ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOCTORAL (PhD) THESIS BOOKLET

ENG. HAYA ALTALEB

Automated Cybersecurity Risk Assessment for Industrial Control Systems (ACSRA-ICS)

Supervisor: Prof. Dr. Rajnai Zoltan

DOCTORAL SCHOOL ON
SAFETY AND SECURITY
SCIENCES

25/07/2024

Contents

Summary

Contemporary industrial infrastructures and applications rely heavily on Supervisory Control and Data Acquisition (SCADA) systems to oversee, monitor, and manage operational and data life cycles. Recognizing the critical importance of safeguarding these systems, particularly in the 5G era with its heightened threats and vulnerabilities, this dissertation introduces a comprehensive penetration testing methodology named Automated Cybersecurity Risk Assessment (ACSRA). The efficacy of this new software was evaluated within an isolated 5G SA system, alongside Moxa devices, Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), and Linux-based computers. Moxa, a network management software, enables centralized oversight of networking devices, offering real-time visibility.

This dissertation aims to develop a tailored Automated Cyber Security Risk Assessment Methodology (ACSRA) for Industrial Control Systems (ICS) and SCADA environments, exploring common aspects across cybersecurity standards and frameworks relevant to SCADA and ICS security. It proposes an integration approach emphasizing risk assessment, security controls implementation, regular testing, incident response planning, and continuous improvement within SCADA and ICS environments. The impact of this integrated approach on risk assessment within SCADA and ICS environments is assessed, alongside investigating automation possibilities for risk assessment, categorizing penetration tests and vulnerabilities, and developing a Vulnerability Modes and Effects Analysis (VMEA) framework. Additionally, the dissertation prioritizes penetration tests based on critical infrastructure components, high-risk vulnerabilities, 5G network security, authentication and access control, and emergency response and recovery. An experimental setup in the Óbuda University 5G lab is conducted to validate the ACSRA methodology, aiming to provide a comprehensive understanding of its applicability in enhancing cybersecurity in SCADA and ICS environments and contributing to the protection of critical infrastructure against cyber threats.

The dissertation findings highlight the fulfillment of its four main hypotheses. The Integrated Approach Hypothesis posits that integrating cybersecurity standards and frameworks into the Automated Cyber Security Risk Assessment Methodology (ACSRA ICS) enhances risk management in SCADA and ICS environments. Automation, as per the Automation Hypotheses, significantly improves risk assessment efficiency and accuracy by automating tasks like device discovery, vulnerability scanning, and incident response plan validation. Penetration Testing Hypotheses underscore the importance of prioritized penetration tests in identifying vulnerabilities across various SCADA/ICS components, thereby enhancing security posture. Additionally, Vulnerability Classification Hypotheses emphasize the significance of categorizing vulnerabilities by authentication, communication protocols, and configuration weaknesses to effectively prioritize mitigation efforts and manage risks strategically.

Summary in Hungarian language - – Magyar nyelvű összefoglaló

A kortárs ipari infrastruktúrák és alkalmazások nagymértékben támaszkodnak a felügyeleti vezérlési és adatgyűjtési (SCADA) rendszerekre a működési és adatéletciklusok felügyelete, monitorozása és kezelése terén. Felismerve e rendszerek védelmének kritikus fontosságát, különösen a fokozott fenyegetettségekkel és sebezhetőségekkel járó 5G-korszakban, ez a disszertáció egy átfogó penetrációs tesztelési módszert mutat be, az Automated Cybersecurity Risk Assessment (ACSRA). Ennek az új szoftvernek a hatékonyságát egy izolált 5G SA rendszeren belül értékelték, a Moxa eszközök, programozható logikai vezérlők (PLC), emberi gép interfészek (HMI) és Linux alapú számítógépek mellett. A Moxa, a hálózatkezelő szoftver lehetővé teszi a hálózati eszközök központi felügyeletét, valós idejű láthatóságot biztosítva.

A disszertáció célja egy személyre szabott automatizált kiberbiztonsági kockázatértékelési módszer (ACSRA) kidolgozása ipari vezérlőrendszerekhez (ICS) és SCADA környezetekhez, feltárva a SCADA és ICS biztonság szempontjából releváns kiberbiztonsági szabványok és keretrendszerek közös szempontjait. Integrációs megközelítést javasol, amely a kockázatértékelést, a biztonsági ellenőrzések végrehajtását, a rendszeres tesztelést, az incidensre adott válaszok tervezését, valamint a SCADA és ICS környezetekben történő folyamatos fejlesztést hangsúlyozza. Felmérik ennek az integrált megközelítésnek a kockázatértékelésre gyakorolt hatását a SCADA és ICS környezeteken belül, a kockázatértékelés automatizálási lehetőségeinek vizsgálata, a behatolási tesztek és a sebezhetőségek kategorizálása, valamint a VMEA (Vulnerability Modes and Effects Analysis) keretrendszer kidolgozása mellett. Emellett a disszertáció előnyben részesíti a kritikus infrastruktúra-komponenseken, a magas kockázatú sebezhetőségeken, az 5G hálózatbiztonságon, a hitelesítésen és a hozzáférés-szabályozáson, valamint a vészhelyzeti reagáláson és helyreállításon alapuló penetrációs teszteket. Az Óbudai Egyetem 5G laborjában kísérleti beállítást végeznek az ACSRA módszertan validálására, melynek célja, hogy átfogó képet adjon annak alkalmazhatóságáról a SCADA és ICS környezetekben a kiberbiztonság fokozásában, valamint hozzájáruljon a kritikus infrastruktúra kiberfenyegetésekkel szembeni védelméhez.

