ACSRA ICS: Automated Cyber Security Risk Assessment Methodology for Industrial Control Systems

Haya Altaleb[1], László Ady[2], Péter János Varga[3], Zoltán Rajnai[4]

[1] Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University, 1034 Budapest, Bécsi út 96/B, haya.altaleb@bgk.uni-obuda.hu

[2] Doctoral School on Safety and Security Sciences, Óbuda University, 1034 Budapest, Bécsi út 96/B, ady.laszlo@kvk.uni-obuda.hu

[3] Kandó Kálmán Faculty of Electrical Engineering, Óbuda University, 1034 Budapest, Bécsi út 96/B, varga.peter@kvk.uni-obuda.hu

[4] Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University, 1034 Budapest, Bécsi út 96/B, rajnai.zoltan@bgk.uni-obuda.hu

Abstract: The adoption of 5G in SCADA and ICS environments represents a paradigm shift, offering enhanced connectivity, flexibility, and responsiveness. However, this transition mandates a comprehensive approach to cybersecurity to mitigate the potential risks associated with the openness of the network. As industries continue to embrace the advantages of 5G, it is imperative to strike a balance between innovation and security to ensure the reliable and secure operation of critical infrastructure. Penetration testing enhances network security by pinpointing and emphasizing security concerns. Cybersecurity assessments are increasingly becoming standard practice. Penetration testing, a strategy employed to mitigate the risk of cyberattacks, involves testers trying to compromise systems using the same tools and techniques as malicious attackers. This approach aims to identify vulnerabilities before any potential cyberattack occurs. In this study, we proposed a novel automated cybersecurity risk assessment to categorize the ICS (Industrial Control Systems) cybersecurity vulnerabilities connected to the 5G network.

Keywords: Penetration testing; Cybersecurity Risk assessment; Industrial control systems;5G, critical infrastructure

1 Introduction

Most contemporary essential industrial infrastructures and applications heavily depend on Supervisory Control and Data Acquisition (SCADA) systems for overseeing, monitoring, and managing the complete operational and data life cycle

of operation systems [1]. Recognizing the significance of safeguarding these critical systems like the 5G operated logistics terminal [2], Water 4.0 [3], and Power Systems [4], particularly in the era of 5G that amplifies threats and vulnerabilities [5]. In this article, we have devised a comprehensive penetration testing methodology known as Automated Cybersecurity Risk Assessment (ACSRA). Our new software was tested in an isolated 5G SA system, along with Moxa devices, PLCs, (Programmable Logic Controller), HMI (Human Machine Interface), and Linux software computer. Where Moxa is a network management software, that empowers you to centrally oversee your networking devices, providing real-time visibility [6]. Moxa's devices serve to prevent the exploitation of recognized vulnerabilities in Windows systems, protecting older Windows devices that cannot receive patches due to unsupported status. These devices are proficient in identifying cyberattacks and restricting them to specific zones. Furthermore, Moxa's devices possess the capability to detect cyber threats and promptly inform administrators through the use of IPS pattern matching [7]. A Siemens-manufactured PLC employed for the automation and control of industrial processes is the S7-1200. This PLC comprises two primary elements: the hardware and the software. The hardware encompasses the power supply, central processing unit (CPU), input/output modules, and communication modules [8].

A penetration test involves security professionals actively attempting to breach your company's network, evaluating security controls by exploiting weaknesses in systems, networks, human resources, or physical assets. Tests cover areas like network services, applications, client-side, wireless, social engineering, and physical aspects. They can be done externally or internally, simulating various attack vectors, with the tester's prior knowledge depending on test goals [9]. This is categorized as black box, white box, and gray box penetration testing [10]. In [11] the authors delve into the examination of security considerations and the incorporation of a Security Operations Center (SOC) into an IIoT system. Considering these factors, they showcase two sample applications aiming to provide readily applicable solutions to specific challenges faced by today's industrial sector. An intelligent algorithm was introduced [12] capable of autonomously making decisions and offering recommendations upon detecting network threats. The finalization of both software and hardware components will prioritize mobility and integrability, all within the framework of the cloud service.

The subsequent segments of this document are organized as follows: Section 2 delves into five existing penetration test methodologies, Section 3 introduces our novel methodology ACSRA ICS: Automated Cyber Security Risk Assessment Methodology for Industrial Control Systems, Section 4 encompasses the laboratory experimental segment, and finally, we provide a concise conclusion.

2 Penetration Testing Methodologies

Penetration testing methodologies exhibit similarities, but subtle distinctions exist among them. In this section, we will elucidate these nuances while offering recommendations for selecting the most suitable methodology for a given penetration testing scenario. Therefore, it's crucial to understand the distinctions between a methodology, a framework, and a standard.

A methodology serves as a specific set of tools and guidelines designed to achieve a particular goal. In contrast, frameworks provide more generalized guidance and recommendations for tools to reach the same objective, offering greater flexibility. When using a framework, one must adapt the prescribed practices to their specific environment. Importantly, both methodologies and frameworks do not mandate strict adherence to their instructions. This stands in contrast to a standard, such as ISO27001 and NIST 800-115, which are precisely defined and necessitates strict compliance with all its instructions.

In this article, we will focus on five methodologies which are the Penetration Testing Execution Standard, NIST SP 800-115, NIST SP 8800-82r3 PenetrationTesting Framework Information Systems Security Assessment Framework (ISSAF), and OWASP Testing Guide.

2.1 NIST SP 800-82r3 and NIST SP 800-115

The American National Standardization Institute NIST (National Institute of Standards and Technology), NIST has Special Publication SP 800-82 r3 (Revision 3) is a comprehensive guide for securing Operational Technology (OT) systems. It addresses the unique requirements of OT systems, covering performance, reliability, and safety considerations. Operational Technology includes various programmable systems and devices interacting with or managing the physical environment, such as Industrial Control Systems (ICS), building automation, and transportation systems. SP 800-82r3 outlines OT system topologies, identifies threats and vulnerabilities, and provides security recommendations. Key updates in this revision include an expanded scope from ICS to OT, addressing updated threats, risk management, recommended practices, and architectures. It also incorporates the latest in OT security activities, and tools, and aligns with other standards like the Cybersecurity Framework (CSF) [13]. The revision introduces tailoring guidance for SP 800-53r5 security controls, offering specific security control baselines for different impact levels in OT systems [14]. In the form of a technical guide to testing, and evaluating information security NIST SP 800–115 standard is considered a methodology that offers a wide range of methods for evaluating information security, the main part of which is penetration testing. This part includes three main groups of techniques [15]:

1) Information security audit review techniques

2) Techniques for identifying and analyzing information systems
3) Techniques for checking information systems for vulnerabilities

2.2 OSSTMM

The Open Source Security Testing Methodology Manual (OSSTMM) is a freely available resource developed by the Institute for Security and Open Methodologies (ISECOM). It offers extensive guidance for conducting penetration tests. Additionally, the manual includes test cases designed to yield validated facts. These facts supply practical information that can significantly enhance your operational security [16]. The methodology outlined in the manual addresses the following five security channels: Human, Physical, Wireless, Networks, and Telecoms. Moreover, The OSSTMM can be categorized into four Phases: Induction Phase, Interaction Phase, Inquest Phase, and Intervention Phase.

