ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOCTORAL (Ph.D) THESIS FOR PUBLIC DEFENSE

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

24-07-2024

Complex Exam

Committee:

President: Prof. Dr. László POKORÁDI; ÓE

Member: Prof. Dr. Tibor KOVÁCS; ÓE

Member: Dr. habil. Farkas Tibor; National University of Public Service

Public Defence Committee:

Reviewers:

Prof. Dr. Gogolák László, associate professor; Technical College of Applied Studies Subotica

Dr. Judit Lukács; associate professor; ÓE

Declaration

I, Haya Altaleb, declare that the content of this dissertation is the product of my original work, and it contains no sources or resources other than the ones mentioned and acknowledged. This work has not been submitted to another institution, neither in Hungary nor outside, nor in the same or similar way.

Acknowledgments

To my ultimate god the Lord of the world who has the praise and thanks.

I am eternally thankful to my parents, Hatem Altaleb and Samihah Alnaimat, for their unwavering support and encouragement in every aspect of my life. Their guidance has propelled me forward and inspired me to strive for excellence. My journey wouldn't be the same without their constant presence and belief in me. I also owe a debt of gratitude to my brother Shareef, whose strength and encouragement have motivated me to persevere in my educational pursuits. Additionally, I am grateful to my sister Fatima, as well as to all my extended family and friends, for their continuous support and companionship.

My research journey owes its success to the steadfast dedication and mentorship of my supervisor, advisor, and esteemed mentor, the Dean of Donát Bánki Faculty of Mechanical and Safety Engineering Prof. Dr. Zoltán Rajnai, I consider myself incredibly fortunate to have had the opportunity to learn under his guidance, and I am deeply grateful for his unwavering patience and boundless support. His encouragement and faith in my research topic and ideas have been invaluable, and for that, I extend my heartfelt thanks.

I extend special appreciation to Professor Lívia Cveticanin, and Professor Goda Tibor for their diligent oversight and guidance throughout each semester of my studies. My heartfelt gratitude also extends to all Obuda University professors, Ph.D. colleagues, friends, and individuals who have contributed to my learning and collaboration during this period and beyond. Each interaction has left a lasting impression on my journey, shaping who I am today.

Furthermore, I am profoundly thankful to the Stipendium Hungaricum program for their generous support of my Ph.D. studies from 2019 until now. Their funding has been instrumental in enabling me to pursue my academic aspirations.

Abstract

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.

Contents

List of Figures

List of Tables

Abbreviations

Error! Reference source not found. below highlights some of the terms and their definitions that were used in this document.

Table 1 List of the Abbreviations

Abbreviations	Full term
ICS	Industrial Control Systems
CI	Critical Infrastructure
SCADA	Supervisory Control And Data Acquisition
PCs	Personal Computers
HMI	Human Machine Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
WAN	Wide-Area Network
IoT	Internet of Things
RTU	Remote Terminal Unit
VCN	Virtual Closed Network
DoS	Denial of Service
MAC	Media Access Control
WAN	Wide-Area Network
IP	Internet Protocol
SLAMMER	A computer worm that impacted a nuclear power plant and utilities in the United States in 2003
Dragonfly	A cyber assault on the energy sector involving spam emails to spread malware
DDoS	Distributed Denial of Service
MITM	MITM - Man-In-The-Middle
MAC	Media Access Control
SSL	Secure Socket Layer
PLCs	Programmable Logic Controllers
ARP	Address Resolution Protocol
DNS	Domain Name System
SIS	Safety Instrumented System
AGA	American Gas Association
IEEE	Institute of Electrical and Electronics Engineers
VFDs	Variable Frequency Drives
LAN	Local Area Network
VFDs	Variable Frequency Drives

GRC	Governance, Risk, and Compliance
POLP	Principle of Least Privilege
SoD	SoD - Separation of Duties
AAA	AAA - Authentication, Authorization, and Accounting
IT	IInformation Technology
RAMM -	Risk Analysis and Management Method
NATO	North Atlantic Treaty Organization
BS7799	BS7799 - British Standard 7799
ISRAM	Information Security Risk Analysis Method
OCTAVE	Operationally Critical Threat and Vulnerability Evaluation
AAA	Authentication, Authorization, and Accounting
PPP	Point-to-Point Protocol
PAP	Password Authentication Protocol
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NIST	National Institute of Standards and Technology
GDPR	General Data Protection Regulation
CPNI	Centre for the Protection of National Infrastructure
CSSC	Cross-Sector Safety & Security Communications
NERC	North American Electric Reliability Corporation
TSA	Transportation Security Administration
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ERM	Enterprise Risk Management
MES	MES - Manufacturing Execution System
ACSRA	Automated Cyber Security Risk Assessment
SOC	Security Operations Center
IIoT	Industrial Internet of Things
OSSTMM	Open Source Security Testing Methodology Manual
ISSAF	Information Systems Security Assessment Framework
PTES	Penetration Testing Execution Standard
OWASP	Open Web Application Security Project
DDoS	Distributed Denial of Service
ASVS	Application Security Verification Standard
SIEM	Security Information and Event Management
GLPI	Gestionnaire Libre de Parc Informatique (Free Computer Inventory Software)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
SIEM	Security Information and Event Management
VMEA	Vulnerability Modes and Effects Analysis

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].SCADA systems (supervisory control and data acquisition) are considered master cyber-attack targets based on the extreme impacts on economies, industrial sectors, properties, and human lives. Existing security solutions, like (access controls, firewalls, intrusion detection, online monitoring, intrusion detection and prevention, live forensics analysis, and intrusion response systems) can protect SCADA systems from cyber-attacks such as (SQL injection attacks, denial of service attacks, and spoofing attacks). Still, they are far from ideal protection. The current SCADA market demonstrates that companies continue to see the advantages of their processes being provided by modern SCADA systems. In fact, by 2025, the industry is forecasted to hit US$47.04 billion. Looking at the weaknesses that characterize each year's count gives a general indication of where vulnerabilities can be discovered when it refers to SCADA systems[6]. To secure our systems Penetration testing methodologies are a must and it need to be updated, the existing standards and methodologies exhibit similarities, but subtle distinctions exist among them. 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 new 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. By Integrating the best existed onces we can come out with ACSRA ICS methodology, the study proposed and tested the ACSRA methodology in an isolated 5G SA system. Evaluation of five prominent penetration testing methodologies highlighted their seamless integration into ACSRA, showcasing positive outcomes such as a comprehensive understanding of risks, identification of system-specific vulnerabilities, and enhancement of incident response plans. Additionally, exploration of automation possibilities for risk assessment tasks aimed at improving efficiency and accuracy.

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 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.

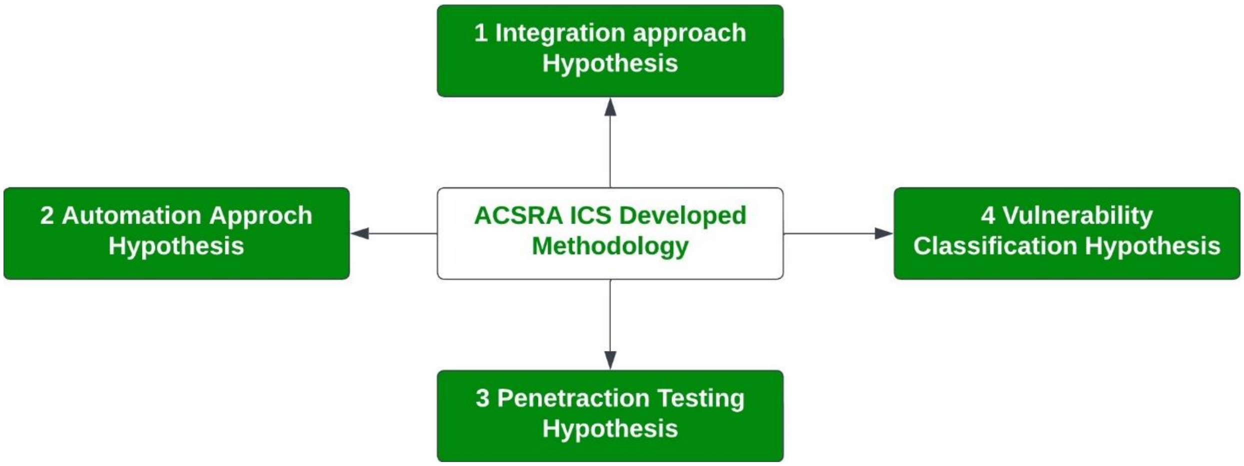

1 Integration approach Hypothesis
2 Automation Approch Hypothesis
ACSRA ICS Developed Methodology
4 Vulnerability Classification Hypothesis
3 Penetraction Testing Hypothesis

Figure 1 The research model

1.2.1 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?

1.2.2 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?

1.2.3 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?

1.2.4 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.

1.4 Dissertation Structure

Chapter 1 Introduction: Chapter 1 of the dissertation delves into the significance of safeguarding SCADA systems from cyber-attacks, highlighting the inadequacies of existing security solutions amidst the burgeoning SCADA market. It identifies the research problem, emphasizing the need for a specialized cybersecurity risk assessment methodology tailored for (ICS) and SCADA environments. The chapter presents research questions and hypotheses aimed at developing an Automated Cyber Security Risk Assessment Methodology (ACSRA) and outlines the dissertation's objectives, including exploring commonalities among cybersecurity standards, proposing an integration approach, assessing automation possibilities, categorizing penetration tests and vulnerabilities, and conducting experimental validation in a

5G-connected SCADA/ICS environment. Finally, the structure of the dissertation is outlined to provide a roadmap for the subsequent chapters.

Chapter 2 Literature review: This chapter provides a comprehensive exploration of the theoretical underpinnings relevant to the study, delving into the evolution of cyber threats and vulnerabilities in (ICS), the intricacies of SCADA networks, and the various types of attacks they face. Through an in-depth analysis of security challenges and potential solutions, the chapter sets the stage for understanding the complexities of safeguarding critical infrastructure against modern-day threats. Grounded in theoretical frameworks, this chapter elucidates key concepts, evaluates existing theories, and elucidates the assumptions shaping the research direction, paving the way for a nuanced investigation into enhancing the security posture of SCADA systems.

Chapter 3 Enhancing Cybersecurity in through GRC Framework: Principles, Regulations, and Risk Assessment: This chapter underscores the significance of information security in protecting vital systems and data, elucidating the CIA triad framework encompassing confidentiality, integrity, and availability. It emphasizes the criticality of safeguarding (ICS) due to their pivotal role in managing essential infrastructures. Furthermore, the chapter's threefold contribution includes an introductory overview of ICS and information security, an in-depth literature review on information security principles, and an exploration of governance, risk, and compliance (GRC) aspects within the context of ICS.

Chapter 4 ACSRA ICS METHODOLOGY: Research Procedure, The methodology chapter of this dissertation provides a structured framework for researching the Automated Cyber Security Risk Assessment Methodology for (ACSRA ICS). Beginning with an overview of the research objectives, the chapter delves into a comprehensive review of existing penetration test methodologies, 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 security.

Chapter 5 Research Results and Analysis: This chapter presents the main findings of the study, focusing on the integrated approach hypothesis and automation hypotheses. The integrated approach hypothesis explores the benefits of combining various security standards and frameworks for risk assessment in SCADA and ICS environments, emphasizing comprehensive coverage, risk prioritization, customization, holistic approach, regulatory compliance, and continuous improvement. Additionally, automation hypotheses investigate how automating risk assessment tasks and penetration testing can enhance efficiency, accuracy, and overall security posture in SCADA and ICS environments. By prioritizing penetration tests based on critical infrastructure components and high-risk vulnerabilities, organizations can optimize resource allocation and effectively mitigate potential cyber threats. Furthermore, classifying vulnerabilities based on authentication, communication protocols, firmware/software, configuration weaknesses, and wireless networks provides a comprehensive understanding of risks, aiding in strategic risk management decisions and enhancing overall security posture.

Chapter 6 Conclusions which presents the main research findings and the overall thesis contributions. In addition, this section includes the study directions and recommendations for future work. this dissertation has successfully achieved its objectives by addressing key hypotheses related to an integrated approach, automation, penetration testing, and vulnerability classification in the context of SCADA and ICS environments. The integration of various cybersecurity standards into the Automated Cyber Security Risk Assessment Methodology (ACSRA ICS) has proven to enhance the comprehensive understanding and management of risks. Automation has been established as a valuable tool in improving the efficiency and accuracy of risk assessment tasks, ultimately enhancing overall security posture. The importance of penetration testing in identifying vulnerabilities in a controlled manner and the significance of vulnerability classification for prioritizing mitigation efforts have been underscored.

Furthermore, the dissertation outlines essential cybersecurity measures and best practices to counteract malware threats in SCADA systems. Strategies such as network segmentation, regular system updates, incident response planning, access controls, employee training, and secure software development practices contribute to a robust security posture, minimizing vulnerabilities exploited by malware. The proactive deployment of Intrusion Detection and Prevention Systems (IDPS) is highlighted as crucial for swiftly detecting and mitigating malware attacks. Looking ahead, the research sets the stage for future advancements by proposing the integration of 5G technology for enhanced cybersecurity measures. The versatile methodology outlined caters to the needs of both large enterprises and small and medium-sized enterprises, with the potential for customization to address vulnerabilities across diverse industrial sectors. This dissertation not only establishes a solid framework for securing critical infrastructures but also encourages ongoing improvement in cybersecurity practices to defend against evolving malware threats, ensuring the integrity, availability, and confidentiality of critical infrastructure.

Chapter 7 Ph.D. Candidate List of publications The author has made significant contributions to the field of cybersecurity and technological advancements, with 14 papers published in various outlets. These include one in a Web of Science and Scopus-indexed international journal, four in Scopus-indexed IEEE conference proceedings, three in Hungarian journals, and one in an online journal. The author also participated in 13 conferences, including five international events. Notably, one paper is scheduled for publication in the Critical Infrastructure Protection in the Light of the Armed Conflicts journal, indexed in Scopus and Web of Science. Another paper has been accepted for presentation at the IEEE 11th International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC 2024) in Hanoi, Vietnam, while two papers are under review for Acta Hungarica Polytechnica.

2 Literature review

This chapter provides insights related to the theoretical approach of this study. It defines the key concepts, evaluates the relevant theories, and explains the assumptions that have guided this research.

2.1 ICS cyber threats, vulnerabilities, and protection

The past two decades have witnessed remarkable advancements in the fields of computing and communication. Any system has the potential to be considered critical when its vulnerabilities evolve into threats that can cause chaos across social structures, energy sectors, security frameworks, healthcare systems, and various other dimensions of society. The breakdown or unavailability of a system's functions can have catastrophic consequences on society, the economy, and overall stability. Traditionally, the focus of infrastructure security was primarily centered on environmental risk[6].

Cyberattacks, despite this, are a reality and have switched the focus to further risks and damages. The attackers attempt to exploit network and Internet weaknesses. Critical Infrastructure (CI) 's susceptibility to cyber threats has necessitated the development of modern security solutions. Inaccessibility or breakdown The cascading failures caused by a single CI can bring massive havoc and harm to society, the economy, the stability of a nation, and numerous other infrastructures[7].

Traditional security solutions aim to accommodate developing threats that are well-known; nevertheless, Innovative, robust assaults are unavoidable Hence, it is imperative to implement adaptable security strategies in order to counteract these threats. The article delves into the realm of security issues and unresolved queries in this domain. The persistent increase in cyber threats targeting SCADA systems is a result of factors such as advancing levels of sophistication, ongoing modernization efforts, the constant demand for real-time operations and distribution, and the intricate multi-component architecture of these systems. To enable the complex tracking of interconnected and integrated systems, it becomes essential to develop advanced SCADA systems that align with the requirements of the forthcoming architectural advancements. Commercial manufacturers have enhanced their firewall capabilities to handle

SCADA protocols or created SCADA-specific firewalls. Although open-source firewalls are utilized effectively in IT networks, their application in SCADA networks has not been well examined[8].

This chapter sheds light on the security problems and unresolved issues surrounding SCADA devices and demonstrates the importance of securing them. Above and beyond, in addition, the author reviews SCADA networks and discusses the available security solutions for SCADA network attacks. (SCADA) systems are utilized by critical infrastructures (CIs). In the following sections, the authors review SCADA networks, SCADA network attacks and solutions, SCADA protocols, and SCADA critical infrastructure with the most common attack on them.

2.2 SCADA networks

SCADA systems are frequently elaborate networks with numerous components. These systems are sorted into three types depending on the operator. They can be found as fully automated by machines and software, fully manual by human engineers and technicians, or hybrid in which part control is handled automatically, and some are performed manually. To accomplish all of these tasks, numerous SCADA systems contain[9][10]:

Field interface devices: Local control devices, including valve actuators, motor controls, and control switch boxes, Sensors reporting and detecting power levels, flow rates, pressure, and temperature.

Operating equipment: The SCADA network controls the motors, pumps, factory automation systems, and valves.

Control PCs: Embedded computers or specialized PCs that receive data from sensor networks, report this data to management systems, and control the associated operational equipment. These computers may automatically make decisions depending on sensor data, or they may relay commands from management computers.

Management PCs: PCs terminals with HMI (Human Machine Interface). These computers provide operators with an interface for monitoring and controlling SCADA network devices.

Network communication (local and remote): SCADA networks employ several communication methods. Short-range communication utilizes serial communication, USB, and custom wired networks. Ethernet, TCP/IP, WiFi, dial-up networking, cellular packet data, and other protocols are utilized for long-distance communication. In addition, SCADA networks increasingly employ the Internet for long-distance communication and remote access.

SCADA networks comprise a mix of personal computers (PCs) and embedded systems using real-time operating systems such as VxWorks, INTEGRITY, or MQX. A significant portion of the PCs within SCADA networks have not received updates or software patches since their initial deployment, rendering them susceptible to potential attacks. The embedded computers present in SCADA networks were designed before security gained paramount importance and thus lacked comprehensive security measures[9]. Typically, efforts are made to protect the PCs within the SCADA network by ensuring they run the latest operational systems with up-to-date security patches and software. However, there are cases where specific SCADA software is only compatible with older operating system versions, impeding the upgrade of the PC and consequently creating a security vulnerability. Addressing the security challenges of these legacy PC systems and embedded SCADA computers requires a distinct approach[9].

Contemporary control centers are furnished with data servers, Human-Machine Interface (HMI) stations, and supplementary servers to assist operators in overseeing the factory network. Generally, this SCADA network is interconnected with an external corporate network and/or the global internet using dedicated gateways. These gateways function as intermediaries between IP-based networks within the factory premises and SCADA networks utilizing the Fieldbus protocol. Their role encompasses protocol translation, and facilitating communication between these separate networks. Furthermore, they incorporate caching mechanisms to enhance gateway performance when handling exchanged data objects between networks. A depiction of a standard SCADA network scenario can be observed in Figure 2.[11].

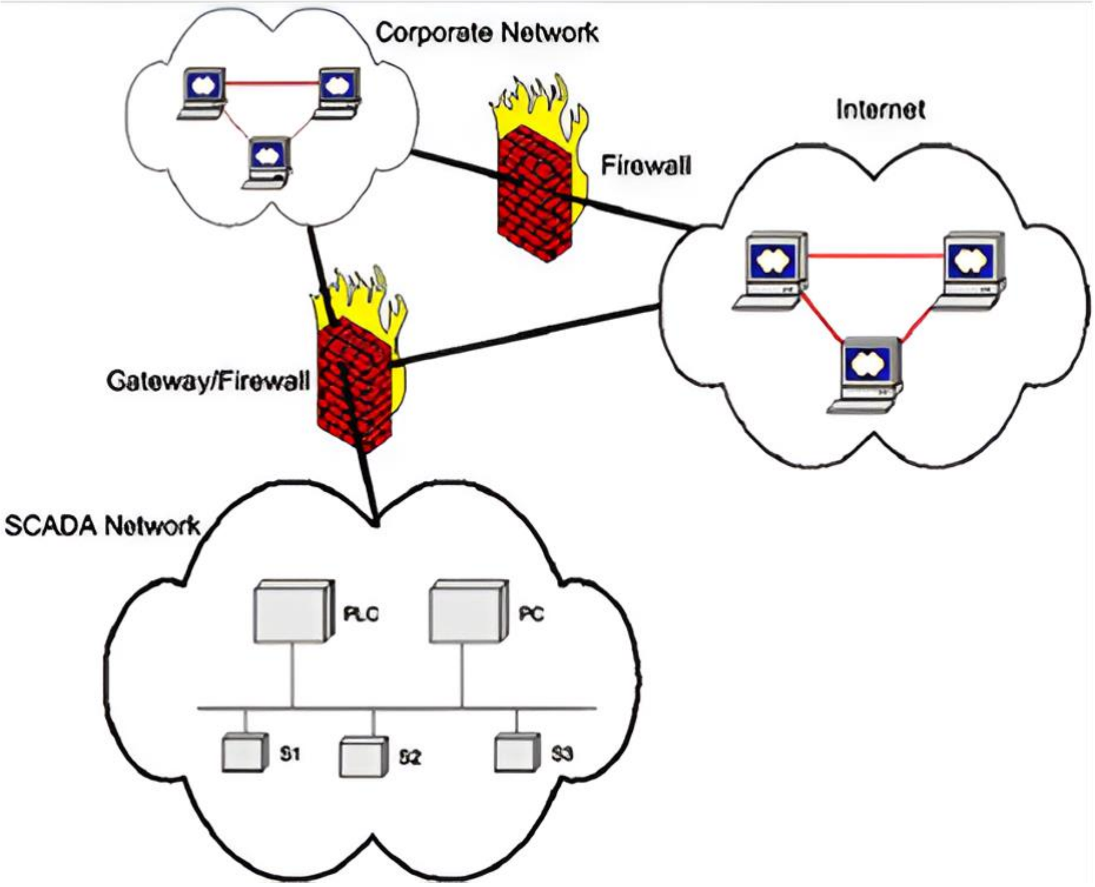


Figure 2 Standard SCADA network structure [11]

2.3 Attacks on SCADA networks

SCADA system attacks mostly aim at Manufacturing plant shutdown, train system delays, and sewage system spillage. SCADA sector should enhance its capability to bolster security measures for both legacy and contemporary devices. This enhancement should be carried out in a manner that ensures profitability, particularly concerning remote SCADA devices situated beyond corporate networks, as well as local SCADA devices, including those deployed on factory premises. By implementing improvements, existing SCADA devices can gain the ability to regulate their communications, identify and alert about unauthorized access or unusual data flow patterns, and incorporate comprehensive policy management for heightened security. These advancements collectively contribute to elevating the security stature of SCADA devices, effectively safeguarding them against the majority of cyber threats[12].

Preventing intrusions through the utilization of a SCADA firewall employing a virtual isolated network. The SCADA firewall may be utilized to protect remote devices without altering the SCADA system itself. It may also be used to preserve SCADA equipment deployed on a factory floor or in another non-remote location. Future SCADA equipment might be protected by firewall software. SCADA firewall should offer:

1. A device's ability to control the packets it processes.
2. Defending against cyberattacks launched over the Internet, the office network, or WiFi networks.
3. Enhance the security against Denial of Service and packet floods.
4. Capability to identify and report unusual traffic, probes, or assaults.
5. Capability to oversee and regulate filtering policy changes.

As noted previously, many SCADA equipment with insufficient safety are now hooked up to the internet, disclosing their security flaws. This may be rectified by establishing a virtual closed network with a SCADA firewall (VCN). To choose a Virtual Closed Network (VCN), the developer needs to establish communication protocols that limit the device's connections to only essential ones. These communication protocols outline the authorized parties the device can interact with, which protocols are permissible, and which ports remain open. These communication guidelines are then translated into firewall rules that the firewall employs to scrutinize communications prior to device processing. By applying these regulations, the firewall constrains the device's communication and establishes a virtual closed network. In scenarios where a hacker tries to breach a system lacking a firewall, methods like default passwords, dictionary attacks, or pilfered credentials might be employed. Often, these attacks are automated, enabling a large number of password-cracking efforts. By configuring a firewall with a whitelist of trusted hosts, the same system can thwart such attacks. Consequently, if the firewall screens out access attempts from hosts not on the whitelist, whether, by IP or MAC address, any login endeavor is hindered preemptively [13][14].

2.3.1 Open-Source Firewalls in SCADA Networks

This section evaluates the potential benefits and limitations of incorporating open-source firewalls into SCADA networks. It examines the effectiveness of open-source firewall solutions in detecting and preventing malware attacks while considering their compatibility, customization options, and community support. By assessing the feasibility and security implications of open-source firewalls, organizations can make informed decisions when selecting appropriate cybersecurity measures for their SCADA systems.

2.3.2 Benefits of Open-Source Firewalls:

2.3.2.1 Cost-Effectiveness:

One of the primary advantages of open-source firewalls is their cost-effectiveness. Open-source software is freely available, eliminating the need for expensive licensing fees associated with proprietary firewall solutions. This cost advantage can be particularly beneficial for organizations with limited budgets, allowing them to allocate resources to other critical areas of their SCADA systems' security. M. Baig et al.[15] designed and implement a P2P energy trading system for this remote community that allows residents to take advantage of distributed energy resources.

2.3.2.2 Customization and Flexibility:

Open-source firewalls offer a high level of customization and flexibility. Organizations can modify the source code to meet their specific requirements, tailoring the firewall rules and configurations to suit their SCADA network architecture and protocols. This customization capability enables organizations to build a firewall solution that aligns precisely with their unique security needs, enhancing the overall effectiveness of the defense against malware attacks[16].

2.3.2.3 Transparency and Trust:

Open-source firewalls promote transparency as the source code is open to public scrutiny. This transparency fosters trust and enables security experts and researchers to identify vulnerabilities, suggest improvements, and contribute to the ongoing development of the firewall solution. The collaborative nature of open-source projects can enhance the overall security of the firewall, as a larger community of users and developers can collectively work towards identifying and resolving security issues[17].

2.3.3 Limitations and Considerations Open-Source Firewalls *:*

2.3.3.1 Technical Expertise:

Implementing and managing open-source firewalls may require a certain level of technical expertise. Organizations need to ensure they have a knowledgeable staff or access to resources capable of effectively configuring and maintaining the firewall. While open-source communities often provide documentation and support, organizations should consider the availability of skilled personnel who can navigate the complexities of open-source firewall implementations within SCADA environments.

2.3.3.2 Compatibility and Interoperability:

SCADA systems often consist of diverse and complex components from various vendors. Compatibility and interoperability can pose challenges when integrating open-source firewalls into existing SCADA networks. Organizations need to thoroughly assess the compatibility of open-source firewall solutions with their specific SCADA infrastructure, protocols, and communication interfaces. Additionally, comprehensive testing is crucial to ensure smooth integration without disrupting critical operations.

2.3.3.3 Support and Maintenance:

The level of support and maintenance available for open-source firewalls can vary. While open-source communities provide forums, documentation, and community-driven support, organizations may not have direct access to dedicated technical support or immediate response times. It is important to consider the reliability of community support and evaluate the organization's ability to address issues promptly and effectively, ensuring the continued protection of SCADA systems against malware threats. Incorporating open-source firewalls in SCADA networks offers cost-effectiveness, customization, and transparency. However, careful consideration of technical expertise, compatibility, and support is necessary. By evaluating these factors, organizations can make informed decisions to enhance SCADA system security against malware attacks.

2.4 SCADA Critical Infrastructure

The critical infrastructure consists of a variety of different subsystems that collaborate within a network. As an illustration, consider power grid systems, where there are interconnected high-voltage transmission lines that connect to transformation substations. These substations, in turn, are linked to transformers, which are then connected to consumers through supply channels. According to several writers, the 1960s saw the beginning of the SCADA system. Alexandru [18] categorized the development of SCADA systems as technological and architectural changes.