A disszertáció eredményei rávilágítanak a négy fő hipotézis teljesülésére. Az integrált megközelítés hipotézise azt feltételezi, hogy a kiberbiztonsági szabványoknak és keretrendszereknek az Automated Cyber Security Risk Assessment Methodology (ACSRA ICS) integrálása javítja a kockázatkezelést a SCADA és ICS környezetekben. Az automatizálási hipotézisek szerint az automatizálás jelentősen javítja a kockázatértékelés hatékonyságát és pontosságát azáltal, hogy automatizálja az olyan feladatokat, mint az eszközfelderítés, a sebezhetőségek vizsgálata és az incidensreagálási terv érvényesítése. A behatolástesztelési hipotézisek hangsúlyozzák a prioritást élvező behatolási tesztek fontosságát a különböző SCADA/ICS-komponensek sebezhetőségeinek azonosításában, ezáltal javítva a biztonsági helyzetet. Ezenkívül a sebezhetőségi besorolási hipotézisek hangsúlyozzák a sérülékenységek azonosítás, kommunikációs protokollok és konfigurációs hiányosságok szerinti kategorizálásának jelentőségét a mérséklési erőfeszítések hatékony priorizálása és a kockázatok stratégiai kezelése érdekében.

1 Introduction

1.1 Research problem statement and the significance of the dissertation

Modern SCADA systems are based on advanced technology systems, therefore it is profoundly sophisticated SCADA systems are exposed to a large-scale cyber threats range because of the standardization of the hardware components and the communication protocols. Cyber threats to SCADA systems are always rising, those are caused by escalating sophistication modernization, continuous real-time operation and distribution, and the multi-component architecture of the systems.

This dissertation is presented along with the risks and possible attacks on the industrial infrastructure and especially control systems. Thus, it aims to develop a new risk assessment methodology for ICS.

The research problem in this study is the need for a comprehensive and effective cybersecurity risk assessment methodology specifically tailored for (ICS) and (SCADA) environments. These critical infrastructure systems are essential for the functioning of various industries, including energy, manufacturing, and transportation. However, they are increasingly vulnerable to cyber threats and attacks, which could have severe consequences, including disruptions to essential services and potential safety hazards.

The research problem can be summarized in the following statement:

The research problem revolves around the lack of a specialized and automated cybersecurity risk assessment methodology for (ICS) and (SCADA) environments. These critical systems are at risk of cyberattacks, and existing methodologies may not adequately address the unique challenges and requirements of these industries. Therefore, there is a pressing need to develop and validate an integrated Automated Cyber Security Risk Assessment Methodology (ACSRA ICS) that can comprehensively assess risks, vulnerabilities, and security controls in SCADA and ICS environments, ultimately enhancing their resilience against cyber threats.

1.2 Research Questions and Hypothesis

The development of a new risk assessment methodology tailored specifically for (SCADA) and (ICS) environments presents an opportunity to address the unique challenges and complexities inherent in securing critical infrastructure. This introduction outlines four main hypotheses, aimed at enhancing the effectiveness and efficiency of risk assessment practices within SCADA and ICS contexts. The research model used for this work is presented in Figure 1.

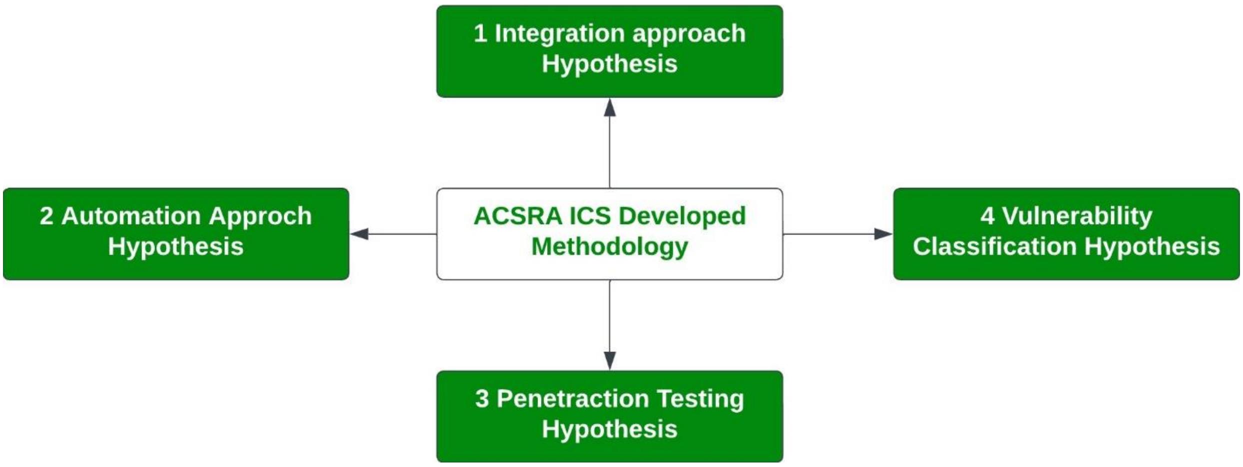
1 Integration approach Hypothesis
2 Automation Approch Hypothesis
ACSRA ICS Developed Methodology
4 Vulnerability Classification Hypothesis
3 Penetraction Testing Hypothesis

Figure 1 The research model

Integrated Approach Hypothesis and Questions:

Hypothesis 1: Combining five security standards and frameworks enhances risk assessment in SCADA and ICS environments, namely the Penetration Testing Execution Standard, NIST SP 800-115, NIST SP 8800-82r3, Open Source Security Testing Methodology Manual (OSSTMM), PenetrationTesting Framework Information Systems Security Assessment Framework (ISSAF), The Penetration Testing Execution Standard (PTES), and the OWASP Testing Guide. Questions to be asked when testing the hypothesis:

> Q: How does the integration of different security standards and frameworks improve the overall risk assessment process in SCADA and ICS environments?
>
> Q: How does adopting an integrated approach contribute to the development of a culture of continuous improvement in cybersecurity within SCADA and ICS environments?
>
> Q: What are the key advantages of using open-source security resources in SCADA and ICS environments, and how do they contribute to cost-effective security practices?
>
> Q: How do standardized frameworks enhance communication and collaboration among stakeholders, and what benefits do they bring to the security domain in SCADA and ICS environments?