Every phase contributes a distinct level of scrutiny to the audit, with none being less crucial than the others concerning actual security. Each phase has different modules and combining all of these modules results in a unified methodology for understanding and managing security. This approach is versatile and applicable to various types of security tests, ensuring a thorough and efficient examination of whether the target is a specific system, location, person, process, or a multitude of them.

2.3 ISSAF

The Information System Security Assessment Framework (ISSAF) is a standardized approach for conducting penetration tests to assess the resilience of a website. It involves nine stages of attack testing and offers multiple advantages compared to existing security controls in addressing threats and security gaps. Additionally, it acts as a link between the technical and managerial perspectives of penetration testing by implementing necessary controls in both areas. The primary goal of penetration testing is to identify security vulnerabilities on a website, which can subsequently be used for assessing risk management based on ISO 31000 principles. This risk management process encompasses stages such as risk identification, risk analysis, and risk evaluation [17]. The following figure shows the ISSAF Framework Methodology.

2.4 PTES

The Penetration Testing Execution Standard (PTES) comprises seven main sections, encompassing all aspects of a penetration test. These sections include initial communication and reasoning, intelligence gathering, threat modeling, vulnerability research, exploitation, post-exploitation, and reporting. This version,

labeled v1.0, reflects a well-established foundation after industry testing for over a year. A forthcoming v2.0 will introduce more detailed work levels to accommodate variations in penetration test intensity, ensuring alignment with an organization's expectations and needs. The groundwork for these levels can be observed in the intelligence gathering section. The main sections defined by the standard are as follows [18]:

1) Pre-engagement Interactions
2) Intelligence Gathering
3) Threat Modeling
4) Vulnerability Analysis
5) Exploitation
6) Post Exploitation
7) Reporting

PTES incorporates a SCADA Audit tool for conducting network audits on sensitive Supervisory Control And Data Acquisition (SCADA) systems, employing only secure checks. Enhancements have been made to packet block delays, increased time intervals between sent packets, disabled protocol handshaking, and restricted simultaneous network access to assets [18].

2.5 OWASP

Open Web Application Security Project OWASP is a non-profit, community-driven organization dedicated to advancing software security through educational resources, open-source software, and related initiatives. The OWASP ASVS serves as an open standard for systematically assessing web application security, aiming to rigorously evaluate technical security controls at both the application and environment levels. This approach enables the identification of potential vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection. The ASVS Project has crafted its standard to be practical and commercially viable, offering comprehensive coverage and adaptability for various scenarios, from internal security assessments to guiding developers in implementing effective security measures or assessing third-party software and contractual development agreements. The most recent stable version of ASVS is 4.0.3, released in October 2021 [19]. Given the widespread use and importance of web applications today, organizations seek assurance that software is securely and robustly developed, incorporating necessary security measures while minimizing risks to assets. To instill the required confidence in acquiring and maintaining software systems, organizations require a comprehensive approach to evaluate and analyze the security of the software [20]. Table 1 is a Comparison between the following methodologies NIST SP 800-82r3, NIST SP 800-115, OSSTMM, ISSAF, and PTES.

Table 1
Comparison between methodologies

	NIST SP 800-82r3	NIST SP 800-115	OSSTMM	ISSAF	PTES
Purpose	Guidelines for ICS	Technical Guide to test	Security testing and metrics framework	Information Systems Security Assessment Framework	Standard for Penetration Testing Execution
Scope	ICS environments	Assessment and testing methodologies	security testing across multiple domains	Broad security assessment for IT environments	Penetration testing methodologies and procedures
Target audience	ICS security professionals, managers, and system operators	Security testers, auditors, and IT professionals	Security professionals and auditors	Security professionals and auditors	Penetration testers and security professionals
Methodology	Risk management, control system security controls, and architecture design	Planning, executing, and reporting on information security tests	Test process including Intelligence Gathering, Enumeration, and Analysis	Structured approach to security assessment covering pre-assessment, assessment, and post-assessment phases	Pre-engagement, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, Reporting
Key components	ICS-specific risk management framework, security controls, and architecture design considerations	Test planning, execution, and analysis, reporting, and post-assessment activities	5 test modules: Controls, Access, Trust, Process, and Limits	Pre-assessment planning, assessment phase, and post-assessment analysis and reporting	Scoping, Information Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, Reporting

3 Automated Cyber Security Risk Assessment Methodology for Industrial Control Systems (ACSRA ICS)

In this section we proposed our new methodology, The Automated Cybersecurity Risk Assessment (ACSRA), The methodology begins with a meticulous examination of methodologies outlined in Section 2, followed by the formulation of recommendations for seamless integration. The common aspects across various standards and frameworks relevant to SCADA and ICS security are explored, encompassing risk management, security testing, incident response, security controls, architecture, penetration testing, open-source security, and web application security.

The integration approach is detailed, emphasizing the importance of risk assessment, security controls implementation, regular testing and assessment, incident response planning, and a continuous improvement mindset. The impact of this integrated approach on risk assessment within SCADA and ICS environments is discussed, highlighting its comprehensive understanding of risks, adaptation to industry-specific requirements, holistic security controls implementation, identification of system-specific vulnerabilities, incident response plan validation, continuous improvement, efficient use of open-source security resources, alignment with industry best practices, enhanced visibility into supply chain risks, and improved communication and collaboration.

The methodology explores automation possibilities for risk assessment in SCADA and ICS environments, covering device discovery, vulnerability scanning, continuous monitoring, threat intelligence integration, configuration management and compliance checking, penetration testing automation, incident response plan automation, risk scoring, and prioritization, documentation, and reporting, integration with ticketing systems, machine learning for anomaly detection, and collaboration platform integration.

Additionally, penetration test classification is outlined, categorizing assessments for SCADA/ICS network, wireless security, protocol and communication, device and controller security, HMI testing, and SCADA/ICS toolkits. Vulnerability classification includes authentication and authorization vulnerabilities, communication protocol vulnerabilities, firmware and software vulnerabilities, configuration weaknesses, and wireless network vulnerabilities.

The methodology introduces Vulnerability Modes and Effects Analysis (VMEA), emphasizing the identification of critical assets, and potential vulnerabilities, assessment of impact and likelihood, and prioritization of vulnerability modes.

Prioritization of penetration tests is discussed, focusing on critical infrastructure components, high-risk vulnerabilities, 5G network security, authentication and access control, emergency response and recovery, and regular security audits.

