Combining Experimental and Analytical Methods for Penetration Testing of AI-Powered Robotic Systems

Artem Abakumov and Vyacheslav Kharchenko

National Aerospace University «Kharkiv Aviation Institute», Chkalova, str. 17, Kharkiv, 61070, Ukraine

Abstract

AI-powered robotic systems (RS) are increasingly vulnerable to cyber-attacks targeting their software and hardware. To evaluate the risks of successful cyber-attacks, it is necessary to apply various assessment techniques. This study aims to propose a risk-oriented approach to assess the cyber security and safety of the RS and choose countermeasures to prevent critical failures. The proposed approach includes a classification table for complex analytical techniques such as Intrusion (Failure) Modes and Effect Criticality Analysis (I(F)MECA), Attack Tree Analysis (ATA), and Risks and Vulnerabilities assessment (R&VA), as well as experimental methods such as Penetration Testing (PT) and F&VIT (Faults and Variabilities Injection Testing). The approach also involves combining these methods with PT to reduce execution time, improve completeness and trustworthiness, and decrease the costs of assessment. The paper focuses on RS architecture, using a collaborative robot as an example.

Keywords

Robotics, safety, cybersecurity, penetration testing, IMECA, AI-powered robots

1. Introduction

Robotic systems (RS) are used daily in manufacturing to increase the efficiency, speed, and accuracy of production processes. The increasing use of RS obliges manufacturers to prioritize safety and cybersecurity issues during the development, deployment, and operation of these systems. Safety is a key factor in the development and use of the RS. These systems can cause serious injuries to workers in case of malfunction or improper use. In addition to safety risks, cybersecurity is also a critical issue for RS, especially in cases where the components of these systems are connected to a single network. RS must be safe and well-protected. If not, they can become dangerous tools capable of causing chaos and significant harm to their environment and the people they provide services to. [1] Humanity has already faced some of the consequences of serious cybersecurity problems with IoT devices that have caused damage to companies and businesses, as well as to individual users. Problems with the safety and cybersecurity of the RS can have a much greater impact. There have been notable incidents involving robots, such as:

- A security robot at the Stanford Shopping Centre in Silicon Valley hit a child, fortunately, the child was not seriously injured.
- A Chinese-made robot crashed at a trade show in Shenzhen, breaking a shop window and injuring a person who was nearby.
- In 2007, a malfunctioning robotic gun killed nine soldiers and seriously injured 14 others during the shooting.
- According to recent research, robotic surgery is associated with 144 deaths in the United States.

Indeed, these incidents demonstrate how dangerous compromised or hacked RS can be. Despite the obvious need for ensuring the safety and cybersecurity of the RS, the heterogeneity of these systems,

COLINS-2023: 7th International Conference on Computational Linguistics and Intelligent Systems, April 20–21, 2023, Kharkiv, Ukraine
EMAIL: a.i.abakumov@csn.khai.edu (A. Abakumov); v.kharchenko@csn.khai.edu (V. Kharchenko)
ORCID: 0000-0002-7742-6515 (A. Abakumov); 0000-0001-5352-077X (V. Kharchenko)

as well as their large numbers and resource constraints, hinder the implementation of powerful security measures.

Moreover, robots powered by AI are being used by industries to bridge the gap between humans and technology, solve issues, and adapt business strategies to changing customer expectations. Robots with AI capabilities operate in shared environments to keep employees safe in industrial workplaces. Additionally, they work independently to complete complicated operations such as cutting, grinding, welding, and inspection [2]. Here is a sum-up of the different applications where AI can be used in the RS:

- Machine learning allows RS to learn from their environment and experiences. It enables robots to adapt and improve their performance over time. For instance, a robot may learn to recognize objects in its environment by analyzing images from a camera.
- Computer vision is another area of AI that is extensively used in robotics. It involves teaching robots to interpret visual data from cameras, sensors, and other sources. Robots can use this information to navigate their environment, identify objects, and avoid obstacles.
- Natural language processing (NLP) is the field of AI that deals with teaching robots to understand human language. This enables robots to interact with humans more effectively. For example, a robot may be trained to understand spoken commands and respond appropriately.
- Autonomous navigation: Autonomous navigation is the ability of RS to move around in their environment without human intervention. This is achieved through a combination of sensors, machine learning, and other AI techniques. Autonomous navigation is particularly important in applications such as self-driving cars and drones.
- Predictive maintenance involves using AI to predict when a robot or its components are likely to fail. This enables preventive maintenance to be performed, which can help to reduce downtime and repair costs.

AI is playing an increasingly important role in robotics, enabling robots to perform tasks that would have been impossible or difficult to achieve without it. But the use of AI entails potentially new threats to RS. For example, AI technologies can be targeted to bypass AI-based threat detection systems. [3] As a result, it is very important to build not only a functionally powerful, but also a safe and secure AI-powered RS that is ready not only for traditional cyberattacks but also for AI-powered attacks. To meet this requirement properly planned and executed measures may help ensure the safety and cybersecurity of the RS. Evaluation of the readiness of the RS for unusual situations and cyberattacks, as well as testing of safety and cybersecurity, should be conducted at every stage of the RS life cycle, from design and development to implementation and operation.