Automation Hypothesis and Questions:

Hypothesis 2: Automating risk assessment tasks significantly enhances efficiency and accuracy in SCADA and ICS environments. Questions to be asked when testing the hypothesis:

> Q: What are the specific risk assessment tasks that automation can significantly improve in terms of efficiency and accuracy within SCADA and ICS environments?
>
> Q: How does automation of vulnerability scanning, continuous monitoring, and incident response plans contribute to enhancing the overall security posture in SCADA and ICS environments?

Penetration Testing Hypothesis and Questions:

Hypothesis 3: Penetration testing is a crucial cybersecurity practice for identifying vulnerabilities in SCADA and ICS systems. Questions to be asked when testing the hypothesis:

> Q: Why is penetration testing considered crucial for identifying vulnerabilities in SCADA and ICS systems, and how does it contribute to security?
>
> Q: How does prioritizing penetration tests based on critical infrastructure components and high-risk vulnerabilities enhance the overall effectiveness of security measures in SCADA and ICS environments?

Vulnerability Classification Hypothesis and Questions:

Hypothesis 4: Classifying vulnerabilities based on authentication, communication protocols, firmware/software, configuration weaknesses, and wireless networks provides a comprehensive understanding of potential risks. Question to be asked when testing the hypothesis:

> Q: How does classifying vulnerabilities based on multiple factors provide a comprehensive understanding of potential risks, and why is this approach important for SCADA and ICS security?

1.3 Dissertation objectives

The key objective of this dissertation is to revolutionize industrial cybersecurity by developing a Comprehensive Automated Cyber Security Risk Assessment Methodology (ACSRA) specifically tailored for (ICS) and SCADA environments. Through an exploration of commonalities among cybersecurity standards and frameworks, the research proposes an integration approach emphasizing risk assessment, security controls implementation, and continuous improvement within SCADA and ICS environments. It assesses the impact of this integrated approach, investigates automation possibilities for risk assessment, categorizes penetration tests and vulnerabilities, and develops a Vulnerability Modes and Effects Analysis (VMEA) framework for 5G-connected SCADA/ICS environments. Prioritizing penetration tests and conducting experimental validation in the Óbuda University 5G lab further elucidates the applicability and effectiveness of the ACSRA methodology, contributing significantly to the protection of critical infrastructure and resilience against cyber threats, these objective are listed as follows:

1. Develop a comprehensive Automated Cyber Security Risk Assessment Methodology (ACSRA) specifically tailored for (ICS) and SCADA environments.
2. Explore common aspects across various cybersecurity standards and frameworks relevant to SCADA and ICS security, including risk management, security testing, incident response, security controls, security architecture, penetration testing, open-source security, and web application security.
3. Propose an integration approach that emphasizes risk assessment, security controls implementation, regular testing and assessment, incident response planning, and a continuous improvement mindset within SCADA and ICS environments.

4. Assess the impact of the integrated approach on risk assessment within SCADA and ICS environments, focusing on its ability to provide a comprehensive understanding of risks, adapt to industry-specific requirements, implement holistic security controls, identify system-specific vulnerabilities, validate incident response plans, support continuous improvement, and efficiently utilize open-source security resources.
5. Investigate 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.
6. Categorize penetration tests and vulnerabilities in SCADA/ICS environments, including assessments related to network security, wireless security, communication protocols, device and controller security, HMI testing, and SCADA/ICS toolkits.
7. Develop a Vulnerability Modes and Effects Analysis (VMEA) framework to identify critical assets, and potential vulnerabilities, assess their impact and likelihood, and prioritize vulnerability modes in 5G-connected SCADA/ICS environments.
8. Prioritize penetration tests based on critical infrastructure components, high-risk vulnerabilities, 5G network security, authentication and access control, emergency response and recovery, and regular security audits in SCADA/ICS environments.
9. Conduct an experimental setup in the Óbuda University 5G lab to monitor ICS devices connected via 5G, search for clear identification points in network traffic, and implement vulnerability checks based on identification patterns to validate the ACSRA methodology.
10. Provide a comprehensive understanding of the methodology and its applicability in enhancing cybersecurity in SCADA and ICS environments, thereby contributing to the protection of critical infrastructure and ensuring resilience against cyber threats.

2 ACSRA ICS METHODOLOGY

This section introduces a novel methodology named ACSRA ICS: Automated Cyber Security Risk Assessment Methodology for Industrial Control Systems and provides an outline of the research methodology. I begin with the research design, which is a chart flow that can easily explain the work in a visualized way the procedure chosen for this study, and its reasons. The hardware and software were used for the lab experimental and penetration test and it was discussed. In this Chapter, I generalize all the work methods, analysis, and theories that can cover all the work that I have done so far.

Most contemporary essential industrial infrastructures and applications heavily depend on (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, particularly in the era of 5G that amplifies threats and vulnerabilities[1][2]

[3][4]. In this Chapter, I have devised a comprehensive penetration testing methodology known as Automated Cybersecurity Risk Assessment (ACSRA). The 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[5]. 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[6]. 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[7]. Top of Form 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[8]. This is categorized as black box, white box, and gray box penetration testing[9]. In [10] 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 [11] 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.

2.1 Research Design and Procedure

The research Design and Procedure are organized as follows; Beginning with a comprehensive review of existing penetration test methodologies, and evaluating their strengths and weaknesses. Subsequently, the chapter introduces the penetration test tools utilized in the research, offering justification for their selection. Central to the methodology chapter is the introduction of ACSRA ICS, detailing its objectives, scope, and the phased approach it entails. The phases include an initial assessment, vulnerability identification, risk analysis, mitigation strategies, and reporting/documentation. Each phase is described in detail, outlining the procedures, tools, and methodologies employed. Additionally, the chapter outlines the laboratory experimental segment, detailing the experimental setup, execution of ACSRA ICS methodology in a controlled environment, and the data collection process. The methodology chapter concludes with a summary of research findings and contributions, emphasizing the implications of the study for the field of ICS security. The following figure represents the research design and procedure.