The ICS Automated Cyber Security Risk Assessment methodology is presented, followed by an experimental setup in the Óbuda University 5G lab. The experiment involves monitoring ICS devices connected via 5G, searching for clear identification points in network traffic, and implementing vulnerability checks based on identification patterns.

3.1 Common Aspects

Overview of common aspects that can be relevant across these standards and frameworks in the context of SCADA and ICS security:

1) Risk management.
2) Security testing and assessment.
3) Incident response.
4) Security controls.
5) Security architecture.
6) Penetration testing.
7) Open source security.
8) Web application security.

Both NIST SP800-115 and SP800-82 emphasize risk management principles. Understanding and managing risks is fundamental in any security framework, including SCADA and ICS environments.

NIST SP800-115 and OSSTMM provide guidelines for security testing and assessment. The PTES framework is specifically designed for penetration testing. In SCADA and ICS, regular security testing and assessments are crucial to identify and mitigate vulnerabilities.

NIST SP800-82 and ISSAF address incident response in the context of ICS. Having a well-defined incident response plan is essential to minimize the impact of security incidents.

NIST SP800-82 defines security controls for ICS, while NIST SP800-115 provides guidance on assessing the effectiveness of these controls. Understanding and implementing security controls are key in SCADA and ICS environments.

NIST SP800-82 provides guidance on designing a secure architecture for ICS. Understanding and implementing a robust security architecture is crucial for protecting critical infrastructure.

PTES is a comprehensive standard for penetration testing, covering various aspects of the process. Penetration testing is valuable in SCADA and ICS to identify and address vulnerabilities.

OSSTMM focuses on open-source security testing methodologies. Leveraging open-source tools and methodologies are relevant in SCADA and ICS environments for cost-effective security practices.

OWASP focuses on web application security. ICS environments may not be typical web applications, but a lot of ICS devices and SCADA systems have web based interfaces. The principles of secure coding, input validation, and protection against common web vulnerabilities are still relevant in any software components used in SCADA and ICS.

3.2 Integration Approach

When working in SCADA and ICS environments, organizations can benefit from an integrated approach:

(i) Risk assessment: Begin with a thorough risk assessment, considering the specific characteristics of SCADA and ICS environments.

(ii) Security controls: Implement security controls based on guidelines provided by NIST SP800-82.

(iii) Testing and assessment: Conduct regular security testing and assessments using methodologies outlined in NIST SP800-115, OSSTMM, and PTES.

(iv) Incident response: Develop and regularly test incident response plans, aligning with principles from NIST SP800-82 and ISSAF.

(v) Continuous Improvement: Adopt a continuous improvement mindset, keeping up with evolving threats and best practices outlined in various frameworks.

3.3 Integration Approach Effect on Risk Assessment

The integrated approach combining various security standards and frameworks has several positive effects on risk assessment in the context of SCADA and ICS environments, like:

(i) Comprehensive understanding of risks: This integrated approach allows for a comprehensive understanding of risks specific to SCADA and ICS. By leveraging various standards, the assessment covers a wide range of potential threats and vulnerabilities.

(ii) Adaptation to industry-specific requirements: SCADA and ICS environments have unique characteristics and requirements. The integrated approach enables

risk assessments to be adapted to the specific needs of critical infrastructure, ensuring relevance and effectiveness.

(iii) Holistic security controls implementation: Combining NIST SP800-82's guidance on security controls with testing methodologies from NIST SP800-115, OSSTMM, and PTES ensures a more holistic implementation of security controls. This, in turn, contributes to a more robust defense-in-depth strategy [21].

(iv) Identification of system-specific vulnerabilities: The integration of various testing methodologies allows for the identification of system-specific vulnerabilities. This includes vulnerabilities related to ICS components, communication protocols, and industrial processes.

(v) Incident response plan validation: Regular testing and assessments, in alignment with frameworks like ISSAF on SCADA / ICS on web management, contribute to the validation of incident response plans. This ensures that the organization is well prepared to handle and mitigate security incidents [22].

(vi) Continuous improvement and adaptation: An integrated approach fosters a culture of continuous improvement. By regularly reviewing and adapting security practices based on the latest standards and frameworks, organizations can stay ahead of emerging threats.

(vii) Efficient use of open-source security resources: Leveraging open-source security testing methodologies and tools from OSSTMM can contribute to cost-effective security practices. This can be particularly valuable in resource-constrained environments.

(viii) Alignment with industry best practices: The integration ensures alignment with industry best practices outlined by organizations like OWASP.

(ix) Enhanced visibility into supply chain risks: The integrated approach, especially when considering supply chain security, allows for enhanced visibility into risks associated with third-party vendors and equipment. This is crucial in ensuring the overall resilience of the ICS ecosystem.

(x) Improved communication and collaboration: Standardized frameworks facilitate communication and collaboration among different stakeholders, including security professionals, ICS engineers, and management. This alignment is critical for implementing effective security measures.

3.4 Risk Assessment Automation Possibilities

Automating risk assessment in the integrated approach for SCADA and ICS environments can significantly enhance efficiency and accuracy. Automation possibilities:

1) Device discovery.

2) Vulnerability scanning.
3) Continuous monitoring.
4) Threat intelligence integration.
5) Configuration management and compliance checking.
6) Penetration testing automation.
7) Incident response plan automation.
8) Risk scoring and prioritization.
9) Documentation and reporting.
10) Integration with ticketing systems.
11) Machine learning for anomaly detection.
12) Collaboration platform integration.

Table 2 outlines various aspects of risk assessment automation, including the difficulty level, achievement, and important notes for each task in the integrated approach for SCADA and ICS environments.

Table 2
Risk Assessment Automation Framework for SCADA and ICS Environments

Task	Difficulty	Achievement	Note
Device discovery	Low	Easy to detect network changes	Wide range methods
Vulnerability scanning	Low	Repeatable	Different databases, static
Continuous monitoring	Low	Real-time information, and automated response	
Threat intelligence integration	High	Proactive	Dynamic
Configuration management and compliance checking	High	Fast and easy reconfigure	Not all SCADA, ICS have open API to manage configuration
Penetration testing automation	High	Repeatable	Not all SCADA, ICS have open API, tests can break the live system
Incident response plan automation	High	Automatic response	Not all SCADA, ICS have open API, and false-positive alerts can break the system
Risk scoring and prioritization	Moderate	Faster repair of the most serious vulnerabilities	

Integration with ticketing systems	Low	Easy tracking	
Machine learning for anomaly detection	High	Proactive	
Collaboration platform integration	High	Easy tracking	

Achieving automatic device discovery is a critical aspect of managing and securing a network in SCADA and ICS. Automatic device discovery helps maintain an up-to-date inventory of devices, which is crucial for security, operational efficiency, and compliance. Here are key steps and technologies to achieve automatic device discovery:

1) Network scanning (Nmap, Nessus, OpenVas).
2) Device management (GLPI).
3) Network monitoring (Wireshark, PRTG, Nagios).
4) DHCP and DNS Logging.