The readiness assessment may include an evaluation of potential threats, identification of critical components and processes that need to be protected, and identification of strategies for detecting and recovering RS after an incident.

Safety and cybersecurity testing can be conducted through various analytical and experimental methods, such as penetration testing (PT), risk and vulnerability assessment (R&VA), Attack Tree Analysis (ATA), Intrusion (Failure) Modes, and Effect Criticality Analysis (I(F)MECA) and Variabilities Injection Testing (F&VIT) as well as a combination of these methods to expand the test coverage and improve the quality of testing.

2. Related works

Our study collected and analyzed existing works in the development and use of methods for ensuring the safety and cybersecurity of the RS.

The authors of the article [4] propose a standardized methodology for conducting security assessments in robotics. They also emphasize the importance of cybersecurity in robotics as robots become increasingly autonomous and connected to other devices. This paper presents the Robot Security Framework (RSF), which consists of a set of guidelines and procedures for identifying, analyzing, and mitigating security risks in robotic systems. The RSF is designed to be flexible and adaptable to different types of robots and environments. The article provides a detailed overview of the

RSF and demonstrates its application. According to the authors, RSF can improve the safety of robotics and facilitate the development of safe and reliable robots.

The article [5] discusses the importance of conducting Robot Operating System (ROS) PT to identify and mitigate possible security risks. The authors provide a detailed overview of the ROS architecture and its security features, as well as common vulnerabilities that may be present in ROS-based systems. The article also offers a case study of the PT approach for ROS-based robots, including tools and techniques used to test and identify security weaknesses. The main idea of the article is that conducting regular PT on ROS-based systems is extremely important to ensure their security and protection against possible cyberattacks.

In this paper [6] a security assessment was conducted for the collaborative robot (cobot) Franka Emika Panda. The authors analyzed the potential areas of cyberattacks and their potential impact on the security and cybersecurity of the cobot. The study is based on the basics of The Open-Source Security Testing Methodology (OSSTM) and the recommendations of The Open Worldwide Application Security Project (OWASP).

The authors of this informative paper [1] have covered a few RS from different manufacturers during their practical research and identified critical issues related to the security and cybersecurity of these systems. This paper also describes in detail the potential threats that a compromised RS may pose, as well as the security and cybersecurity issues identified in these systems.

In the study [7] another cobot model, Universal Robots UR3, was considered as the RS under study. By using a simulator of this RS, the authors investigated the security of the cobot firmware update process. This analysis revealed four hitherto unknown vulnerabilities in the software update process that could lead to a complete compromise of the cobot.

In addition, the authors of [8] theoretically and experimentally investigated the challenges and security implications of the modern RS. The authors of this paper reviewed the standard architecture of the IRS and analyzed it from the point of view of system safety and cybersecurity. An attacker model was also proposed, with the help of which the authors showed how an attacker can compromise the cobot controller and gain full control over it, which can lead to significant changes in the production process, which may result in manufacturing defects. The authors also investigated the potential consequences of such cyberattacks and experimentally assessed the resistance of widespread robots to these types of attacks.

Also, in this article [9] the authors summarized the results of some of the previously mentioned studies in the field of security and cybersecurity of the RS and analyzed the main problems and difficulties that hinder the development of robot security, among which were the lack of awareness of manufacturers in the issue of security and cybersecurity of robotic systems, the lack of real test benches, the weak security of firmware and communication protocols of RS, as well as the limited computing resources of these systems.

Previously, we considered the issue of conducting PT of IoT systems in [10] and proposed a model for conducting such testing for the RS using the semi-formal IMECA method as a tool for assessing the criticality of the impact of identified threats, vulnerabilities, and potential cyberattacks on the RS in [11].

This work is the next step in our research in the field of RS penetration testing. The purpose of this study is to develop a comprehensive method for ensuring the safety and cybersecurity of the RS that will provide maximum test coverage, considering the detection of design anomalies of evolution systems and the evolution of sets and types of vulnerabilities at each level of development, deployment, and use of RS.

3. Methods

During our study, we have researched various methods of safety & cybersecurity assessment. These methods' classification by the type of method is summarized in Table 1. In the safety and cybersecurity field, the analytical method might involve using mathematical models or logical frameworks to identify potential safety or security risks and to develop risk management strategies. For example, an analyst might use attack tree analysis (ATA) to identify potential threats in a safety-critical system and to develop strategies for preventing those threats. The experimental method might involve conducting

controlled experiments to evaluate the effectiveness of safety or security measures or to test the performance of safety-critical systems. For example, an experiment might involve possible system vulnerability exploitation (in the context of PT) testing to assess system response to such actions. The analytical-experimental method might involve combining elements of both approaches to develop and test new safety or security technologies or to refine existing ones. For example, an analyst might use data from experiments to refine a mathematical model of a safety-critical system and to identify potential improvements to the system.