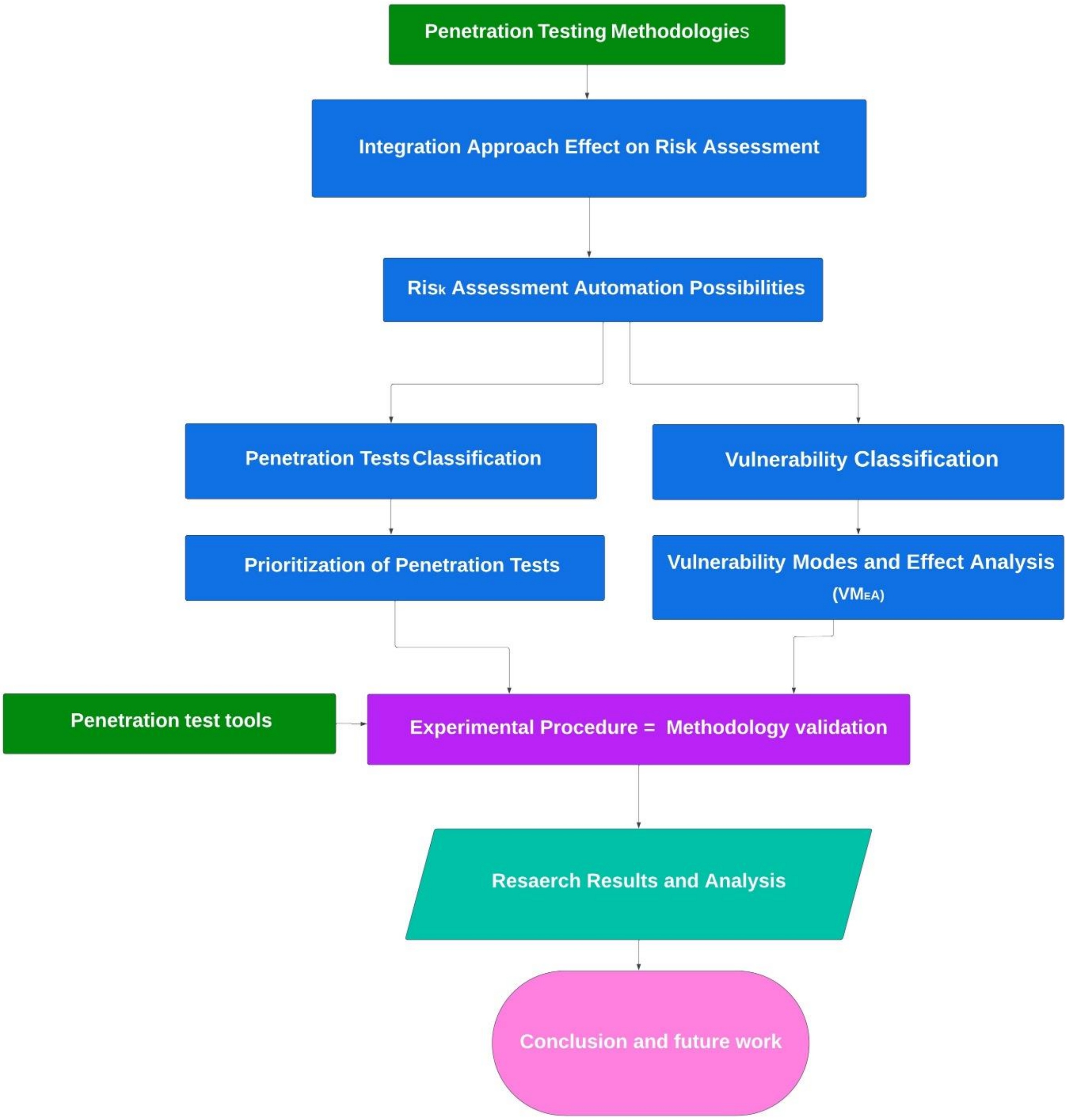
Penetration Testing Methodologies
Integration Approach Effect on Risk Assessment
Risk Assessment Automation Possibilities
Penetration Tests Classification
Vulnerability Classification
Prioritization of Penetration Tests
Vulnerability Modes and Effect Analysis (VMEA)
Penetration test tools
Experimental Procedure = Methodology validation
Resaerch Results and Analysis
Conclusion and future work

Figure 2 The Research Design and Procedure.

2.2 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 Methodology, we will focus on five methodologies which are the Penetration Testing Execution Standard, NIST SP 800-115, NIST SP 8800-82r3, Open Source Security Testing Methodology Manual (OSSTMM), PenetrationTesting Framework Information Systems Security Assessment Framework (ISSAF), The Penetration Testing Execution Standard (PTES), and the OWASP Testing Guide. In conclusion, the following table shows a comparison between the tools.

2.3 Penetration test tools

To lay the groundwork for this study, my attention is directed toward comprehending the scalability and performance of vulnerability scanning for the wireshark and Nmap tools. Additionally, a review of benchmarking literature is conducted to determine the suitability of assessment tools for carrying out comprehensive vulnerability assessments.

Wireshark is a packet analyzer that is both free and open-source. providing insights into network performance, protocol behavior, and security threats[12]. As well as it is a vital tool for network analysis and troubleshooting, supporting professionals in diagnosing issues, optimizing performance, and bolstering security. However, its potent capabilities make it an attractive target for adversaries aiming to compromise networks and access sensitive data. While most users employ Wireshark legitimately, it is essential to acknowledge and address the associated risks. Network administrators and security professionals must stay vigilant, implementing robust security measures such as regular monitoring, strong encryption, and keeping security protocols up-to-date to thwart potential threats and unauthorized access[13].