As indicated in Figure 3 SCADA system evolution: (a) 1st generation; Monolithic SCADA systems with remote terminal units, (b) 2nd generation; Distributed SCADA systems, (c) 3rd generation Networked SCADA System (d) 4th generation; IOT Cloud-based SCADA System[19]., the evolution of architecture may be further subdivided into four prior generations based on their functional capabilities. The initial phase was characterized by traditional SCADA setups featuring Remote Terminal Units (RTUs). As distributed systems emerged, the second phase emerged, linking RTUs to interaction servers via wide-area networks (WAN). The expansion of the industrial landscape, the influx of new equipment providers, and the surge in automated processes collectively drove the evolution of networked SCADA systems, denoted as the third generation of SCADA. The fourth generation is heavily influenced by the Internet of Things (IoT) and cloud technology. IoT encompasses an array of devices and sensors that collect data from remote locations, establishing a wireless LAN connection to the SCADA master. This gathered data is subsequently transmitted to the cloud for further analysis. Apart from their user-friendliness and seamless integration, these systems deliver accelerated data scalability, heightened availability, enhanced efficiency, and cost advantages[19].

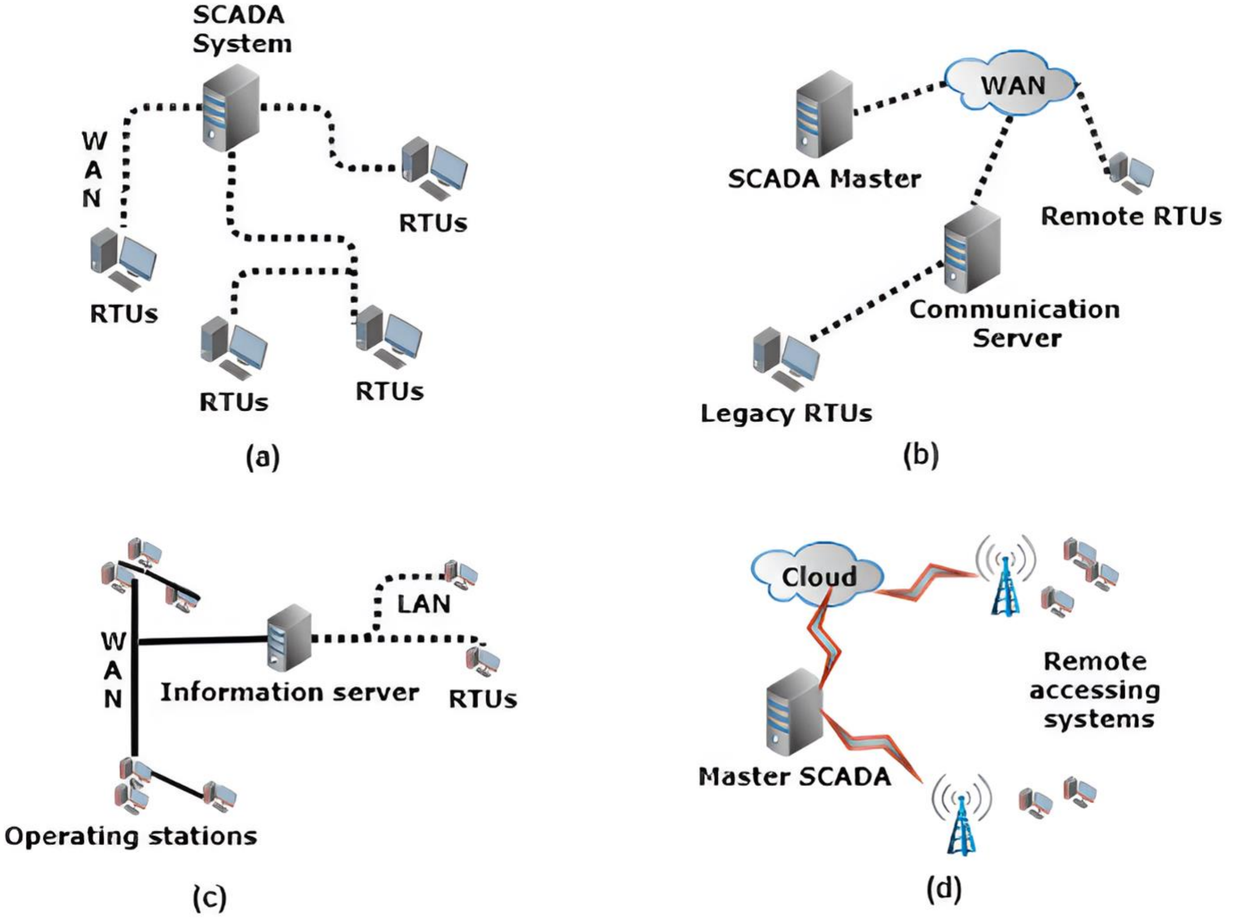


Figure 3 SCADA system evolution: (a) 1st generation; Monolithic SCADA systems with remote terminal units, (b) 2nd generation; Distributed SCADA systems, (c) 3rd generation Networked SCADA System (d) 4th generation; IOT Cloud-based SCADA System[19].

2.5 Cyber attacks on SCADA-based Critical infrastructure

Both government and NGOs view cyber issues as their primary issue at now. The vast majority of assaults are carried out by "Trojan horses" that are transmitted via email links and files. They are extremely tough to identify since they resemble authentic. Back in 2003, the 'SLAMMER' worm impacted a nuclear power plant and two utilities in the United States[20]. In a second cyber assault on the energy sector, dubbed 'Dragonfly,' spam emails were used to spread malware. An attacker can get access to a system using social engineering and then use it to carry out their malevolent plans. The presence of intruders from within the organization also poses a hazard. Because the attacker understands how to get through security measures, this form of assault is regarded to be the most harmful. For instance, a sewage flood in Queensland, Australia, was created by an attack on the sewage management system. Attackers used a USB flash drive to begin their attack [21]. Phishing is an additional technique of cyberattack that is meant to steal private information for financial purposes. These assaults are carried out in various techniques, including contacting users through a bogus website to obtain their financial information. A different form of cyber attack is the Distributed Denial of Service (DDoS) attack, where a substantial volume of data and traffic is sent to nodes/servers to exhaust their resources. These attacks create challenges in discerning between genuine and fraudulent entities. Man-In-The-Middle (MITM) attack is an additional advanced sort of cyberattack. Operates by interfering with device-to-device connection and transmitting malicious malware to infect a system.

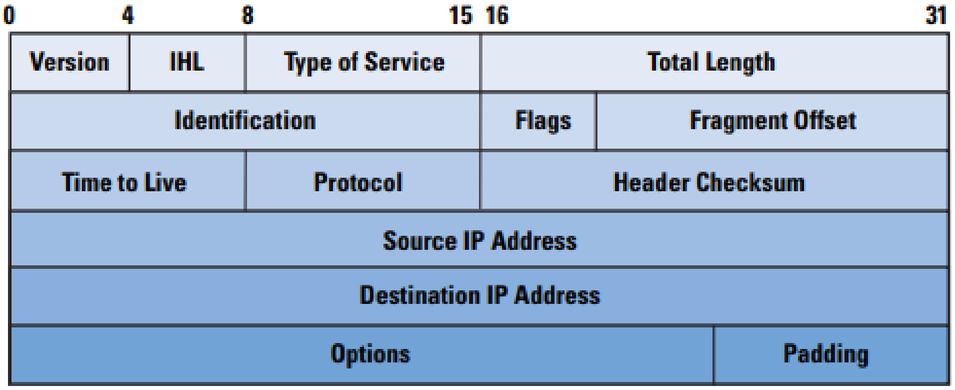
The expansion of Critical Infrastructure (CI) and the Internet of Things (IoT) underscores the necessity to enhance current SCADA systems in order to effectively manage the substantial amounts of large data produced by these devices. For instance, extensive and intelligent grids generate vast quantities of data that the present cloud computing techniques can amass. However, CISCO's observation indicates that the existing cloud infrastructure struggles with the magnitude, variety, and speed of the generated data. Furthermore, the direct uploading of data to the cloud for storage, processing, and analysis necessitates a high-capacity data transmission capability. Consequently, the emergence of cloud computing has tackled several common challenges linked with cloud-based SCADA systems. It enables temporary data storage and processing at the network's periphery, diminishing the volume of data transmitted and stored in the cloud. This strategy provides an enhanced resolution for applications that are sensitive to delays. However, integrating CI data with cloud computing systems is impeded by stringent security prerequisites, low latency demands, and seamless integration with high-availability services. A pivotal concern is the deficiency of effective and robust privacy and user authentication mechanisms on cloud platforms, where data replication management and screening are limited. Hence, the implementation of essential data security methods and protocols becomes imperative, coupled with comprehensive control over authentication and authorization procedures.[22].

2.5.1 Man-in-the-middle (MITM)

A Man-in-the-Middle (MITM) attack pertains to security breaches that occur when a user communicates with a legitimate organization. Among the most concerning aspects of an MITM attack is its capacity to intercept and inspect packets within encrypted communication channels. This kind of assault typically involves three participants: two individuals or entities engaged in information exchange and the "man-in-the-middle" actor who covertly intercepts the victim's communications. Neither of the communicating parties is typically aware of the MITM presence, making it one of the most commonly exploited methods that cybercriminals employ to steal information and funds in the realm of online communication[23]. Below, you will find a list of some of the most prevalent types of MITM attacks:

IP Spoofing: The Internet protocol address on a network identifies a device. This addressis similar to a location address used to locate a place. An attacker can spoof an IP address by masking himself as an application and altering packet headers in an IP address, IP relies on the upper-level TCP/IP suite layers to ensure accountability and reliability[24]. At the core of the IP protocol is the IP datagram, which is a packet transmitted across the Internet in a connectionless manner. An IP datagram carries sufficient network information to facilitate its forwarding to the intended destination. It consists of a header followed by a series of data bytes. The header contains essential details, including the type of IP datagram, the duration it should remain on the network (or the number of hops it should traverse), special flags indicating any specific purposes the datagram serves, as well as the source and destination addresses, among other fields, as shown in Table 2. The users trying to access a URL connected to such applications are sent to the hacker's website. Consequently, their information and data end up being available to the hacker. Considering that thousands of packets at a time should be modified, this method is not easy on a remote system[25]. Nonetheless, it is effective when trust exists between endpoints, such as insecure networks. There are specific tools that can send a spoofed datagram to any target. Usingsuch spoofing IP datagrams, a MITM attacker hijacks the communication to get exchanged public keys between communicators so that he can modify those keys. He can also hijack the encrypted messages and responses and then use the correct public keys to decrypt and encrypt them again for all the communication segments to avoid any possible suspicion.

Table 2 The IP Header [26]



<table>
<tr><th>0</th><th>4</th><th>8 … 15</th><th colspan="3">16 … 31</th></tr>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="6">Source IP Address</td></tr>
<tr><td colspan="6">Destination IP Address</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

Higher layers in the networking stack, above IP, utilize the source address found in an incoming packet to identify the sender. When a receiving station needs to communicate with the sender, it replies using the source address from the received datagram. Notably, IP does not make any attempts to validate whether the source address in a packet, generated by a node, genuinely belongs to that node. This lack of verification creates an opening for source address spoofing, where an attacker can manipulate the source address, leading the receiver to believe the packet originates from the spoofed address [26].

Numerous programs that allow the creation of spoofed IP datagrams are freely accessible on the Internet. For instance, tools like "hping" enable the generation of spoofed IP datagrams with a simple one-line command, which can then be sent to virtually anyone worldwide. Source address spoofing can occur at various network layers; for example, Address Resolution Protocol (ARP) spoofing redirects traffic intended for one station to another recipient. Additionally, Simple Mail Transfer Protocol (SMTP) is susceptible to spoofing, as it lacks sender address verification, enabling the sending of emails to recipients while pretending to be someone else [26].

Domain Name Server (DNS) Spoofing: DNS Spoofing, also known as Domain Name Server Spoofing: DNS primarily functions to translate domain names into corresponding IP addresses.

In this form of attack, the attacker intercepts the ID of a DNS request and responds to the target's request with an incorrect ID before the genuine DNS server has a chance to reply. This DNS spoofing technique causes the user to be directed to a counterfeit website created by the hacker, rather than the legitimate site the user intended to access. Users remain oblivious to the fact that they are not visiting a secure and trusted website but instead engaging with the hacker, potentially putting their login credentials and other critical information at risk of being captured[27]. Figure 4 shows the Domain Name System structure.

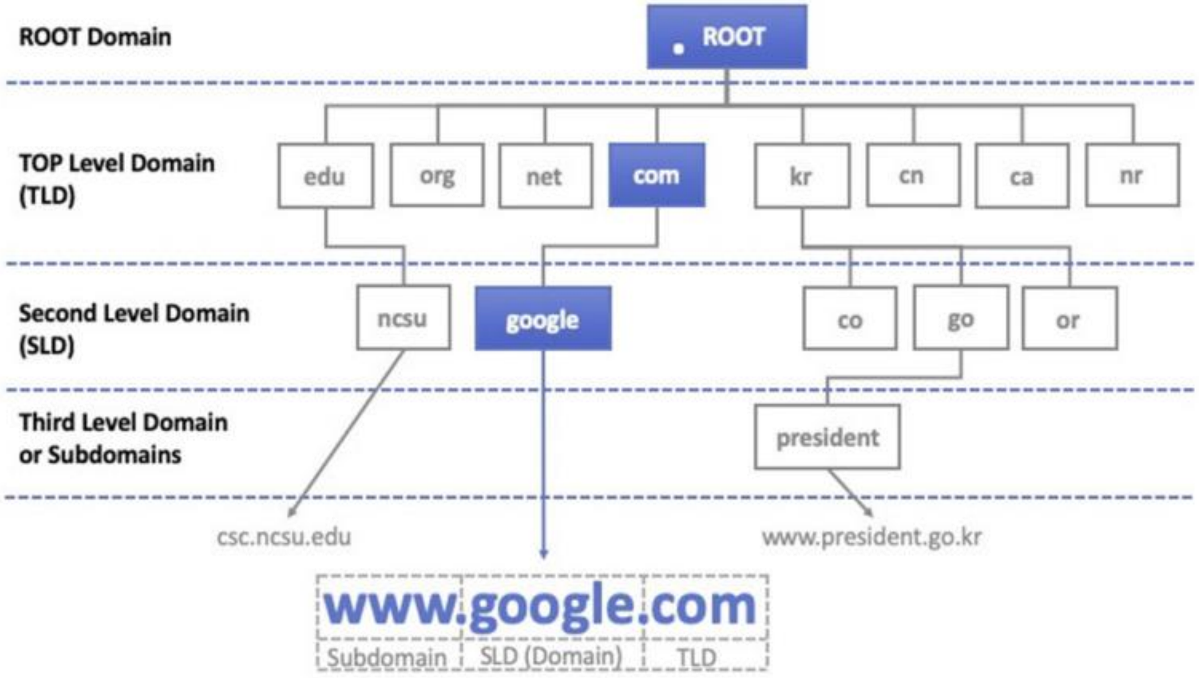


Figure 4 Domain Name System Structure [27]

DNS attacks may be separated into four categories: DNS data tampering, DNS data flooding, abuse of DNS, and DNS server structure. The following Figure shows the list of 11 DNS attacks that are categorized.

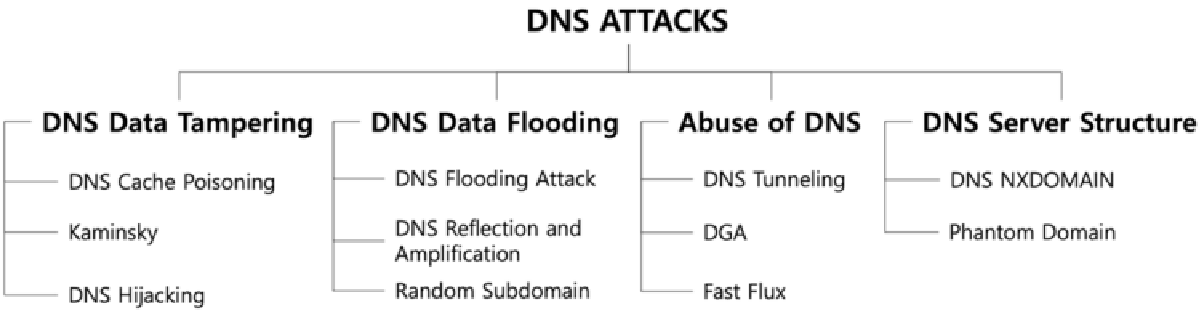


Figure 5 11 DNS attacks. DNS: Domain Name System; DGA: domain generation algorithm [27].

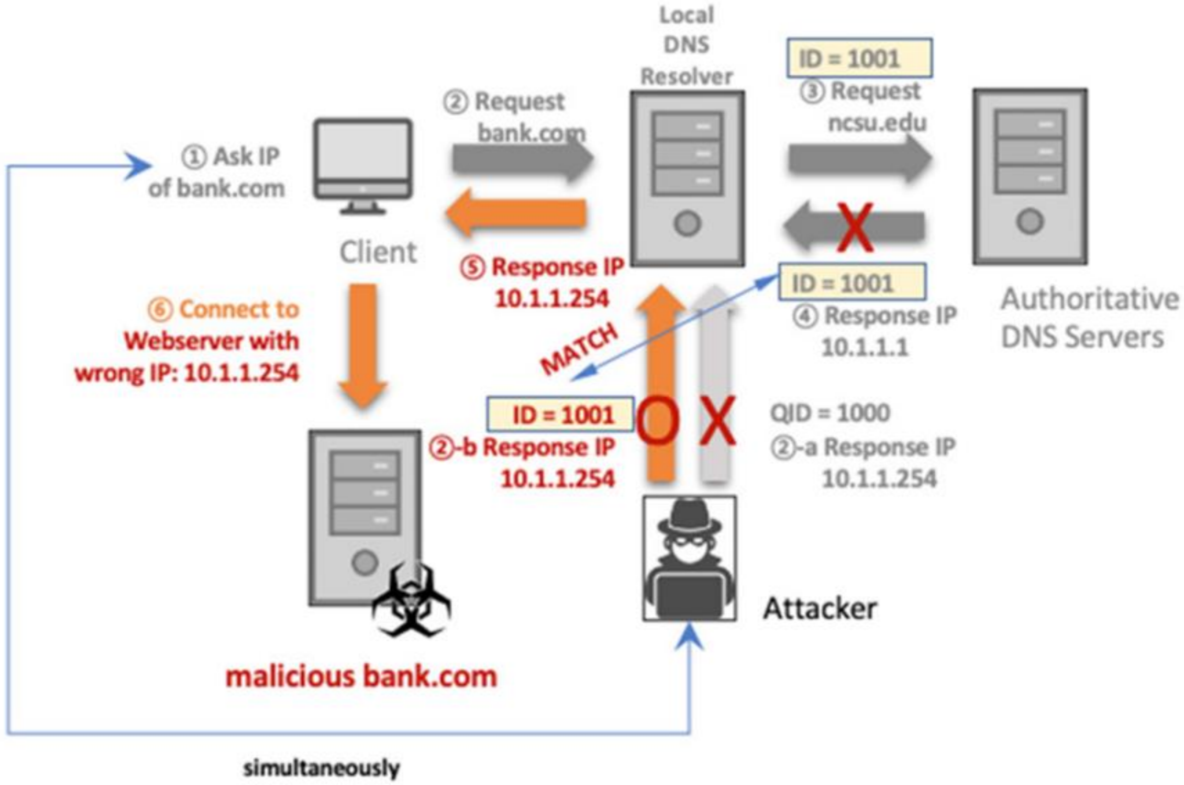


Figure 6 DNS attack: DNS data tampering. DNS: Domain Name System; QID: Query ID; “-a”, “-b”: the process order [27].

The attack leverages the weakness of unprotected DNS information. Figure 6 illustrates the process of a standard DNS data manipulation attack.

2.5.1.1 Address Resolution Protocol (ARP) Spoofing:

The Address Resolution Protocol (ARP) serves as a fundamental mechanism for translating Internet Protocol (IP) addresses into corresponding Media Access Control (MAC) addresses, widely employed in networking. However, ARP exhibits several inherent weaknesses. Notably, it lacks a built-in mechanism for a receiving node to authenticate the sender of a packet [28]. ARP operates without any authentication or integrity verification, showing indifference to the legitimacy of the packet's source. Essentially, any packet conforming to the permissible set of values is accepted. Consequently, ARP is characterized as a stateless protocol, permitting nodes to issue ARP responses without prior receipt of an ARP request. Exploiting these vulnerabilities, attackers conduct ARP Cache Poisoning attacks in traditional networks, wherein they introduce fraudulent or falsified IP-to-MAC address mappings into the target's ARP cache table.

Detecting and mitigating ARP Poisoning attacks assume critical importance due to their potential for facilitating other malicious actions, including Denial of Service (DoS), Distributed Denial of Service (DDoS), and Man-In-The-Middle (MITM) attacks. Attackers can employ ARP to establish communication with the system they intend to compromise, as ARP enables the establishment of connections between networks using both IP and MAC addresses. ARP Spoofing essentially involves intercepting or discarding target packets without forwarding them[29].

In [30], a comprehensive survey was conducted on the theory of ARP spoofing attacks and the array of techniques put forth to safeguard ARP from such threats. The research has underscored that for optimal security, it is advisable to deploy both detection and prevention systems within the network, all while seeking to streamline cryptographic procedures. Furthermore, the study advocated for the adoption of four essential security criteria as a foundation for devising a mechanism to detect and prevent ARP spoofing attacks, as depicted in Figure 7.

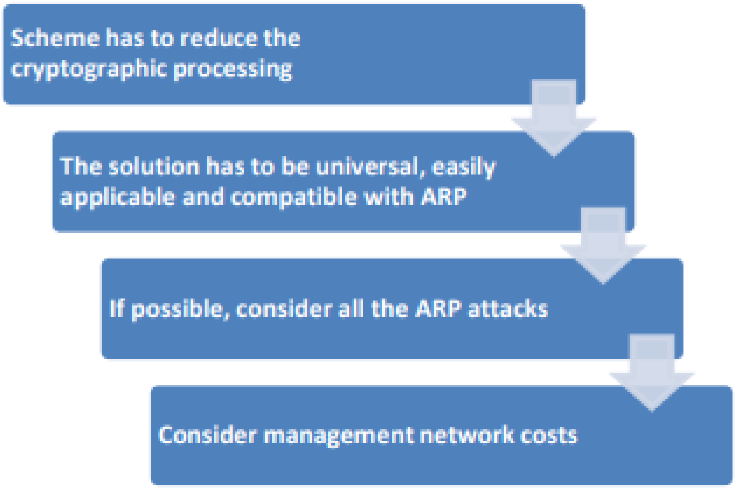

Scheme has to reduce the cryptographic processing
The solution has to be universal, easily applicable and compatible with ARP
If possible, consider all the ARP attacks
Consider management network costs

Figure 7 ARP Detection and Prevention Requirement[30].

2.5.1.2 Secure Socket Layer (SSL) hijacking:

The SSL protocol plays a crucial role in establishing secure connections between a web browser and a web server. In the context of hacking, the focus isn't on directly attacking the SSL protocol itself, but rather on exploiting the phase where the transition occurs from non-encrypted communication to encrypted communication. During this critical phase, attackers execute a deceptive maneuver by providing counterfeit authentication keys to both the user and the application sides of the communication. As a result, the connection gives off the illusion of being secure, when in reality, a Man-in-the-Middle (MITM) attacker gains control over the entire session. This vulnerability underscores the importance of vigilance and robust security measures when it comes to SSL-protected communications.[31]

2.5.2 MALWARE ATTACKS ON SCADA SYSTEMS

As adversaries become increasingly sophisticated in their tactics, organizations must remain vigilant and proactive in defending their SCADA systems. Robust cybersecurity measures are essential to identify and prevent potential malware attacks, minimize their impact, and enable rapid recovery. These measures include[32]:

1. Network segmentation.
2. Intrusion detection and prevention systems.

3. Access controls.
4. Secure software development practices.
5. Regular system updates.
6. Fostering a culture of cybersecurity awareness.
7. Implementing incident response plans.

The evolving landscape of malware attacks on SCADA systems requires a holistic approach to cybersecurity. Organizations must focus on preventive measures, adopt continuous monitoring strategies, and share threat intelligence to stay abreast of emerging threats. Collaboration with cybersecurity organizations and information-sharing forums can provide valuable insights into the latest attack vectors and techniques, enabling organizations to fortify their defenses. C. Kaura et al. [33], introduced a novel classification framework that revolves around the severity of cyber attacks. The pervasive influence of computers and related technologies in our daily lives, particularly within the industrial sector, has brought forth an era of automation and transformative advancements.

By understanding the growing threats posed by malware attacks on SCADA systems and their potential consequences, critical infrastructure operators can prioritize cybersecurity and allocate resources accordingly. Implementing robust defense mechanisms and cultivating a proactive cybersecurity mindset will help mitigate the risks associated with malware attacks, ensuring the resilience and reliability of SCADA systems in the face of evolving cyber threats.

In the subsequent sections of this section, we will delve into specific case studies of malware attacks on SCADA systems, explore the techniques employed by adversaries, and examine the resulting consequences. Through these real-world examples, we will reinforce the importance of implementing robust cybersecurity practices and emphasize the need for continuous monitoring and threat intelligence sharing to effectively defend against malware attacks on critical infrastructures.

Various types of malware are specifically designed to target SCADA systems. It examines the characteristics and functionalities of prevalent malware families, such as Stuxnet, Triton, and Industroyer, and explores their specific objectives and techniques employed to compromise

SCADA systems. Additionally, it discusses the potential consequences of successful malware attacks, including service disruptions, safety risks, and financial losses[34].

Drawing from real-world examples, this section presents notable case studies of malware attacks on SCADA systems. It explores the attack vectors, techniques employed, and the resulting consequences. These case studies serve as valuable lessons to reinforce the importance of robust cybersecurity practices and the need for continuous monitoring and threat intelligence sharing. This section provides an in-depth examination of notable case studies involving malware attacks on SCADA systems, highlighting the attack vectors, techniques employed by adversaries, and the consequential impact on critical infrastructures. These case studies serve as real-world examples that underscore the criticality of implementing robust cybersecurity practices and the necessity of continuous monitoring and threat intelligence sharing to prevent and mitigate the effects of such attacks.

2.5.2.1 Case Study 1:

Stuxnet and the Iranian Nuclear Program; The Stuxnet malware, discovered in 2010, targeted the Iranian nuclear program's SCADA systems. This case study analyzes the sophisticated attack, which exploited zero-day vulnerabilities and utilized various propagation mechanisms, including USB drives. Stuxnet specifically targeted (ICS) and manipulated programmable logic controllers (PLCs) to sabotage uranium enrichment centrifuges. The attack successfully disrupted Iran's nuclear program, illustrating the potential consequences of a well-planned and targeted malware attack on SCADA systems[35].

2.5.2.2 Case Study 2:

Triton and the Petrochemical Plant; The Triton malware attack, identified in 2017, targeted a petrochemical plant's safety instrumented system (SIS). This case study explores the attack methodology, which aimed to disable the SIS, compromising the plant's safety mechanisms. Triton sought to manipulate the SIS controllers, potentially leading to catastrophic consequences such as fires, explosions, or toxic releases. The case study highlights the importance of protecting not only operational functionality but also the safety and integrity of critical infrastructures[36].

2.5.2.3 Case Study 3:

Industroyer and the Ukrainian Power Grid; The Industroyer malware, observed in 2016, targeted the Ukrainian power grid, resulting in a major blackout. This case study investigates the attack's impact, which involved disrupting SCADA systems responsible for electricity distribution. Industroyer exploited known vulnerabilities in the ICS protocols and communication infrastructure, causing significant disruptions and leaving a large number of people without power. The case study emphasizes the need for constant vigilance and proactive defense measures to safeguard critical infrastructures from similar attacks[37].