Table 1
Safety & cybersecurity methods classification by type

Type	Name
Analytical	Risk & Vulnerability Assessment (R&VA)
	Attack Tree Analysis (ATA)
Experimental-analytical	Intrusion (Failure) Modes and Effect Criticality Analysis (I(F)MECA)
Experimental	Penetration Testing (PT)
	Faults and Variabilities Injection (FVI) testing

3.1. Risk & Vulnerability Assessment

This method is often used to identify and evaluate potential weaknesses and vulnerabilities in a system to develop a plan to address and mitigate these vulnerabilities and maintain ongoing security. R&VA typically consists of 6 stages [12]:

- Creating baseline: Establishing goals with management and obtaining approval before beginning the assessment.
- Vulnerabilities assessment (VA): Conducting a vulnerability scan to identify weaknesses in the system.
- Risk assessment (RA): Categorizing vulnerabilities based on their impact level and creating a plan to address them.
- Mitigation: Mitigating vulnerabilities according to their impact level.
- Verification: Verifying that the plan was effective in addressing the vulnerabilities.
- Monitor: Regularly monitor and update the system to ensure ongoing security.

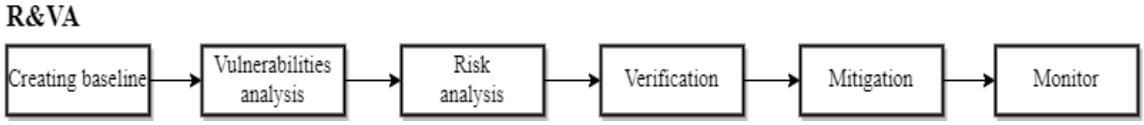

Figure 1: R&VA stages

3.2. Attack Tree Analysis

Attack Tree Analysis (ATA) provides a formal, methodical way of describing the security of systems, based on varying attacks. It represents attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes [13]. The stages of ATA are:

- Define the scope and goal of the analysis: The first step is to clearly define the system or organization being analyzed and the goal of the analysis. This will help to focus the analysis on the most important threats.

- Identify the potential threats: The next step is to brainstorm all the potential threats that could occur against the system or organization. This can be done through various methods such as brainstorming sessions or by analyzing historical attack patterns.
- Create an AT: The AT is a hierarchical diagram that shows the different stages of an attack, from the initial point of entry to the final objective of the attacker. The tree is built by breaking down the attack scenario into smaller, more manageable pieces.
- Analyze each node: Once the AT is created, each node is analyzed to determine the likelihood and impact of the attack occurring. This helps to prioritize the threats and determine which ones require the most attention.
- Develop countermeasures: After the analysis is complete, countermeasures are developed to address the identified threats. These can range from technical controls such as firewalls and access controls to procedural controls such as training and awareness programs.
- Test and validate the countermeasures: Finally, the effectiveness of the countermeasures is tested and validated to ensure that they are effective in addressing the identified threats. This can be done through various methods such as PT or scenario-based exercises.

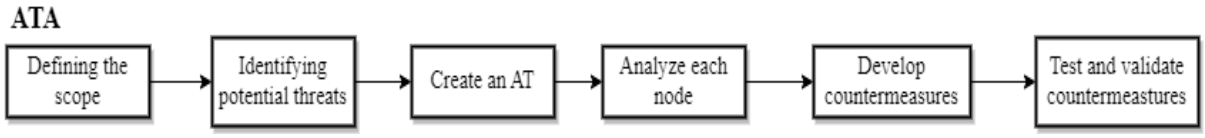

Figure 2: ATA stages

3.3. Intrusion (Failure) Modes and Effect Criticality Analysis

System analysis is aimed at showing the characteristics of the system as availability, security, and vulnerability through using two techniques the IMECA (for intrusion) and FMECA (for failure) [14,15]. The main stages of an I(F)MECA include:

- System/Process Analysis: In this stage, the system or process is broken down into its components or steps, and each is analyzed to identify potential intrusion/failure modes.
- Intrusion/Failure Mode Analysis: Once potential intrusion/failure modes are identified, they are analyzed to determine their effects on the system or process. This stage looks at how each intrusion/failure mode could affect the performance, reliability, safety, cybersecurity, or other critical aspects of the system/process.
- Criticality Analysis: After analyzing the effects of each intrusion/failure mode, the next stage is to determine the criticality of each intrusion/failure mode. This involves assigning a score to each intrusion/failure mode based on factors such as the likelihood of occurrence, the severity of impact, and detectability.
- Risk Mitigation: Finally, based on the criticality scores, risk mitigation strategies are developed to address the most critical intrusion/failure modes. This may involve redesigning the system or process, implementing additional safeguards or redundancy, or developing contingency plans.