Nmap, an acronym for "Network Mapper," stands as a powerful, open-source tool readily available for network exploration and security assessments. Its utility extends across various domains, serving as a valuable asset for tasks such as network reconnaissance, monitoring service updates, and scrutinizing the operational status of hosts and services. Utilizing cutting-edge methodologies involving raw IP packets, Nmap adeptly discerns active hosts within a network and retrieves comprehensive details about the services they offer, including application names and versions, even when targeting individual hosts[14].

2.4 Integration Approach Effect on Risk Assessment

First, we Overview the 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 is 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.

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:

1. 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.
2. 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.
3. 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[15].
4. 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.
5. 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 [16].

6. 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.
7. 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.
8. Alignment with industry best practices: The integration ensures alignment with industry best practices outlined by organizations like OWASP.
9. 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.
10. 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.

2.5 Risk Assessment Automation Possibilities

Automating risk assessment in the integrated approach for SCADA and ICS environments can significantly enhance efficiency and accuracy[17]. 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 1 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 1Risk 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:

1. Using automatic device discovery.
2. Using automatic vulnerability scanning.
3. Using automatic incident response automation.

2.6 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:

1. SCADA/ICS Network Assessment: Evaluate the security of the network architecture, communication protocols, and configurations in SCADA/ICS environments connected through 5G.
2. Wireless Security Assessment: Assess the security of 5G connectivity for SCADA/ICS devices, focusing on vulnerabilities in wireless communication protocols.
3. Protocol and Communication Testing: Evaluate the security of communication protocols used in SCADA/ICS systems over 5G, identifying potential vulnerabilities and weaknesses.
4. Device and Controller Security Assessment: Assess the security of SCADA/ICS devices and controllers connected through 5G, including firmware vulnerabilities and configuration weaknesses.
5. Human-Machine Interface (HMI) Testing: Evaluate the security of HMI systems in SCADA/ICS, identifying potential vulnerabilities that could be exploited through 5G.
6. SCADA/ICS toolkits: Evaluate the security of the ICS programmer, tester, and updater tools/environments.
7. SCADA desktop and server components: Evaluate the security of the desktop and server software system components.

2.7 Vulnerability Classification

1. Authentication and authorization vulnerabilities: Identify weaknesses in user authentication and authorization mechanisms in SCADA/ICS systems.
2. Communication protocol vulnerabilities: Assess vulnerabilities in communication protocols used for data transfer between SCADA/ICS components over 5G.
3. Firmware and software vulnerabilities: Identify vulnerabilities in the firmware and software of SCADA/ICS devices and controllers.
4. Configuration weaknesses: Assess insecure configurations that may lead to unauthorized access or disruption in SCADA/ICS operations.
5. Wireless network vulnerabilities: Identify weaknesses in the 5G network infrastructure supporting SCADA/ICS communication.

2.8 Vulnerability Modes and Effect Analysis (VMEA)

1. Define critical assets: Identify critical assets and components within the SCADA/ICS infrastructure connected via 5G.
2. Identify potential vulnerability: Enumerate potential crack modes, considering vulnerabilities and weaknesses in the system.

3. Assess impact and likelihood: Evaluate the impact and likelihood of each vulnerability mode, considering potential consequences on operations.
4. Prioritise vulnerability modes: Prioritise crack modes based on their potential impact, likelihood, and overall risk to the SCADA/ICS environment.

Table 2. 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 2 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

2.9 Prioritization of Penetration Tests

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

1. High-Risk Vulnerabilities: Focus on penetration tests that target high-risk vulnerabilities, such as those with severe consequences or a high likelihood of exploitation.
2. 5G Network Security: Prioritise testing the security of the 5G network infrastructure supporting SCADA/ICS communication.
3. Authentication and Access Control: Prioritise testing authentication and access control mechanisms to prevent unauthorized access to critical systems.

4. Emergency Response and Recovery: Assess the effectiveness of emergency response and recovery mechanisms in the event of a security incident or failure.
5. Regular Security Audits: Conduct regular security audits to ensure continuous monitoring and improvement of the SCADA/ICS security posture.

Table 3 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 3 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

2.10 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.

2.10.1 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 3.

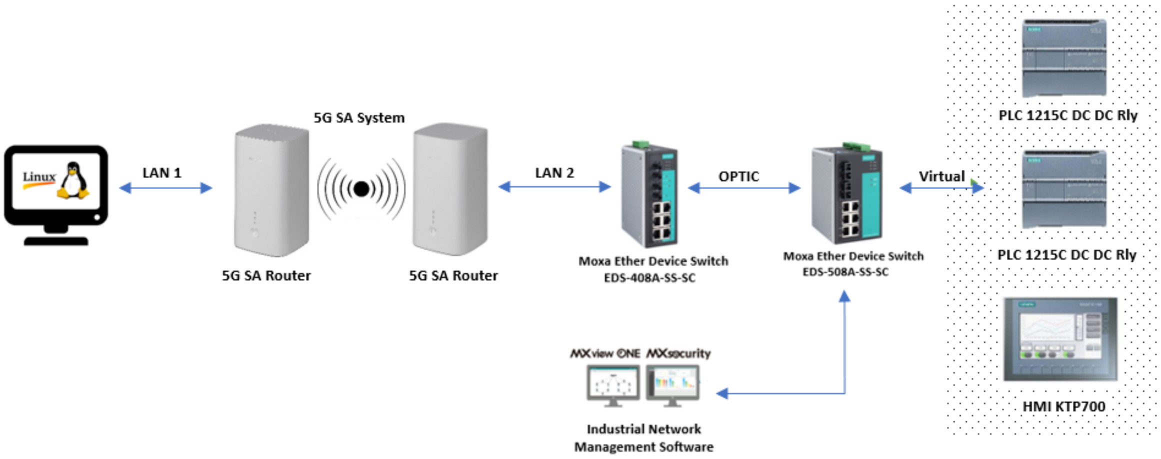

Figure 3 System Structure:5G-Enabled ICS Device Identification and Version Discovery in Óbuda University's Test Network

2.10.2 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 utilized 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 4 shows the ACSRA ICS system Block diagram.