Lessons Learned and Best Practices Drawing from the aforementioned case studies, this section distills the key lessons learned and best practices to fortify SCADA systems against malware attacks. It emphasizes the significance of implementing defense-in-depth strategies, including regular patching and software updates, network segmentation, strong access controls, continuous monitoring, and incident response planning. Additionally, it underscores the importance of sharing threat intelligence and collaborating with relevant cybersecurity organizations to stay ahead of emerging threats. The following figure shows the Timeline of cyberattacks targeting the energy sector and other critical infrastructure facilities [38]

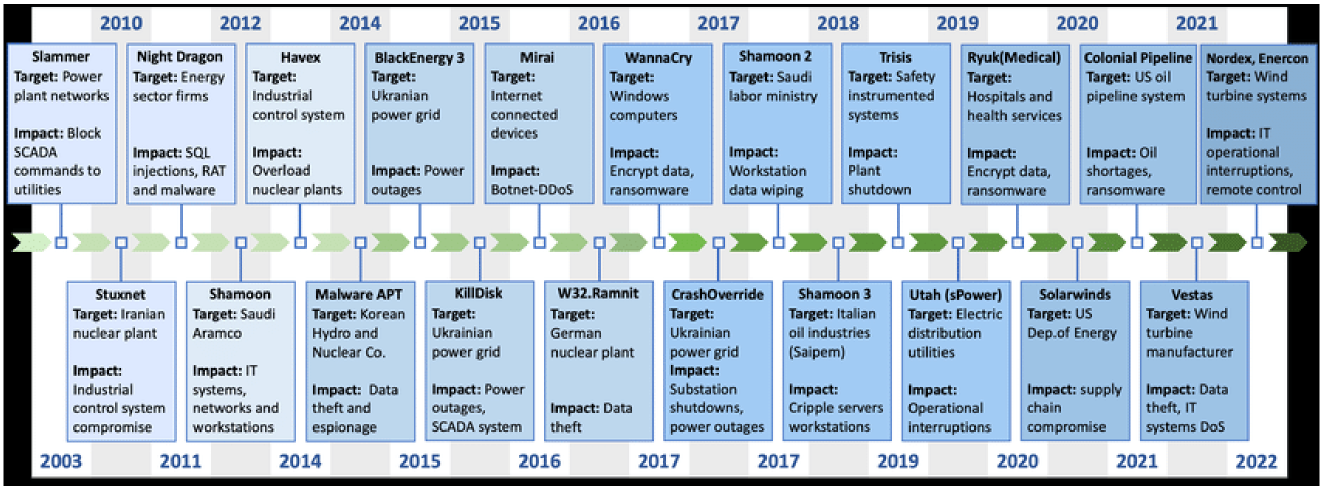

2010
2012
2014
2015
2016
2017
2018
2019
2020
2021
Slammer Target: Power plant networks Impact: Block SCADA commands to utilities
Night Dragon Target: Energy sector firms Impact: SQL injections, RAT and malware
Havex Target: Industrial control system Impact: Overload nuclear plants
BlackEnergy 3 Target: Ukranian power grid Impact: Power outages
Mirai Target: Internet connected devices Impact: Botnet-DDoS
WannaCry Target: Windows computers Impact: Encrypt data, ransomware
Shamoon 2 Target: Saudi labor ministry Impact: Workstation data wiping
Trisis Target: Safety instrumented systems Impact: Plant shutdown
Ryuk(Medical) Target: Hospitals and health services Impact: Encrypt data, ransomware
Colonial Pipeline Target: US oil pipeline system Impact: Oil shortages, ransomware
Nordex, Enercon Target: Wind turbine systems Impact: IT operational interruptions, remote control
Stuxnet Target: Iranian nuclear plant Impact: Industrial control system compromise
Shamoon Target: Saudi Aramco Impact: IT systems, networks and workstations
Malware APT Target: Korean Hydro and Nuclear Co. Impact: Data theft and espionage
KillDisk Target: Ukrainian power grid Impact: Power outages, SCADA system
W32.Ramnit Target: German nuclear plant Impact: Data theft
CrashOverride Target: Ukrainian power grid Impact: Substation shutdowns, power outages
Shamoon 3 Target: Italian oil industries (Saipem) Impact: Cripple servers workstations
Utah (sPower) Target: Electric distribution utilities Impact: Operational interruptions
Solarwinds Target: US Dep.of Energy Impact: supply chain compromise
Vestas Target: Wind turbine manufacturer Impact: Data theft, IT systems DoS
2003
2011
2014
2015
2016
2017
2017
2019
2020
2021
2022

Figure 8 Timeline of cyberattacks targeting the energy sector and other critical infrastructure facilities[38]

The examination of case studies showcasing malware attacks on SCADA systems provides valuable insights into the evolving nature of cyber threats targeting critical infrastructures. By understanding the attack vectors, techniques employed, and the resulting consequences, organizations can reinforce the urgency of adopting robust cybersecurity practices. Continuous monitoring, threat intelligence sharing, and the implementation of multi-layered defense measures are vital to detect, prevent, and mitigate the impact of malware attacks on SCADA systems. Ultimately, by learning from these case studies, critical infrastructure operators can bolster their resilience and protect vital services from evolving cyber threats[39].

2.5.3 Vulnerabilities Exploited by Malware

Understanding the vulnerabilities exploited by malware is crucial for developing effective defense mechanisms. This section analyzes the common vulnerabilities in SCADA systems, including insecure remote access, weak authentication mechanisms, and insufficient network segmentation. By identifying these vulnerabilities, organizations can take proactive measures to fortify their SCADA systems against potential malware attacks[40].

The vulnerabilities discussed below highlight the weak points that malware often exploits within SCADA systems.

2.5.3.1 Insecure Remote Access[41]:

SCADA systems frequently require remote access for maintenance and monitoring purposes. However, inadequately secured remote access mechanisms can serve as a gateway for malware infiltration. Weak or default credentials, lack of encryption, and unpatched vulnerabilities in remote access components can leave SCADA systems exposed to unauthorized access and subsequent malware injection.

2.5.3.2 Weak Authentication Mechanisms:

Authentication mechanisms form the first line of defense against unauthorized access. Unfortunately, SCADA systems have often been found to have weak authentication practices. Insufficient password policies, shared credentials, and the absence of multifactor authentication can make it easier for malware to bypass authentication measures, enabling attackers to gain control over critical SCADA infrastructure[42].

2.5.3.3 Insufficient Network Segmentation:

Proper network segmentation is crucial to prevent the lateral movement of malware within SCADA systems. When SCADA networks lack appropriate segmentation, malware can spread rapidly from one compromised device to another, potentially causing widespread disruption. Inadequate network zoning, absence of firewalls, and insufficient access controls can lead to the compromise of critical components, allowing malware to propagate and inflict extensive damage[43].

2.5.3.4 Outdated Software and Unpatched Vulnerabilities:

Maintaining up-to-date software and promptly applying security patches is vital to mitigate vulnerabilities exploited by malware. Failure to install patches and updates can leave SCADA systems susceptible to known vulnerabilities that malware can easily exploit. The exploitation of these vulnerabilities may result in unauthorized control, data exfiltration, or even sabotage of SCADA systems[44].

2.6 SCADA protocols

(SCADA) systems commonly employ a variety of protocols for communicating with Programmable Logic Controllers (PLCs). The selection of a protocol is influenced by factors such as the particular requirements of the industrial process, the type of equipment in use, and considerations for interoperability. According to the AGA-12 standard of the American Gas Association, there are between 150 and 200 SCADA protocols. The majority of these protocols were individual company-developed proprietary standards. The industry has shifted over the years to accept common open standard protocols[45]. Even with open protocols, numerous professional groups strive for increased industry acceptance of their respective protocol standards. Below are some frequently utilized SCADA protocols for PLC communication[46]:

Modbus:

Overview: Modbus is a well-established communication protocol widely used in industrial automation, known for its simplicity and effectiveness in serial communication.

Characteristics: Modbus supports both serial (Modbus RTU) and Ethernet (Modbus TCP) communication. It operates as a master/slave protocol, with the SCADA system typically serving as the master and PLCs as slaves[47].

DNP3 (Distributed Network Protocol 3):

Overview: DNP3 is designed for deployment in SCADA and remote monitoring applications, commonly applied in the utility and energy sectors.

Characteristics: DNP3 supports robust communication across various media, including serial and TCP/IP. It incorporates features such as time synchronization and event reporting, making it well-suited for critical infrastructure applications[48].

IEC 60870-5:

Overview: IEC 60870-5 is an international standard for telecontrol protocols in SCADA systems, outlining communication profiles for telecontrol and telesignaling.

Characteristics: IEC 60870-5 supports various modes of communication, including balanced and unbalanced approaches. It finds common use in the electric power industry for communication with devices like remote terminal units (RTUs) and PLCs[49].

EtherNet/IP:

Overview: EtherNet/IP is an industrial Ethernet protocol widely used in manufacturing and process control applications.

Characteristics: As an open protocol, EtherNet/IP enables devices like PLCs to communicate over standard Ethernet networks. It is often employed in applications where high-speed communication and real-time control are crucial[50].

Profibus:

Overview: Profibus is a widely utilized fieldbus communication protocol in industrial automation, facilitating communication between PLCs, sensors, and other automation devices.

Characteristics: Profibus supports both process automation (Profibus PA) and factory automation (Profibus DP), offering high-speed communication suitable for applications with complex network architectures[51].

CANopen:

Overview: CANopen is a communication protocol based on the Controller Area Network (CAN) bus, frequently used in motion control and automation applications.

Characteristics: CANopen facilitates communication among devices like PLCs, sensors, and actuators, recognized for its real-time capabilities and common use in applications requiring precise timing[52]. These protocols represent just a selection, and the choice depends on the specific needs of the industrial process and device compatibility. Each protocol has distinct strengths and weaknesses, allowing organizations to select the one that aligns best with their requirements for SCADA system-to-PLC communication, Figure 9 illustrates the Use of Industrial Communication Protocols in 2019.

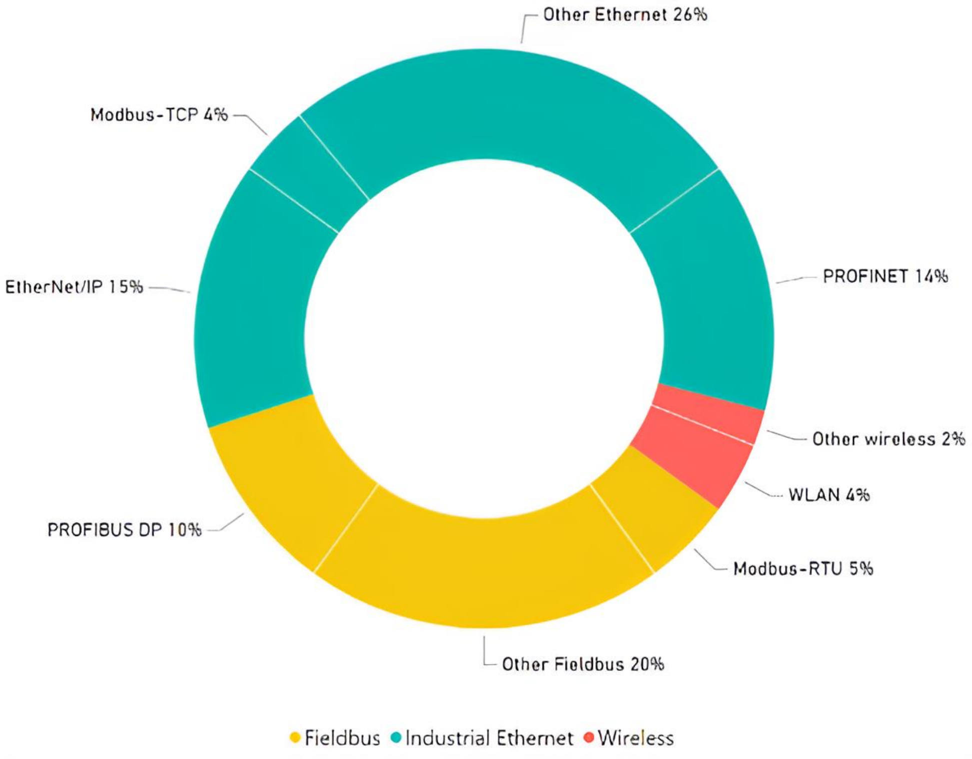
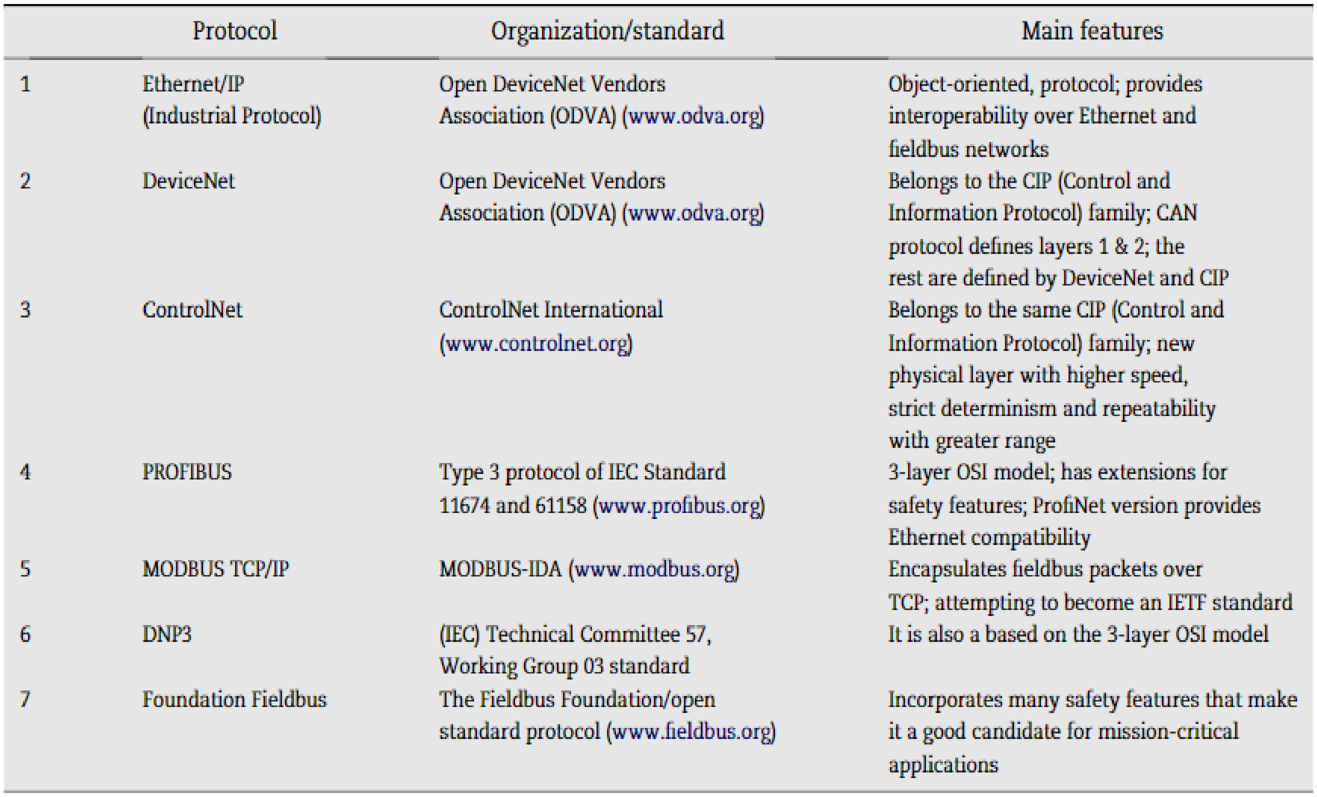


Figure 9 The Use of Industrial Communication Protocols in 2019[46]

Table 3 SCADA protocals [12]



	Protocol	Organization/standard	Main features
1	Ethernet/IP (Industrial Protocol)	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Object-oriented, protocol; provides interoperability over Ethernet and fieldbus networks
2	DeviceNet	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Belongs to the CIP (Control and Information Protocol) family; CAN protocol defines layers 1 & 2; the rest are defined by DeviceNet and CIP
3	ControlNet	ControlNet International (www.controlnet.org)	Belongs to the same CIP (Control and Information Protocol) family; new physical layer with higher speed, strict determinism and repeatability with greater range
4	PROFIBUS	Type 3 protocol of IEC Standard 11674 and 61158 (www.profibus.org)	3-layer OSI model; has extensions for safety features; ProfiNet version provides Ethernet compatibility
5	MODBUS TCP/IP	MODBUS-IDA (www.modbus.org)	Encapsulates fieldbus packets over TCP; attempting to become an IETF standard
6	DNP3	(IEC) Technical Committee 57, Working Group 03 standard	It is also a based on the 3-layer OSI model
7	Foundation Fieldbus	The Fieldbus Foundation/open standard protocol (www.fieldbus.org)	Incorporates many safety features that make it a good candidate for mission-critical applications

The PROFINET protocol is an industrial ethernet-based system specifically engineered to facilitate rapid data communication between field devices connected via Ethernet, employing a provider-consumer model. It allows for the smooth integration of field devices located in a subordinate Profibus line into the Profinet system through the use of an IO-Proxy, which acts as a representative of the subordinate bus system[53]. While IEEE802.3, the standard Ethernet protocol, doesn't consider the environment, Industrial Ethernet is specifically designed to account for the rugged conditions encountered in industrial settings. Industrial Ethernet takes into consideration the challenging industrial environments characterized by factors like vibration, electromagnetic interference, oily vapors, and extreme temperatures. Essentially, Industrial Ethernet remains electrically the same as Ethernet, but its components are built robustly to endure these harsh conditions[54].

Moreover, the industrial sector imposes additional demands beyond just environmental concerns. For instance, in industrial processes, there's a critical need for rapid response times.

Unlike emails, which can take their time to arrive, a signal to halt a conveyor must arrive within milliseconds to prevent products from spilling onto the floor. PROFINET achieves this high-speed performance by bypassing the TCP/IP layers. This approach not only meets the industry's need for speed but also delivers more deterministic performance, ensuring that data arrives precisely when it's expected, consistently, and reliably.

2.6.1 PROFINET operation

PROFINET operates across all four layers of the Internet model. It leverages TCP/IP for configuration and diagnostic purposes but omits TCP/IP for real-time data transmission, utilizing layers 1, 2, and 7 within the seven-layer model instead[55], see the following Figure. this communication protocol is mainly used by Siemens PLC. With Profinet, it's possible to interconnect various facilities such as PLCs, HMIs, Distributed I/O systems, various types of transmitters, sensors, actuators, VFDs, and more within a single network.

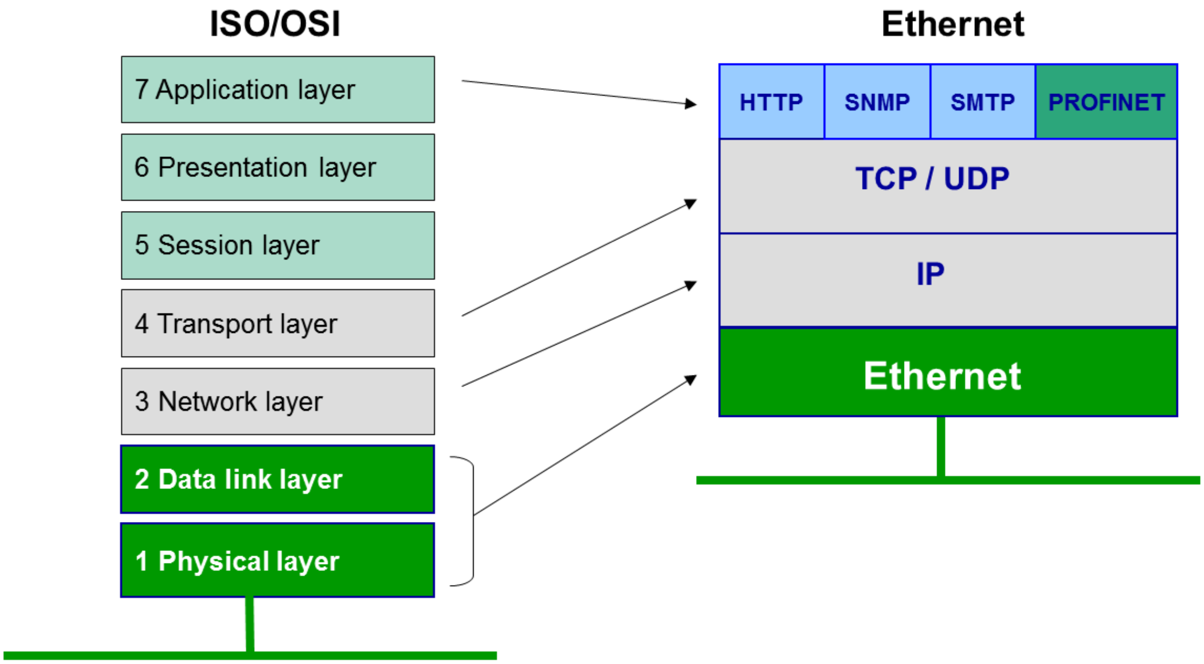


Figure 10 PROFINET uses all four of the Internet model layers. It uses TCP/IP for configuration and diagnostics and skips TCP/IP for real time data (using layers 1, 2, and 7 of the 7-layer model).[55]

2.6.2 PROFINET Network Structure

When it comes to designing networks, PROFINET stands out for its emphasis on flexibility and layout. It offers nearly limitless possibilities for combining various Ethernet topologies. Given the existence of different fundamental PROFINET network structures, selecting the right one is crucial when designing an automation plant with PROFINET. Furthermore, adjustments may be necessary after this initial design phase, which might involve the addition of extra switches to establish the desired PROFINET network configuration. The basic PROFINET topologies at your disposal include options such as star, tree, and line configurations.

2.6.2.1 Star Topology

The star topology is well-suited for scenarios with limited geographical coverage. This configuration is established automatically when multiple communication nodes are connected to a central switch. If a single PROFINET node experiences a failure or is disconnected, the remaining PROFINET nodes will continue to function without interruption. However, if the central switch encounters a failure, it will disrupt communication to all connected nodes[56].

2.6.2.2 Tree Topology

A tree topology is established by interconnecting multiple star networks into a single overarching network. The operational unit consists of the segments of the automation plant linked to these star points. These segments are interconnected through adjacent switches. Within each star point, a single switch serves as a distributor for signals[56].

2.6.2.3 Line Topology

In automation plants, the linear topology finds extensive application, especially in scenarios like conveyor belt systems and smaller machinery setups. PROFINET devices are designed with built-in switches to facilitate the recognition of linear topologies. However, it's important to note that in the event of a line interruption within linear topologies, devices situated beyond the failed point become inaccessible. To mitigate this issue, one can opt to transform the linear configuration into a ring structure, implementing a redundancy protocol to ensure continuous connectivity[56].

2.6.3 PROFINET Advantages

Why profinet used in the industrial environment [57];

1. Profinet offers quicker response times, enhancing the efficiency of data collection.
2. In an electrically noisy industrial environment, Industrial Profinet, equipped with shielding, delivers superior performance.
3. To identify Profinet devices, they need to be configured with both an IP address and a device name.
4. In order for devices to communicate within the network, each one must be allocated a specific IP address.
5. Similar to Profibus-DP, Profinet can function as a remote I/O, enabling exceptionally fast communication rates.

2.6.4 PROFINET Applications

PROFINET is employed across the entire spectrum of automation engineering disciplines.This open Industrial Ethernet solution, compliant with international standards, facilitates data exchange between devices and controllers within automation environments. Siemens PLCs utilize Process Field Net for their operations. PROFINET is versatile, serving different fields for the implementation of automation solutions, including process automation, building automation, and factory automation. PROFINET operates over Industrial Ethernet for data communication purposes. It is commonly used in automation processes for monitoring and regulating substances such as liquids and gases. It also plays a crucial role in various sectors, including fuel gas supply, wastewater and water treatment control, and automation. The beverage industry, dairies, and food production facilities benefit from PROFINET in their processing plants. Its applicability extends across a wide range of industries, encompassing gas, automotive, oil, logistics, and many others[58].

3 Enhancing Cybersecurity in Industrial Control Systems through GRC Framework: Principles, Regulations, and Risk Assessment

Information security is a critical aspect of modern society, as it helps to protect sensitive information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Confidentiality pertains to shielding information from unauthorized parties. Integrity relates to preventing unauthorized alterations or corruption of information. Availability pertains to authorized individuals' ability to access information and systems as required [21]. The CIA triad serves as a framework directing the fundamentals of information security. It encompasses Confidentiality, Integrity, and Availability. It stands for Confidentiality, Integrity, and Availability (see Figure 11). Protecting (ICS) is particularly important, as these systems are used to control and monitor critical infrastructures such as power plants, water treatment facilities, and manufacturing plants. If these systems were to be compromised, it could have serious consequences for the organization and the wider community. Therefore, it is important to implement appropriate security measures to protect ICS networks and infrastructure from cyber threats. This can include measures such as network segmentation, access controls, and regular security updates and patches[21].

The contributions of this Chapter are threefold. Section 1 is a brief introduction to ICS and information security. In section 2 we provide an extensive literature review on Information security Principles- Definitions include (Defense in depth, the Principle of least privilege (POLP), the Principle of separation of duties (SoD), and information security Principles- AAA. Section 3 provides a review of the literature on the GRC- Governance, Risk, and Compliance topic, including; the ICS GRC –Regulation and international standards, and the ICS GRC –Risk Assessment (Value, practices, and results) approaches.

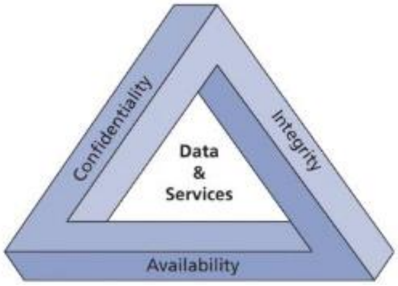


Figure 11 The C.I.A triad [59]

3.1 General IT Risk Assessment Methods.

SCADA systems Risk assessment aims to evaluate the system components in terms of their vulnerability to an assault and their relevance to the system's efficient operation. As well as, the danger they pose and their likelihood. The risk assessment leads the engineers and managers of SCADA systems to enhance and develop adequate security policies and the design of the security system and rational allocation of often scarce resources. It shall also facilitate communication between business, security, and SCADA[60].

Risk is described as the following[61]:

R= {si, pi, xi}, i=1, 2, N (1)

Where

R: Risk;

{}: must be interpreted as a "set of".

s: A scenario (undesirable event) description.

p: The probability of a scenario.

x: The measure of consequences or damage caused by a scenario.

N: The number of possible scenarios that may cause damage to a system.

The formula for calculating cybersecurity risks in SCADA systems risk when we applied to quantify is accepted as follows (Henrie 2013b):

$$R = t\ v\ xtv \tag{2}$$

Where

t: Threat.
v: Vulnerability.
Xtv: the consequences of the threat successfully exploiting the vulnerability.
There is a range of general IT risk assessment methodologies that can be modified to be used in the industry.

3.1.1 Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM)

RAMM serves as an inclusive instrument for the identification of security and contingency requisites, as well as the justification of expenses related to specific countermeasures, particularly in the realm of IT operations[62]. CRAMM is actively employed by entities such as NATO, the Dutch military, and security-focused corporations like Unisys.

The benefits of CRAMM, as outlined by Yazar in 2002 [62], encompass:

1. Providing a systematic approach to the analysis and management of risks, grounded in established methodologies.
2. Aiding in the development of contingency plans, certification under BS7799, and facilitating audits.
3. Fostering security awareness and fostering acceptance of security measures.
4. Offering the flexibility of conducting both comprehensive and rapid reviews, including high-level assessments supporting policy formulation.
5. Regularly updating an extensive hierarchical database of countermeasures, encompassing non-technical domains.

6. Relatively ranking countermeasures, considering effectiveness criteria and implementation costs.
7. Ensuring consistency through the application of similar solutions to comparable risk profiles.

However, it's worth noting the downsides of CRAMM as identified by Yazar in 2002:

1. Dependency on qualified and experienced professionals for effective utilization of the tool.
2. The potential for prolonged duration in conducting full reviews leads to substantial hard-copy output (though this can be mitigated by limiting the analysis to essential components as required).

CRAMM tool guides the review with a process-flow-oriented interface, see the following Figure 12.

