International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

CYBERSECURITY VULNERABILITIES AND RISK MITIGATION IN TIER-1 SCADA SYSTEMS: A COMPREHENSIVE ASSESSMENT OF THREATS AND SOLUTIONS

DANDU RAMESH[1], Dr. SUNIL BHUTADA[2]
[1]Research Scholar, [2]Dept of Computer Science Engineering , P.K. university, Shivpuri (MP),
drameshceh@gmail.com
[2]Dept of Computer Science Engineering, PK University, Shivpuri(MP),
sunilbhutada@gmail.com

ABSTRACT:
This study seeks to analyse the security threats of Tier-1 SCADA systems in enterprise networks. Nevertheless, since SCADA systems are used to manage important facilities and services, they require integration with IT networks, which in turn exposes them to a great number of risks. The study further reveals that there are several weaknesses with the SCADA components including input validation weakness, buffer overflow, hard-coded credentials, and archaic encryption. It also ventures into poor patch management practices as well as their effects on operational security. From this analysis of these risks, the research presents the following possible remedies like enhancing the depth of encryption, providing the dynamic nature in firewall rules, and granting autonomy to patching. The work employs the standard stages of cyber risk assessment including identification, analysis, risk prioritization, risk control, and ongoing risk monitoring while providing a step-by-step methodology to improve the protection of SCADA systems. The gains achieved depict the fact that, in the case of enhancing security to specific assets, it is possible to enhance the system defences against current and future threats. This work enriches the contemporary knowledge base on SCADA system security threats and offers original, context-aware recommendations for enhancing protection.

Keywords: ***SCADA SYSTEMS, CYBERSECURITY VULNERABILITIES ,RISK MITIGATION, PATCH MANAGEMENT, CRITICAL INFRASTRUCTURE SECURITY***

Received: 12-12-2024 Accepted: 18-01-2025 Published: 25-01-2025

1. INTRODUCTION

1.1 Overview of SCADA Systems in Critical Infrastructure

SCADA systems play a vital role in managing the critical sectors of infrastructure such as ENERGY SECTOR, WATER RESOURCE AND MANAGEMENT, TRANSPORTATION AND MANUFACTURING[1]. Such system are aimed at sensing and managing industrial processes meant for data collection and plant automation across different regions. A SCADA system largely comprises of components that include, Hardware and software which are sub- divided into sensors, controllers, and Human Machine Interface (HMI)'s that are used to monitor and control a variety of processes and utility services effectively as well as safely. In power plant, for instance, the SCADA systems controls the flow and distribution of power in power plants, in water treatment plant, SCADA systems controls the flow and purification of water, water distribution, among others, in manufacturing companies, SCADA controls production processes and quality assurance, among others. Sophisticated integrated systems are at the base of our national stability and security, and their reliable working is critical. However, the continuous integration of SCADA systems to corporate networks as well as the internet has called for new forms of vulnerability to attacks[2].

1.2 Importance of Cybersecurity in SCADA Systems

With the growth in the integration of SCADA systems in enterprise IT infrastructures, the consequences associated with it cyber security threats are enormous. It is Cybersecurity not only in SCADA systems and about technicalities, but also a matter of nations' security. An attacker when he gains unauthorized access to

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

a SCADA system can result to unfavourable outcomes such as the internet of specific services, damage to physical assets, environmental pollution, and potential hazards to the lives of the people[3]. SCADA environments differ from traditional IT systems by their requirements for availability and processing of data in real time, these features present difficulties to traditional models of security implementation. For instance, the temporary isolation of a SCADA system for regular servicing or upgrades spawns larger monetary or safety consequences. Consequently, to safeguard the security of the SCADA systems, appropriate measures have to be taken into consideration regarding such specific features of these systems' operation while addressing internal and external threats[4]. Recent advancements in SCADA systems revealed that there has been a constant increase in cases of cyberattacks on critical infrastructural systems subsequently emphasizing the need to improve the level of security in SCADA systems.

1.3 Research Scope

It is possible that filling these gaps would improve the understanding of the ways to improve the Tier1 SCADA security and increase its resistance to existing and newly emerging threats.

- Limited Focus on Tier1 SCADA Systems[5]: There is an overall awareness or concern about the security threats that exist in SCADA systems but such research focused on the Tier1 SCADA systems in the large-scale enterprises is missing. This gap suggests that current literature may not necessarily capture the nature of security risks and threats relating to Tier1 systems and their importance to infrastructure protection.
- Component Specific Vulnerabilities[6]: While there is information about SCADA system risks, there is no study of risks associated with different aspects of Tier1 SCADA components. There is a lack of similar analysis performed at a micro level with regards to individual components and their particular security risks that might be helpful for the understanding of how each component contributes to the general level of risk in the system.
- Development Phases and Risk Assessment Models[7]: The concept of integrating the phases of development in cyber risk assessment and model in case of SCADA systems is limited. Therefore, there is a need to conduct research that considers not only all these phases but also make sure that models that finally come up have been modified to suit SCADA systems in that they address their security issues appropriately.

