximum security. Granite computing allows robots to collaboratively process data and perform tasks while minimizing the risk of leaking sensitive information.

4. Conclusion

We concluded that cybersecurity systems in industrial robots often lag behind in development compared to modern methods and threats. One of the reasons is that many robotic systems run on outdated operating systems and software that are not regularly updated or adequately monitored for vulnerabilities. This leaves the door open to potential attacks.

In light of these factors, industrial robot developers should attach great importance to updating and strengthening cybersecurity systems. This includes regular software updates, implementation of modern authentication and authorization methods, and so on. Without such measures, industrial automation systems may remain vulnerable to the ever-changing cyber threat landscape. In addition, we believe that the creation of mandatory cybersecurity certification for industrial robots has the potential to be a significant step in ensuring security in industrial sectors.

Our future research will focus on using lightweight cryptography and granite computing to secure manufacturing robots, a promising direction in industrial automation. We envision that this will enable secure communication and data storage with limited computing resources.

5. Acknowledgements

This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Project No. AP19677508).

6. References

[1] F. Botta, S. Rotbei, S. Zinno and G. Ventre (2023). Cyber security of robots: A comprehensive survey, Intell. Syst. with Applic. https://doi.org/10.1016/j.iswa.2023.200237.

[2] D. Vibekananda and T. Zielińska (2021). Cybersecurity of Robotic Systems: Leading Challenges and Robotic System Design Methodology, Electronics 10, no. 22: 2850. https://doi.org/10.3390/electronics10222850.

[3] TXOne Networks blog, "FANUC Robot Off-Line Programming Path Traversal Vulnerability (CVE-2023-1864)", April 2023. URL: https://www.txone.com/blog/fanuc-robot-off-line-programming-path-traversal-vulnerability-cve20231864/.

[4] A. Petrosyan, "Anticipated results of successful cyber attack against automation and/or robotics systems worldwide as of 2017.", August 2023. URL: https://www.statista.com/statistics/780375/worldwide-anticipated-result-of-cyber-attacks-against-automation-and-or-robotics-systems/.

[5] Kuka, " Security Advisory for the KUKA V/KSS WorkVisual Service Host access control vulnerability (CVE-2022-2242)", 2022. URL: https://www.kuka.com/-/media/kuka-downloads/manual-upload/services/kuka_psirt_advisory_kss_wov_sh_2022-08-04.pdf?rev=8ec87e743f5c43b8b7a3da93bb409b02.

[6] F. Maggi and M. Pogliani (2020). Rogue Automation: Vulnerable and Malicious Code in Industrial Programming.

[7] ABB, " CYBER SECURITY ADVISORY. SECURITY - OPC Server for AC 800M - Remote Code Execution Vulnerability. CVE ID: CVE-2021-22284.", 2022.

[8] Cybersecurity and Infrastructure Security Agency, " ICS Alert. Robot Motion Servers.ICS-ALERT-20-217-01.", 2020. URL: https://www.cisa.gov/news-events/ics-alerts/ics-alert-20-217-01.

[9] A. Bhardwaj, V. Avasthi and S. Goundar (2019). Cyber security attacks on robotic platforms, Netw. Sec., 13–19.

[10] S. Rivera and R. State (2021). Securing robots: An integrated approach for security challenges and monitoring for the robotic operating system (ros)", 2021 IFIP/IEEE Intern. Symp. on Integr. Netw. Managem. (IM), pp. 754–759.

[11] H. Pu, L. He, P. Cheng, J. Chen and Y. Sun (2023). CORMAND2: A Deception Attack Against Industrial Robots", Engineering, ISSN 2095-8099.

[12] J. P. A. Yaacoub, H. N. Noura, O. Salman and A. Chehab (2021). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. Int. Jour. of Inf. Sec. https://doi.org/10.1007/s10207-021-00545-8.

[13] B. Dieber, B. Breiling, S. Taurer, S. Kacianka, S. Rass, and P. Schartner (2017). Security for the robot operating system. Rob. and Auton. Syst., 98, 192–203. https://doi.org/10.1016/j.robot.2017.09.017.

[14] A. Khalid, P. Kirisci, Z. H. Khan., Z. Ghrairi, K. D. Thoben and J. Pannek (2018). Security framework for industrial collaborative robotic cyber-physical systems. Comp. in Indust., 97, 132–145. https://doi.org/10.1016/j.compind.2018.02.009.

[15] M. Pogliani, D. Quarta, M. Polino, V. Vittone, F. Maggi and S. Zanero (2019). Security of controlled manufacturing systems in the connected factory: The case of industrial robots. Jour. of Comp. Virol. and Hack. Tech., 15, 161–175. https:// doi.org/10.1007/s11416-019-00329-8.