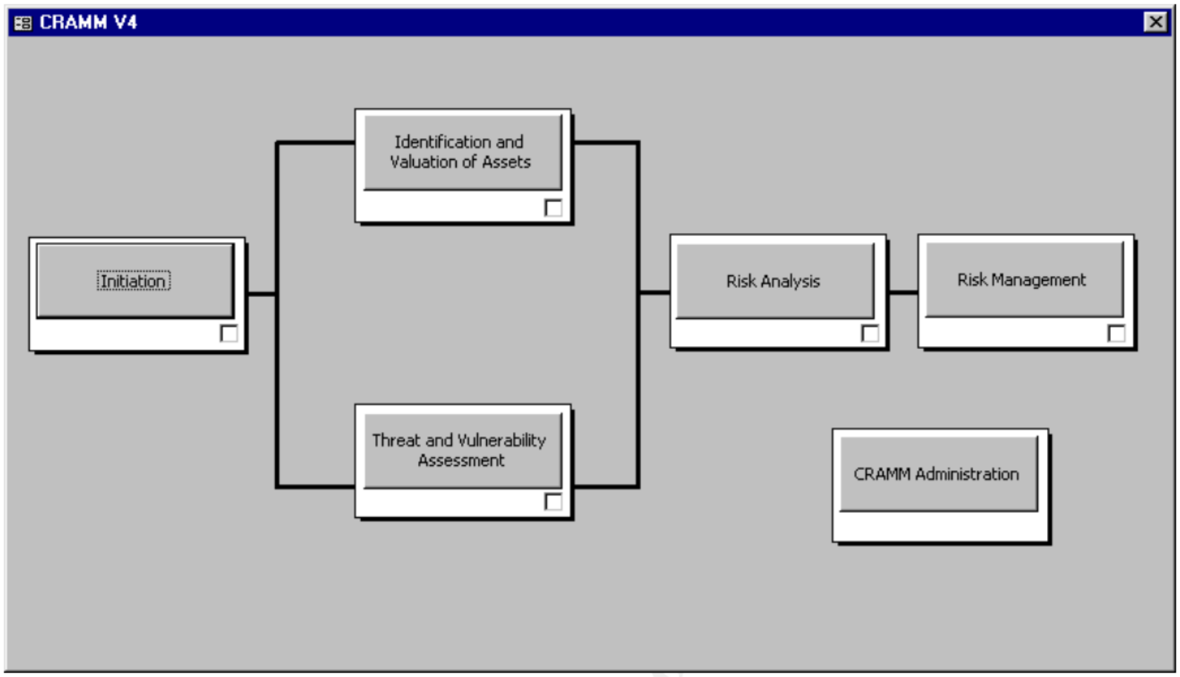

CRAMM V4
Initiation
Identification and Valuation of Assets
Threat and Vulnerability Assessment
Risk Analysis
Risk Management
CRAMM Administration

Figure 12: CRAMM overview screen [CUS01] [62].

For Risk Calculation, CRAMM assesses the risks associated with each asset group concerning the potential threats they face. This assessment is conducted on a scale ranging from 1 to 7, utilizing a risk matrix with pre-established values. It involves comparing the values of assets to the levels of threat and vulnerability. Within this scale, a rating of "1" signifies a minimal security requirement, while a rating of "7" signifies a stringent and very high-security necessity.

Based on the results of the risk analysis, CRAMM generates a set of countermeasures that are deemed necessary to address the identified risks within the system or network. This recommended security profile is then compared to the existing countermeasures in place to pinpoint any areas of weakness or potential over-provisioning.

CRAMM boasts an extensive array of countermeasures, totaling nearly 4000, which are organized into groups and sub-groups based on their shared "security aspect," such as hardware, software, communications, procedures, physical elements, personnel, and the environment. These countermeasures are also structured hierarchically, falling into three distinct categories, ranging from high-level security objectives to detailed implementation examples[62].

Each countermeasure is assigned a security level on a scale of 1 (Very Low) to 7 (Very High), determined by a risk comparison. As a decision support tool for management, CRAMM recommends prioritizing and reporting on higher-level countermeasures. CRAMM's strength in this regard lies in its ability to give higher priority to a countermeasure if:

1. It safeguards against multiple threats.
2. It is essential for protecting a high-risk system.
3. There are no alternative countermeasures already in place.
4. It is more cost-effective to implement (based on a general cost estimate).
5. It is more effective in achieving the objectives of its sub-group.
6. It focuses on prevention rather than detection or recovery from an incident.

In this way, CRAMM partially addresses one of the criticisms leveled against this generation of tools, which is the neglect of cost and efficiency evaluations of countermeasures while emphasizing asset value. While CRAMM doesn't offer a traditional cost/benefit analysis, it does provide a measure to consider the cost-effectiveness of countermeasures given the intangible nature of risk[62].

The final step in a CRAMM review involves presenting a summary of the findings and conclusions from the risk analysis to management. This summary includes an explanation of the recommended countermeasures, offering a broad overview of their priority and associated costs. Furthermore, the risk management report, similar to the analysis report, can be exported to Microsoft Word, allowing for organization-specific editing and formatting[62].

3.1.2 Information security risk analysis method ISRAM:

ISRAM has been specifically developed to assess the risks associated with complex information systems, with the unique feature of involving both administrators and staff members in the process. The primary goal of ISRAM is to evaluate the likelihood of encountering information security issues. To accomplish this aim, ISRAM incorporates a public perspective on the matter, which is gathered through a survey. This survey comprises inquiries and responses related to various aspects of information security. The intended respondents for this survey encompass managers, directors, technical experts, and regular users of the systems. The overarching objective of this survey is to gain insights into how information security issues may impact the system or the organization [63]. The Figure below illustrates the fundamental workflow of ISRAM.

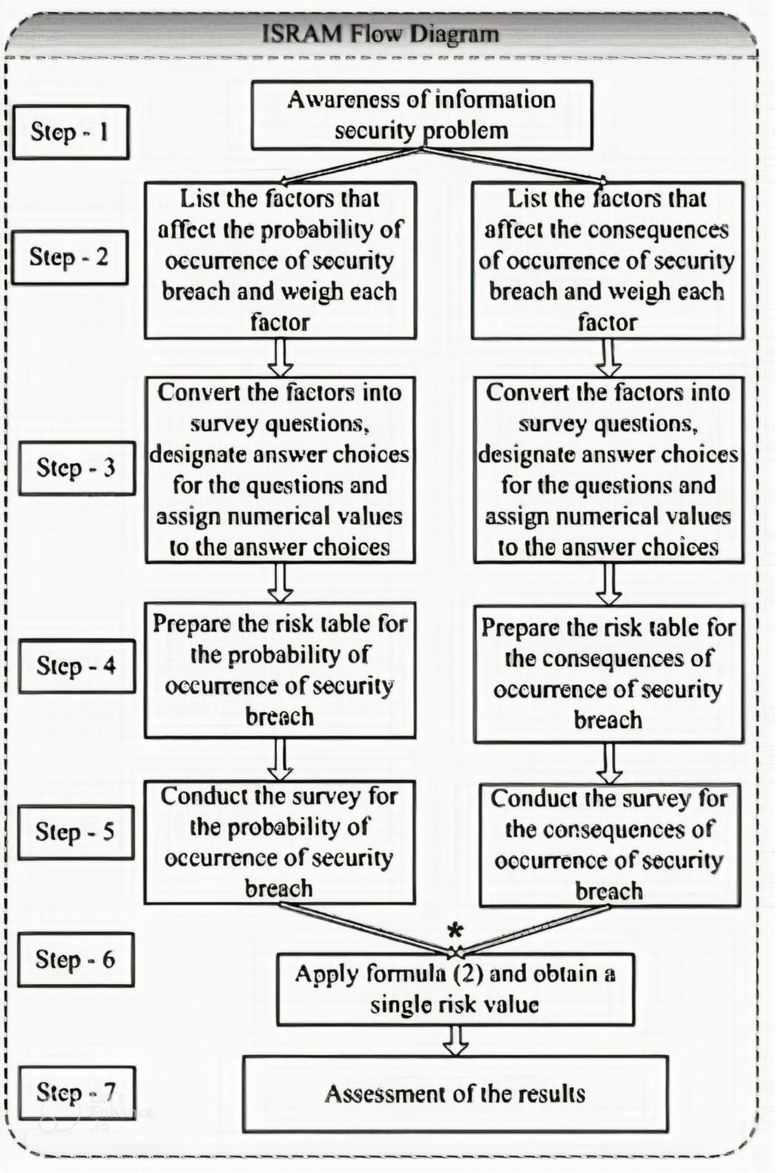

ISRAM Flow Diagram
Step - 1
Awareness of information security problem
Step - 2
List the factors that affect the probability of occurrence of security breach and weigh each factor
List the factors that affect the consequences of occurrence of security breach and weigh each factor
Step - 3
Convert the factors into survey questions, designate answer choices for the questions and assign numerical values to the answer choices
Convert the factors into survey questions, designate answer choices for the questions and assign numerical values to the answer choices
Step - 4
Prepare the risk table for the probability of occurrence of security breach
Prepare the risk table for the consequences of occurrence of security breach
Step - 5
Conduct the survey for the probability of occurrence of security breach
Conduct the survey for the consequences of occurrence of security breach
*
Step - 6
Apply formula (2) and obtain a single risk value
Step - 7
Assessment of the results

Figure 13 The Basic flow diagram of ISRAM[63].

3.1.3 Operationally Critical Threat and Vulnerability Evaluation (OCTAVE)

OCTAVE operates in a self-coordinated manner, meaning that individuals within an organization take responsibility for shaping the organization's security strategy. This approach leverages their knowledge of the organization's security-related practices and processes to assess the current state of security practices within the organization. Critical asset vulnerabilities are used to pinpoint areas requiring improvement and to formulate the organization's security strategy. The following diagram illustrates the interplay between these activities. It's worth noting that risk management activities follow a plan-do-check-act cycle. By employing the OCTAVE methodology, an organization makes data protection decisions based on threats to the confidentiality, integrity, and availability of vital information-related assets. All aspects of risk (assets, threats, vulnerabilities, and organizational impact) are factored into decision-making, enabling an organization to align its security risk mitigation strategy with best practices[64].

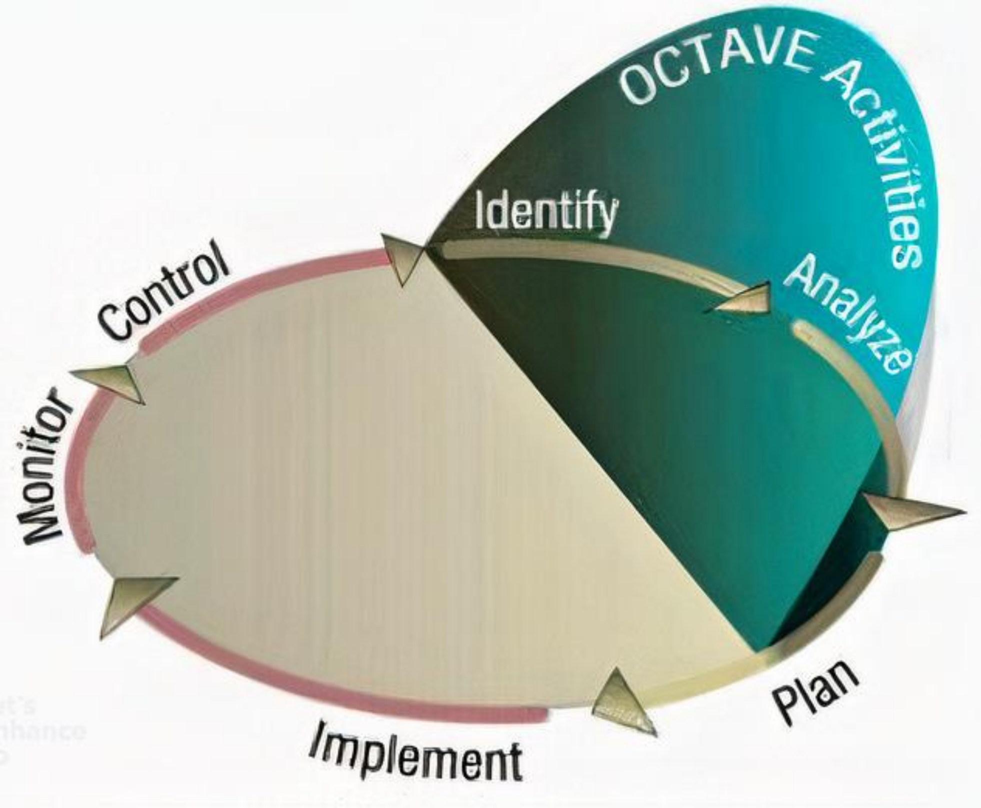


Figure 14 Risk Management Activities[64].

3.2 Information Security Principles- Definitions

There are four key terms used in the field of information security [65]:

1. Threat: A threat is any agent or entity with the ability to do damage to the information systems or data of an organization. This might be an individual, a group, or even malware.

2. Vulnerability: A vulnerability is a system or process's weakness or fault that can be exploited by a threat. A vulnerability might be a software flaw that allows an attacker to obtain unauthorized access to a system, for instance.
3. Risk: Risk is the possibility of harm arising from a threat exploiting a vulnerability. Risk is determined by the likelihood of a threat exploiting a vulnerability and its potential consequence.
4. Exploit: An exploit is a technique or method that a threat uses to exploit a vulnerability. Exploits can be used to obtain unauthorized access to a system, execute malicious code, and carry out other operations that are detrimental to an organization. Vulnerabilities must always be identified and addressed to limit the possibility of exploitation by threats.

3.2.1 Defense in depth

Defense in depth refers to the strategy of employing numerous layers of protection against cyber attacks. Implementing a mix of technological, physical, and administrative controls to establish a robust and resilient security posture. Defense in depth proposes a tiered approach to security that makes it more challenging for an attacker to penetrate a system. Each layer of defense functions to stop, detect, or neutralize a cyber threat, and if one layer fails, the others can still provide security[66]. Defense in depth is a common strategy that utilizes multiple layers of firewalls to protect (SCADA) subnets and essential resources within business networks. The introduction of NetSPA presents a solution that assesses firewall rules and vulnerabilities to create attack graphs. These instances illustrate how attackers, whether internal or external, could progress by gradually exploiting vulnerable hosts in a sequence, aiming to access critical internal targets[67].

Examples of several layers of defense in depth might include:

1. **Firewalls and network segmentation**: These safeguards secure the network perimeter and restrict access to authorized users.
2. **Access controls and authentication**: These controls guarantee that only authorized users may gain access to sensitive data and systems.

3. **Antivirus software and endpoint protection**: These measures aid in detecting and preventing the infection of computers with malware.
4. **Intrusion detection and prevention systems**: These safeguards enable to discovery and thwarting of cyber threats in real-time.
5. **Physical security measures**: These controls defend against physical risks, such as unauthorized entry to data centers and servers.

Overall, a defense-in-depth approach is considered the best cybersecurity practice, as it helps to reduce the risk of successful attacks and breaches. For the defense in depth architecture (see Figure 15).

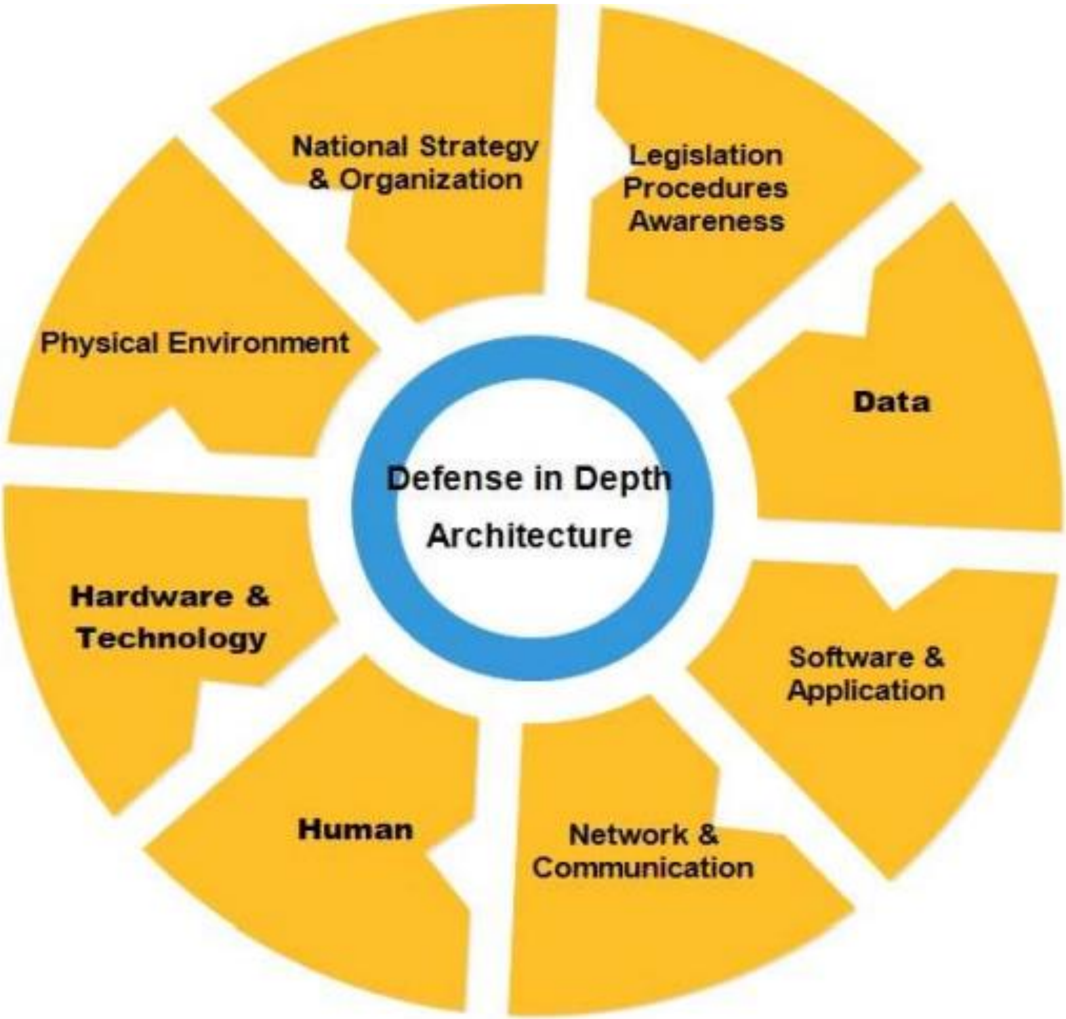


Figure 15 Layers of defense in depth architecture.

3.2.2 Principle of least privilege (POLP)

The principle of least privilege (POLP) is a notion in computer security that refers to the practice of restricting access permissions for users to the minimal level necessary to execute their duties. This concept aims to decrease the danger of unauthorized access to sensitive data and systems and to prevent users from making unintentional modifications or harming the system. In practice, the notion of least privilege entails allowing users just the privileges they require to do their tasks. For instance, if a person simply needs read-only access to a database, they should not be provided write access. This helps prevent inadvertent or malicious data modifications and decreases the chance of data breaches and other security events[68].

Implementing the concept of least privilege can enhance the security of a system by reducing the possible damage that can be performed by an individual user or group of users. It is a vital component of a defense-in-depth security approach and is frequently employed in conjunction with other security controls such as access limits, encryption, and monitoring.

3.2.3 Principle of separation of duties (SoD)

The principle of separation of duties (SoD) is a concept in computer security and internal controls that refers to the practice of dividing responsibilities for specific tasks among different individuals or groups. The goal of this principle is to prevent errors, fraud, and other security incidents by ensuring that no single individual has the ability to complete a critical task on their own. As discussed by Simon and Zurko [69] " Separation of Duty is a security principle used to formulate multi-person control policies, requiring that two or more different people be responsible for the completion of a task or set of related tasks The purpose of this principle is to discourage fraud by spreading the responsibility and authority for an action or task over multiple people, thereby raising the risk involved in committing a fraudulent act by requiring the involvement of more than one individual". In practice, tasks are divided into smaller parts and assigned to different people. For example, in a financial system, someone may enter transactions while another person approves them. This requires multiple people to be involved in the process and provides checks to ensure data integrity. The separation of duties principle can improve security and reliability and is often used with other security controls like access controls, monitoring, and auditing [70].

There are many examples of the principle of separation of duties (SoD) in action. Here are a few examples:

1. **Financial systems**: In a financial system, the separation of duties might involve separating the roles of entering transactions, approving transactions, and reconciling accounts. This helps to prevent errors and fraud by requiring multiple individuals to be involved in the process and by providing checks and balances to ensure the integrity of the data. As an example of SoD in the financial systems " THE IMPACT OF INTERNAL CONTROLS ON FINANCIAL MANAGEMENT: A CASE OF PRODUCTION COMPANIES IN NIGERIA " [71].
2. **Manufacturing**: In a manufacturing setting, the separation of duties might involve separating the roles of ordering raw materials, receiving the materials, and issuing payment for the materials. This helps to prevent errors and fraud by requiring multiple individuals to be involved in the process and by providing checks and balances to ensure the accuracy of the data.
3. **Information systems**: In an information system, the separation of duties might involve separating the roles of the database administrator, network administrator, and system administrator. This helps to prevent unauthorized access to sensitive data, and systems and to prevent unintended changes or harm to the system[72].
4. **Government**: In a government setting, the separation of duties might involve separating the roles of legislation, execution, and oversight. This helps to prevent abuses of power and to ensure that government actions are accountable and transparent [73].

Overall, the principle of separation of duties can be applied to many different types of systems and processes in order to improve security and reliability.

3.2.4 Information security Principles- AAA

This access control is provided by the AAA framework, which includes three steps: Authentication, Authorization, and Accounting. This framework emphasizes the importance of securing the data by filtering out those who do not have access to it, using an authentication process in which the user's authorization level is specified, and auditing their access session statistics for security purposes, such as the detection of suspicious behavior. Certainly, the mentioned fundamental concepts are relevant to the client security architecture[74]. Industrial Automation and Control Systems (IACS) and (SCADA) systems of the future generation provide significant cybersecurity monitoring issues. We have witnessed the confluence of operational technology (OT) and information technology (IT) networks, coupled with massively dispersed metering and control situations, such as smart grids. Larger and more widely dispersed attack surfaces, as well as naturally greater amounts of data to analyze, will become the norm. L. Rosa *et al.* introduced an all-encompassing structure for an Intrusion and Anomaly Detection System (IADS), which includes specific detection probes, an event processing layer, and a central anomaly detection component. Furthermore, they provide an assessment of the framework's performance within an extensive hybrid testbed, along with a juxtaposition of diverse anomaly detection scenarios utilizing various machine learning algorithms [75].

Point-to-Point Protocol (PPP) authentication mechanisms are scalable and field-tested. ISPs can keep track of millions of customers and send out bills using the client-server architecture of RADIUS, which is the best-known example of an authentication, authorization, and accounting protocol (AAA), and the Password Authentication Protocol (PAP). The Point-to-Point Tunneling Protocol (PPTP) adds new authentication and encryption options to PPP and makes it work for connections all over the Internet. In [76] the authors Revealed major security vulnerabilities in PPTPv1 Version 1 is a classic example of the disadvantages of prioritizing backward compatibility over security, despite its extended obsolescence. Even the second generation of PPTP had compatibility issues with older versions.

3.3 GRC- Governance, Risk, and Compliance

GRC abbreviates Governance, Risk, and Compliance, serving as a structured approach for overseeing legal, regulatory, and operational risks. It is a holistic strategy for managing the activities, processes, and choices of an organization to achieve its objectives. GRC assists firms in identifying, assessing, and managing risks, as well as ensuring compliance with relevant laws, regulations, and standards. GRC also assists businesses in establishing and sustaining a compliance and risk management culture. GRC is an integral component of an organization's overall risk management strategy and aids in ensuring that activities are handled ethically and responsibly[77].

Governance refers to the overall administration and direction of an organization and includes the processes and structures in place to guarantee that it is operated effectively and efficiently[78], with appropriate consideration for its legal and ethical obligations. Risk is the possibility of harm or loss to an organization. This might include financial risks, risks to the organization's reputation, and risks to its operations or resources. Organizations utilize risk management methods to identify and assess possible hazards, and to implement steps to minimize or avoid the occurrence of such risks. Compliance refers to the observance of laws, rules, standards, and other external obligations by an entity. Compliance management entails finding and comprehending applicable rules and regulations, as well as ensuring that an organization's policies and processes comply with them. The GRC framework assists firms in managing the intricate relationship between governance, risk, and compliance, ensuring that they are not only compliant but also successfully control and manage risks[79].

3.3.1 ICS GRC –Regulation and international standards

(ICS) regulation refers to the laws and guidelines that govern the use and security of systems that control critical infrastructure, encompassing power generation plants, water purification facilities, transportation networks, etc. [80]. These regulations are implemented to guarantee the security and resilience of these systems against cyberattacks. The specific regulations will vary depending on the country and the industry in question, but generally, they will include guidelines for securing network communication, implementing access controls, and regularly monitoring and testing the system for vulnerabilities. Following a list for both type of standards:

- International standards for Information security
    1. ISO/IEC 27001 Information security management system.
    2. NIST Cybersecurity Framework: A risk-based approach to managing cybersecurity.
    3. PCI DSS Payment Card Industry Data Security Standard.
    4. GDRP General Data Protection Regulation.

- International standards specific to (ICS)[81].
    1. IEC 62443 Industrial control systems security standards
    2. ISA99/IEC 62443 A series of international standards for industrial automation and control systems security.
    3. CPNI: The Centre for the Protection of National Infrastructure.
    4. NIST 800- 82 Guide to (ICS) Security.
    5. CSSC Cross-sector Safety & Security Communications.
    6. ISA99 Industrial Automation and Control Systems Security.
    7. NERC The North American Electric Reliability Corporation.
    8. TSA Transportation Security Administration.

These standards provide organizations with a set of guidelines and best practices for ensuring the confidentiality, integrity, and availability of their ICS systems and data. The added values are as follow:

1. Continuous monitoring.
2. Self-reporting.
3. Self Certification.
4. Periodic audit.
5. Built and enforce controls.

3.3.2 ICS GRC –Risk Assessment

In the COSO ERM framework, risk assessment is a crucial step that follows event identification and precedes risk response. Its primary objective is to evaluate the magnitude of risks, both individually and collectively, to direct management's attention towards the most significant threats and opportunities. This process lays the foundation for implementing effective risk response strategies. Risk assessment involves the measurement and prioritization of risks to ensure they are managed within defined tolerance levels, without excessive control or missed opportunities[82].

Events that may trigger risk assessment include the initiation of an ERM program, periodic reviews, project commencements, mergers, acquisitions, divestitures, or major organizational changes. Some risks are dynamic and necessitate continuous monitoring and assessment, such as market fluctuations and production risks. Conversely, other risks are more stable and require periodic reassessment, with ongoing monitoring prompting a reassessment if circumstances change[83]. Within the realm of cybersecurity, risk assessment plays a crucial role in identifying and prioritizing potential threats to an organization's information systems and data. By systematically evaluating risks, organizations can allocate resources effectively to mitigate vulnerabilities and protect against cyberattacks. Moreover, risk assessment serves as a proactive measure to ensure compliance with regulatory requirements and industry standards, ultimately enhancing the overall cybersecurity posture of the organization[84]. The following table presents the steps involved in risk assessment, the methods used for assessment, and the corresponding responses to identified risk

Table 4 Risk Assessment Framework: Identification, Assessment, and Response

Risk assessment Steps	Risk assessment	Respond to Risk
Step 1 Risk identification	Quantitative Risk Assessment	Accept
Step 2 Risk analysis	Qualitative Risk Assessment	Avoid
Step 2 Risk analysis		Transfer
		Mitigate

3.3.3 Enhancing (ICS) Security Through Risk Assessment; ICS Risk Assessment Value.

Industrial Control Systems form the backbone of critical infrastructure, facilitating the operation of essential services across various sectors. However, their interconnected nature and reliance on digital technologies expose them to evolving cyber threats. In response, rigorous risk assessment practices are paramount to fortify the security of ICS environments. This sub section delineates the significance of ICS risk assessment and its implications in safeguarding against potential vulnerabilities.

1. Understanding ICS Vulnerabilities:
Comprehending the intricacies of vulnerabilities within ICS is fundamental to bolstering security protocols. By identifying weaknesses in control systems, stakeholders can proactively address potential loopholes that adversaries might exploit for malicious intent. This proactive approach not only enhances system resilience but also mitigates the risk of operational disruptions and adverse impacts on human safety, the environment, and financial stability.