Automatic vulnerability scanning is a crucial aspect of maintaining a secure and resilient network in SCADA and ICS. Vulnerability scanning helps identify potential weaknesses in systems, networks, and applications, allowing organizations to proactively address security risks. Here's how to achieve automatic vulnerability scanning:

1) Vulnerability scanning tools.
2) Automated scanning schedules.
3) Integration with device management.
4) Continuous monitoring.
5) Agent-based scanning.
6) Integration with patch management.
7) Automated report generation.
8) Scanning authentication.
9) Risk-based prioritization.
10) Integration with incident response.
11) Integration with Security Information and Event Management (SIEM).

Automatic continuous monitoring is essential for maintaining the security and integrity of systems. Continuous monitoring enables real-time visibility into the security posture of the network, applications, and devices. Here's how to achieve automatic continuous monitoring:

(i) Using automatic device discovery.

(ii) Using automatic vulnerability scanning.

(iii) Using automatic incident response automation.

3.5 Penetration Tests Classification

Penetration testing, commonly known as ethical hacking or "pen testing," is a critical cybersecurity practice employed by organizations to assess the security of their systems, networks, and applications. The primary goal of penetration testing is to identify vulnerabilities and weaknesses in a controlled manner, allowing organizations to proactively address and mitigate potential security risks.

Classification of penetration tests:

(i) SCADA/ICS Network Assessment: Evaluate the security of the network architecture, communication protocols, and configurations in SCADA/ICS environments connected through 5G.

(ii) Wireless Security Assessment: Assess the security of 5G connectivity for SCADA/ICS devices, focusing on vulnerabilities in wireless communication protocols.

(iii) Protocol and Communication Testing: Evaluate the security of communication protocols used in SCADA/ICS systems over 5G, identifying potential vulnerabilities and weaknesses.

(iv) Device and Controller Security Assessment: Assess the security of SCADA/ICS devices and controllers connected through 5G, including firmware vulnerabilities and configuration weaknesses.

(v) Human-Machine Interface (HMI) Testing: Evaluate the security of HMI systems in SCADA/ICS, identifying potential vulnerabilities that could be exploited through 5G.

(vi) SCADA/ICS toolkits: Evaluate the security of the ICS programmer, tester, and updater tools/environments.

(vii) SCADA desktop and server components: Evaluate the security of the desktop and server software system components.

3.6 Vulnerability Classification

Vulnerability Classification:

(i) Authentication and authorization vulnerabilities: Identify weaknesses in user authentication and authorization mechanisms in SCADA/ICS systems.

(ii) Communication protocol vulnerabilities: Assess vulnerabilities in communication protocols used for data transfer between SCADA/ICS components over 5G.

(iii) Firmware and software vulnerabilities: Identify vulnerabilities in the firmware and software of SCADA/ICS devices and controllers.

(iv) Configuration weaknesses: Assess insecure configurations that may lead to unauthorized access or disruption in SCADA/ICS operations.

(v) Wireless network vulnerabilities: Identify weaknesses in the 5G network infrastructure supporting SCADA/ICS communication.

3.7 Vulnerability Modes and Effect Analysis (VMEA)

Vulnerability Modes and Effects Analysis (VMEA):

(i) Define critical assets: Identify critical assets and components within the SCADA/ICS infrastructure connected via 5G.

(ii) Identify potential vulnerability: Enumerate potential crack modes, considering vulnerabilities and weaknesses in the system.

(iii) Assess impact and likelihood: Evaluate the impact and likelihood of each vulnerability mode, considering potential consequences on operations.

(iv) Prioritise vulnerability modes: Prioritise crack modes based on their potential impact, likelihood, and overall risk to the SCADA/ICS environment.

Table 3 provides an organized assessment of vulnerabilities in SCADA/ICS environments connected via 5G, including critical assets, potential vulnerabilities, and prioritization based on impact, likelihood, and overall risk.

Table 3
Vulnerability Modes and Effects Analysis (VMEA) for 5G-Connected SCADA/ICS Environments

Location	Change PLC output	Can stop PLC	Detect difficulty	Impact	Level
Local	Not	Not	Low	Negligible	Low
Local	Not	Not	High	Negligible	Low
Local	Not	Yes	Low	Moderate	Low
Local	Not	Yes	High	Moderate	Medium
Local	Yes	Not	Low	Significant	Low
Local	Yes	Not	High	Severe	Medium
Local	Yes	Yes	Low	Significant	Low
Local	Yes	Yes	High	Severe	Medium
Remote	Not	Not	Low	Negligible	Low
Remote	Not	Not	High	Negligible	Medium

Remote	Not	Yes	Low	Significant	High
Remote	Not	Yes	High	Severe	Critical
Remote	Yes	Not	Low	Significant	High
Remote	Yes	Not	High	Severe	Critical
Remote	Yes	Yes	Low	Severe	High
Remote	Yes	Yes	High	Severe	Critical

3.8 Prioritisation of Penetration Tests

Prioritization of penetration tests:

(i) Critical Infrastructure Components: Prioritise penetration testing on critical SCADA/ICS components and assets connected through 5G.

(ii) High-Risk Vulnerabilities: Focus on penetration tests that target high-risk vulnerabilities, such as those with severe consequences or a high likelihood of exploitation.

(iii) 5G Network Security: Prioritise testing the security of the 5G network infrastructure supporting SCADA/ICS communication.

(iv) Authentication and Access Control: Prioritise testing authentication and access control mechanisms to prevent unauthorized access to critical systems.

(v) Emergency Response and Recovery: Assess the effectiveness of emergency response and recovery mechanisms in the event of a security incident or failure.

(vi) Regular Security Audits: Conduct regular security audits to ensure continuous monitoring and improvement of the SCADA/ICS security posture.

Table 4 outlines the prioritization of penetration tests for 5G-connected SCADA/ICS environments, focusing on critical infrastructure components, high-risk vulnerabilities, and specific aspects like network security, authentication, and emergency response mechanisms. The prioritization factors include priority, difficulty, speed, and the potential impact on the system.

Table 4
Prioritization of Penetration Tests for 5G-connected SCADA/ICS Environments

Name	Priority	Difficulty	Speed	Effect
Network scanning	High	Low	Fast	Minimal
Port scanning from the database by MAC	High	Low	Moderate	Minimal
Port scanning opened ports	High	Low	Moderate	Minimal
Port scanning by application scanner	Medium	Moderate	Slow	Minimal
Network monitoring	Medium	High	Moderate	Minimal

Identify application and version	High	Moderate	Fast	Minimal
Vulnerabilities from databases	High	Moderate	Fast	None
Fuzz testing	Low	High	Slow	High in product system, test system needed
Static code analysis	Low	High	Slow	None, but the source code needed

4 Experimental Procedure

In our laboratory experiment, our objective is to validate our novel methodology. For this purpose, we establish a SCADA/ICS network based on 5G using our laboratory equipment. We intend to develop software that comprehensively performs all necessary functions to demonstrate automatic risk assessment. Once this software is implemented, we will conduct a thorough scan of our prepared environment.

