Cyber Resilience Issues of Medical Cyber-Physical Systems

Rasim Alguliyev[1], Ramiz Aliguliyev[2], Lyudmila Sukhostat[3]
Institute of Information Technology of MSERA, Baku, Azerbaijan
[1]*r.alguliev@gmail.com*, [2]*r.aliguliyev@gmail.com*, [3]*lsuhostat@hotmail.com*

***Abstract*— Medical cyber-physical system is a critical component of the medical device network. The application of cyber-physical systems in healthcare ranges from patient monitoring to various devices. Existing technologies in this area require constant updating and rapid response to ever-increasing cyberattacks. Among the most well-known threats to medical cyber-physical systems are tampering, phishing, spoofing, data exfiltration, ransomware, DoS, etc. Attackers try to disrupt the operation of medical cyber-physical systems and gain access to confidential medical data. Existing threats violate integrity, confidentiality, and availability. In this regard, various issues of medical cyber-physical systems' cyber resilience are considered in the paper.**

Keywords*— *medical cyber-physical system; cyber resilience; medical device; cyberthreat; cyber-risk

I. Introduction

Modern organizations are increasingly facing cyberthreats that continue to grow exponentially (in complexity and volume). One of the significant industries that is subject to cyberattacks is healthcare [1].

In healthcare infrastructures, medical cyber-physical systems (MCPS) are personal monitoring devices that can record and transmit multiple physiological signals [2]. The most notable feature of MCPS is the feedback that interacts with the physical environment. Data is provided to MCPS through sensors, which feed into control algorithms to manipulate actuators, changing the physical environment.

The integration of connected MCPSs has led to improved diagnosis of various diseases, their treatment, and patient care methodology [3, 4]. However, the introduction of such devices has raised a number of cybersecurity-related issues.

The dependence of healthcare on these devices and their various vulnerabilities requires the adoption of different cybersecurity measures. Cyber resilience is a key objective that will ensure that organizations can continue to operate during a cyberattack on medical devices.

Dupont et al. (2023) [5] define cyber resilience as the capacity to withstand, recover from, and adapt to external shocks caused by cyber risks. Cyber resilience considers not only information technology cybersecurity but also cyber risks. It includes the interaction of people, devices, and algorithms.

MCPS vulnerabilities can lead to various risks, including delays in patient care, device failure and shutdown, theft of patient personal data, and claims for monetary gain, among others [6]. These can compromise healthcare operations, as well as availability, confidentiality, and integrity [7].

The significant increase in vulnerabilities highlights the need for robust measures and steps in ensuring MCPS cybersecurity and cyber resilience [8].

II. Cyber Resilience Issues of Medical Cyber-Physical Systems

- *Privacy protection* is paramount for healthcare cyber resilience [9]. DoS (denial of service) attacks, as well as ransomware, can limit access to electronic health records. The integrity of healthcare data can be compromised due to disruption of wireless access to medical devices.
- *Cloud computing* [10]. Despite the numerous benefits of cloud computing in healthcare for data storage and analysis, it may expose patient data to risk and raise personal data protection concerns.
- *Healthcare application security*. The large volume of healthcare data generated may lead to privacy and data integrity breaches. To address these issues, improved privacy policies and robust security measures are needed to protect patient data.
- *Human factor*. Phishing attacks and weak passwords increase insider threats and highlight the importance of cybersecurity awareness among healthcare professionals. Incorporating the human factor into cyber resilience risk assessments is essential to understanding and mitigating the impact of malicious cyberattacks on healthcare.

III. Cyberthreats to Medical Cyber-Physical Systems

The emergence of MCPS devices, both implantable and wearable, has revolutionized healthcare [9]. With an expected number of 50 billion connected devices by 2028, MCPS have become indispensable tools for monitoring patient health.

Medical devices include cochlear implants, brain stimulators, cardiac defibrillators, gastric stimulators, insulin pumps, etc. [11]. Implantable medical devices have limited resources. This limits the self-protection of such devices. Such devices are often susceptible to buffer overflow when receiving false signals. Pacemakers, mechanical ventilators, and kidney

DOI: 10.25045/SPCDH4.0.2025.01

replacement devices can be completely disabled by cyberattacks [12]. Most wearable devices are susceptible to man-in-the-middle attacks [13]. An attacker can intercept communications between a doctor and a patient and gain access to confidential information (Fig. 1).