2. Mitigating Potential Losses:
Effective risk assessment empowers organizations to prevent potential losses across multiple domains. By actively identifying and resolving vulnerabilities, stakeholders can avert human casualties, minimize environmental degradation, mitigate financial setbacks, prevent operational disruptions, and safeguard their reputations. This proactive stance serves as a linchpin in fostering resilience against cyber threats and ensuring the sustained functionality of critical infrastructure[85].

3. Compliance with Regulatory Standards:
Evaluation of system adherence to pertinent ICS security regulations, tailored to specific geographical areas and sectors, is imperative. Standards such as the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) [86], and National Cybersecurity

Authority Operational Technology and Telecommunications Certification (NCA OTTC) provide frameworks for assessing and enhancing cybersecurity posture. Compliance not only fosters regulatory alignment but also fortifies overall security resilience.

4. Adherence to Mandates:
Governmental, industry-specific, and internal corporate mandates necessitate the performance of comprehensive security assessments within ICS environments. Compliance with these mandates not only mitigates legal and regulatory risks but also instills a culture of cybersecurity diligence. By adhering to mandated security assessments, organizations demonstrate their commitment to safeguarding critical infrastructure and upholding the trust of stakeholders, so the value of ICS risk assessment cannot be overstated in the contemporary cybersecurity landscape. By comprehending vulnerabilities, preventing potential losses, ensuring regulatory compliance, and adhering to mandates, stakeholders can fortify the security posture of . This proactive approach not only mitigates cyber risks but also safeguards essential services, thereby ensuring the resilience and reliability of critical infrastructure[87].

3.3.4 ICS Risk Assessment Practices

Effective risk assessment practices are essential for ensuring the security and reliability of (ICS) across various operational levels. In this section, we delve into key methodologies and considerations involved in conducting comprehensive risk assessments within ICS environments. From assessing risks across different operational levels to adapting to emerging technologies and evolving demands, this analysis explores the multifaceted approach to identifying and mitigating potential risks. Additionally, we examine the importance of aligning risk acceptance decisions with the responsibilities of process owners, emphasizing the need for proactive risk management strategies to safeguard critical infrastructure assets[88].

1. Determine risk for each level.
2. From safety to auxiliary service.

3. Emerging technology and demand.
4. Any expectations and new requirements.
5. Risk acceptance should be decided by the process owner.

3.3.5 ICS Risk Assessment results

Conducting a thorough risk assessment of ICS environments is essential for identifying and mitigating potential security risks. In this context, the following analysis presents the results of an ICS risk assessment, highlighting key vulnerabilities and areas of concern within . By understanding and addressing these risks, organizations can enhance the resilience and security of their critical infrastructure assets against cyber threats[89].

1. Inadequate Physical Safeguards for ICS Equipment.
2. Fragile Network Architecture and Insufficient Network Safeguards.
3. Vulnerabilities in ICS Components like SCADA, PLCs, and Smart Meters.
4. Insufficient Authentication and Authorization Across Various Services.
5. Weak User Credentials.
6. Configuration Weaknesses, Including Excessive User Privileges and Noncompliance with Security Standards, and vendor recommendations.
7. Vulnerabilities in communication between the analyzed ICS and other systems (for instance, through an MES).
8. Vulnerabilities Stemming from Application Code Errors (e.g., Code Injection, Path Traversal).
9. Vulnerabilities Arising from Outdated Hardware and Software Versions Lacking the Latest Security Updates.
10. Information Disclosure Vulnerabilities.

4 ACSRA ICS METHODOLOGY

This chapter 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. The subsequent segments of this Chapter are organized as follows: Section 2 delves into five existing penetration test methodologies, Section 3 Introduced the used penetration test Tools, Section (4-9), introduces our novel methodology ACSRA ICS: Automated Cyber Security Risk Assessment Methodology for ICS, Section 10 encompasses the laboratory experimental segment, and finally, we provide a concise conclusion.

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][3] [5][90]. 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[91]. 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[92]. 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[93]. 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[94]. This is categorized as black box, white box, and gray box penetration testing[95]. In [45] 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 [96] 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.

4.1 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.

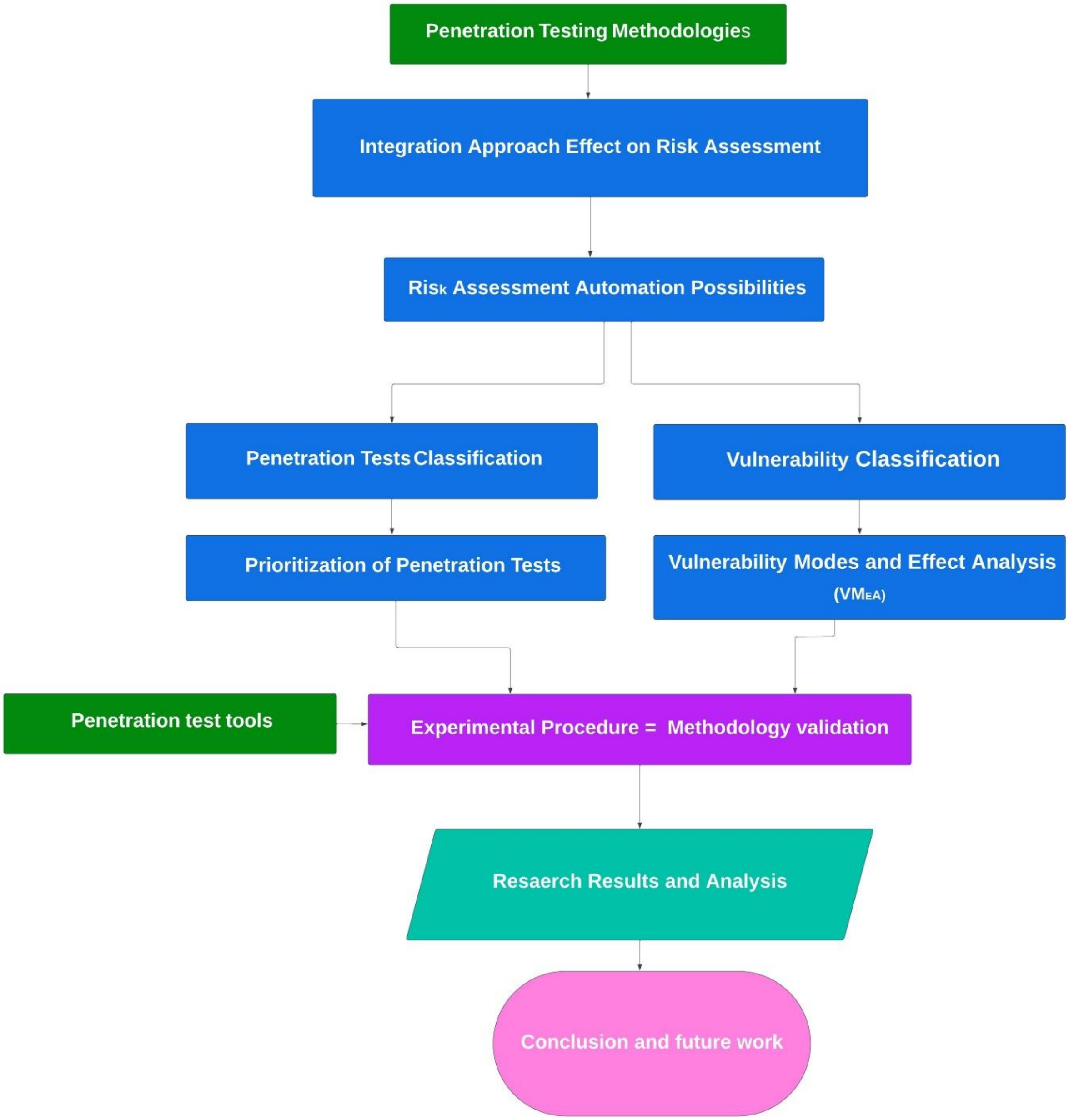

Penetration Testing Methodologies
Integration Approach Effect on Risk Assessment
Risk Assessment Automation Possibilities
Penetration Tests Classification
Vulnerability Classification
Prioritization of Penetration Tests
Vulnerability Modes and Effect Analysis (VMEA)
Penetration test tools
Experimental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

Figure 16 The Research Design and Procedure.

4.2 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.

4.2.1 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 (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)[97]. The revision introduces tailoring guidance for SP

800-53r5 security controls, offering specific security control baselines for different impact levels in OT systems[98]. 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[99]:

4.2.1.1 Information Security Audit Review Techniques

Technicians of the first group collect and analyze primary information about the information system which may include:

1. Review of documentation (security policies and architecture, security requirements, security plans, incident response plans, etc.), the results of which can be used to fine-tune other testing methods;
2. A review of service logs (for example, system or authentication server logs, intrusion detection and prevention logs, firewall logs, etc.) to determine whether security controls are recording valid information and whether the organization is complying with log management policies (often suggested to be used to check logs). automatic means);
3. Rule review (examination of a set of rules or signatures for network traffic or system activity, including access lists on routers, firewall rules, and intrusion detection system rules), used to identify vulnerabilities (weak spots) in security devices and in all multi-layered tools protection;
4. Review of system configuration (comparing system settings with the security requirements for a given system, or with the requirements defined in standards), used when searching for vulnerabilities in security configuration controls;
5. Analysis of network activity (tracking user flow, decoding protocols, checking headers and payloads to track information of interest), used for further analysis by other methods.

4.2.1.2 Techniques for identifying and analyzing information systems

Techniques for identifying and analyzing information systems are focused on specifying active devices and associated ports and services for the purpose of further analysis of potential vulnerabilities. This information is needed for further research of information systems for vulnerabilities. Techniques in this group include:

1. Network research (various methods are used, the list of which is constantly updated, and the use of automatic tools is assumed), as a result of which information appears about network devices, which is the input data for the following technology;
2. Identification of ports and services allows you to determine open ports and services running on network devices identified at previous stages (this information can be obtained through other techniques, for example, during the analysis of network activity);
3. Vulnerability scanning involves the use of automated procedures, which are the main penetration testing techniques.

4.2.1.3 Techniques for checking information systems for vulnerabilities

The NIST manual defines penetration testing as security testing that simulates real-life attacks to determine how to bypass the security features of a computer. Penetration tests involve searching for multiple vulnerabilities in the system being tested in order to carry out more attacks on that system than if only one vulnerability were used.

The penetration testing algorithm using the specified methodology, is divided into four stages:

1. Planning, in which rules are defined and testing goals are established (actual testing is not carried out at this stage).
2. Detection consists of collecting information about the system and analyzing vulnerabilities.
3. Simulating an attack is the main stage of testing, at which the actions of the intruder are simulated and the vulnerabilities identified at the previous stage are confirmed (when new information about the system is

identified, additional data is used to further study the true risk for the information object).

4. Preparation of a report, which takes place permanently with other stages throughout the entire testing process, at the end of which a final report is issued.

4.2.2 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[100]. 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.

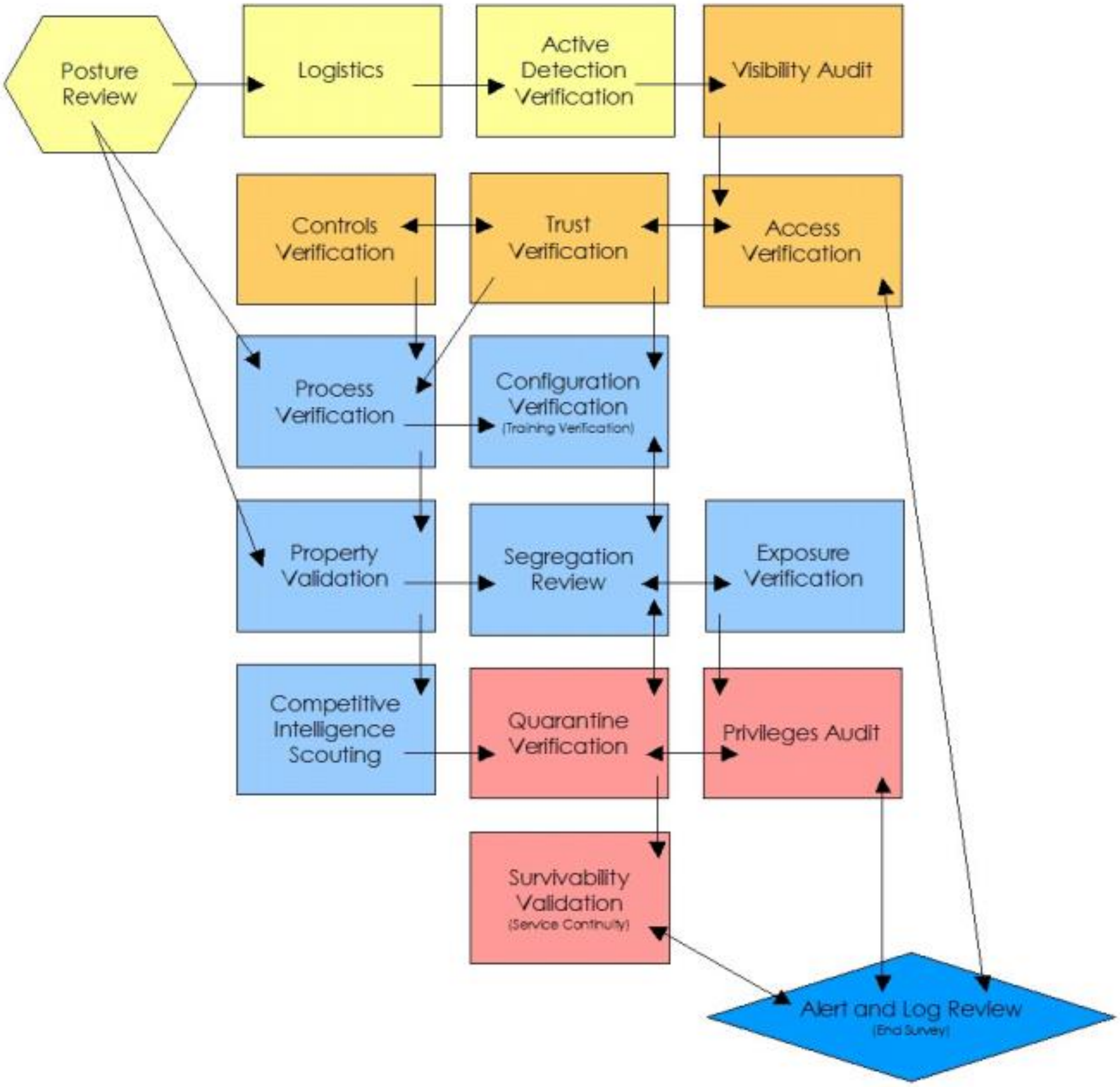


Figure 17 One Methodology applies to all types of security tests [100].

4.2.3 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 utilized for assessing risk management based on ISO 31000 principles. This risk management process encompasses stages such as risk identification, risk analysis, and risk evaluation[101]. The following figure shows the ISSAF Framework Methodology.

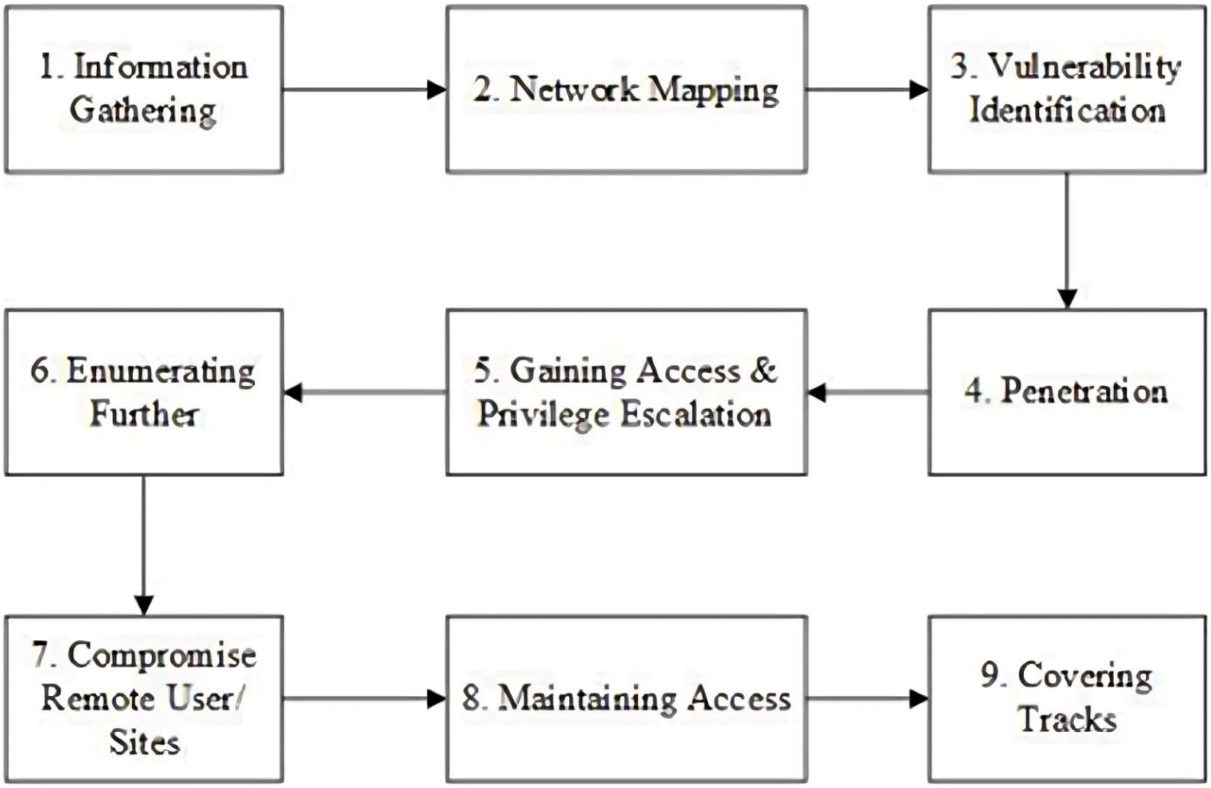


Figure 18 ISSAF Framework Methodology [101].

4.2.4 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[102]:

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 (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[102].

4.2.5 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[103]. 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[104].

4.3 Penetration test tools

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

4.3.1 Wireshark

Wireshark is a packet analyzer that is both free and open-source. providing insights into network performance, protocol behavior, and security threats[105]. 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[106]. Organizations should also educate their staff about the risks tied to Wireshark and similar tools. By fostering awareness and enforcing strict access controls, organizations can reduce the chances of adversaries gaining unauthorized access to sensitive network information. In the following I delve into the dual role of Wireshark, emphasizing its significance as a valuable tool for both analysis and adversarial activities.

4.3.1.1 Analysis

In the sub-section dedicated to Analysis, Wireshark emerges as an indispensable tool for network troubleshooting, protocol analysis, and security assessment. Through its robust packet capture and examination capabilities, Wireshark empowers professionals to identify and resolve network performance issues, scrutinize diverse protocols for behavior anomalies, and bolster network defenses by detecting and mitigating potential security threats. Its comprehensive features for filtering and analyzing packet data render it invaluable in enhancing network reliability, optimizing performance, and fortifying cybersecurity measures.

Network Troubleshooting: Wireshark provides a comprehensive overview of network traffic, empowering network administrators and analysts to pinpoint and resolve various issues. Through the capture and examination of packets, professionals can identify network performance bottlenecks, diagnose configuration problems, and detect faulty devices. Wireshark's robust filtering and analysis features facilitate efficient problem diagnosis[107].

Protocol Analysis: Wireshark supports a broad spectrum of protocols, allowing experts to scrutinize the behavior and performance of diverse network protocols. Whether it involves HTTP, DNS, TCP, or any other protocol, Wireshark's capability to decode and present packet information in a human-readable format aids in understanding protocol behavior, spotting anomalies, and optimizing network performance[107].

Security Analysis: Wireshark plays a pivotal role in network security analysis, enabling security professionals to scrutinize packets for signs of malicious activities like suspicious traffic patterns, unauthorized access attempts, or data exfiltration. Through packet capture and analysis, security analysts can identify potential threats, assess vulnerabilities, and fortify network defenses[107]. Following some of examples of security analysis:

- Detecting a DDoS Attack: Wireshark can unveil a sudden surge in traffic from multiple sources, indicative of a distributed denial-of-service (DDoS) attack. Analysis of packet headers and payloads assists in identifying attack vectors, involved IP addresses, and the types of traffic flooding the network [108].
- Identifying Malware Infections: Wireshark can discern communication patterns associated with malware infections, such as unusual traffic, connections to suspicious IP addresses, or unexpected data transfers. Analysis of packet payloads provides insights into the malware's behavior and its impact on the network [109].

4.3.1.2 Adversarial Use

In the sub-section on Adversarial Use, Wireshark emerges as a potent instrument wielded by adversaries across various stages of cyber operations. From reconnaissance activities, where attackers leverage packet capture to dissect network structures and vulnerabilities, to traffic sniffing, enabling the interception of sensitive data, to exploitation, where Wireshark aids in pinpointing weaknesses for unauthorized access and attacks, its utility underscores the challenges posed by its misuse in the cybersecurity landscape. Balancing its legitimate utility with the imperative to guard against malicious exploitation highlights the necessity for proactive measures to uphold network security and integrity.

Reconnaissance: Wireshark becomes a tool for adversaries in the reconnaissance phase of an attack. Through packet capture on a target network, attackers acquire crucial insights into the network's structure, discerning hosts, services, and potential vulnerabilities. This reconnaissance enables adversaries to plan attacks more effectively and select appropriate exploitation methods[107].

Traffic Sniffing: Wireshark allows adversaries to capture and scrutinize network traffic, facilitating the interception of sensitive information like passwords, usernames, or financial data. The decryption capability of Wireshark, with the right keys, further aids adversaries in extracting valuable data from intercepted packets[107].

Exploitation:Wireshark aids adversaries in identifying exploitable vulnerabilities within a network. By analyzing captured packets, attackers can pinpoint weaknesses, misconfigurations, or unpatched systems. Armed with this information, adversaries can exploit vulnerabilities to gain unauthorized access, launch attacks, or execute lateral movement within the network[107].

In conclusion, Wireshark remains an invaluable tool for network analysis and troubleshooting, providing valuable insights into network performance, protocol behavior, and security threats. However, its attractiveness to adversaries underscores the importance of responsible and ethical usage. Safeguarding the integrity of Wireshark's role in enhancing network security demands a proactive stance to mitigate potential risks and thwart malicious activities.

4.3.2 Nmap

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.

Notably, Nmap boasts compatibility with major operating systems, offering official binary packages tailored for Linux, Windows, and Mac OS X environments. Beyond its traditional command-line interface, Nmap encompasses a comprehensive suite of utilities, featuring a sophisticated graphical user interface and results viewer recognized as Zenmap. Additionally, Nmap includes auxiliary tools such as Ncat, facilitating seamless data transfer, redirection, and debugging, along with Ndiff, a utility indispensable for comparing scan results, and Nping, a tool engineered for packet generation and response analysis.

The versatility of Nmap extends far beyond its diverse array of tools, encompassing a rich repertoire of advanced techniques essential for mapping networks effectively. Nmap adeptly navigates through obstacles like IP filters, firewalls, and routers, offering an assortment of port scanning mechanisms, robust OS detection capabilities, version detection functionalities, and the ability to conduct ping sweeps, among other features. In essence, Nmap stands as an indispensable asset for network professionals, offering unparalleled flexibility and reliability in the realm of network exploration and security assessments.[110].

To perform a good penetration test first need to discover the target devices opened ports. For this in literature research, I find more examples to use Nmap. My target device has an ethernet connection and I read in the documentation [111] that have http, https, profinet protocol, and SMP. The rationale for utilizing Nmap can be delineated as follows:

1. Potent: Nmap has demonstrated its prowess by effectively scanning vast networks housing hundreds of thousands of machines.

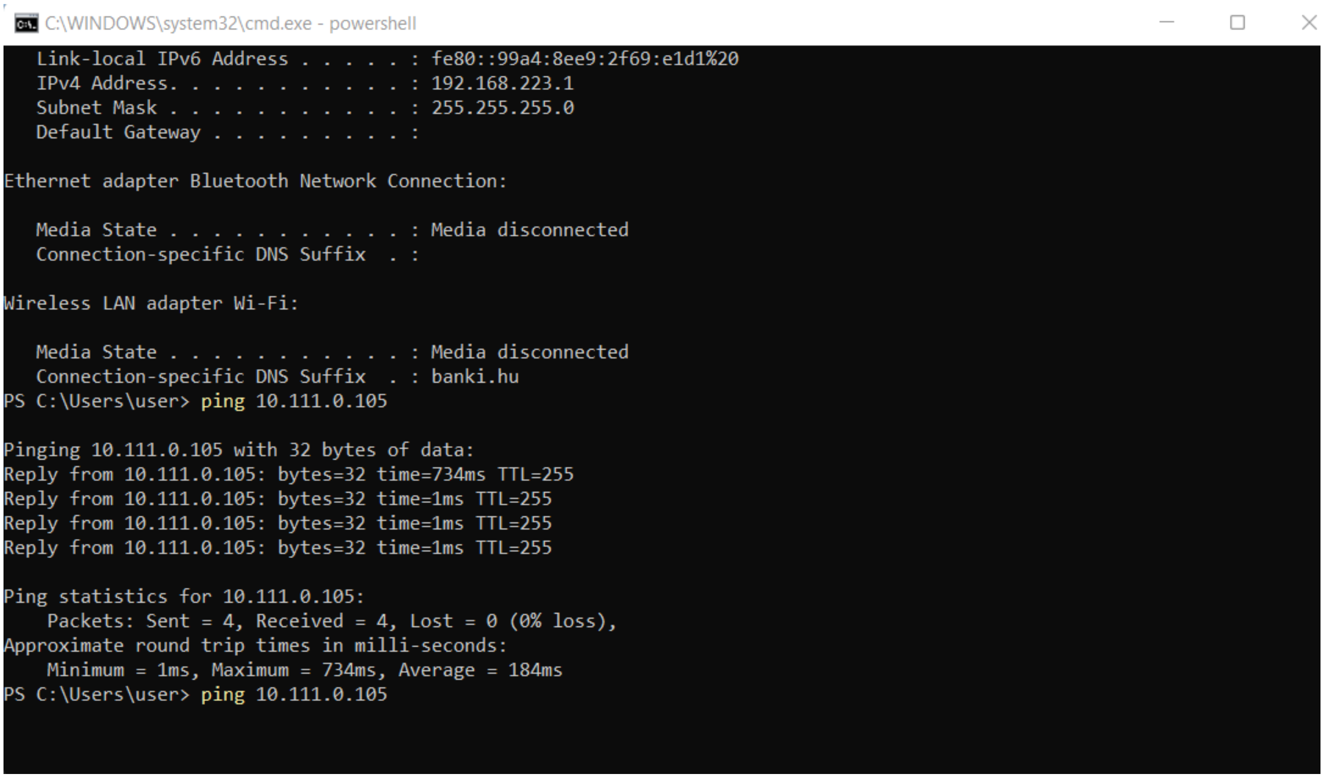
2. Versatile: Compatible across major operating systems such as Linux, Windows, FreeBSD, OpenBSD, Solaris, Mac OS X, and more, Nmap offers portability and accessibility.
3. User-Friendly: Nmap caters to users of all levels, offering a simple command line interface with commands like "nmap -v -A target host" for beginners, as well as graphical (GUI) versions. Installation is hassle-free with readily available binaries.
4. Free and Open Source: In alignment with the Nmap Project's mission to bolster internet security, Nmap is freely downloadable and its source code is open for modification and redistribution.
5. Extensive Documentation: Nmap provides thorough documentation, encompassing man pages, whitepapers, tutorials, and a dedicated book, accessible in multiple languages.
6. Community Support: Although Nmap is not warranted, a dynamic community of developers and users offers support through mailing lists and real-time chat channels on platforms like Freenode or EFNet.
7. Accolades: Nmap has garnered numerous awards, including "Information Security Product of the Year," and has been featured in various media forms such as articles, movies, books, and comic book series.
8. Popularity: With widespread daily downloads, inclusion in various operating systems, and a consistent presence among the top ten programs on Freshmeat.Net, Nmap fosters a robust community for both development and user support.