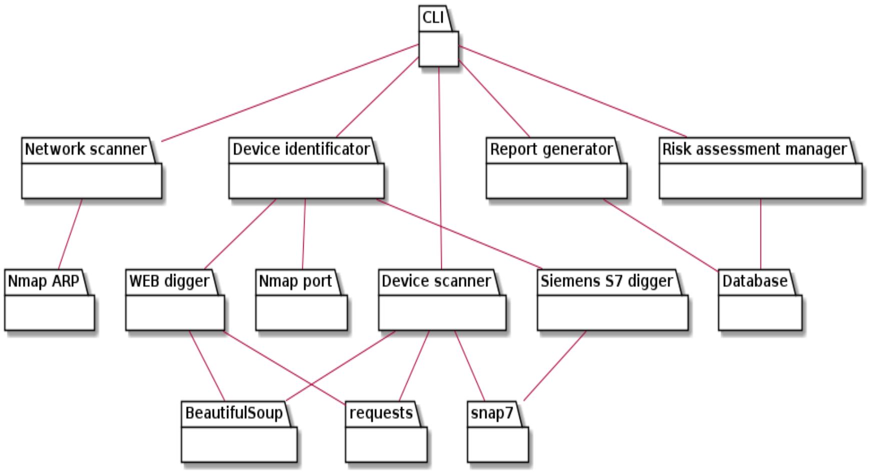

Figure 4 Block diagram of the ACSRA ICS system

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.

2.10.3 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:

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.

Open database searches with ACSRA ICS Python web scraper: A Python-based web scraper is utilized to search open databases, gathering relevant information to enhance the security assessment of the ICS.

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.

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 iden, and searching for network assets. This helps in identifying and cataloging all devices connected to the network.

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.

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 5, 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.

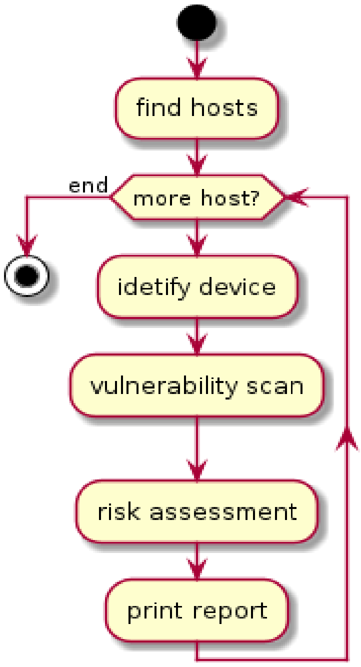

Figure 5 ACSRA ICS workflow

3. System Validation

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, utilizing 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.

During the validation of the ACSRA ICS system, I 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 I 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 4 compares ACSRA ICS with selected open-source ICS tools.

Table 4 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)

4. RESEARCH RESULTS AND ANALYSIS

Hypothesis 1: Combining five security standards and frameworks enhances risk assessment in SCADA and ICS environments, namely the Penetration Testing Execution Standard, NIST SP 800-115, NIST SP 8800-82r3, Open Source Security Testing Methodology Manual (OSSTMM), PenetrationTesting Framework Information Systems Security Assessment Framework (ISSAF), The Penetration Testing Execution Standard (PTES), and the OWASP Testing Guide.

Q1: Integration of Security Standards and Frameworks in SCADA and ICS Environments

Integrating various security standards and frameworks in SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems) environments enhances the risk assessment process by offering a diverse perspective on potential vulnerabilities and threats. This comprehensive coverage allows for improved decision-making through multi-criteria risk prioritization, while also enabling tailored risk assessments specific to operational environments. A holistic approach aligns security measures with business objectives, ensuring both technical and operational aspects are considered. Furthermore, integration helps ensure adherence to relevant regulations, reducing legal risks, and supports continuous improvement through ongoing updates and refinements based on emerging threats and technological advancements. Overall, this leads to a more effective, efficient, and adaptable approach to security management in SCADA and ICS environments.

Q2: Contribution of Integrated Approach to Continuous Improvement in Cybersecurity

Adopting an integrated approach fosters a culture of continuous improvement in cybersecurity within SCADA and ICS environments by establishing continuous refinement of security measures through feedback loops. This approach promotes collaboration and shared expertise among different teams and stakeholders, encouraging flexibility and innovation in response to evolving threats. Benchmarking against industry standards drives the pursuit of excellence, while enhancing organizational resilience through ongoing assessment and optimization. Leadership commitment to cybersecurity reinforces the importance of integration and supports initiatives for enhancement. Collectively, these elements contribute to a collaborative, adaptable, and excellence-driven culture in cybersecurity practices.

Q3: Advantages of Open-Source Security Resources in SCADA and ICS Environments

Using open-source security resources offers several key advantages that contribute to cost-effective security practices. Transparency allows organizations to validate the security of solutions and identify vulnerabilities, while community collaboration enhances the quality and reliability of these resources through diverse contributions. Cost savings are achieved as open-source software is typically free or low-cost, reducing the financial burden on organizations. Customization capabilities enable tailored security solutions without additional expenses, and rapid innovation facilitates quick updates and enhancements to address emerging threats. Additionally, leveraging open-source resources mitigates risks associated with vendor lock-in and provides flexibility in choosing the best solutions. These advantages collectively support effective and economical security management in SCADA and ICS environments.