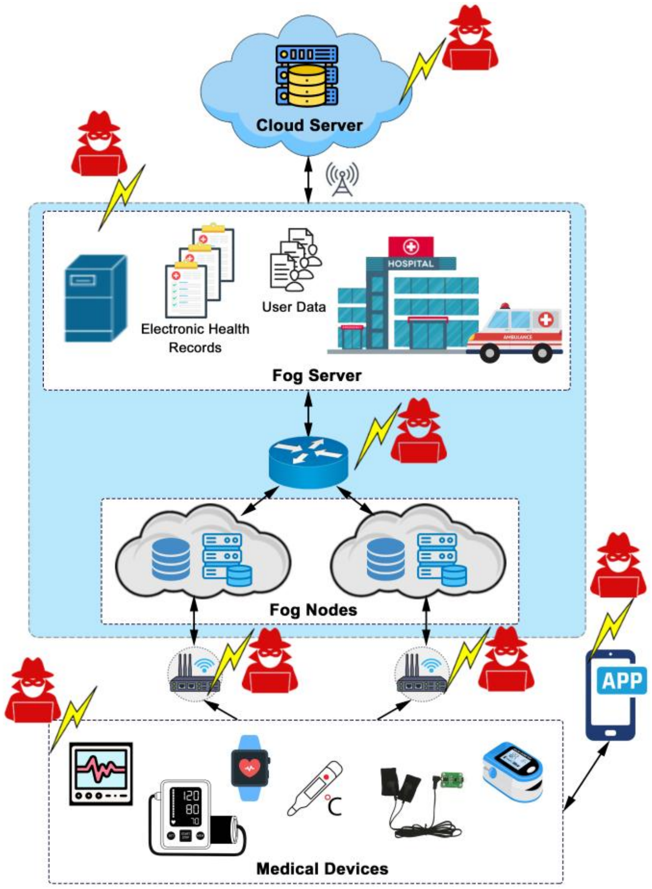

Figure 1. MCPS architecture reflecting cyberthreat emergence points.

Software problems in healthcare facilities pose a risk and can harm the patient. An example is the Therac-25 accelerator failure [14]. In addition, a drug delivery machine can cause critical availability issues [15].

The number of cyberattacks on healthcare has increased in recent years [16]. Thus, one of the most recent incidents occurred in the UK in 2024. Hackers attacked the company Synnovis, which analyzes blood transfusions. The attack occurred after malware was introduced into its IT system. The virus blocked the entire system, and the attackers demanded a ransom to regain control of the system.

IV. VULNERABILITIES OF MEDICAL CYBER-PHYSICAL SYSTEMS

A. *Electronic health record vulnerabilities* [17]:

- Cross-site scripting;
- File inclusion;
- HTTP response splitting;
- Control flow attacks;
- Reflection injection;
- Encryption and decryption issues related to patient medical history information.

B. *Some of the most well-known vulnerabilities in medical devices include:*

- Weak passwords.
- Command injection flaw. These attacks include SQL injection.
- Insecure web interface. Attackers can use intrusive methods to track users, leading to data leakage.
- No account lockout. Continuous generation of different passwords allows attackers to access data.

C. *Network vulnerabilities include:*

- Unencrypted communications and data storage.
- Open ports. Although all ports are open by default, security can be improved.
- Insecure network services have vulnerabilities related to ransomware infections, such as Petya or NotPetya.
- Insecure cloud interface uses insecure protocols without SSL (Secure Socket Layer) encryption, which can allow an attacker to reset a password or search for login credentials.
- Lack of authorization. Authorization is required to access medical data and perform actions, no matter how destructive.

V. CYBER RESILIENCE STANDARDS IN HEALTHCARE

The standards below describe contextual constraints that need to be used in healthcare systems to provide cyber resilience.