4.3.2.1 Experimental PLC Network Security Assessment: A Comparative Analysis Using Zenmap and Nmap

In this laboratory experiment, a PLC network was constructed with targeted PLCs, and a computer was connected to the same network. This setup was enacted at the Riev TECH PLC lab within the Banki Donat Faculty. The objective was to perform a network configuration check between the laptop and the PLCs. Utilizing Zenmap on Windows and Nmap on Kali

Linux, a comprehensive network scan was conducted to identify all connected devices and assess their configurations. The subsequent analysis aimed to reveal insights into the network topology and provide detailed information about the PLCs, including port statuses and security implications.

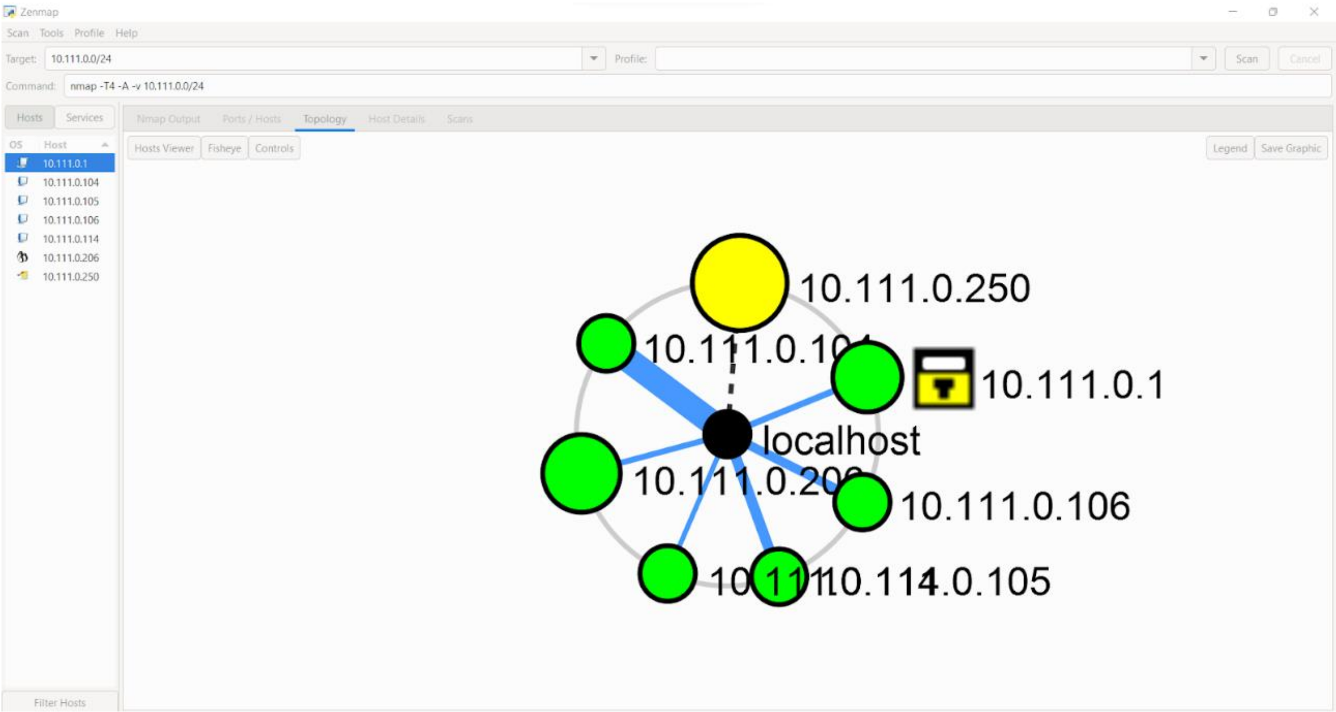
The following Figure is the Network configuration check between the laptop and the Plc.



```
   Link-local IPv6 Address . . . . . : fe80::99a4:8ee9:2f69:e1d1%20
   IPv4 Address. . . . . . . . . . . : 192.168.223.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : banki.hu
PS C:\Users\user> ping 10.111.0.105

Pinging 10.111.0.105 with 32 bytes of data:
Reply from 10.111.0.105: bytes=32 time=734ms TTL=255
Reply from 10.111.0.105: bytes=32 time=1ms TTL=255
Reply from 10.111.0.105: bytes=32 time=1ms TTL=255
Reply from 10.111.0.105: bytes=32 time=1ms TTL=255

Ping statistics for 10.111.0.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 734ms, Average = 184ms
PS C:\Users\user> ping 10.111.0.105
```

Figure 19 Network configure check

Then I made a network scan for all connected devices by Zenmap on Windows and by Nmap on Kali Linx, the following figures contain the results of the Zenmap and by Nmap on Kali Linx.



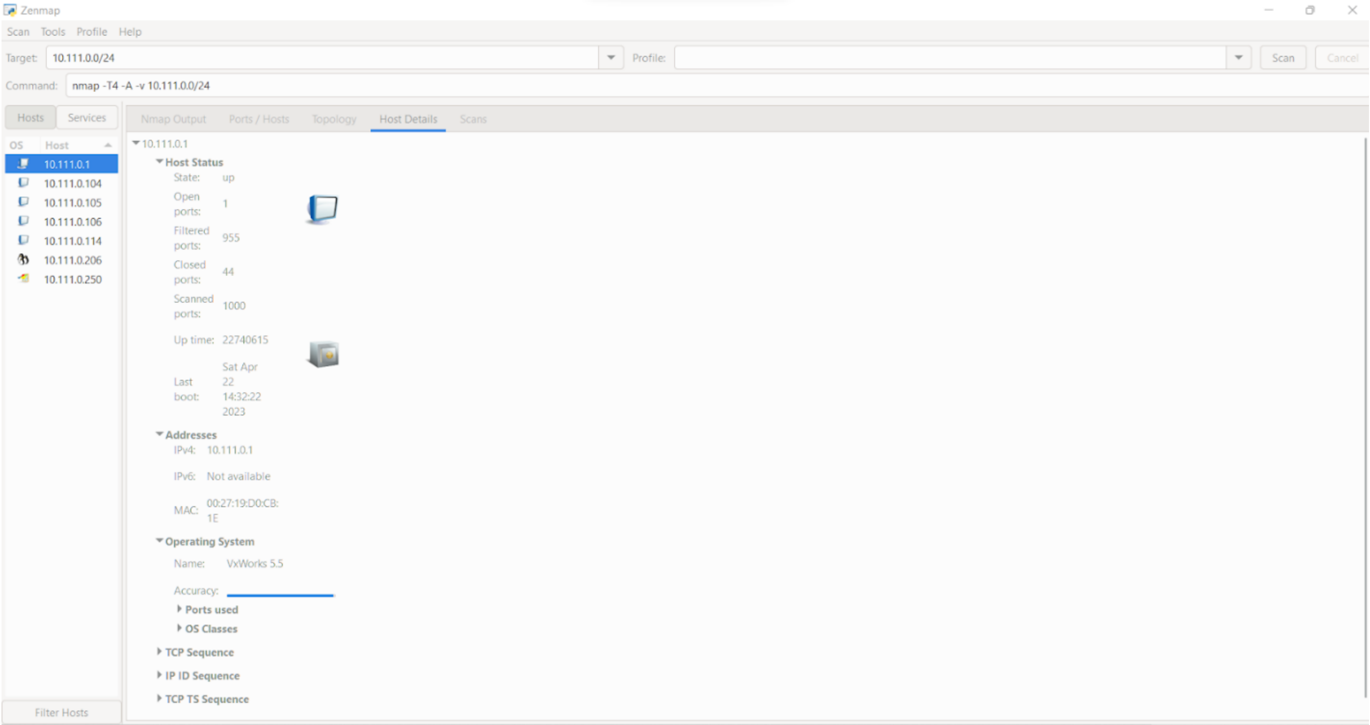
Target: 10.111.0.0/24

Command: nmap -T4 -A -v 10.111.0.0/24

```
OS  Host
    10.111.0.1
    10.111.0.104
    10.111.0.105
    10.111.0.106
    10.111.0.114
    10.111.0.206
    10.111.0.250
```

Figure 20 Network Topology

The Network topology showed all connected devices including the laptop, Figure 21 and Figure 22 specifically showed the PLCs details.



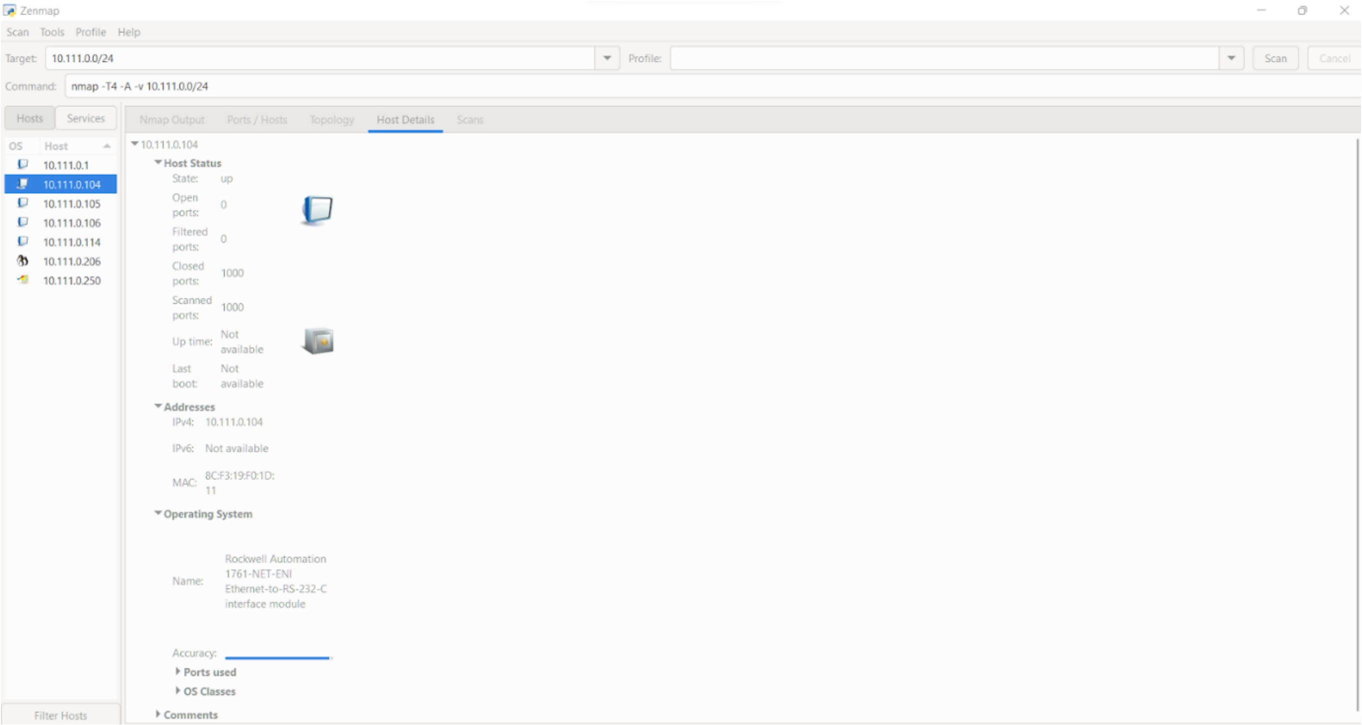
Target: 10.111.0.0/24

Command: nmap -T4 -A -v 10.111.0.0/24

```
10.111.0.1
10.111.0.104
10.111.0.105
10.111.0.106
10.111.0.114
10.111.0.206
10.111.0.250
```

```
▾ 10.111.0.1
  ▾ Host Status
      State:          up
      Open ports:     1
      Filtered ports: 955
      Closed ports:   44
      Scanned ports:  1000
      Up time:        22740615
      Last boot:      Sat Apr 22 14:32:22 2023
  ▾ Addresses
      IPv4: 10.111.0.1
      IPv6: Not available
      MAC:  00:27:19:D0:CB:1E
  ▾ Operating System
      Name:     VxWorks 5.5
      Accuracy:
      ▸ Ports used
      ▸ OS Classes
  ▸ TCP Sequence
  ▸ IP ID Sequence
  ▸ TCP TS Sequence
```

Figure 21 The Host Details For Plc 1



Target: 10.111.0.0/24

Command: nmap -T4 -A -v 10.111.0.0/24

```
10.111.0.1
10.111.0.104
10.111.0.105
10.111.0.106
10.111.0.114
10.111.0.206
10.111.0.250
```

```
▾ 10.111.0.104
  ▾ Host Status
      State:          up
      Open ports:     0
      Filtered ports: 0
      Closed ports:   1000
      Scanned ports:  1000
      Up time:        Not available
      Last boot:      Not available
  ▾ Addresses
      IPv4: 10.111.0.104
      IPv6: Not available
      MAC:  8C:F3:19:F0:1D:11
  ▾ Operating System
      Name:     Rockwell Automation 1761-NET-ENI Ethernet-to-RS-232-C interface module
      Accuracy:
      ▸ Ports used
      ▸ OS Classes
  ▸ Comments
```

Figure 22 The Host Details for Plc 2

The default Zenmap/nmap scanning did not find the PLC-specific ports. With s7-info script nmap I find the PLC-s details information. So for security-related checks, Linux software is recommended.

Through the utilization of Zenmap and Nmap, this experiment successfully examined the network configuration and security posture of the PLC network. The network topology revealed all connected devices, with specific attention given to the details of the PLCs. While default scanning methods initially yielded closed ports for the PLCs, the utilization of the s7-info script in Nmap facilitated the retrieval of PLC-specific information, underscoring the importance of employing Linux software for security-focused assessments. This experiment highlights the significance of thorough network analysis and emphasizes the role of specialized tools in enhancing cybersecurity practices within industrial control systems.

4.3.2.2 Results

The findings of the laboratory experiment conducted to assess the network configuration and security posture of the PLC network are as follows:

- Network Configuration Check: The initial step involved verifying the network configuration between the laptop and the PLCs. The setup was confirmed to be operational at the Riev TECH PLC lab within the Banki Donat Faculty.
- Network Topology: Through network scanning using Zenmap and Nmap, the topology of the network was mapped, revealing all connected devices. This included the identification of the laptop and specific details regarding the PLCs present in the network.
- PLC Details: Detailed information about the PLCs was extracted, focusing on aspects such as IP addresses, host names, and services running on the devices. Specific figures (Figure 20 and Figure 21) were utilized to showcase the host details for each PLC.
- Port Status: Zenmap revealed that all ports on the PLCs were initially closed. However, further analysis using Nmap, particularly with the s7-

info script, provided insight into PLC-specific ports and services. This finding underscores the importance of employing specialized scripts and tools for comprehensive security assessments.

- Security Implications: The experiment highlighted the need for robust security measures within PLC networks. While default scanning methods may not uncover all vulnerabilities, utilizing advanced techniques and specialized software, particularly on Linux platforms, can enhance security assessments and reveal critical information for mitigating potential risks.

4.4 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[112].
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 [113].
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.

4.5 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 5 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 5 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:

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

4.6 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.

4.7 Vulnerability Classification

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.

4.8 Vulnerability Modes and Effect Analysis (VMEA)

Vulnerability Modes and Effects 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 6. 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 6 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

4.9 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 7 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 7 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

4.10 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.

4.10.1 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 23.

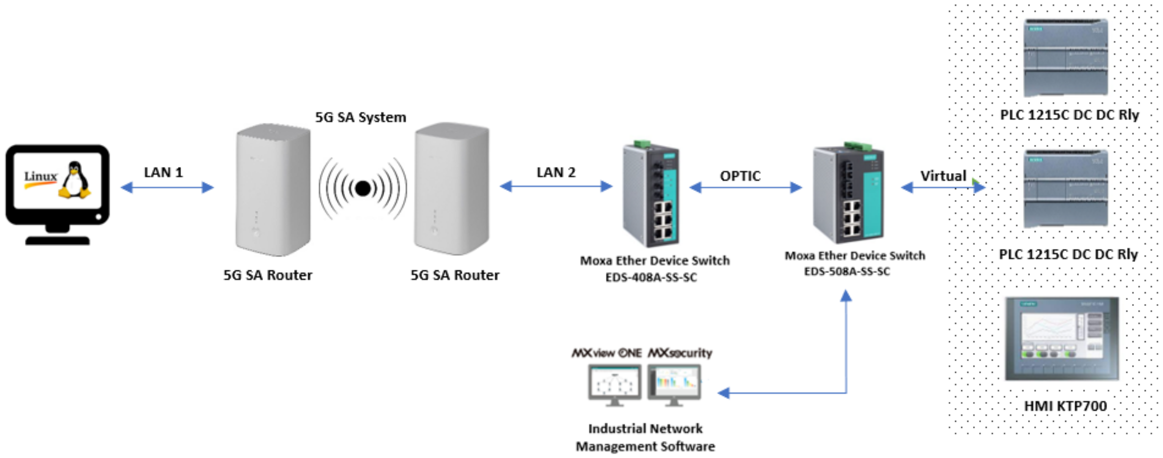


Figure 23 System Structure:5G-Enabled ICS Device Identification and Version Discovery in Óbuda University's Test Network

4.10.2 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 24 shows the ACSRA ICS system Block diagram.

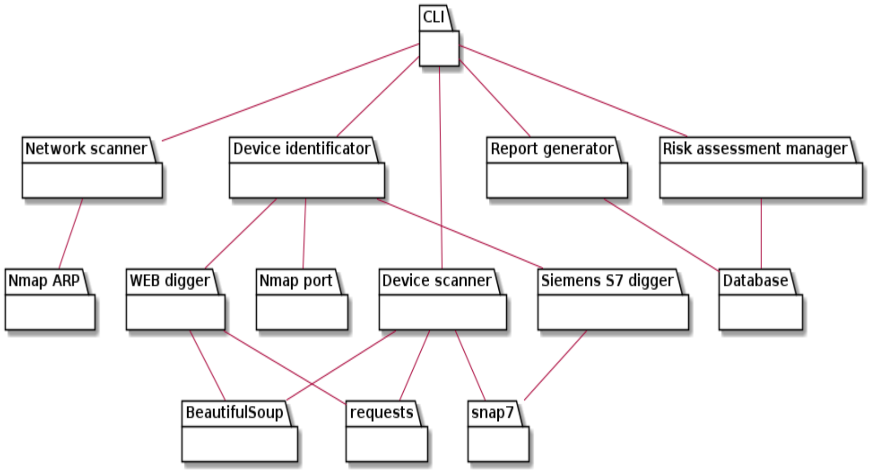


Figure 24 Block diagram of the ACSRA ICS system

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.

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 utilized 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 ide n, 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 25, 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.

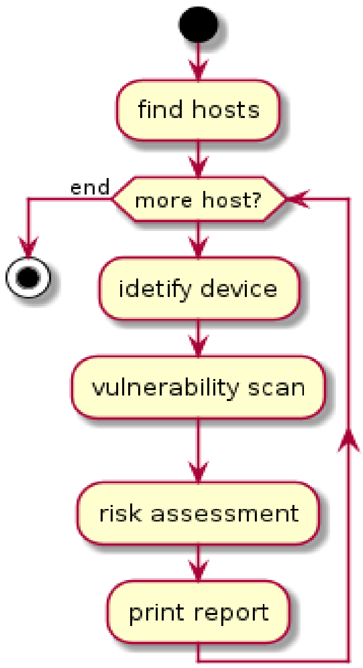
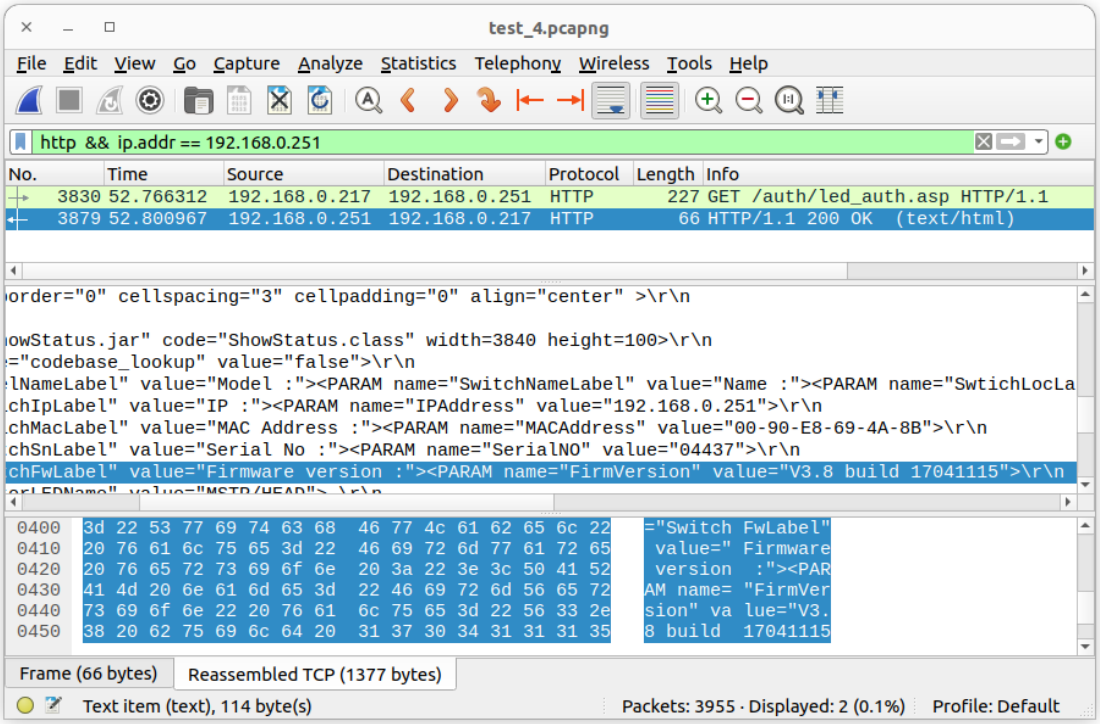


Figure 25 ACSRA ICS workflow

4.10.3 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 26 serves as a visual representation of a meticulous exploration- undertaken through Wireshark network analysis focused on the identification of software versions within HTTP communication. By 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. showcases stages and components, offering clear insight into systematic steps for precise model name identification embedded within network data.


test_4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http && ip.addr == 192.168.0.251
```

```
No.     Time       Source         Destination    Protocol  Length Info
   3830 52.766312  192.168.0.217  192.168.0.251  HTTP         227 GET /auth/led_auth.asp HTTP/1.1
   3879 52.800967  192.168.0.251  192.168.0.217  HTTP          66 HTTP/1.1 200 OK  (text/html)
```

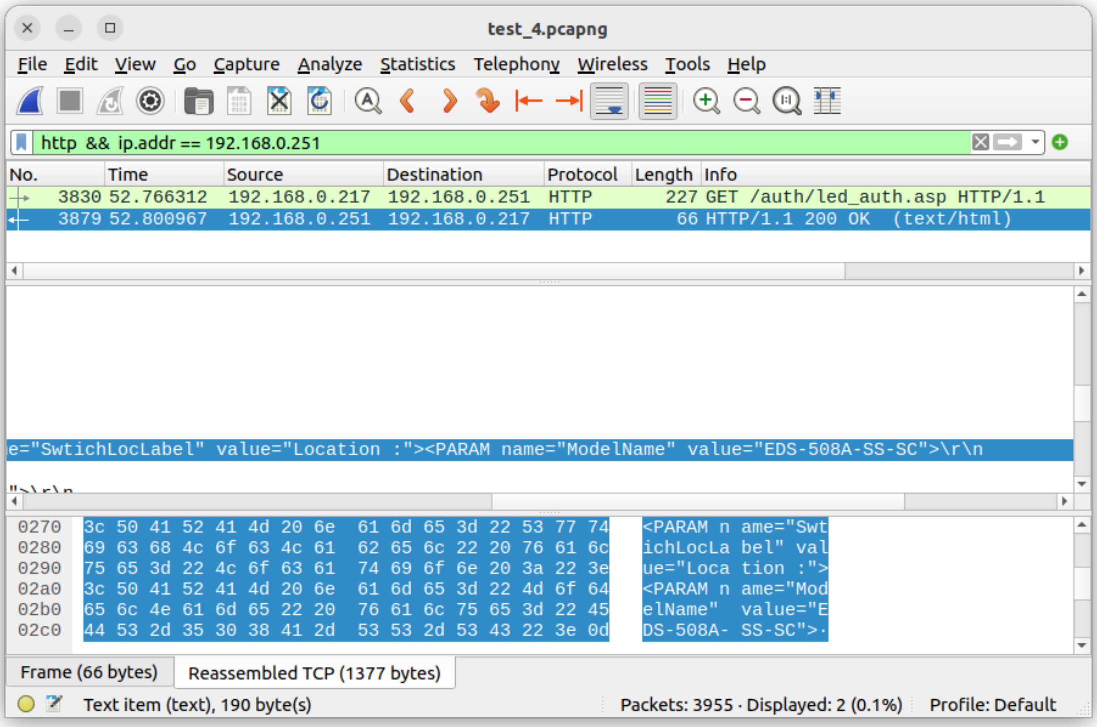
```
order="0" cellspacing="3" cellpadding="0" align="center" >\r\n

owStatus.jar" code="ShowStatus.class" width=3840 height=100>\r\n
="codebase_lookup" value="false">\r\n
lNameLabel" value="Model :"><PARAM name="SwitchNameLabel" value="Name :"><PARAM name="SwtichLocLa
chIpLabel" value="IP :"><PARAM name="IPAddress" value="192.168.0.251">\r\n
chMacLabel" value="MAC Address :"><PARAM name="MACAddress" value="00-90-E8-69-4A-8B">\r\n
chSnLabel" value="Serial No :"><PARAM name="SerialNO" value="04437">\r\n
chFwLabel" value="Firmware version :"><PARAM name="FirmVersion" value="V3.8 build 17041115">\r\n
orLEDName" value="MSTP/HEAD"> \r\n
```

```
0400  3d 22 53 77 69 74 63 68  46 77 4c 61 62 65 6c 22   ="Switch FwLabel"
0410  20 76 61 6c 75 65 3d 22  46 69 72 6d 77 61 72 65    value=" Firmware
0420  20 76 65 72 73 69 6f 6e  20 3a 22 3e 3c 50 41 52    version  :"><PAR
0430  41 4d 20 6e 61 6d 65 3d  22 46 69 72 6d 56 65 72   AM name= "FirmVer
0440  73 69 6f 6e 22 20 76 61  6c 75 65 3d 22 56 33 2e   sion" va lue="V3.
0450  38 20 62 75 69 6c 64 20  31 37 30 34 31 31 31 35   8 build  17041115
```

Frame (66 bytes) | Reassembled TCP (1377 bytes)

Text item (text), 114 byte(s) Packets: 3955 · Displayed: 2 (0.1%) Profile: Default

Figure 26 Moxa device version detecting with Wireshark


test_4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http && ip.addr == 192.168.0.251
```

```
No.     Time       Source         Destination    Protocol  Length Info
   3830 52.766312  192.168.0.217  192.168.0.251  HTTP         227 GET /auth/led_auth.asp HTTP/1.1
   3879 52.800967  192.168.0.251  192.168.0.217  HTTP          66 HTTP/1.1 200 OK  (text/html)
```

```
e="SwtichLocLabel" value="Location :"><PARAM name="ModelName" value="EDS-508A-SS-SC">\r\n

">\r\n
```

```
0270  3c 50 41 52 41 4d 20 6e  61 6d 65 3d 22 53 77 74   <PARAM n ame="Swt
0280  69 63 68 4c 6f 63 4c 61  62 65 6c 22 20 76 61 6c   ichLocLa bel" val
0290  75 65 3d 22 4c 6f 63 61  74 69 6f 6e 20 3a 22 3e   ue="Loca tion :">
02a0  3c 50 41 52 41 4d 20 6e  61 6d 65 3d 22 4d 6f 64   <PARAM n ame="Mod
02b0  65 6c 4e 61 6d 65 22 20  76 61 6c 75 65 3d 22 45   elName"  value="E
02c0  44 53 2d 35 30 38 41 2d  53 53 2d 53 43 22 3e 0d   DS-508A- SS-SC">·
```