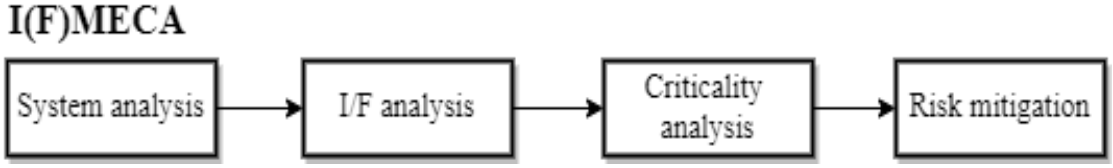

Figure 3: I(F)MECA stages

3.4. Penetration Testing

PT is a widely used methodological approach, that allows assessing the security of a system by simulating a real attack [16]. Qualitatively conducted testing allows you to determine the level of security of the system and the presence of vulnerabilities in it, identify the most likely ways to violate the established security policy, and determine how well the complexity of security features of such a system works. [10] Several methodological approaches to PT have been discussed in detail in [11]. Usually, PT includes the next 5 stages:

- Planning and reconnaissance: This stage involves gathering information about the target system, such as its network topology, IP addresses, and applications, to identify potential entry points and vulnerabilities.
- Scanning: In this stage, various scanning tools are used to identify and map out the target system's vulnerabilities, such as open ports, services, and potential vulnerabilities in the application or operating system.
- Gaining access: Once potential vulnerabilities have been identified, attempts are made to exploit them to gain access to the system or application.
- Maintaining access: If access is successfully gained, the penetration tester attempts to maintain access to the system for as long as possible, to further evaluate its security.
- Analysis and reporting: Finally, the results of the PT are analyzed, and a report is generated, which details the vulnerabilities that were identified, the methods used to exploit them, and recommendations for addressing and mitigating these vulnerabilities.

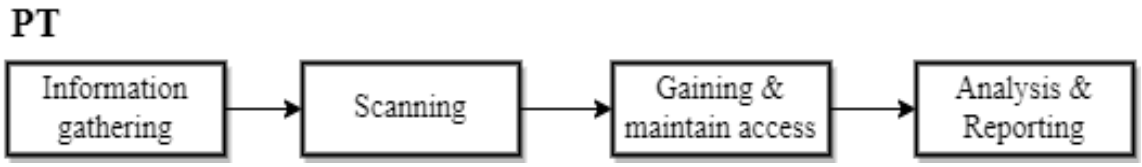

Figure 4: PT stages

3.5. Faults and Variabilities Injection Testing

FVI testing is a commonly used experimental technique to assess the dependability of microprocessor-based systems [18] such as RS also. The general stages of FVI testing are as follows:

- Planning: The FVI testing strategy is defined in this stage. This includes identifying the system components to be tested, selecting the types of faults and variabilities to be introduced, and determining the testing environment.
- Injection: This stage involves introducing faults and variabilities into the system. The types of faults and variabilities that can be injected include hardware faults (such as memory errors and disk failures), software faults (such as coding errors and logic errors), and environmental variabilities (such as network latency and power fluctuations).
- Observation: In this stage, the system's response to the injected faults and variabilities is observed. This involves monitoring system behavior, gathering performance metrics, and identifying any unexpected behaviors or errors.
- Analysis: In this stage, the data gathered during observation is analyzed to identify patterns and root causes of faults and variabilities. This helps determine areas of the system that need improvement and identify potential solutions.
- Reporting: Finally, a report is generated that summarizes the findings of the FVI testing. The report may include recommendations for improving the system's resilience and dependability, as well as any identified areas for further testing and analysis.

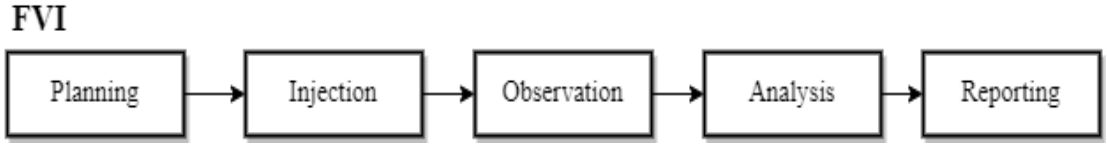

Figure 5: FVI testing stages

3.6. Modeling methods combinations

During our study, we analyzed each stage of all these methods and developed a combined safety & cybersecurity assessment cycle shown in Figure 6. We summarized similar stages and grouped them, for example, we noticed that all 5 methods have an initial stage when testers perform a pre-processing task/activity without direct interaction with the target system like planning, identifying the assets, etc. We simply named this stage a Pre-processing stage.

Most parts of the other stage were processed in the same way, but we also highlighted the such type of possible testing stages like System Preparation which describes the additional steps to be done (for example, vulnerabilities injection) before the start of the assessment process.