- NIST has released NIST SP 800-160, "Developing Cyber Resilient Systems: A Systems Security Engineering Approach," which defines a set of cyber-resilience techniques [18]. Each technique includes standard methodologies and practices for developing systems that are resilient to attack.
- The NIST SP 1800-1 [19] guide provides a cybersecurity reference design for healthcare organizations. It considers the healthcare information that caregivers exchange through mobile devices.
- ISO 27799:2016 focuses on the confidentiality, integrity, and availability of healthcare data. It explains the controls in ISO/IEC 27002 so that it suits the cybersecurity of healthcare information.
- NIST SP 800-66r1 [20] supports the implementation of the Health Insurance Portability and Accountability Act (HIPAA). It concentrates on protecting the cybersecurity properties of confidentiality, integrity,

and availability for Electronically Protected Health Information (EPHI).

- The ISO/IEC 27032:2012 guide describes how cybersecurity is related to information, network, internet, and critical infrastructure security.
- The NIST SP 800-82r2 [21] report presents threats and vulnerabilities common to industrial control systems and suggests mitigation controls for cybersecurity risks.
- The ISO/TR 22100-4:2018 report contributes to the consideration and resolution of cyber threats that can impact a system's safety.
- The ISO/IEC 27001:2013 standard addresses cybersecurity risks, along with their assessment and handling.

VI. Managing Cybersecurity Risks in MCPS

For optimal risk management, cybersecurity must be proactive and multi-layered.

- Risk assessment enables the detection of potential consequences of cyberattacks on critical MCPS data.
- Risk mitigation is possible through identification and remediation of various vulnerabilities, including patching processes, preventive controls, and incident response protocols [9, 22].
- Monitoring. Continuous monitoring of MCPS using modern security solutions enables rapid detection of cyberattacks.
- Knowledge sharing and collective response to cyber threats [9].

VII. Application of artificial intelligence technologies to MCPS

AI-based methods widely use virtualization, remote big data processing, various communication technologies, etc. They are capable of ensuring cybersecurity and cyberresilience of such systems from information-control cyber threats. The following areas of AI application in healthcare can be highlighted:

- Application of Explainable Artificial Intelligence (XAI). AI will help in clinical decision-making, reduce medical errors, and improve the quality of patient care [23].
- Cognitive imagery and computer vision. Using methods based on deep learning enriched with cognitive approaches will improve the accuracy and efficiency of diagnosis and treatment [24].
- Differential diagnostics involving additional data can confirm or exclude hypotheses [25].
- Validation of decision support systems. Value-based engineering is a proactive consideration of potential risk in decision support systems for critical applications [26].
- Convergence of artificial intelligence systems. Integrating linguistic and visual information is an essential task in decision making [27].

VIII. Cybersecurity and cyber resilience measures for MCPS

Ensuring the cyber resilience and cybersecurity of MCPS requires data analysis and the implementation of appropriate measures to mitigate and limit the consequences of incidents (Table I):

- Raising awareness.
- Implementing authentication, authorization, and audit-based systems.
- Cryptographic key exchange between developers and medical devices [28-30].
- Wireless networks should be regularly tested and updated.
- Using firewalls, routers, and network segmentation to protect systems.
- Using a proxy server prevents attackers from decrypting messages between devices [31].
- Disabling all unused ports.

TABLE I. MCPS Threats and Mitigation Measures

Cyberthreat	**Measures to prevent cyberattacks**
Ransomware	Zero trust architecture implementation, multi-factor authentication, privileged access management, offline backup
Phishing	spam filtering, domain authentication protocols, cybersecurity awareness
DoS	leveraging proactive solutions, effective response strategies, software updates
Man in the Middle	data encryption, multi-factor authentication, automatic updates on all devices and applications, network traffic monitoring, implementing secure protocols

IX. Conclusion

In this paper, the issues of ensuring the cyber resilience of MCPS were studied. A brief study of cyberthreats to such systems was also conducted. Standards for cyber resilience in healthcare were provided. The use of artificial intelligence technologies in MCPS was analysed. The article presented a number of measures to ensure the cybersecurity and cyber resilience of MCPS, which need to be addressed in the future.

Acknowledgment

This work was supported by the Azerbaijan Science Foundation – Grant № AEF-MCG-2023-1(43)-13/04/1-M-04.