Frame (66 bytes) | Reassembled TCP (1377 bytes)

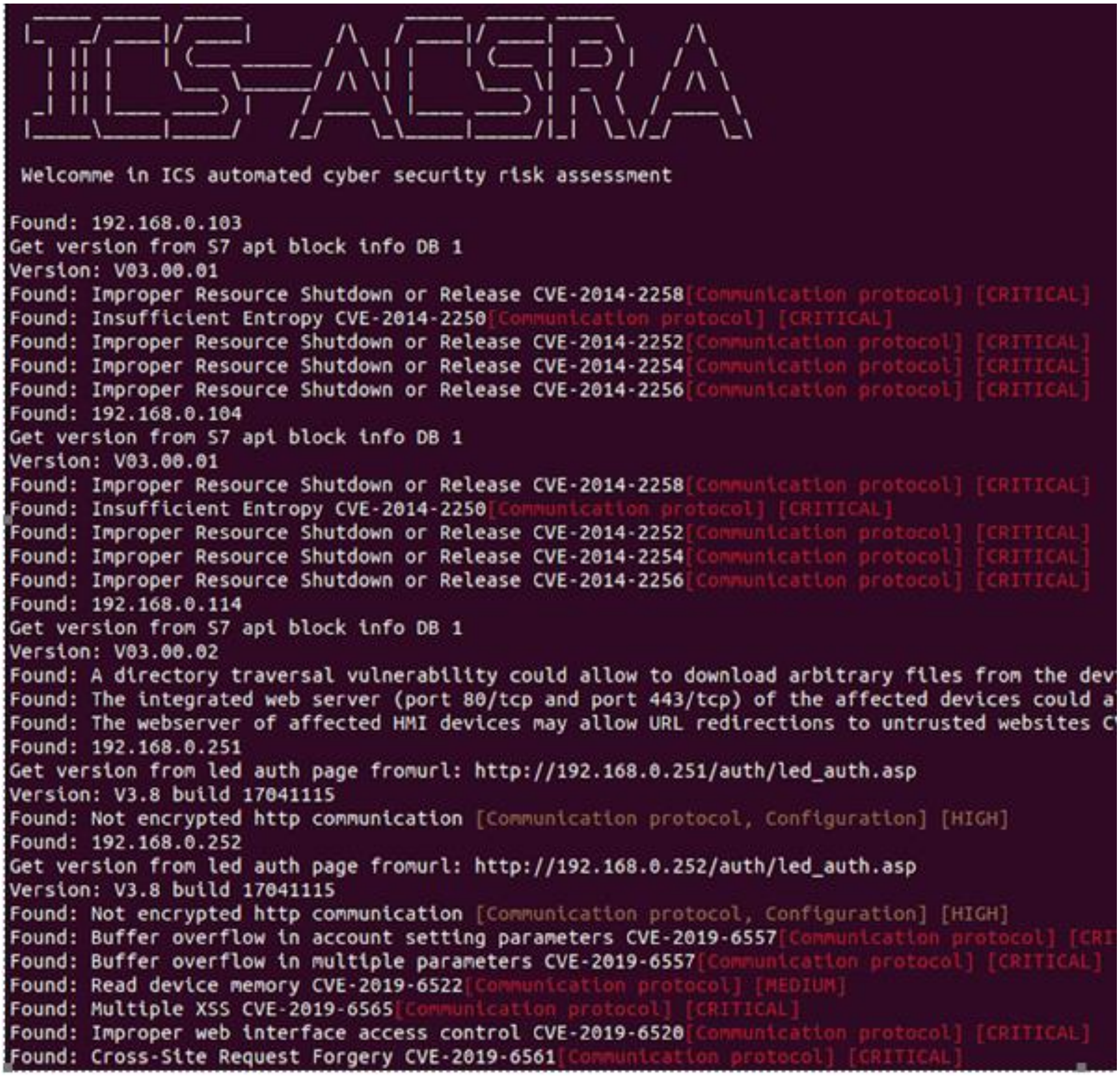
Text item (text), 190 byte(s) Packets: 3955 · Displayed: 2 (0.1%) Profile: Default

Figure 27 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. 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 29 is a screenshot of our automated risk assessment process utilizing our solution in the laboratory.



```
 _____ _____  _____            _____  _____ _____            
|_   _/ ____|/ ____|     /\   / ____|/ ____|  __ \     /\    
  | || |    | (___      /  \ | |    | (___ | |__) |   /  \   
  | || |     \___ \____/ /\ \| |     \___ \|  _  /   / /\ \  
 _| || |____ ____) |  / ____ \ |____ ____) | | \ \  / ____ \ 
|_____\_____|_____/  /_/    \_\_____|_____/|_|  \_\/_/    \_\

 Welcomme in ICS automated cyber security risk assessment

Found: 192.168.0.103
Get version from S7 api block info DB 1
Version: V03.00.01
Found: Improper Resource Shutdown or Release CVE-2014-2258[Communication protocol] [CRITICAL]
Found: Insufficient Entropy CVE-2014-2250[Communication protocol] [CRITICAL]
Found: Improper Resource Shutdown or Release CVE-2014-2252[Communication protocol] [CRITICAL]
Found: Improper Resource Shutdown or Release CVE-2014-2254[Communication protocol] [CRITICAL]
Found: Improper Resource Shutdown or Release CVE-2014-2256[Communication protocol] [CRITICAL]
Found: 192.168.0.104
Get version from S7 api block info DB 1
Version: V03.00.01
Found: Improper Resource Shutdown or Release CVE-2014-2258[Communication protocol] [CRITICAL]
Found: Insufficient Entropy CVE-2014-2250[Communication protocol] [CRITICAL]
Found: Improper Resource Shutdown or Release CVE-2014-2252[Communication protocol] [CRITICAL]
Found: Improper Resource Shutdown or Release CVE-2014-2254[Communication protocol] [CRITICAL]
Found: Improper Resource Shutdown or Release CVE-2014-2256[Communication protocol] [CRITICAL]
Found: 192.168.0.114
Get version from S7 api block info DB 1
Version: V03.00.02
Found: A directory traversal vulnerability could allow to download arbitrary files from the dev
Found: The integrated web server (port 80/tcp and port 443/tcp) of the affected devices could a
Found: The webserver of affected HMI devices may allow URL redirections to untrusted websites C
Found: 192.168.0.251
Get version from led auth page fromurl: http://192.168.0.251/auth/led_auth.asp
Version: V3.8 build 17041115
Found: Not encrypted http communication [Communication protocol, Configuration] [HIGH]
Found: 192.168.0.252
Get version from led auth page fromurl: http://192.168.0.252/auth/led_auth.asp
Version: V3.8 build 17041115
Found: Not encrypted http communication [Communication protocol, Configuration] [HIGH]
Found: Buffer overflow in account setting parameters CVE-2019-6557[Communication protocol] [CRI
Found: Buffer overflow in multiple parameters CVE-2019-6557[Communication protocol] [CRITICAL]
Found: Read device memory CVE-2019-6522[Communication protocol] [MEDIUM]
Found: Multiple XSS CVE-2019-6565[Communication protocol] [CRITICAL]
Found: Improper web interface access control CVE-2019-6520[Communication protocol] [CRITICAL]
Found: Cross-Site Request Forgery CVE-2019-6561[Communication protocol] [CRITICAL]
```

Figure 28 The automated risk assessment process utilizing our solution in our laboratory.

4.10.4 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 8 compares ACSRA ICS with selected open-source ICS tools.

Table 8 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 RESEARCH RESULTS AND ANALYSIS

This chapter reports the main findings of the study based on the applied methodology.

Answers to the research questions are given, and results concerning hypothesized statements are arranged in a logical sequence.

5.1 Integrated Approach Hypothesis

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: How does the integration of the studied security standards and frameworks improve the overall risk assessment process in SCADA and ICS environments?

Integrating various security standards and frameworks in SCADA and ICS environments enhances the risk assessment process in several ways:

1. Comprehensive Coverage: Different standards and frameworks provide diverse perspectives on security risks. By integrating them, organizations can achieve a more comprehensive understanding of potential vulnerabilities and threats.
2. Risk Prioritization: Each standard may prioritize risks differently. By combining them, organizations can prioritize risks based on multiple criteria, such as likelihood, impact, and regulatory compliance, leading to more informed decision-making.
3. Customization: Integrating various standards allows organizations to tailor risk assessment processes to their specific operational environment, considering unique requirements and constraints.

4. Holistic Approach: Integration promotes a holistic approach to risk assessment, considering both technical and operational aspects. This ensures that security measures align with business objectives and operational needs.
5. Regulatory Compliance: Many standards and frameworks address specific regulatory requirements. Integration helps organizations ensure compliance with relevant regulations, reducing the risk of penalties and legal liabilities.
6. Continuous Improvement: Integrating standards facilitates ongoing refinement of the risk assessment process. Organizations can continuously update their approach based on emerging threats, technological advancements, and lessons learned from past incidents.

Overall, the integration of different security standards and frameworks improves the effectiveness and efficiency of risk assessment in SCADA and ICS environments by providing a more holistic, customizable, and continuously improving approach to security management.

Q2: How does adopting an integrated approach contribute to the development of a culture of continuous improvement in cybersecurity within SCADA and ICS environments?

1. Feedback Loop: Integrating various security practices enables organizations to establish feedback loops where insights from different sources are utilized to refine security measures continually.
2. Shared Knowledge: Integration encourages collaboration among different teams and stakeholders involved in cybersecurity. This sharing of knowledge and expertise cultivates a culture of learning and innovation.
3. Adaptability: An integrated approach emphasizes flexibility and adaptability in responding to evolving cyber threats and challenges. This mindset of adaptability encourages experimentation and innovation in cybersecurity practices.

4. Benchmarking: By integrating diverse security standards and frameworks, organizations can benchmark their cybersecurity practices against industry best practices and standards. This comparison helps identify areas for improvement and drives the pursuit of excellence.
5. Organizational Resilience: Continuous improvement in cybersecurity practices enhances organizational resilience against cyber threats. This resilience is built upon a foundation of ongoing assessment, adaptation, and optimization of security measures.
6. Leadership Commitment: An integrated approach requires leadership commitment to promote a culture of continuous improvement. When leaders prioritize cybersecurity and support initiatives for integration and enhancement, it sets a precedent for the entire organization.

Adopting an integrated approach contributes to the development of a culture of continuous improvement by fostering collaboration, adaptability, and a commitment to excellence in cybersecurity within SCADA and ICS environments.

Q3: 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?

1. Transparency: Open-source security resources provide transparency into the underlying code and methodologies, allowing organizations to validate the security of the solutions and identify any vulnerabilities or weaknesses.
2. Community Collaboration: Open-source projects often benefit from a diverse community of contributors who collaborate to improve the security and functionality of the software. This collaborative effort enhances the quality and reliability of open-source security resources.
3. Cost Savings: Open-source software is typically available for free or at a lower cost compared to proprietary solutions. This affordability reduces the financial burden on organizations, especially those with limited

budgets, making it a cost-effective option for implementing security measures.

4. Customization: Open-source security resources offer flexibility for customization to meet specific requirements and integrate seamlessly with existing systems and infrastructure. This customization capability enables organizations to adapt security solutions to their unique needs without incurring additional expenses for proprietary customization.
5. Rapid Innovation: Open-source projects often embrace a culture of innovation and agility, leading to rapid development cycles and the timely implementation of security enhancements and updates. This agility helps organizations stay ahead of emerging threats and maintain a proactive security posture.
6. Vendor Independence: By leveraging open-source security resources, organizations reduce dependence on specific vendors or proprietary technologies. This vendor independence mitigates the risks associated with vendor lock-in and provides greater freedom to choose the best solutions based on performance, security, and compatibility.

The key advantages of using open-source security resources, including transparency, community collaboration, cost savings, customization, rapid innovation, and vendor independence, contribute to cost-effective security practices in SCADA and ICS environments.

Q4: 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?

Standardized frameworks enhance communication and collaboration among stakeholders in the security domain within SCADA and ICS environments by providing a common language, reference point, and set of guidelines for security practices. The benefits they bring include:

1. Common Vocabulary: Standardized frameworks establish a common vocabulary and terminology for discussing security risks, controls, and

best practices. This common language facilitates effective communication among stakeholders, including IT professionals, engineers, management, and regulatory bodies.

2. Interoperability: Standardized frameworks promote interoperability among different systems, tools, and technologies used in SCADA and ICS environments. This interoperability simplifies integration efforts, streamlines information sharing, and enhances collaboration across organizational boundaries.
3. Consistency: Standardized frameworks ensure consistency in security practices and procedures across various departments, teams, and projects within an organization. This consistency fosters alignment with industry standards, regulatory requirements, and best practices, reducing the risk of miscommunication or misunderstandings.
4. Risk Management: Standardized frameworks provide structured methodologies for risk assessment, mitigation, and management. By following established frameworks, stakeholders can systematically identify, evaluate, and address security risks in a coordinated manner, leading to more effective risk management practices.
5. Compliance: Many standardized frameworks incorporate regulatory requirements and industry standards, helping organizations ensure compliance with legal and regulatory mandates. Compliance with recognized frameworks enhances trust and credibility with stakeholders, including customers, partners, and regulators.
6. Continuous Improvement: Standardized frameworks often include mechanisms for continuous improvement, such as regular updates, revisions, and feedback mechanisms. This emphasis on continuous improvement encourages stakeholders to stay abreast of evolving threats, technologies, and best practices, driving ongoing enhancement of security measures.

Standardized frameworks enhance communication and collaboration among stakeholders by establishing a common language, promoting interoperability, ensuring consistency, facilitating risk management, supporting compliance efforts, and fostering a culture of continuous improvement in the security domain within SCADA and ICS environments.

5.2 Automation Hypothesis

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

Q1: What are the specific risk assessment tasks that automation can significantly improve in terms of efficiency and accuracy within SCADA and ICS environments?

Automation has the potential to revolutionize risk assessment processes within SCADA and ICS environments by streamlining repetitive tasks, reducing human error, and improving overall efficiency and accuracy. Specific risk assessment tasks that automation can significantly improve include:

1. **Data Collection:** Automation can gather data from various sources, such as network logs, system configurations, and vulnerability databases, more efficiently than manual methods. This includes gathering information on system configurations, network traffic, and historical incident data.
2. **Risk Identification:** Automated tools can analyze collected data to identify potential vulnerabilities, threats, and risks to SCADA and ICS systems. This includes analyzing system configurations for misconfigurations, identifying outdated software versions, and flagging suspicious network activity.
3. **Risk Prioritization:** Automation can prioritize identified risks based on predefined criteria such as severity, likelihood, and potential impact on operations. This enables security teams to focus on addressing the most critical risks first, optimizing resource allocation and response efforts.

4. **Reporting and Documentation:** Automation can generate detailed reports and documentation summarizing the results of risk assessments, including identified vulnerabilities, recommended remediation actions, and compliance status. This facilitates communication with stakeholders and regulatory bodies, ensuring transparency and accountability.

Q2: How does automation of vulnerability scanning, continuous monitoring, and incident response plans contribute to enhancing the overall security posture in SCADA and ICS environments?

Automation plays a crucial role in enhancing the overall security posture of SCADA and ICS environments by enabling proactive identification and response to security threats and vulnerabilities. The automation of vulnerability scanning, continuous monitoring, and incident response plans contributes to this improvement in several ways:

1. **Timely Detection of Vulnerabilities:** Automated vulnerability scanning tools can regularly scan SCADA and ICS systems for known vulnerabilities, including software flaws, misconfigurations, and outdated patches. This enables security teams to identify and address vulnerabilities promptly before they can be exploited by malicious actors.
2. **Real-Time Threat Detection:** Continuous monitoring solutions can detect anomalous behavior and suspicious activities in SCADA and ICS networks in real-time. By analyzing network traffic, system logs, and user behavior patterns, these tools can identify potential security incidents and alert security teams to take immediate action.
3. **Rapid Incident Response:** Automation can streamline incident response processes by automating repetitive tasks such as alert triage, investigation, and containment. Incident response plans can be preconfigured with automated response actions, allowing for rapid

containment and mitigation of security incidents, minimizing their impact on operations.

4. **Adaptive Security Measures:** Automated systems can dynamically adjust security controls and configurations based on changing threat landscapes and operational requirements. This adaptive approach ensures that security measures remain effective and up-to-date in mitigating emerging threats and vulnerabilities.

5.3 Penetration Testing Hypothesis

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 crucial for SCADA and ICS systems because it allows organizations to systematically assess the security of their critical infrastructure. In the context of SCADA/ICS Network Assessment, penetration testing evaluates the security of network architecture and communication protocols, helping identify vulnerabilities that could be exploited through 5G connectivity. Similarly, the Wireless Security Assessment focuses on assessing the security of 5G connectivity for SCADA/ICS devices, crucial in identifying vulnerabilities in wireless communication protocols. Protocol and Communication Testing specifically targets potential vulnerabilities in communication protocols used in SCADA/ICS systems over 5G, ensuring the security of data transmission. Device and Controller Security Assessment helps identify firmware vulnerabilities and configuration weaknesses in SCADA/ICS devices and controllers connected through 5G, mitigating potential security risks. Human-Machine Interface (HMI) Testing ensures the security of HMI systems, addressing vulnerabilities that could be exploited via 5G. Additionally, evaluations of SCADA/ICS toolkits and desktop/server components further bolster security measures by identifying vulnerabilities in critical software components. Overall, penetration testing plays a pivotal role in identifying and mitigating vulnerabilities within SCADA and ICS systems, thereby enhancing their security posture against potential 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 based on critical infrastructure components and high-risk vulnerabilities enhances the effectiveness of security measures in SCADA and ICS environments by focusing resources on areas of greatest concern. By prioritizing SCADA/ICS Network Assessment, Wireless Security Assessment, Protocol and Communication Testing, Device, and Controller Security Assessment, HMI Testing, evaluations of SCADA/ICS toolkits, and desktop/server components, organizations can address vulnerabilities that pose the most significant risks. This targeted approach ensures that vulnerabilities affecting critical infrastructure components and high-risk areas are identified and remediated promptly, reducing the likelihood of successful cyber attacks. By aligning penetration testing efforts with organizational priorities and risk management objectives, organizations can strengthen the security posture of SCADA and ICS systems, thereby enhancing resilience against potential cyber threats and vulnerabilities.

5.4 Vulnerability Classification Hypothesis

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 based on multiple factors, such as authentication, communication protocols, firmware/software, configuration weaknesses, and wireless networks, offers a comprehensive understanding of potential risks in SCADA and ICS systems. This approach allows for a nuanced assessment of vulnerabilities, considering various aspects of system security.

For instance, authentication and authorization vulnerabilities (i) highlight weaknesses in user authentication mechanisms, crucial for preventing unauthorized access to critical systems. Communication protocol vulnerabilities (ii) assess weaknesses in data transfer protocols over 5G, essential for securing communication channels between SCADA/ICS components. Firmware and software vulnerabilities (iii) target weaknesses in the core software and firmware of devices and controllers, which, if exploited, could compromise system integrity. Configuration weaknesses (iv) focus on insecure configurations that may lead to unauthorized access or operational disruptions, addressing potential vulnerabilities stemming from misconfigurations.

Additionally, wireless network vulnerabilities (v) identify weaknesses in the 5G infrastructure supporting SCADA/ICS communication, crucial for safeguarding against wireless-based attacks. By categorizing vulnerabilities based on these factors, organizations gain a holistic view of potential risks, allowing for targeted mitigation efforts and resource allocation.

This comprehensive vulnerability classification approach is essential for SCADA and ICS security because it enables organizations to prioritize mitigation efforts effectively. By understanding the specific vulnerabilities present in different aspects of their systems, organizations can allocate resources based on the severity and likelihood of exploitation. This targeted approach ensures that critical vulnerabilities are addressed promptly, minimizing the risk of cyber threats and enhancing the overall security posture of SCADA and ICS environments connected via 5G.

6 CONCLUSIONS

This section summarizes the main achievements, recommendations, and future work.

The dissertation concludes with the introduction of a groundbreaking risk assessment methodology, ACSRA ICS (Automated Cyber Security Risk Assessment for Industrial Control Systems), designed to evaluate cybersecurity risks in 5G-connected SCADA and ICS environments. The increasing integration of 5G technology into critical infrastructures brings both opportunities and challenges, underscoring the need for a robust cybersecurity approach.

Emphasizing penetration testing as a proactive strategy for identifying vulnerabilities, the study proposed and tested the ACSRA methodology in an isolated 5G SA system. Evaluation of five prominent penetration testing methodologies highlighted their seamless integration into ACSRA, showcasing positive outcomes such as a comprehensive understanding of risks, identification of system-specific vulnerabilities, and enhancement of incident response plans. Additionally, exploration of automation possibilities for risk assessment tasks aimed at improving efficiency and accuracy.

The dissertation also categorized penetration tests, introduced Vulnerability Modes and Effects Analysis (VMEA), and prioritized tests specifically tailored for 5G-connected SCADA/ICS environments. Through an experimental setup, the study successfully demonstrated the identification of 5G-enabled ICS devices. In summary, ACSRA ICS offers a systematic and automated approach to cybersecurity in 5G-connected SCADA/ICS environments, bolstered by the integration of methodologies, risk assessment automation, and practical experimentation.

Furthermore, this research lays the foundation for further advancements in securing critical infrastructures with 5G technology. The approach presented is applicable to both large enterprises with private networks and SMEs with public networks. Moreover, the methodology and analysis can be extended to address various types of vulnerabilities. By customizing the testing software, specialized tools can be developed for deployment in smaller company settings, providing the functionalities outlined in the dissertation.

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.

6.1 Main Research Achievements

This study's aims were achieved by answering the research's main Hypothesis points.

Hypothesis 1 Integrated Approach Results
I proved that the integration of various cybersecurity standards and frameworks, including NIST SP800-115, SP800-82, OSSTMM, PTES, ISSAF, and OWASP, into the Automated Cyber Security Risk Assessment Methodology (ACSRA ICS) will lead to a more comprehensive understanding and management of risks in SCADA and ICS environments.

Hypothesis 2 Automation Approach results
Research has proven that automation can significantly improve the efficiency and accuracy of risk assessment tasks in SCADA and ICS environments by automating specific tasks such as device discovery, vulnerability scanning, continuous monitoring, threat intelligence integration, incident response plan validation, and documentation/reporting. By automating these tasks, organizations can ensure a comprehensive understanding of risks, timely identification of vulnerabilities, real-time monitoring of security posture, proactive threat detection, and validation of incident response plans, ultimately enhancing the overall security posture.

Moreover, organizations can achieve greater efficiency and accuracy in evaluating the security posture of SCADA and ICS environments, enabling more informed decision-making and proactive risk management.

Hypothesis 3 Penetration Testing Results

I verified that a testing procedure of penetration testing, a critical cybersecurity practice for SCADA and ICS systems, is essential for identifying vulnerabilities and weaknesses in a controlled manner. Through various classifications like SCADA/ICS Network Assessment, Wireless Security Assessment, Protocol and Communication Testing, Device and Controller Security Assessment, HMI Testing, and evaluations of SCADA/ICS toolkits and components, penetration testing ensures comprehensive security assessment. Prioritizing tests based on critical infrastructure components and high-risk vulnerabilities optimizes resource allocation, enabling organizations to address the most significant risks promptly. Ultimately, penetration testing enhances the security posture of SCADA and ICS systems, mitigating potential cyber threats and vulnerabilities.

Hypothesis 4 Vulnerability Classification Results

In my research, I have proven that classifying vulnerabilities in SCADA and ICS systems by authentication, communication protocols, firmware/software, configuration weaknesses, and wireless networks provides a comprehensive understanding of risks. This approach aids in prioritizing mitigation efforts effectively, minimizing the risk of cyber threats, and enhancing overall security posture. The Vulnerability Modes and Effects Analysis (VMEA) further assists in prioritizing vulnerabilities based on impact, likelihood, and overall risk, aiding strategic risk management decisions.

6.2 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.

6.3 Benefits of ACSRA ICS

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. By analyzing the detailed configuration of PLCs, ACSRA ICS can uncover vulnerabilities that generic tools might overlook, providing a more comprehensive security assessment.
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 cyber-attacks, 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.
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.

6.4 Limitations of ACSRA ICS

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.

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.

6.5 Cybersecurity Measures and Best Practices

To counteract the threat of malware attacks, this section outlines a range of cybersecurity measures and best practices that can enhance the security posture of SCADA systems. It explores the implementation of network segmentation, intrusion detection and prevention systems, access controls, and secure software development practices. Furthermore, it emphasizes the significance of regular system updates, employee training, and incident response planning to mitigate the impact of malware attacks and expedite recovery. This section outlines a range of strategies that organizations can employ to enhance the security posture of their SCADA systems, minimizing the vulnerabilities that malware can exploit:

Network Segmentation: Network segmentation is a fundamental security measure that involves dividing a SCADA network into smaller, isolated segments. By implementing logical or physical separation, organizations can limit the propagation of malware within the network.

Each segment can be assigned specific access controls, firewalls, and monitoring mechanisms, reducing the potential impact of successful malware infiltration[114].

Regular System Updates: Keeping SCADA systems up to date with the latest security patches and updates is crucial for minimizing vulnerabilities that malware exploits. Organizations should establish a systematic approach for regularly updating operating systems, firmware, applications, and security software. Patch management procedures should be implemented to ensure the timely installation of security updates, reducing the risk of known vulnerabilities being exploited by malware[115].

Incident Response Planning: Developing a robust incident response plan is essential for efficiently addressing and recovering from malware attacks. The plan should outline clear roles and responsibilities, define escalation procedures, and establish communication protocols. Regular testing and updating of the incident response plan can ensure its effectiveness when responding to malware incidents, minimizing downtime and mitigating potential damages[116].

Access Controls: Implementing strong access controls is vital to prevent unauthorized access to SCADA systems. Limit access to SCADA systems to authorized personnel only. Use strong authentication mechanisms such as two-factor authentication (2FA) or multi-factor authentication (MFA) to ensure that only authenticated users can access the system. In addition, Organizations should enforce strict user authentication practices, such as implementing complex passwords, utilizing multi-factor authentication, and regularly reviewing and revoking access privileges[117]. By limiting access to authorized personnel and regularly reviewing user permissions, the risk of malware infiltration can be significantly reduced.

Employee Training and Awareness: Employees play a critical role in maintaining the security of SCADA systems. Comprehensive training programs should be conducted to educate employees about malware threats, social engineering tactics, and best practices for secure system usage. Regular awareness campaigns can help employees identify and report potential security incidents, thereby minimizing the impact of malware attacks[118].

Secure Software Development Practices: Integrating secure software development practices into the SCADA system lifecycle is critical. Organizations should adhere to secure coding guidelines, conduct regular security code reviews, and perform robust vulnerability testing during the development and maintenance phases. By proactively addressing security flaws and eliminating vulnerabilities, organizations can reduce the likelihood of successful malware attacks[119].

Intrusion Detection and Prevention Systems (IDPS): Deploying IDPS solutions is crucial for detecting and mitigating malware attacks on SCADA systems. These systems monitor network traffic, analyze patterns, and detect suspicious activities that may indicate the presence of malware. Additionally, IDPS can proactively prevent malicious actions by blocking or alerting administrators to potential threats, helping organizations respond swiftly to mitigate the impact of malware attacks[120].

Implementing effective cybersecurity measures and adhering to best practices is imperative for safeguarding SCADA systems against the vulnerabilities exploited by malware. By incorporating network segmentation, deploying IDPS, enforcing access controls, following secure software development practices, maintaining regular system updates, providing comprehensive employee training, and establishing a well-defined incident response plan, organizations can significantly enhance the security posture of their SCADA systems. Proactive measures and continuous improvement in cybersecurity practices will enable organizations to defend against malware threats, ensuring the integrity, availability, and confidentiality of critical infrastructure.

6.6 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.

6.7 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.

6.8 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.