Q4: Benefits of Standardized Frameworks for Communication and Collaboration

Standardized frameworks enhance communication and collaboration among stakeholders in SCADA and ICS environments by providing a common vocabulary and shared language for discussing security risks, controls, and best practices. This common language facilitates effective communication among IT professionals, engineers, management, and regulatory bodies. The promotion of interoperability simplifies integration efforts and streamlines information sharing, while ensuring consistency in security practices across the organization. Structured methodologies for risk management allow stakeholders to systematically identify, evaluate, and address security risks in a coordinated manner, supporting compliance with regulatory requirements and industry standards. Furthermore, standardized frameworks encourage continuous improvement through regular updates and feedback mechanisms, driving ongoing enhancement of security measures. These benefits lead to improved communication, collaboration, and overall security within SCADA and ICS environments.

Hypothesis 2: Automating risk assessment tasks significantly enhances efficiency and accuracy in SCADA and ICS environments.

Automation significantly enhances risk assessment, vulnerability management, and incident response in SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems) environments by increasing efficiency, accuracy, and proactive threat management.

Q1: Specific Risk Assessment Tasks Improved by Automation

Automation in risk assessment within SCADA and ICS environments can streamline data collection from network logs, system configurations, and vulnerability databases, ensuring comprehensive and efficient data acquisition. Automated tools can analyze this data to identify potential vulnerabilities, misconfigurations, and suspicious activities. By prioritizing risks based on severity, likelihood, and impact, automation allows for focused resource allocation. Additionally, it can generate detailed reports on identified vulnerabilities, recommended actions, and compliance status, facilitating clear communication with stakeholders.

Q2: Enhancing Security Posture through Automation

Automated vulnerability scanning tools enable timely detection of vulnerabilities such as software flaws and misconfigurations, preventing exploitation. Continuous monitoring solutions detect anomalous and suspicious activities in real-time, alerting security teams to potential incidents. Automation streamlines incident response by automating repetitive tasks, allowing for swift triage, investigation, and containment of security incidents, thus minimizing operational impact. Furthermore, automated systems dynamically adjust security controls in response to evolving threats and operational changes, maintaining effective protection against new vulnerabilities.

Hypothesis 3: Penetration testing is a crucial cybersecurity practice for identifying vulnerabilities in SCADA and ICS systems.

Q1: Why is penetration testing considered crucial for identifying vulnerabilities in SCADA and ICS systems, and how does it contribute to security?

Penetration testing is vital for SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems) because it systematically evaluates the security of critical infrastructure. This involves assessing the network architecture, communication protocols, and specific components connected via 5G. Key aspects include SCADA/ICS Network Assessment, which evaluates network security to identify vulnerabilities exploitable via 5G, and Wireless Security Assessment, which assesses the security of 5G connectivity for SCADA/ICS devices. Protocol and Communication Testing targets vulnerabilities in communication protocols over 5G, while Device and Controller Security Assessment identifies firmware and configuration weaknesses in devices and controllers connected through 5G. Human-Machine Interface (HMI) Testing ensures HMI systems' security, addressing potential 5G exploitation. Additionally, toolkit and desktop/server component evaluations identify vulnerabilities in critical software components. Overall, penetration testing is pivotal in detecting and mitigating vulnerabilities, thus enhancing the security posture of SCADA and ICS systems against cyber threats.

Q2: How does prioritizing penetration tests based on critical infrastructure components and high-risk vulnerabilities enhance the overall effectiveness of security measures in SCADA and ICS environments?

Prioritizing penetration tests on critical infrastructure components and high-risk vulnerabilities optimizes security measures in SCADA and ICS environments. This focused approach involves concentrating on areas of greatest concern, such as high-risk vulnerabilities and critical infrastructure. It includes performing assessments like SCADA/ICS Network, Wireless Security, Protocol and Communication Testing, Device and Controller Security, and HMI Testing. Ensuring timely identification and mitigation of vulnerabilities affecting crucial components is key to this approach. By aligning testing efforts with organizational priorities and risk management objectives, organizations can strengthen their overall security posture. Targeting the most significant risks helps reduce the likelihood of successful cyber attacks, thereby enhancing the resilience of SCADA and ICS systems against potential threats.

Hypothesis 4: Classifying vulnerabilities based on authentication, communication protocols, firmware/software, configuration weaknesses, and wireless networks provides a comprehensive understanding of potential risks.

Q1: How does classifying vulnerabilities based on multiple factors provide a comprehensive understanding of potential risks, and why is this approach important for SCADA and ICS security?

Classifying vulnerabilities by examining factors like authentication, communication protocols, firmware/software, configuration, and wireless networks offers a thorough understanding of potential risks in SCADA and ICS systems. This method helps identify weaknesses across various security aspects: issues with authentication address the risk of unauthorized access, while communication protocol vulnerabilities focus on securing data transfer channels. Firmware and software vulnerabilities target the integrity of core system components, and configuration weaknesses involve risks from misconfigurations. Additionally, evaluating wireless network vulnerabilities reveals threats within the 5G infrastructure.

Such a comprehensive classification approach enables organizations to effectively prioritize and address specific vulnerabilities, allocate resources efficiently, and improve overall security against cyber threats in SCADA and ICS environments connected via 5G.

5. Conclusions

This section summarizes the key achievements, recommendations, and future work. The dissertation introduces ACSRA ICS (Automated Cyber Security Risk Assessment for Industrial Control Systems), a novel risk assessment methodology for cybersecurity in 5G-connected SCADA and ICS environments. As 5G technology integrates into critical infrastructures, the need for robust cybersecurity is highlighted.

The study emphasizes penetration testing as a proactive strategy, validating ACSRA in a 5G SA system. It successfully integrated five major penetration testing methodologies, providing a comprehensive risk assessment, identifying system-specific vulnerabilities, and improving incident response plans. Automation for risk assessment tasks was also explored to enhance efficiency and accuracy.

Additionally, the dissertation categorized penetration tests, introduced Vulnerability Modes and Effects Analysis (VMEA), and prioritized tests for 5G-connected SCADA/ICS environments. It demonstrated the identification of 5G-enabled ICS devices and showed that ACSRA ICS effectively detects a wide range of vulnerabilities while being non-disruptive and reliable.