4.1 5G-Enabled ICS System Structure

In the 5G laboratory of Óbuda University, we established a testing network where ICS devices were interconnected via 5G technology as Figure 1.

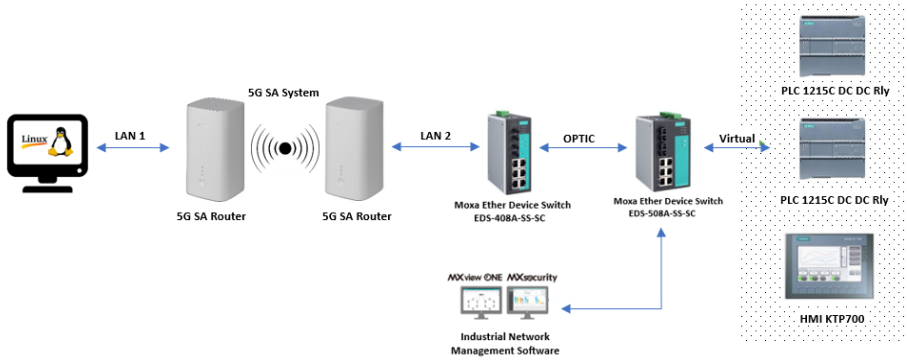
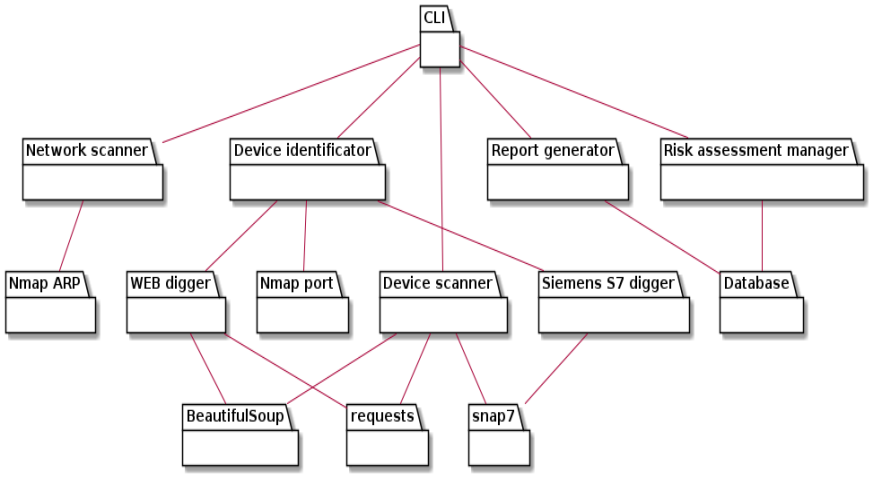


Figure 1
System Structure:5G-Enabled ICS Device Identification and Version Discovery in Óbuda University's Test Network

4.2 ACSRA ICS System Block Diagram

After establishing the network, we employed Wireshark to monitor the device configuration process. Within the network traffic, we looked for distinctive indicators that revealed the application and version number. MOXA devices featured a login-free webpage on their web management interface, serving as a clear identification point that also displayed the version number. Given the complexities of reversing the Siemens S7 protocol, an alternative approach was taken. We used Python snap7, an S7 API implementation, to identify the PLCs. Specifically, the client's get_block_info function was employed to extract the DB 1 index, facilitating the identification of both the device and version number in a single step. Figure 2 shows the ACSRA ICS system Block diagram.



Block diagram of the ACSRA ICS system

During the main operation of the ACSRA ICS, the exploration of larger groups is based on their analysis. Initially, it identifies all hosts connected to the specified network. Subsequently, it Scans for the available ports on the discovered hosts. Based on these ports, it proceeds to recognize the devices and conducts an in-depth analysis of vulnerabilities associated with each identified device.

4.3 ACSRA ICS Workflow

A detailed explanation of methodological overall workflow including specific tools and techniques for automation tasks, the first three steps are the pre-risk assessment, and the last three steps are the operation:

1) Communication analysis using Wireshark:

Wireshark is employed to capture and analyze network traffic, providing detailed insights into communication patterns and existing vulnerabilities within the ICS environment.

2) Open database searches with ACSRA ICS Python web scraper:

A Python-based web scraper is used to search open databases, gathering relevant information to enhance the security assessment of the ICS.

3) Risk analysis using ACSRA ICS:

Risk analysis is conducted through VMEA classification developed in ACSRA ICS, allowing for a thorough evaluation of potential threats and their implications on the ICS.

4) Network Scanning with ACSRA ICS:

The integrated Python Nmap module is imported to the ACSRA ICS Python scripts, and it is used for network scanning, device identification, and searching for network assets. This helps in identifying and cataloging all devices connected to the network.

5) Evaluation based on database findings:

Collected data is evaluated based on the existing databases to determine the presence of vulnerabilities, enabling a comprehensive assessment of the ICS security posture.

6) Display and reporting:

The final results are visualized and displayed in an understandable format, facilitating informed decision making regarding the security measures to be implemented in the ICS.

This structured approach ensures a meticulous and thorough examination of the ACSRA ICS, leveraging advanced tools and techniques to enhance the security and reliability of industrial control systems.

The sequential steps of the ACSRA ICS workflow are outlined in Figure 3, emphasizing the continuous cycle of finding hosts, identifying devices, conducting vulnerability scans, performing risk assessments, and generating reports. The loop indicates the iterative nature of the process, ensuring a thorough and ongoing security assessment in the ICS environment.

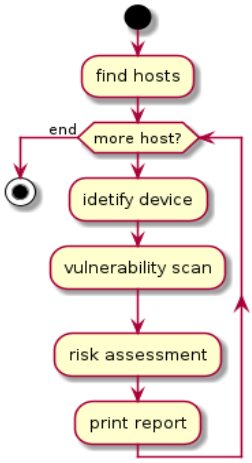


Figure 3
ACSRA ICS workflow

4.4 Wireshark's Methodology for Model Name Identification in HTTP Responses

In the realm of network analysis, understanding the intricacies of communication protocols is vital for gaining insights into the dynamics of information exchange. Figure 4 serves as a visual representation of a meticulous exploration- undertaken through Wireshark network analysis focused on the identification of software versions within HTTP communication. Through delving into the essential steps involved in this process, the visualization aims to provide a comprehensive overview of how version identification unfolds during the analysis. The intricate interplay of data within HTTP communication is unveiled, shedding light on the methodologies employed to discern and unravel the nuances of software versions in a network environment. Uncovering precise details about network responses is paramount. This exploration highlights Wireshark's methodology in discovering the exact model name within HTTP responses. Figure 5 showcases stages and components, offering clear insight into systematic steps for precise model name identification embedded within network data.