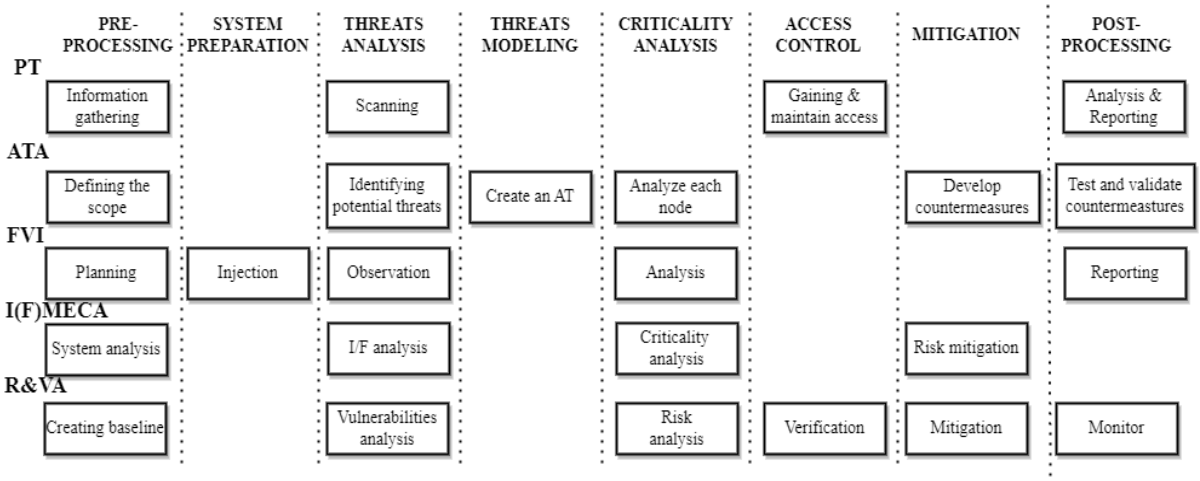

Figure 6: Combined cycle of safety & cybersecurity assessment

4. Experiment

The choice of method depends on the specific problem being addressed and the resources available. Using a combination of approaches can help to ensure that safety and security risks are effectively identified and managed and that safety-critical systems are reliable and effective. In our previous research [9] we already tried to combine PT with I(F)MECA to assess the criticality of possible RS threats. During this work, we want to analyze a few more options of existing safety and cybersecurity assessment methods to be combined with PT. As an object of study, we will keep using the RS architecture, as we did before, but this time we will use a black-box view described in Figure 7.

The programmer or the operator issues high-level commands to the controller (e.g., via a REST API, with a program on the HRI interface, moving the joystick). The controller translates such commands into low-level inputs for the actuators (e.g., end effectors, servo motors) through dedicated I/O interfaces. The controller is also reachable through a remote-access interface. [9] Also, cobots can be equipped with AI-powered components such as 2D cameras, force sensors, etc. [2].

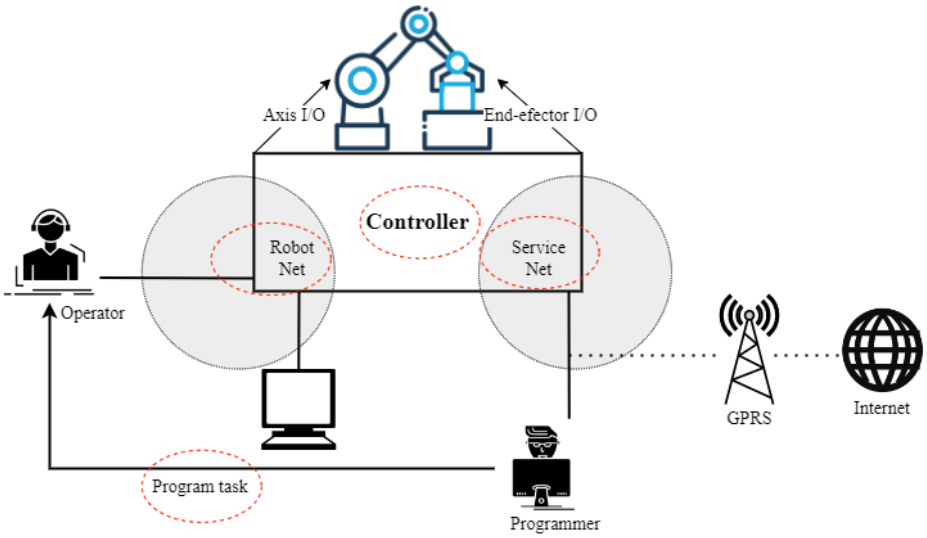

Figure 7: Black box view of a standard RS architecture

4.1. Analytical and experimental methods combinations

In this section, we described 4 analytical and experimental methods combinations. The goal of this combination is to reduce PT execution time, improve its completeness and trustworthiness, and decrease the costs of safety and cybersecurity assessment.

4.1.1. I(F)MECA-PEN Stages

Such methods combination is fully applicable for a safety-cybersecurity-critical system such as RS. All the possible attack surfaces (marked in the dashed oval in Fig.7), such as robot/service networks, controllers, or a program task, can be assessed using this method's combination. I(F)MECA-PEN allows the pentester to assess and perform Intrusion/Failure analysis and assess findings (threats/vulnerabilities/attacks) criticality after PT phases such as scanning, gaining access, and maintaining access. Figure 8 describes the way how I(F)MECA stages can be integrated into the PT flow.