Key findings include:

1. Traditional vulnerability scanners may disrupt critical processes in 5G-connected PLCs.
2. 5G connectivity introduces new attack vectors not covered by traditional scanners.

The research sets the stage for further advancements in securing critical infrastructures with 5G technology and suggests that the methodology can be adapted for both large enterprises and SMEs, with the potential for customization and development of specialized tools.

5.1 Benefits of ACSRA ICS

ACSRA ICS stands out for its advanced vulnerability detection, identifying not only known vulnerabilities from public databases but also unique ones specific to the configurations of Programmable Logic Controllers (PLCs). The tool's ability to be customized with user-defined patterns enhances its detection capabilities beyond standard databases, allowing it to uncover vulnerabilities that generic tools might miss, thus providing a more thorough security assessment. Additionally, ACSRA ICS offers continuous traffic analysis with real-time alerts for detected vulnerabilities. This proactive approach aids in early detection and prevention of cyber-attacks, maintaining the operational integrity of industrial control systems (ICS) by enabling immediate identification and response to threats, which minimizes potential damage. The tool's flexible deployment options—either on-premises or cloud-based—simplify installation and maintenance, catering to various operational needs and ensuring scalability for different sizes of operations, from small facilities to large industrial complexes.

5.2 Limitations of ACSRA ICS

However, ACSRA ICS has some limitations. Its effectiveness can be restricted by device compatibility, as it may not support all PLC types, depending on their models and configurations. Additionally, using ACSRA ICS effectively requires substantial expertise in both PLCs and cybersecurity. Users need advanced skills for detailed data analysis and tool performance, which necessitates specialized training and experience. Furthermore, each deployment might need significant customization and fine-tuning to meet the specific needs of the controlled environment, requiring ongoing attention from skilled personnel.

5.3 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.

5.4 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[18]. 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.

5.5 Research Future and Direction

This research not only establishes a robust framework for securing critical infrastructures but also paves the way for future advancements in leveraging 5G technology for enhanced cybersecurity measures. The methodology outlined in this dissertation is versatile, catering to the needs of both large enterprises operating private networks and small and medium-sized enterprises (SMEs) relying on public networks. Furthermore, the methodology's adaptability allows for the extension of its application to address a wide array of vulnerabilities across diverse industrial sectors. Through the customization of testing software, tailored solutions can be developed to suit the specific requirements of smaller companies, ensuring the effective deployment of advanced security functionalities as elucidated in this study.

Scientific Publications Related to the Thesis Points

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. H. Altaleb and Z. Rajnai, “Enhancing Cybersecurity in Industrial Control Systems Through GRC Framework: Principles, Regulations, and Risk Assessment,” *Adv. Sci. Technol. Secur. Appl.*, vol. Part F2433, pp. 223–233, 2024, doi: 10.1007/978-3-031-47990-8_20.
3. H. Altaleb and Z. Rajnai, "Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures," 2023 IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics (SISY), Pula, Croatia, 2023, pp. 000625-000630, doi: 10.1109/SISY60376.2023.10417951
4. Zoltán Rajnai, Haya Altaleb”Risk assessments methods and cyber vulnerabilities in scada systems”NATIONAL SECURITY REVIEW : PERIODICAL OF THE MILITARY NATIONAL SECURITY SERVICE 2021 : 2 pp. 181-194. , 14 p. (2021)
5. H. Altaleb and R. Zoltan, “A Comprehensive Analysis and Solutions for Enhancing SCADA Systems Security in Critical Infrastructures,” *ICCC 2024 - IEEE 11th Int. Conf. Comput. Cybern. Cyber-Medical Syst. Proc.*, pp. 247–252, 2024, doi: 10.1109/ICCC62278.2024.10582956
6. ACSRA ICS: Automated Cyber Security Risk Assessment Methodology for Industrial Control Systems, Accepted to Acta Hungarica Polyticnica.
7. H. Altaleb, “Security services in 5G wireless networks,” *Biztonságtudományi Szle.*, vol. 4, no. 2. Ksz., pp. 25–34, 2022, doi: 10.1002/9781119244400.ch14.

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] 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.

[3] M. Čergeť 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.

[4] H. Altaleb, “Security services in 5G wireless networks,” *Biztonságtudományi Szle.*, vol. 4, no. 2. Ksz., pp. 25–34, 2022, doi: 10.1002/9781119244400.ch14.

[5] 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.

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

[7] 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.

[8] A. Whitaker and D. P. Newman, “Penetration testing and network defense,” p. 598, 2006.

[9] 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.

[10] 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.

[11] 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.

[12] S. Sandhya, S. Purkayastha, E. Joshua, and A. Deep, “Assessment of website security by penetration testing using Wireshark,” *2017 4th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2017*, 2017, doi: 10.1109/ICACCS.2017.8014711.

[13] R. Soepeno, “Wireshark: An Effective Tool for Network Analysis,” *CYBV - Introd. Methods Netw. Anal.*, pp. 1–15, 2023.

[14] G. Lyon, “Nmap network scanning,” *Nmap.Org*, p. 270, 2008.

[15] 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.

[16] 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.

[17] H. Altaleb and R. Zoltan, “A Comprehensive Analysis and Solutions for Enhancing SCADA Systems Security in Critical Infrastructures,” *ICCC 2024 - IEEE 11th Int. Conf. Comput. Cybern. Cyber-Medical Syst. Proc.*, pp. 247–252, 2024, doi: 10.1109/ICCC62278.2024.10582956.

[18] H. Altaleb and Z. Rajnai, “Enhancing Cybersecurity in Industrial Control Systems

Through GRC Framework: Principles, Regulations, and Risk Assessment,” *Adv. Sci. Technol. Secur. Appl.*, vol. Part F2433, pp. 223–233, 2024, doi: 10.1007/978-3-031-47990-8_20.