REFERENCES

[1] C. M. Mejía-Granda, J. L. Fernández-Alemán, J. M. Carrillo-de-Gea, and J. A. García-Berná, "Security vulnerabilities in healthcare: an analysis of medical devices and software," Medical & Biological Engineering & Computing, vol. 62, pp. 257–273, 2024. https://doi.org/10.1007/s11517-023-02912-0

[2] O. Kocabas, T. Soyata, and M. K. Aktas, Emerging security mechanisms for medical cyber physical systems, IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 13, no. 3, pp. 401–416, 2016. https://doi.org/10.1109/TCBB.2016.2520933

[3] F. Xiao, Q. Miao, X. Xie, L. Sun, and R. Wang, "Indoor anti-collision alarm system based on wearable Internet of Things for smart healthcare," IEEE Communications Magazine, vol. 56, no. 4, pp. 53–59, 2018. https://doi.org/10.1109/MCOM.2018.1700706

[4] J. Phua, L. Weng, L. Ling, M. Egi, C. Lim, J. V. Divatia, B. R. ShresthaY. M. Arabi, J. Ng, C. D. Gomersall, M. Nishimura, Y. Koh, and B. Du, "Intensive care management of coronavirus disease 2019 (COVID-19): Challenges and recommendations," The Lancet Respiratory Medicine, vol. 8, no. 5, pp. 506-517, 2020. https://doi.org/10.1016/S2213-2600(20)30161-2

[5] B. Dupont, C. Shearing, M. Bernier, and R. Leukfeldt, "The tensions of cyber-resilience: From sensemaking to practice," Computers & Security, vol. 132, 103372, 2023. https://doi.org/10.1016/j.cose.2023.103372

[6] GAO, "Healthcare Cybersecurity: HHS Continues to Have Challenges as Lead Agency," GAO-25-107755, 2024. [Online]. Available: https://www.gao.gov/assets/gao-25-107755.pdf

[7] E. Iannone, R. Guadagni, F. Ferrucci, A. De Lucia, and F. Palomba, "The secret life of software vulnerabilities: a large-scale empirical study," IEEE Transactions on Software Engineering, vol. 49, no. 1, pp. 44-63, 2022. https://doi.org/10.1109/TSE.2022.3140868

[8] G. Marquez, H. Astudillo, and C. Taramasco, "Security in telehealth systems from a software engineering viewpoint: A systematic mapping study," IEEE Access, vol. 8, pp. 10933–10950, 2020. https://doi.org/10.1109/ACCESS.2020.2964988

[9] A. Abdi, H. Bennouri, and A. Keane, "Emerging cyber risks & threats in healthcare systems: A case study in resilient cybersecurity solutions," In Proc. of IEEE Mediterranean Conference on Embedded Computing (MECO), 2024, pp. 1-8. https://doi.org/10.1109/MECO62516.2024.10577790

[10] O. Tomashchuk, "Threat and risk management framework for ehealth IoT applications," In Proc. of the 24th ACM International Systems and Software Product Line Conference, 2020, pp. 120–126. https://doi.org/10.1145/3382026.3431250

[11] P. Kumar, A. Singh, and A. Sengupta, "Securing cyber-resilience in healthcare sector," In Cyber Security in Intelligent Computing and Communications. Studies in Computational Intelligence, vol 1007, R. Agrawal, J. He, E. Shubhakar Pilli, and S. Kumar, Eds., Singapore: Springer, 2022. https://doi.org/10.1007/978-981-16-8012-0_17

[12] A. Boddy, W. Hurst, M. Mackay, and A. E. Rhalibi, "A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures," In Proc. of the 1st International Conference on Internet of Things and Machine Learning, 2017, pp. 1-7. https://doi.org/10.1145/3109761.3109793

[13] M. A. Allouzi and J. I. Khan, "Identifying and modeling security threats for IoMT edge network using Markov chain and common vulnerability scoring system (CVSS)," 2021, arXiv preprint arXiv:2104.11580.