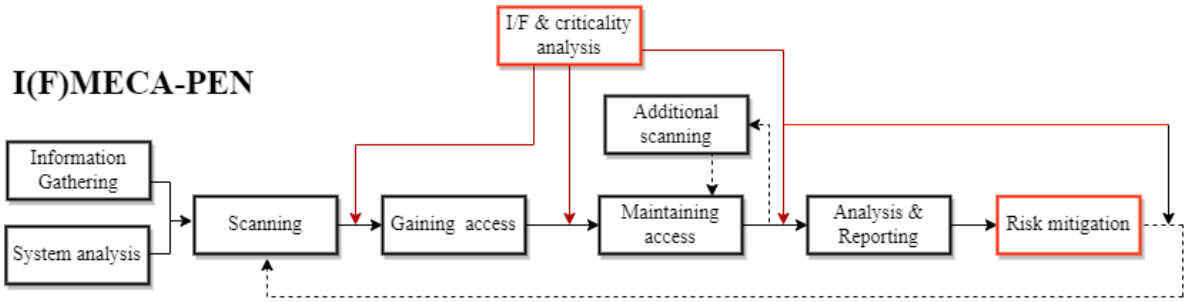

Figure 8: I(F)MECA-PEN stages

4.1.2. ATA-PEN Stages

ATA is very often used technique as an addition to the PT activities, especially after the Scanning stage. The stages of ATA-PEN are described in Figure 9.

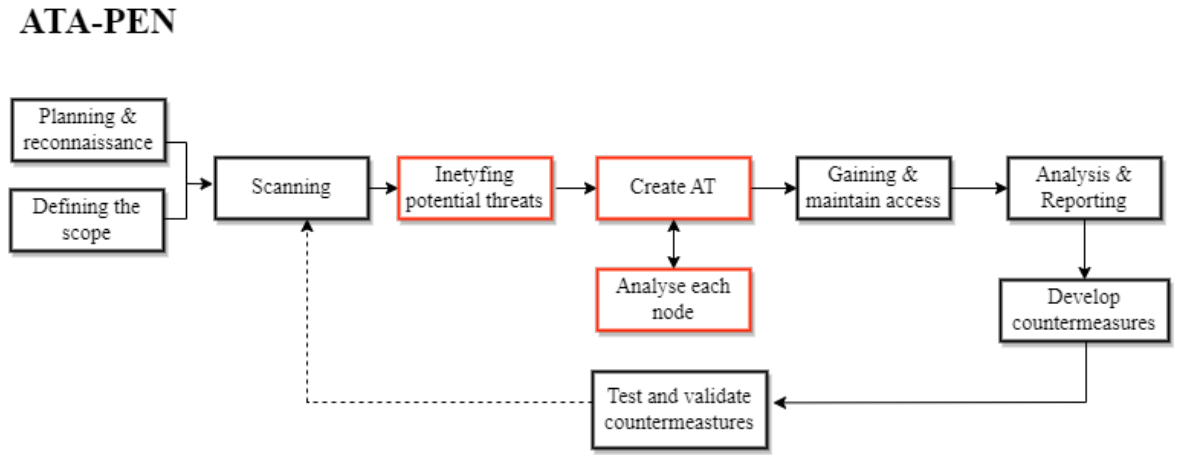

Figure 9: ATA-PEN stages

4.1.3. R&VA-PEN Stages

This combination of methods is so widespread that sometimes PT is confused with VA and vice versa. R&VA-PEN is a very large-scale and long-time-consuming process that covers not only safety & cybersecurity assessment, but also vulnerability monitoring and reporting activities. The stages of R&VA-PEN are described in Figure 10.

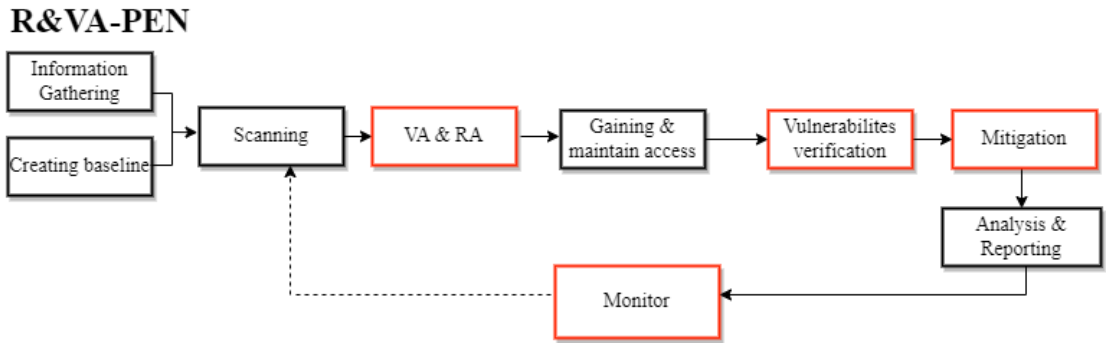

Figure 10: R&VA stages

4.1.4. FVI-PEN Stages

The unique stage of the FVI-PEN method is the Injection stage. This technique may be useful to test the completeness and trustworthiness of the PT process. The idea is that the development team injects certain known vulnerabilities before starting the testing phase, and pen-testers must check how the RS will react to their appearance and what exactly they can lead to. Unfortunately, this method is quite risky, because fault or vulnerability injection can lead to unexpected RS behavior, so it is not recommended to perform it on a real existing system. The stages of FVI-PEN are described in Figure 11. Gaining & maintaining access might be an optional step.