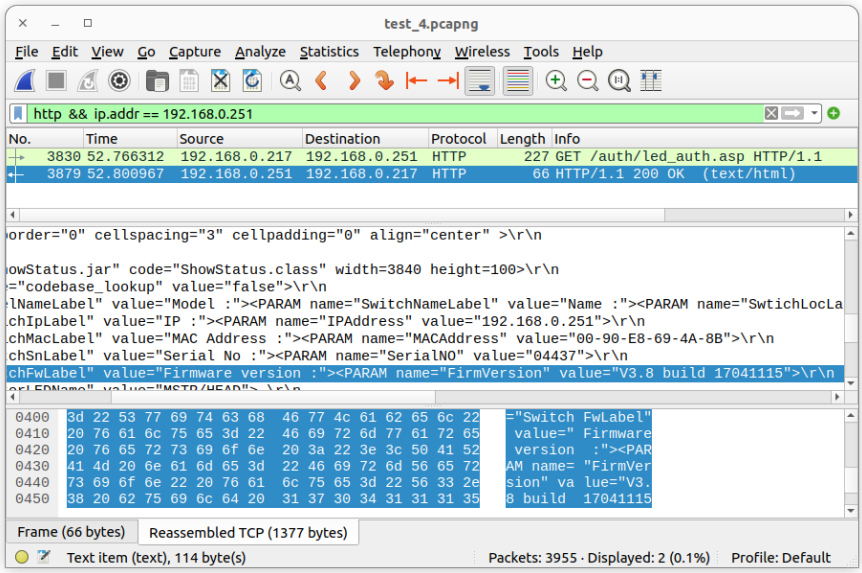


Figure 4

Moxa device version detecting with Wireshark

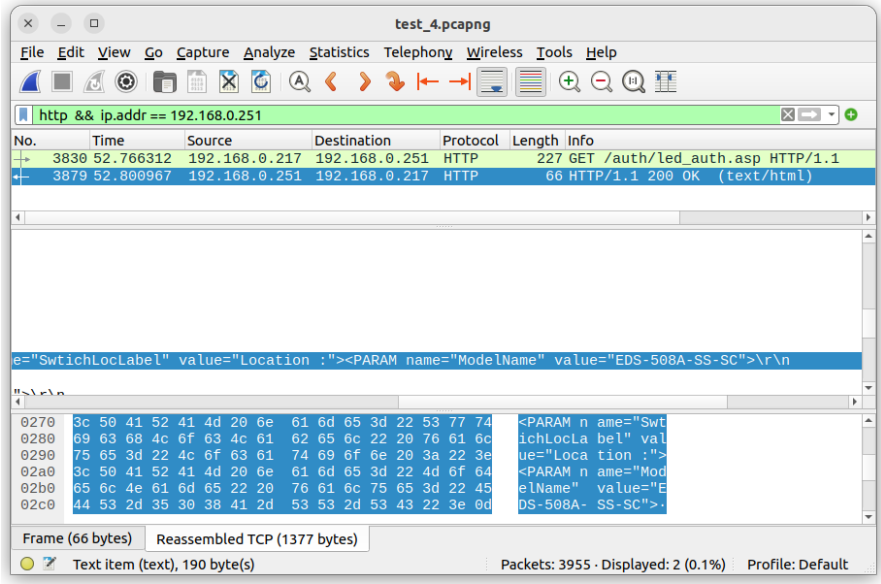


Figure 5

Moxa device model detecting with Wireshark

Wireshark screenshots provide insight into the communication between the client software in the control center and the PLC. During the analysis of the packets shown in the screenshots, we found clear detection packets that can be used to extract data from PLC devices with minimal risk. These packets can provide valuable information about the configuration and status of PLCs, which can also be useful in identifying vulnerabilities. In addition to the packages shown in the screenshots, we also found packages that can be used to detect the PLC. These packets contain information such as the PLC's IP address, MAC address, and firmware version. With this information, it is possible to map the PLC and identify vulnerabilities.

The ACSRA ICS database stores valuable information about PLC versions, configurations, and vulnerabilities. This information can be compared with the information shown in the Wireshark screenshots for more accurate identification of vulnerabilities.

Following that, we implemented the scan check functions based on the revealed clear identification patterns. Subsequently, we added the vulnerabilities to the vulnerability database. Figure 6 is a screenshot of our automated risk assessment process using our solution in the laboratory.

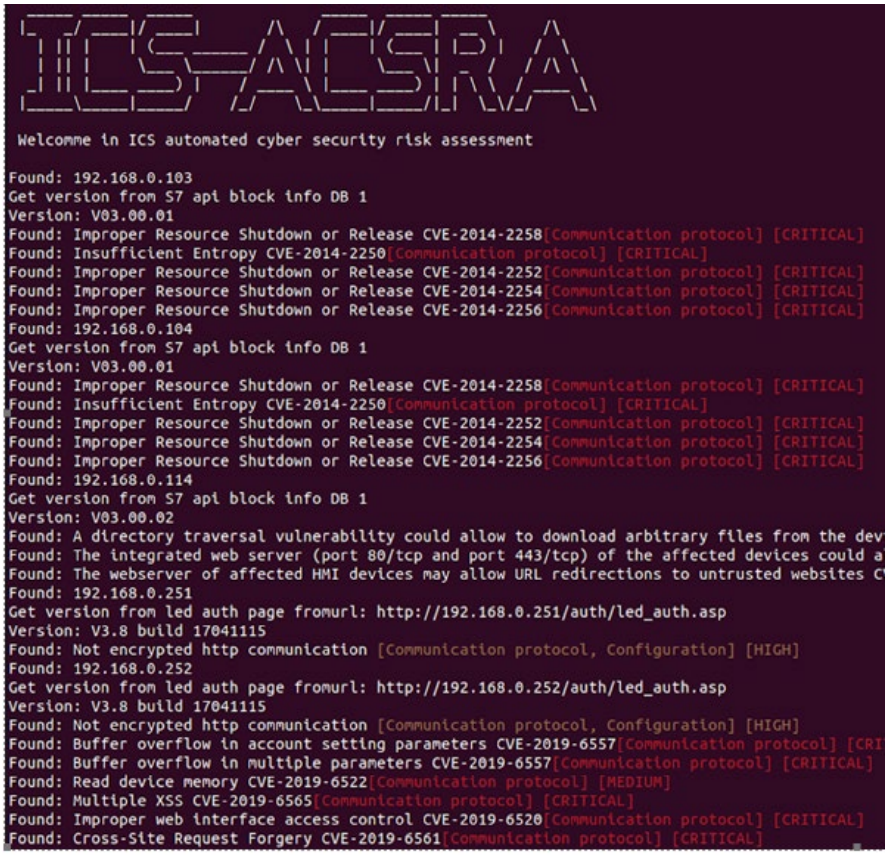


Figure 6
The automated risk assessment process utilizing our solution in our laboratory.