[14] A. J. Burns, M. E. Johnson, and P. Honeyman, "A brief chronology of medical device security," Communications of the ACM, vol. 59, no. 10, pp. 66–72, 2016. https://doi.org/10.1145/2890488

[15] L. Coventry and D. Branley, "Cybersecurity in healthcare: a narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48–52, 2018. https://doi.org/10.1016/j.maturitas.2018.04.008

[16] J. Beavers and S. Pournouri, "Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions," In Blockchain and Clinical Trial. Advanced Sciences and Technologies for Security Applications, H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, and H. Al-Khateeb, Eds., Cham: Springer, 2018. https://doi.org/10.1007/978-3-030-11289-9_11

[17] M. Farhadi, H. Haddad, and H. Shahriar, "Static analysis of HIPPA security requirements in electronic health record applications," In Proc. of IEEE International Computer Software and Applications Conference, 2018, pp. 474–479. https://doi.org/10.1109/COMPSAC.2018.10279

[18] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing cyber resilient systems: a systems security engineering approach," Technical Report NIST, 2021. https://doi.org/10.6028/NIST.SP.800-160v2r1

[19] G. O'Brien, S. Edwards, K. Littlefield, N. McNab, S. Wang, and K. Zheng, "Securing wireless infusion pumps in healthcare delivery organizations," NIST Special Publication, National Institute of Standards and Technology, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-8.pdf

[20] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," Technical Report NIST SP 800-66r1, National Institute of Standards and Technology, Gaithersburg, MD, 2008. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=890098

[21] R. Ross, R. Graubart, D. Bodeau, and R. McQuaid, "Systems security engineering cyber resiliency considerations for the engineering of trustworthy secure systems," Technical Report NIST, 2018. https://doi.org/10.6028/NIST.SP.800-160v2

[22] S. G. Langer, "Cyber-security issues in healthcare information technology," Journal of Digital Imaging vol. 30, no. 1, pp. 117–125, 2017. https://doi.org/10.1007/s10278-016-9913-x

[23] R. Rosenbacke, Å. Melhus, M. McKee, and D. Stuckler, "How explainable artificial intelligence can increase or decrease clinicians' trust in AI applications in health care: Systematic review," JMIR AI, vol. 3, e53207, 2024. https://doi.org/10.2196/53207

[24] H. N. Fakhouri, S. Alawadi, F. M. Awaysheh, F. Alkhabbas, and J. Zraqou, "A cognitive deep learning approach for medical image processing," Scientific Reports, vol. 14, no. 1, pp. 1-17, 2024. https://doi.org/10.1038/s41598-024-55061-1

[25] O. Kostopoulou and B. Delaney, "AI for medical diagnosis: does a single negative trial mean it is ineffective?" The Lancet Digital Health, vol. 7, no. 2, pp. e108-e109, 2025. https://doi.org/10.1016/j.landig.2025.01.005

[26] P. Jayakumar, K. D. Oude Nijhuis, J. H. Oosterhoff, and K. J. Bozic, "Value-based Healthcare: Can Generative Artificial Intelligence and Large Language Models be a Catalyst for Value-based Healthcare?" Clinical Orthopaedics and Related Research®, vol. 481, no. 10, pp. 1890-1894, 2023. https://doi.org/10.1097/CORR.0000000000002854

[27] Y. Lu and A. Wang, "Integrating language into medical visual recognition and reasoning: A survey," Medical Image Analysis, vol. 102, 103514, 2025. https://doi.org/10.1016/j.media.2025.103514

[28] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," ACM Transactions on Computing for Healthcare, vol. 2, no. 3, pp. 1-44, 2021. https://doi.org/10.1145/3453176

[29] K. Rindell, J. Ruohonen, J. Holvitie, S. Hyrynsalmi, and V. Leppänen, "Security in agile software development: A practitioner survey," Inf Softw Technol 131:106488, 2021. https://doi.org/10.1016/j.infsof.2020.106488

[30] A. Serhane, M. Raad, R. Raad, and W. Susilo, "PLC code-level vulnerabilities," in Proc. of IEEE International Conference on Computer and Applications (ICCA), 2018, pp. 348–352. https://doi.org/10.1109/COMAPP.2018.8460287

[31] E. Marin, D. Singelée, B. Yang, V. Volski, G. A. Vandenbosch, B. Nuttin, and B. Preneel, "Securing wireless neurostimulators," In Proc. of the eighth ACM conference on data and application security and privacy, 2018, pp. 287-298. https://doi.org/10.1145/3176258.3176310