Figure 11: FVI-PEN stages

4.2. Methods combinations advantages and disadvantages

We compared and discussed method combinations and summarized their advantages and disadvantages in the tables 2-5.

4.2.1. I(F)MECA-PEN advantages and disadvantages

Table 2
I(F)MECA-PEN advantages and disadvantages

Advantages	Disadvantages
+ Pentester can predict the impact of vulnerabilities he found without exploitation of these findings. In cases when the goal is assessing the impact of possible threats, this method's combination can save a lot of time by excluding the low criticality scenarios from the testing scope.	- Vulnerabilities can be "known" issues that refer the pentester to the vulnerabilities databases like NVD with already assigned CVE, assessed criticality level, and described steps to exploit and there is no critical need for criticality analysis before the exploitation.
+ When access to the RS is gained, the pentester can redo the I(F)MECA analysis again to identify the most critical threats and begin the exploitation process from them.	- If access to the system is gained for a very short period pentester might have no time to perform an I(F)MECA analysis.
+ Might be very helpful also after regression testing to understand the level of risk mitigation.	

4.2.2. ATA-PEN advantages and disadvantages

Table 3
ATA-PEN advantages and disadvantages

Advantages	Disadvantages
+ This helps the pentester to identify possible attack vectors on the RS like robot/service networks, controller, or a program task, and analyze their components to understand the way to perform an intrusion to the RS.	- Requires extra time for creating attack trees.
+ Applied countermeasures can be validated using ATA-PEN methods combinations.	

4.2.3. R&VA-PEN advantages and disadvantages

Table 4
R&VA-PEN advantages and disadvantages

Advantages	Disadvantages
+ The method has the largest testing coverage.	- Cost- and time-consuming method.
+ Simplifies mitigation of the "false-positive" findings by verifying them using exploitation activities.	

4.2.4. FVI-PEN advantages and disadvantages

Table 5
FVI-PEN advantages and disadvantages

Advantages	Disadvantages
+ This method's combination allows for the assessment of the quality of pentesters' work.	- Risky if used in a real RS condition.
+ By using this method development team can see how RS will work in unexpected/critical situations.	- Time-consuming method.
	- Requires robotic simulators to be used for testing.

4.3. Methods comparison

Based on the analysis of possible options for combining existing methods of ensuring the safety and cyber security of RS and a review of the advantages and disadvantages of these methods, it is possible to build a generalized matrix of influence on certain aspects of PT.

We evaluated the impact methods combining on the PT metrics (completeness, trustworthiness, execution time, cost) using the scale from -2 to 2, where -2 is a significant decrease in the metric, -1 is a slight decrease in the metric, 0 means that the value of the metric doesn't change, 1 is a slight increase in the metric, 2 is a significant increase in the metric. Before the evaluation, all the metrics score values are equal to 0. The results are summarized in Table 6.

Table 6
Methods combinations evaluation

Method\Effect	completeness	trustworthiness	execution time	cost	total score
FVI-PEN	1	2	-1	-1	1
I(F)MECA-PEN	2	2	-1	-1	2
ATA-PEN	1	2	-1	-1	1
R&VA-PEN	2	1	-1	-2	0

I(F)MECA-PEN doesn't significantly increase the execution time and cost of PT but incomparably improves its completeness and trustworthiness. Meanwhile, the ATA-PEN combination also raises PT execution time and cost but also slightly improves its completeness and trustworthiness. R&VA is a very cost- & time-consuming method combination, but it significantly improves PT completeness. FVI-PEN is a method combination, which requires an additional environment to be used for PT, but this method can significantly improve RS dependability.

5. Conclusions

During this study, we analyzed a few analytical and experimental methods of safety and cybersecurity assessment to be combined with PT and evaluated them. As a preliminary result, we have determined that the combination of I(F)MECA with PT [11] is the best of the considered ones but requires practical confirmation in the conditions of application in a real RS or its emulator.

Future research can be dedicated to, firstly, the addition of other methods and analysis of their extended combination, and secondly, simulation and field investigation of the RS cyber security assessment using the suggested approach. Finally, it would be interesting to continue research on cybersecurity analysis and assurance issues for the Internet of Robots as a part of IoT systems [19,20].

6. References

[1] IOActive.Com, Hacking Robots before Skynet, url: https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf.

[2] A. Borboni, K.V.V. Reddy, I. Elamvazuthi, M.S. AL-Quraishi, E. Natarajan and S.S. Azhar Ali, The Expanding Role of Artificial Intelligence in Collaborative Robots for Industrial Applications: A Systematic Review of Recent Works, Machines 11(111) (2023), doi: 10.3390/machines11010111.