7 Ph.D. Candidate List of Publications

This breakdown showcases a variety of scholarly contributions across conferences, publications, and journals, covering diverse topics related to cybersecurity, infrastructure protection, digital education, and technological advancements. To elaborate further, out of the 18 papers published, Two appeared in a Web of Science (WOS) and Scopus-indexed international journal, six in Scopus-indexed IEEE conference proceedings, three in Hungarian journals, and one in an online journal. The remaining were IEEE conference papers. Moreover, I contributed to 15 conferences, Moreover, the following papers related to the Hypothesis points.

Scientific Publications Related to the Thesis Points

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.

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.

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

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)

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

ACSRA ICS: Automated Cyber Security Risk Assessment Methodology for Industrial Control Systems, Accepted to Acta Hungarica Polyticnica.

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

Table 9 List of publications (P: Publication C: Conference J: Journal A: Accepted)

	Publication
P1 C1	5G Evolution and Supply Chain Security in MENA Region: Challenges and Opportunities IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics: SAMI 2024 Haya Altaleb, Fregan Beatrix, Fatmir Azemi, Rajnai Zoltán “5G Evolution and Supply Chain Security in MENA Region: Challenges and Opportunities”,IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics : SAMI 2024,pp. 149-156. , 8 p.
P2 C2	Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures IEEE 21st International Symposium on Intelligent Systems and Informatics: SISY 2023. 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.
P3 C3	Addressing Cybersecurity Challenges in 5G-enabled IoT and Critical Infrastructures: A Comprehensive Overview IEEE 27th International Conference on Intelligent Engineering Systems 2023 (INES 2023) H. Altaleb and R. Zoltán, "Addressing Cybersecurity Challenges in 5G-enabled IoT and Critical Infrastructures: A Comprehensive Overview," 2023 IEEE 27th International Conference on Intelligent Engineering Systems (INES), Nairobi, Kenya, 2023, pp. 000131-000136, doi: 10.1109/INES59282.2023.10297774.
P4 C4 J1	Digital Education: Governments' Strategies, Teaching Tools in the European Union and a Case Study of Digital Transformation in Budapest Smart Sustainable and Safe Cities Conference 2022 INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS H. Altaleb, M. Shatnawi i Z. Rajnai, "Digital Education: Governments’ Strategies, Teaching Tools in the European Union and a Case Study of Digital Transformation in Budapest", Interdisciplinary Description of Complex Systems, vol.21, br. 2, str. 148-160, 2023. [Online]. https://doi.org/10.7906/indecs.21.2.3
P5 C5	Decentralized autonomous organizations review, importance, and applications IEEE 26th International Conference on Intelligent Engineering Systems (INES 2022) H. Altaleb and R. Zoltán, "Decentralized autonomous organizations review, importance, and applications," *2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES)*, Georgioupolis Chania, Greece, 2022, pp. 000121-000126, doi: 10.1109/INES56734.2022.9922656.
P6 C6	The Digital Revolution with NESAS Assessment and Evaluation IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems ICCC 2022 M. Shatnawi, H. Altaleb and R. Zoltán, "The Digital Revolution with NESAS Assessment and Evaluation," *2022 IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC)*, Reykjavík, Iceland, 2022, pp. 000099-000104, doi: 10.1109/ICCC202255925.2022.9922821.
P7 C7	A BRIEF OVERVIEW OF SYSTEMS RELIABILITY

	Publication
J2	ICCECIP 2021 3rd International Conference on Central European Critical Instrastructure Protection CYBER SECURITY REVIEW 2021 Altaleb Haya, Rajnai Zoltán,”A BRIEF OVERVIEW OF SYSTEMS RELIABILITY”CYBER SECURITY REVIEW 2021 : 05 p. online , 6 p. (2021)
P8 C8	ASSESSMENT OF THE RISK MANAGEMENT FOR VARIOUS TYPES OF DISASTERS: IMPACT AND SUSTAINABILITY 12th ICEEE–2021 International Conference “Global Environmental Development & Sustainability: Research, Engineering & Management” : ICEEE 2021 Malak Shatnawi, Haya Altaleb, Rajnai Zoltán, ASSESSMENT OF THE RISK MANAGEMENT FOR VARIOUS TYPES OF DISASTERS: IMPACT AND SUSTAINABILITY, 12th ICEEE–2021 International Conference “Global Environmental Development & Sustainability: Research, Engineering & Management” : ICEEE 2021, Budapest, Magyarország : Óbudai Egyetem (2021) pp. 370-378. , 9 p.
P9 C9 J3	Risk Assessments Methods and cyber vulnerabilities in scada systems ICCECIP 2020 2nd International Conference on Central European Critical Infrastructure Protection CYBER SECURITY REVIEW 2020 NATIONAL SECURITY REVIEW: PERIODICAL OF THE MILITARY NATIONAL SECURITY SERVICE 2021 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)
P10 C10 J4	Electric Vehicle Charging Infrastructure and Charging Technologies ICCECIP 2019 1st International Conference on Central European Critical Infrastructure Protection HADITECHNIKA Altaleb, Haya and Rajnai, Zoltán (2020) Electric Vehicle Charging Infrastructure and Charging Technologies. HADITECHNIKA, 54 (4). pp. 8-12. ISSN 0230-6891doi.org/10.23713/HT.54.4.03
P11 C11	Application of lean techniques within SMEs in Kosovo Manufacturing Industry and benefits of Implementation 9thAnnual International ConferenceInternational Conference Mechatronics, System EngineeringAnd Robotics & Informations System And Engineering
P12 C12	The Risk of Using Biometrics FIKUSZ 2018 - Symposium for Young Researchers Proceedings : Celebration of Hungarian Science 2018
P13 J5	Security services in 5G wireless networks BIZTONSÁGTUDOMÁNYI SZEMLE Haya, Altaleb, “Biztonsági szolgáltatások az 5G vezeték nélküli hálózatokban” BIZTONSÁGTUDOMÁNYI SZEMLE 4 : 2 - Rajnai 60 különszám pp. 25-33. , 9 p. (2022).
P14	Enhancing Cybersecurity in Industrial Control Systems through GRC Framework: Principles, Regulations, and Risk

	Publication
C13 J6	Assessment ICCECIP 2022 4th International Conference on Central European Critical Infrastructure Protection Critical Infrastructure Protection in the light of the armed conflicts March 2024 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.
P15 C14	A Comprehensive Analysis and Solutions for Enhancing SCADA Systems Security in Critical Infrastructures. IEEE 11th International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC 2024) to be organized on April 4-6, 2024 in Hanoi, Vietnam. 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
P16 C15	Fortifying Decentralized Governance: Introducing Decentralized Autonomous Verification (DAVe) for Decentralized Autonomous Organization (DAOs) Security IEEE 28th International Conference on Intelligent Engineering Systems (INES 2024)
A1 J7	ACSRA ICS: Automated Cyber Security Risk Assessment Methodology for Industrial Control Systems Accepted to Acta Hungarica Polyticnica
A2 J8	Optimising Production Processes through 5G-Enabled Job Shop Scheduling: A Case Study Accepted in Acta Hungarica Polyticnica

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. 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.

[6] A. H. Rajnai Zoltan, “Risk assessments Methods and Cyber Vulnerabilities in SCADA systems,” *Natl. Secur. Rev. Period. Mil. Natl. Secur. Serv. 2021*, pp. 181–194, 2021.

[7] J. Jaskolka and J. Villasenor, “An approach for identifying and analyzing implicit interactions in distributed systems,” *IEEE Trans. Reliab.*, vol. 66, no. 2, pp. 529–546, Jun. 2017, doi: 10.1109/TR.2017.2665164.

[8] K. Stouffer, J. Falco, and K. Scarfone, “GUIDE to industrial control systems (ICS) security,” *Stuxnet Comput. Worm Ind. Control Syst. Secur.*, pp. 11–158, 2011.

[9] J. Gantz, “The Embedded Internet: Methodology and Findings,” 2009.

[10] T. S. Tamir *et al.*, “Developing SCADA Systems to Monitor and Control Liquid

and Detergent Factories," *IEEE Int. Conf. Autom. Sci. Eng.*, vol. 2020-Augus, pp. 691–696, 2020, doi: 10.1109/CASE48305.2020.9217002.

[11] T. Sauter and C. Schwaiger, "Achievement of secure Internet access to fieldbus systems," *Microprocess. Microsyst.*, vol. 26, no. 7, pp. 331–339, Sep. 2002, doi: 10.1016/S0141-9331(02)00044-3.

[12] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, Oct. 2006, doi: 10.1016/J.COSE.2006.03.001.

[13] D. Li, H. Guo, J. Zhou, L. Zhou, and J. W. Wong, "SCADAWall: A CPI-enabled firewall model for SCADA security," *Comput. Secur.*, vol. 80, pp. 134–154, Jan. 2019, doi: 10.1016/J.COSE.2018.10.002.

[14] J. Nivethan and M. Papa, "On the use of open-source firewalls in ICS/SCADA systems," *http://dx.doi.org/10.1080/19393555.2016.1172283*, vol. 25, no. 1–3, pp. 83–93, Apr. 2016, doi: 10.1080/19393555.2016.1172283.

[15] M. J. A. Baig, M. T. Iqbal, M. Jamil, and J. Khan, "A Low-Cost, Open-Source Peer-to-Peer Energy Trading System for a Remote Community Using the Internet-of-Things, Blockchain, and Hypertext Transfer Protocol," *Energies 2022, Vol. 15, Page 4862*, vol. 15, no. 13, p. 4862, Jul. 2022, doi: 10.3390/EN15134862.

[16] E. A. Smith, M. B. Mulder, and K. Hill, "Controversies in the evolutionary social sciences: A guide for the perplexed," *Trends Ecol. Evol.*, vol. 16, no. 3, pp. 128–135, 2001, doi: 10.1016/S0169-5347(00)02077-2.

[17] I. Alsharif and A. Khelifi, "Exploring the Opportunities and Challenges of Open Source Software and Its Economic Impact on the Cybersecurity Market," *Adv. Sci. Technol. Innov.*, pp. 115–127, 2019, doi: 10.1007/978-3-030-01659-3_16/COVER.

[18] A. Ujvarosi, "EVOLUTION OF SCADA SYSTEMS," *Bull. Transilv. Univ. Braşov •*, vol. 9, no. 58, 2016.

[19] N. Tariq, M. Asim, and A. Khan, "ScienceDirect Securing SCADA-based Critical Infrastructures: Challenges and Open Issues," *Procedia Comput. Sci.*,

vol. 00, pp. 0–000, 2018, doi: 10.1016/j.procs.2019.08.086.

[20] J. Peterson, M. Haney, and R. A. Borrelli, “An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants,” *Nucl. Eng. Des.*, vol. 346, pp. 75–84, 2019, doi: 10.1016/j.nucengdes.2019.02.025.

[21] H. Altaleb and Z. Rajnai, “Risk assessments Methods and Cyber Vulnerabilities in SCADA systems,” *Natl. Secur. Rev. Period. Mil. Natl. Secur. Serv.*, vol. 2, pp. 181–194, 2021.

[22] T. Baker *et al.*, “A secure fog-based platform for SCADA-based IoT critical infrastructure,” *Softw. - Pract. Exp.*, vol. 50, no. 5, pp. 503–518, May 2020, doi: 10.1002/SPE.2688.

[23] M. Thankappan, H. Rifà-Pous, and C. Garrigues, “Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review,” *Expert Syst. Appl.*, vol. 210, 2022, doi: 10.1016/j.eswa.2022.118401.

[24] N. E. Hastings and P. A. McLean, “TCP/IP spoofing fundamentals,” *Conf. Proc. - Int. Phoenix Conf. Comput. Commun.*, pp. 218–224, 1996, doi: 10.1109/pccc.1996.493637.

[25] S. Mcclure, J. Scambray, and G. Kurtz, “Hacking Exposed 7: Network Security Secrets and Solutions,” 2012.

[26] F. Ali, “IP spoofing,” *Internet Protoc. J.*, vol. 10, no. 4, pp. 1–9, 2007.

[27] T. H. Kim and D. Reeves, “A survey of domain name system vulnerabilities and attacks,” *J. Surveillance, Secur. Saf.*, 2020, doi: 10.20517/jsss.2020.14.

[28] Z. Shah and S. Cosgrove, “Mitigating arp cache poisoning attack in software-defined networking (sdn): A survey,” *Electron.*, vol. 8, no. 10, 2019, doi: 10.3390/electronics8101095.

[29] A. A. Galal, A. Z. Ghalwash, and M. Nasr, “A New Approach for Detecting and Mitigating Address Resolution Protocol (ARP) Poisoning,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 6, pp. 377–382, 2022, doi: 10.14569/IJACSA.2022.0130647.

[30] S. Hijazi and M. S. Obaidat, “Address resolution protocol spoofing attacks and

security approaches: A survey," *Secur. Priv.*, p. e49, 2018, doi: 10.1002/spy2.49.

[31] A. R. Chordiya, S. Majumder, and A. Y. Javaid, "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools," *IEEE Int. Conf. Electro Inf. Technol.*, vol. 2018-May, pp. 438–443, 2018, doi: 10.1109/EIT.2018.8500144.

[32] A. A. Mughal, "View of The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection," *18-International J. Intell. Autom. Comput.*, vol. 1, no. 1, 2018.

[33] C. Kaura, N. Sindhwani, and A. Chaudhary, "Analysing the Impact of Cyber-Threat to ICS and SCADA Systems," *2022 Int. Mob. Embed. Technol. Conf. MECON 2022*, pp. 466–470, 2022, doi: 10.1109/MECON53876.2022.9752425.

[34] A. Carcano, I. N. Fovino, M. Masera, and A. Trombetta, "Scada malware, a Proof of concept," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5508 LNCS, pp. 211–222, 2009, doi: 10.1007/978-3-642-03552-4_19/COVER.

[35] S. Collins and S. McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications," *http://dx.doi.org/10.1080/18335330.2012.653198*, vol. 7, no. 1, pp. 80–91, Apr. 2012, doi: 10.1080/18335330.2012.653198.

[36] T. Alladi, V. Chamola, and S. Zeadally, "Industrial Control Systems: Cyberattack trends and countermeasures," *Comput. Commun.*, vol. 155, pp. 1–8, Apr. 2020, doi: 10.1016/J.COMCOM.2020.03.007.

[37] K. E. Hemsley, R. E. Fisher, Kevin E. Hemsley;, and Dr. Ronald E. Fisher, "History of Industrial Control System Cyber Incidents," *INL/CON-18-44411-Revision-2*, no. December, pp. 1–37, Dec. 2018, doi: 10.2172/1505628.

[38] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations," *IEEE Syst. J.*, vol. 17, no. 4, pp. 6695–6709, 2023, doi: 10.1109/JSYST.2023.3305757.

[39] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *Int. J. Crit. Infrastruct. Prot.*, vol. 8, pp. 53–66,

Jan. 2015, doi: 10.1016/J.IJCIP.2014.12.002.

[40] A. Haya and Z. Rajnai, “Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures,” in *SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics*, IEEE Hungary Section, 2023, pp. 625–629.

[41] Y. Mo *et al.*, “Cyber-physical security of a smart grid infrastructure,” *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, 2012, doi: 10.1109/JPROC.2011.2161428.

[42] I. N. Fovino, M. Masera, L. Guidi, and G. Carpi, “An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants,” *3rd Int. Conf. Hum. Syst. Interact. HSI’2010 - Conf. Proc.*, pp. 679–686, 2010, doi: 10.1109/HSI.2010.5514494.

[43] B. Genge and C. Siaterlis, “Physical process resilience-aware network design for SCADA systems,” *Comput. Electr. Eng.*, vol. 40, no. 1, pp. 142–157, Jan. 2014, doi: 10.1016/J.COMPELECENG.2013.11.018.

[44] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, “SCADA security in the light of Cyber-Warfare,” *Comput. Secur.*, vol. 31, no. 4, pp. 418–436, Jun. 2012, doi: 10.1016/J.COSE.2012.02.009.

[45] 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.

[46] E. Tapia, L. Sastoque-Pinilla, U. Lopez-Novoa, I. Bediaga, and N. López de Lacalle, “Assessing Industrial Communication Protocols to Bridge the Gap between Machine Tools and Software Monitoring,” *Sensors*, vol. 23, no. 12, 2023, doi: 10.3390/s23125694.

[47] W. Staszewski, A. Jabłoński, and K. Dziedziech, “A survey of communication protocols in modern embedded condition monitoring systems,” *Diagnostyka*, vol. 19, no. 2, pp. 53–62, 2018, doi: 10.29354/diag/86409.

[48] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, “DNPSec: Distributed network protocol version 3 (DNP3) security framework,” *Adv. Comput.*

Information, Syst. Sci. Eng. - Proc. IETA 2005, TeNe 2005, EIAE 2005, pp. 227–234, 2006, doi: 10.1007/1-4020-5261-8_36.

[49] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, “A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020, doi: 10.1109/COMST.2020.2987688.

[50] J. Sottile, “Alpha Foundation for the Improvement of Mine Safety and Health,” *Alpha-Foundation.Org*.

[51] PROFIBUS Nutzerorganisation e. V. (PNO), “PROFIBUS System Description,” p. 30, 2010.

[52] National Instruments, “The Basics of CANopen,” 2022. [Online]. Available: https://www.ni.com/fi-fi/innovations/white-papers/13/the-basics-of-canopen.html.

[53] J. Feld, “Realtime communication in profinet V2 and V3 designed for industrial purposes,” *IFAC Proc. Vol.*, vol. 36, no. 13, pp. 285–289, 2003, doi: 10.1016/S1474-6670(17)32496-5.

[54] J. Muñoz, T. Chang, X. Vilajosana, and T. Watteyne, “Evaluation of IEEE802.15.4g for environmental observations,” *Sensors (Switzerland)*, vol. 18, no. 10, 2018, doi: 10.3390/s18103468.

[55] C. Henning, “A Beginner’s Guide to PROFINET - PI North America Blog,” 2015.

[56] Elprocus, “What is ProfiNet : Architecture, Working, Types & Its Applications,” p. 1.

[57] A. L. Dias, G. S. Sestito, A. C. Turcato, and D. Brandao, “Panorama, challenges and opportunities in PROFINET protocol research,” *2018 13th IEEE Int. Conf. Ind. Appl. INDUSCON 2018 - Proc.*, pp. 186–193, 2019, doi: 10.1109/INDUSCON.2018.8627173.

[58] J. Feld, “Profinet - Scalable factory communication for all applications,” *IEEE Int. Work. Fact. Commun. Syst. - Proceedings, WFCS*, pp. 33–38, 2004, doi: 10.1109/wfcs.2004.1377673.

[59] M. E. Whitman and H. J. Mattord, “Principles of Information Security,” *Cengage Learning*, 2018. [Online]. Available: www.cengage.com. [Accessed: 29-Dec-2022].

[60] A. H. Rajnai Zoltan, “Risk assessments Methods and Cyber Vulnerabilities in SCADA systems,” *National Security Review: Periodical of the Military National Security Service 2021*, 2021. [Online]. Available: https://www.researchgate.net/publication/358705563_Risk_assessments_Methods_and_Cyber_Vulnerabilities_in_SCADA_systems. [Accessed: 24-Nov-2022].

[61] S. Kaplan and B. J. Garrick, “On The Quantitative Definition of Risk,” *Risk Anal.*, vol. 1, no. 1, pp. 11–27, 1981, doi: 10.1111/j.1539-6924.1981.tb01350.x.

[62] Yazar Zeki, “A qualitative risk analysis and management tool – CRAMM,” *SANS Inst. Inf. Secur. Read. Room*, pp. 1–13., 2021.

[63] B. Karabacak and I. Sogukpinar, “ISRAM: Information security risk analysis method,” *Comput. Secur.*, vol. 24, no. 2, pp. 147–159, Mar. 2005, doi: 10.1016/j.cose.2004.07.004.

[64] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, “Introduction to the OCTAVE Approach,” 2003.

[65] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/J.COSE.2013.04.004.

[66] J.-E. Holmberg, “Defense-in-Depth,” *Handb. Saf. Princ.*, pp. 42–62, Jan. 2018, doi: 10.1002/9781119443070.CH4.

[67] R. Lippmann *et al.*, “Validating and restoring defense in depth using attack graphs,” *Proc. - IEEE Mil. Commun. Conf. MILCOM*, 2006, doi: 10.1109/MILCOM.2006.302434.

[68] M. Sanders and C. Yue, “Automated least privileges in cloud-based web services,” vol. 6, pp. 1–6, 2017, doi: 10.1145/3132465.3132470.

[69] R. T. Simon and M. E. Zurko, “Separation of duty in role-based environments,” *Proc. - IEEE Comput. Secur. Found. Symp.*, pp. 183–194, 1997, doi: 10.1109/CSFW.1997.596811.

[70] C. Barnes *et al.*, “A Security Primer,” *Hackproofing Your Wirel. Netw.*, pp. 75–124, Jan. 2002, doi: 10.1016/b978-192899459-6/50022-8.

[71] I. Uwaoma and P. A. Ordu, “THE IMPACT OF INTERNAL CONTROLS ON FINANCIAL MANAGEMENT: A CASE OF PRODUCTION COMPANIES IN NIGERIA,” *Int. J. Econ. Commer. Manag. United Kingdom*, vol. III, 2015.

[72] “Separation of Duties within Information Systems - Seton Hall University.” [Online]. Available: https://www.shu.edu/technology/separation-duties-information-systems.cfm. [Accessed: 04-Jan-2023].

[73] R. D. Behn, “The new public management paradigm and the search for democratic accountability,” *Int. Public Manag. J.*, vol. 1, no. 2, pp. 131–164, Jan. 1998, doi: 10.1016/S1096-7494(99)80088-9.

[74] R. Fekolkin, “A Full Disk Encryption: AAA and CIA principles,” 2014.

[75] L. Rosa *et al.*, “Intrusion and anomaly detection for the next-generation of industrial automation and control systems,” *Futur. Gener. Comput. Syst.*, vol. 119, pp. 50–67, Jun. 2021, doi: 10.1016/J.FUTURE.2021.01.033.

[76] B. Schneier and Mudge, “Cryptanalysis of Microsoft’s Point-to-Point Tunneling Protocol (PPTP),” *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 132–141, 1998, doi: 10.1145/288090.288119.

[77] P. Michelberger and Á. Kemendi, “DATA, INFORMATION AND IT SECURITY - SOFTWARE SUPPORT FOR SECURITY ACTIVITIES,” *Probl. Manag. 21st Century*, vol. 15, no. 2, pp. 108–124, Dec. 2020, doi: 10.33225/pmc/20.15.108.

[78] A. M. Kjaer, *Governance*. polity press, 2023.

[79] M. Chauhan and S. Shiaeles, “An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions,” *Network*, vol. 3, no. 3, pp. 422–450, 2023, doi: 10.3390/network3030018.

[80] M. Chuprunov, “Legal Requirements in ICS Compliance,” *Audit. GRC Autom. SAP*, pp. 3–18, 2013, doi: 10.1007/978-3-642-35302-4_1.

[81] S. Maesschalck, V. Giotsas, B. Green, and N. Race, “Don’t get stung, cover your ICS in honey: How do honeypots fit within industrial control system security,”

Comput. Secur., vol. 114, p. 102598, Mar. 2022, doi: 10.1016/J.COSE.2021.102598.

[82] (COSO) “Comitttee of Sponsoring Organizations of the Treadway Commission,” “Enterprise risk management -- Integrated framework,” 2004.

[83] M. Talabis and J. Martin, “Information Security Risk Assessment Toolkit,” *Inf. Secur. Risk Assess. Toolkit Pract. Assessments through Data Collect. Data Anal.*, pp. 1–258, 2012, doi: 10.1016/C2010-0-69579-4.

[84] K. L. Henebry and G. E. Rejda, “Principles of Risk Management and Insurance,” *J. Risk Insur.*, vol. 62, no. 4, p. 797, 1995, doi: 10.2307/253600.

[85] J. Moteff, “Risk Management and Critical Infrastructure Protection : Assessing , Integrating , and Managing Threats , Vulnerabilities and Consequences,” *Sci. Technol.*, pp. 1–29, 2005.

[86] R. Awati and B. Cole, “North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP),” pp. 9–11, 2022.

[87] “MITIGATING ICT SUPPLY CHAIN RISKS WITH QUALIFIED BIDDER AND MANUFACTURER LISTS,” *CYBERSECURITY Infrastruct. Secur. AGENCY*, 2021.

[88] A. Kim, J. Oh, K. Kwon, and K. Lee, “Consider the Consequences: A Risk Assessment Approach for Industrial Control Systems,” *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/3455647.

[89] S. McLaughlin *et al.*, “The Cybersecurity Landscape in Industrial Control Systems,” *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016, doi: 10.1109/JPROC.2015.2512235.

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

[91] 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.

[92] “Defense Against Threats,” 2024. [Online]. Available: https://www.moxa.com/en/spotlight/portfolio/industrial-network-

security/industrial-cybersecurity#networktreatsdefense. [Accessed: 29-Jan-2024].

[93] 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.

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

[95] 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.

[96] 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.

[97] 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].

[98] Joint Task Force, “Security and Privacy Controlsfor Information Systems and Organizations,” *NIST Spec. Publ.*, vol. 1, no. 5, p. 465, 2020.

[99] 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.

[100] ISECOM, “Manual The Open Source Security Testing Methodology,” *Recuper. el 06 Mayo 2020* , 2020.

[101] 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.

[102] PTES Team, “The Penetration Testing Execution Standard (PTES),” p. 227, 2022.

[103] 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.

[104] 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.

[105] 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.

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

[107] S. Gautam, “What is Wireshark? Applications, Features & How It Works,” *knowledgehut*, 2023. [Online]. Available: https://www.knowledgehut.com/blog/security/what-is-wireshark. [Accessed: 06-Feb-2024].

[108] K. Alexis Fidele, Suryono, and W. Amien Syafei, “Denial of Service (DoS) attack identification and analyse using sniffing technique in the network environment,” *E3S Web Conf.*, vol. 202, 2020, doi: 10.1051/e3sconf/202020215003.

[109] B. Dodiya and U. K. Singh, “Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise,” *Int. J. Comput. Appl.*, vol. 183, no. 53, pp. 1–6, 2022, doi: 10.5120/ijca2022921876.

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

[111] S. Ag, *Learn-/Training Textbook S7-1200 from Version V14 SP1*. 2017.

[112] 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.

[113] 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.

[114] E. Knapp, "Industrial network security: Securing critical infrastructure networks for smart grid, scada, and other industrial control systems," *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2011. [Online]. Available: https://books.google.pt/books?hl=pt-PT&lr=&id=V2RzAwAAQBAJ&oi=fnd&pg=PP1&dq=scada+layer+explained&ots=54zgWbnzjk&sig=ze-UeGq5VCtuSFRZp2GInu01_C0&redir_esc=y#v=onepage&q&f=false. [Accessed: 29-May-2023].

[115] J. Reeser, T. Jankowski, and G. M. Kemper, "Maintaining HMI and SCADA systems through computer virtualization," *IEEE Trans. Ind. Appl.*, vol. 51, no. 3, pp. 2558–2564, May 2015, doi: 10.1109/TIA.2014.2384132.

[116] P. Eden *et al.*, "Forensic Readiness for SCADA/ICS Incident Response," *scienceopen.com*, Aug. 2016, doi: 10.14236/ewic/ics2016.16.

[117] A. Kumar, B. Bhushan, A. Malik, and R. Kumar, "Protocols, Solutions, and Testbeds for Cyber-Attack Prevention in Industrial SCADA Systems," *Stud. Big Data*, vol. 99, pp. 355–380, 2021, doi: 10.1007/978-981-16-6210-2_17.

[118] F. Abu-Amara, R. Almansoori, S. Alharbi, M. Alharbi, and A. Alshehhi, "A novel SETA-based gamification framework to raise cybersecurity awareness," *Int. J. Inf. Technol.*, vol. 13, no. 6, pp. 2371–2380, Dec. 2021, doi: 10.1007/S41870-021-00760-5/METRICS.

[119] D. Upadhyay and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations," *Comput. Secur.*, vol. 89, p. 101666, Feb. 2020, doi: 10.1016/J.COSE.2019.101666.

[120] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems,"

IEEE Access, vol. 7, pp. 46595–46620, 2019, doi: 10.1109/ACCESS.2019.2909807.