5 System Validation, Novelty, Benefits, and Limitations

Following the successful laboratory trials, the ACSRA ICS software was transitioned to a production environment for further evaluation. This phase involved testing on a network of programmable logic controllers (PLCs) integrated with 3,300 sensors, using unique RS485 and Ethernet communication protocols. During this phase, discovery messages were transmitted at a rate of 1/40th of the standard messaging frequency, ensuring minimal disruption to the system's operational integrity. The software consistently identified vulnerabilities within the PLC network, confirming its reliability and effectiveness under real-world conditions.

5.1 Validation and Comparison

During the validation of the ACSRA ICS system, we compared it with existing software solutions. The market offers a variety of industrial cybersecurity scanners, such as Tenable, Claroty, and CyberX, each providing unique functionalities tailored to different needs and budgets. These tools generally offer a range of features, including automated vulnerability assessments, network monitoring, and integration capabilities. Of these, we had access to the open-source code, so we did it with that. With the PLC Scan compatible S7 protocol, samples can be recorded for Yara Rules. We could not find ready-made samples for Yara Rules on the Internet. Table 5 compares ACSRA ICS with selected open-source ICS tools.

Table 5
Comparison between ACSRA ICS with selected open-source ICS tools

	ICS-ACSRA	PLCScan	Yara Rules
File scanning	No	No	Yes
Memory scanning	No	No	Yes
Network scanning	Yes	Yes	Yes
Device identification	Yes	Limited (S7, Modbus)	Limited (only pattern)
Custom queries	Limited (only prepared)	Yes	Limited (custom rule)
S7 protocol	Yes	Yes	No
Vulnabity database	Yes	No	Not for Siemens S7
Prepared risk assessment	Yes	No	No
Moxa (web admin)	Yes	No	No
Safe scan (not degrade PLCs functionality)	Yes	No	Limited (pattern match)
	ICS-ACSRA	PLCScan	Yara Rules
File scanning	No	No	Yes
Memory scanning	No	No	Yes
Network scanning	Yes	Yes	Yes
Device identification	Yes	Limited (S7, Modbus)	Limited (only pattern)

5.2 Novelty

This enhanced methodological workflow, rigorous validation, and novel integration of advanced tools, positions the ACSRA ICS software as a cutting-edge solution in industrial control system security. This approach ensures a comprehensive security

assessment that surpasses traditional methods. An automated and systematic risk analysis implemented in Python, enhancing precision and efficiency in identifying potential threats. Additionally, by leveraging open databases and real-time data scraping, the software proactively identifies and addresses vulnerabilities before they can be exploited, setting a new standard in ICS security management. Furthermore, the advanced data visualization and reporting mechanisms ensure that complex security data is presented in an accessible and actionable manner, facilitating rapid decision-making and response.

5.3 Benefits of ACSRA ICS

5.3.1 In-Depth Analysis

ACSRA ICS excels in advanced vulnerability detection by identifying not only vulnerabilities listed in public databases but also unique vulnerabilities arising from specific configurations of Programmable Logic Controllers (PLCs). This tool can be customized with user-defined patterns, enhancing its detection capabilities beyond standard databases. Through analyzing the detailed configuration of PLCs, ACSRA ICS can uncover vulnerabilities that generic tools might overlook, providing a more comprehensive security assessment.

5.3.2 Real-Time Monitoring

ACSRA ICS provides continuous traffic analysis by monitoring PLC traffic and issuing real-time alerts for detected vulnerabilities. This proactive approach aids in the early detection and prevention of potential cyberattacks, thereby ensuring the operational integrity of industrial control systems (ICS). Its real-time capabilities allow for the immediate identification and response to threats, minimizing the window of exposure and potential damage.

5.3.3 Flexible Deployment

ACSRA ICS architecture offers versatile installation options, allowing it to be deployed either on-premises at a control center or as a cloud-based service. This flexibility simplifies installation and maintenance, enabling organizations to choose the deployment model that best fits their operational needs. Additionally, the tool's adaptable deployment options ensure its scalability and suitability for various scales of operation, from small facilities to large industrial complexes.

5.4 Limitations of ACSRA ICS

5.4.1 Device Compatibility

Limited PLC Support: ACSRA ICS may not be compatible with all types of PLCs. Its effectiveness depends on the specific models and configurations of the PLCs in use, which may limit its applicability in diverse environments.

5.4.2 Expertise Requirement

Specialized knowledge needed: Effective utilization of ACSRA ICS requires substantial expertise in both PLCs and cybersecurity. Users need to be proficient in handling detailed data analyses beyond what is available in open databases. This necessitates specialized training and experience for optimal tool performance.

Customized configuration: Each deployment may require significant customization and fine-tuning to address the specific needs of the controlled environment, demanding ongoing attention from skilled personnel.

Conclusions and Future Research Directions

The study introduced a novel risk assessment methodology; ACSRA ICS methodology for evaluating cybersecurity risks in 5G-connected SCADA and ICS environments. The adoption of 5G in critical infrastructures presents opportunities and challenges, necessitating a robust cybersecurity approach.

Penetration testing, a key element of ACSRA, was highlighted as a strategy to identify vulnerabilities proactively. The study proposed an automated risk assessment methodology, ACSRA, tested in an isolated 5G SA system. Five prominent penetration testing methodologies were analyzed, emphasizing their integration into ACSRA. The integration approach showcased positive effects, including a comprehensive understanding of risks, system-specific vulnerability identification, and improved incident response plans. Automation possibilities for risk assessment tasks were explored, enhancing efficiency and accuracy.

The study classified penetration tests, introduced Vulnerability Modes and Effects Analysis (VMEA), and prioritized tests for 5G-connected SCADA/ICS environments. An experimental setup demonstrated the identification of 5G-enabled ICS devices. In conclusion, ICS ACSRA provides a systematic, automated approach for cybersecurity in 5G-connected SCADA/ICS. The integration of methodologies, risk assessment automation, and practical experimentation contribute to a robust framework.

This study sets the groundwork for further advancements in securing critical infrastructures with 5G technology. Our approach is well suited for large enterprises with a private network and SMEs with a Public network. The methodology and analysis can be extended to address various vulnerability types. Through tailoring

the software used for testing, a specialized tool can be developed for deployment in smaller company settings, offering the functionalities outlined in the article.