[3] O. Veprytska and V. Kharchenko, AI-powered attacks against AI-powered protection: classification, scenarios and risk analysis, in: Proceedings of the IEEE Conference on Dependable Systems, Services and Technologies, DESSERT, 2022, doi: 10.1109/DESSERT58054.2022.10018770.

[4] V. Vilches, L. Alzola Kirschgens, A. Calvo, A. Cordero, R. Izquierdo Pisón, D. Mayoral Vilches, A. Muñiz Rosas, G. Olalde Mendia, L. J. Usategui San, I. Ugarte, E. Gil-Uriarte, E. Tews, and A. Peter, Introducing the Robot Security Framework (RSF), A Standardized Methodology to Perform Security Assessments in Robotics (2018), url: https://arxiv.org/abs/1806.04042.

[5] B. Dieber, R. White, S. Taurer, B. Breiling, G. Caiazza, H. Christensen, and A. Cortesi, Penetration Testing ROS, Studies in Computational Intelligence 831 (2019), doi: 10.1007/978-3-030-20190-6_8.

[6] S. Hollerer, C. Fischer, B. Brenner, M. Papa, S. Schlund, W. Kastner, J. Fabini, and T. Zseby, Cobot attack: a security assessment exemplified by a specific collaborative robot, Procedia Manufacturing 54 (2021), pp. 191–196, doi: 10.1016/j.promfg.2021.07.029.

[7] C.F. Chan, K.P. Chow, and T. Tang, Security Analysis of Software Updates for Industrial Robots, Critical Infrastructure Protection XV. ICCIP 2021. IFIP Advances in Information and Communication Technology 636 (2022), pp. 229–245, doi: 10.1007/978-3-030-93511-5_11.

[8] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A.M. Zanchettin, and S. Zanero, An Experimental Security Analysis of an Industrial Robot Controller, in: Proceeding of the 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 268–286, doi: 10.1109/SP.2017.20.

[9] H. Pu, L. He, P. Cheng, M. Sun, and J. Chen, Security of Industrial Robots: Vulnerabilities, Attacks, and Mitigations, IEEE Network (2022), doi: 10.1109/MNET.116.2200034.

[10] A. Abakumov and V. Kharchenko, Penetration testing for IoT systems: cyber threats, methods, and stages, Electronic Modeling 44(4) (2022), pp. 79–104, doi: 10.15407/emodel.44.04.079.

[11] A. Abakumov and V. Kharchenko, Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems, in: Proceedings of the 12th IEEE Conference on Dependable Systems, Services and Technologies, DESSERT, 2022, doi: 10.1109/DESSERT58054.2022.10018823.

[12] ECCouncil.org, Vulnerability Assessment: 6 Best Steps to Better Security, url: https://egs.eccouncil.org/wp-content/uploads/2020/12/Risk-and-Vulnerability-Assessment-Do-You-Know-the-Other-Side.pdf.

[13] Md. A. R. Likhon, Attack Trees: Cyber Security, 2020, url: https://www.academia.edu/62051416/Attack_Trees_Cyber_Security.

[14] V. Torianyk, V. Kharchenko, and H. Zemlianko, IMECA Based Assessment of Internet of Drones Systems Cyber Security Considering Radio Frequency Vulnerabilities, in: Proceeding of the IntelITSIS'2021: 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security (2021), url: https://ceur-ws.org/Vol-2853/paper50.pdf.

[15] V. Pevnev, V. Torianyk, and V. Kharchenko, Cyber Security of Wireless Smart Systems: Channels of Intrusions and Radio Frequency Vulnerabilities, Radioelectronic and Computer Systems, 4 (96) (2020), pp. 79–92, doi: 10.32620/reks.2020.4.07.

[16] M. Denis, C. Zena, and T. Hayajneh, Penetration testing: Concepts, attack methods, and defense strategies, in: Proceedings of the 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT) (2016), doi: 10.1109/LISAT.2016.7494156.

[17] V. Shelekhov, N. Barchenko, V. Kalchenko and V. Obodyak, A Hierarchical Fuzzy Quality Assessment of Complex Security Information Systems, Radioelectronic and Computer Systems, 4 (2022), pp. 106–115, doi: 10.32620/reks.2020.4.10.

[18] A. Aponte-Moreno, J. Isaza-GonzÃlez, A. Serrano-Cases, A. Martínez-Álvarez, S. Cuenca-Asensi, and F. Restrepo-Calle, Evaluation of fault injection tools for reliability estimation of microprocessor-based embedded systems, Microprocessors and Microsystems 96 (2023), doi: 10.1016/j.micpro.2022.104723.
[19] M. Kolisnyk, Vulnerability analysis and method of selection of communication protocols for information transfer in Internet of Things systems, Radioelectronic and Computer Systems, 1 (2021), pp. 133–149, doi: 10.32620/reks.2021.1.12.
[20] O. Morozova, A. Nicheporuk, A. Tetskyi, and V. Tkachov, Methods and technologies for ensuring cybersecurity of industrial and web-oriented systems and networks, Radioelectronic and Computer Systems, 4 (2021), pp. 145–156, doi: 10.32620/reks.2021.4.12.