The comprehensive measurement process revealed several significant outcomes. Firstly, the ACSRA ICS software demonstrated its efficacy in identifying a broad spectrum of vulnerabilities, including software bugs, firmware inconsistencies, and network security flaws, across both laboratory and live production environments. Secondly, the software proved to be non-disruptive, successfully sending reconnaissance messages at a greatly reduced frequency - 1/40th of the normal rate - without causing any operational interruptions. Lastly, the tests validated the software's reliability and repeatability, confirming its ability to consistently detect vulnerabilities across various environments with high precision. After analysis, we can conclude that:

1) Traditional vulnerability scanners might disrupt critical processes in 5G connected PLCs.
2) 5G connectivity introduces new attack vectors that traditional scanners might not cover.

Considerations for 5G Connected PLCs

When selecting vulnerability assessment tools for industrial control systems (ICS), it is essential to prioritize those specifically designed to address the unique protocol risks associated with ICS. Additionally, a thorough evaluation of the potential disruption caused by scanning tools within a 5G-connected PLC environment is crucial to ensure operational stability. Tools should also be chosen based on their ability to address 5G-specific vulnerabilities, including novel attack vectors introduced by this advanced connectivity.

Recommendations

To achieve a comprehensive vulnerability assessment for 5G-connected PLCs, it is advisable to integrate information-gathering tools with dedicated ICS vulnerability scanners. This approach ensures a well-rounded evaluation by addressing both general and specific security risks. Given the unique security challenges posed by 5G connectivity, it is crucial to prioritize scanners designed to address these specific vulnerabilities. Additionally, employing a safe scan mode is recommended for critical systems to balance thoroughness with operational safety, thereby ensuring a secure and effective assessment strategy.

References

[1] H. Altaleb and R. Zoltan, “Addressing Cybersecurity Challenges in 5G-enabled IoT and Critical Infrastructures: A Comprehensive Overview,” *INES 2023 - 27th IEEE Int. Conf. Intell. Eng. Syst. 2023, Proc.*, pp. 131-136, 2023, doi: 10.1109/INES59282.2023.10297774

[2] “Europe’s first 5G-operated logistics terminal opens in Hungary,” *Xinhua News Agency*, 2022 [Online] Available: https://news.cgtn.com/news/2022-

10-19/Europe-s-first-5G-logistics-terminal-opens-in-Hungary-1efTfv0q7dK/index.html [Accessed: 23-Jul-2024]

[3] T. Szádeczky, "Water 4.0 in Hungary: Prospects and Cybersecurity Concerns," *Acta Polytech. Hungarica*, Vol. 20, No. 7, pp. 211-230, 2023, doi: 10.12700/APH.20.7.2023.7.12

[4] T. H. Le, "Feed-Forward and Long Short-Term Neural Network Models for Power System State Estimation," *Acta Polytech. Hungarica*, Vol. 21, No. 6, pp. 223-241, 2024, doi: 10.12700/APH.21.6.2024.6.12

[5] M. Čerger and J. Hudec, "Cyber-Security Threats Origins and their Analysis," *Acta Polytech. Hungarica*, Vol. 20, No. 9, pp. 23-41, 2023, doi: 10.12700/APH.20.9.2023.9.2

[6] R. Li, "Implementation of serial communication based on MOXA multiport serial boards in VC++," *ICIC 2010 - 3rd Int. Conf. Inf. Comput.*, Vol. 2, pp. 230-232, 2010, doi: 10.1109/ICIC.2010.152

[7] "Defense Against Threats," 2024 [Online] Available: https://www.moxa.com/en/spotlight/portfolio/industrial-network-security/industrial-cybersecurity#networktreatsdefense [Accessed: 29-Jan-2024]

[8] H. Salih, H. Abdelwahab, and A. Abdallah, "Automation design for a syrup production line using Siemens PLC S7-1200 and TIA Portal software," *Proc. - 2017 Int. Conf. Commun. Control. Comput. Electron. Eng. ICCCCEE 2017*, 2017, doi: 10.1109/ICCCCEE.2017.7866702

[9] A. Whitaker and D. P. Newman, "Penetration testing and network defense," p. 598, 2006

[10] S. Nidhra, "Black Box and White Box Testing Techniques - A Literature Review," *Int. J. Embed. Syst. Appl.*, Vol. 2, No. 2, pp. 29-50, 2012, doi: 10.5121/ijesa.2012.2204

[11] K. Ferencz, J. Domokos, and L. Kovács, "Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations," *Acta Polytech. Hungarica*, Vol. 21, No. 4, pp. 7-28, 2024, doi: 10.12700/aph.21.4.2024.4.1

[12] A. Ospanova, A. Zharkimbekova, L. Kussepova, A. Tokkuliyeva, and M. Kokkoz, "Cloud Service for Protecting Computer Networks of Enterprises Using Intelligent Hardware and Software Devices, Based on Raspberry Pi Microcomputers," *Acta Polytech. Hungarica*, Vol. 19, No. 4, pp. 85-103, 2022, doi: 10.12700/APH.19.4.2022.4.5

[13] NIST, "Guide to Operational Technology (OT) Security: NIST Publishes SP 800-82, Revision 3," 2023 [Online] Available: https://csrc.nist.gov/News/2023/nist-publishes-sp-800-82-revision-3#:~:text=SP 800-82r3 provides an,to manage the associated risks [Accessed: 10-Jan-2024]

[14] Joint Task Force, "Security and Privacy Controlsfor Information Systems and Organizations," *NIST Spec. Publ.*, Vol. 1, No. 5, p. 465, 2020

[15] NIST 800-115, M. Denis, C. Zena, and T. Hayajneh, "Technical Guide to Information Security Testing and Assessment," *2016 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2016*, Vol. 800, pp. 1-80, 2016

[16] ISECOM, "Manual The Open Source Security Testing Methodology," *Recuper. el 06 Mayo 2020*, 2020

[17] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. Sri Arsa, "Information technology risk management using ISO 31000 based on issaf framework penetration testing (Case study: Election commission of x city)," *Int. J. Comput. Netw. Inf. Secur.*, Vol. 12, No. 4, pp. 30-40, 2020, doi: 10.5815/ijcnis.2020.04.03

[18] PTES Team, "The Penetration Testing Execution Standard (PTES)," p. 227, 2022

[19] S. F. Wen and B. Katt, "A quantitative security evaluation and analysis model for web applications based on OWASP application security verification standard," *Comput. Secur.*, Vol. 135, 2023, doi: 10.1016/j.cose.2023.103532

[20] B. Erşahin and M. Erşahin, "Web application security," *South Florida J. Dev.*, Vol. 3, No. 4, pp. 4194-4203, 2022, doi: 10.46932/sfjdv3n4-002

[21] M. Alhamed and M. M. H. Rahman, "A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions," *Appl. Sci.*, Vol. 13, No. 12, 2023, doi: 10.3390/app13126986

[22] M. A. Nabila, P. E. Mas'udia, and R. Saptono, "Analysis and Implementation of the ISSAF Framework on OSSTMM on Website Security Vulnerabilities Testing in Polinema," *Jartel*, Vol. 13, No. 1, 2023, doi: 10.33795/jartel.v13i1.511