1.4 Research Objectives

The formulated Research Objectives for this research paper are

As such, the following formulated Research Objectives for this research paper are as follows:

1. INVESTIGATE CYBERSECURITY VULNERABILITIES AND THREATS IN TIER-1 SCADA SYSTEMS:

This objective aims at analysing the concrete cybersecurity threats and risks relating to Tier-1 SCADA solutions in large organisations. The objective is to enhance the understanding of the varied threats for these significant systems.

2. IDENTIFY SCADA SYSTEM COMPONENTS AND THEIR ASSOCIATED SECURITY RISKS:

This objective of this research focuses on the analysis of various SCADA elements, with a view of establishing the overall security risks/ threats associated with each element. The objective is to ensure that the study gives out of the effects of these components on the system security.

3. **EXPLORE DEVELOPMENT PHASES IN CYBER RISK ASSESSMENT AND MODEL DEVELOPMENT**:

This objective aims to scrutinise and assess various phases that may be in cyber risk assessment and model development process. In this work, emphasis shall be on identifying how these phases can be leveraged in improving the security of SCADA systems where emphasis will be on how risk assessment models can be properly developed to suit this sector.

2. SCADA SYSTEM ARCHITECTURE AND OPERATIONS

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

2.1 Components of a Tier1 SCADA System

A Tier1 SCADA system represents the highest level of complexity and criticality within an organization's infrastructure, often responsible for managing essential operations across vast and geographically dispersed sites. The architecture of a Tier1 SCADA system is typically composed of several key components, each playing a crucial role in ensuring seamless control and monitoring of industrial processes. The primary components include:

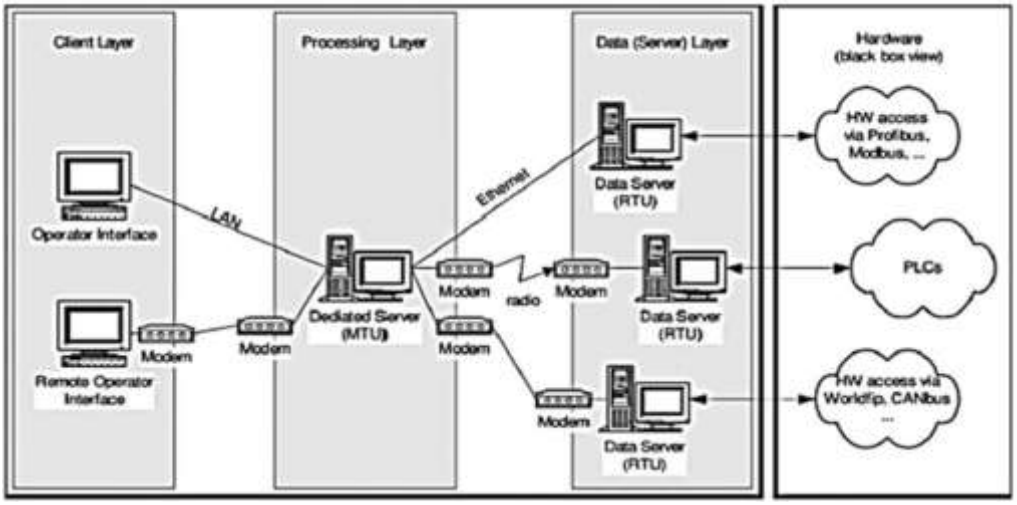


Fig1: Architecture of SCADA

- Supervisory Computers: These are the main servers in the control centre responsible for controlling and coordinating the whole system of SCADA. These people operate computer software that among other things, gathers data from the remote units, displays and analyses it before presenting it to the operators who in turn have the immediate control over the system.
- Remote Terminal Units (RTUs): These are units that are microprocessor based and local interface that communicate with sensors and other related devices out in the field. RTUs gather data from such devices and relay it to the supervisory computers besides carrying out instructions from the control centre and implementing specific actions in the field.
- Programmable Logic Controllers (PLCs): PLCs are tough built industrial computers that manage and automate equipment as well as processes at the lowermost tier. These are similar to RTUs, though they are more complex in control, and are greatly programmable for most functions.
- Human Machine Interfaces (HMIs): HMIs offer the SCADA system operators an interface in form of graphics to enable them manage the SCADA system easily. They provide real time data, alarm and system status, thus enabling the operators on the system to make right decisions.
- Communication Infrastructure: This consist of hard wired or wireless connections of data communication pathways that link RTUs, PLCs, HMIs and supervisory computers. As this communication network plays the vital role in operation, the dependence, reliability and security of this strategy has the direct consequence.

The architecture of a Tier1 SCADA system is designed to be highly reliable and resilient, with redundancy built into every layer to ensure continuous operation even in the event of component failures.

2.2 SCADA Systems with Enterprise IT Networks Integration of and Requirements of Real time Operational

With organizations trying to attain more efficiencies, data visibility, and insight in decision- making, SCADA systems are increasingly being integrated into enterprise IT networks. This allows for smooth information flow between the OT environment in which the SCADA systems operate and the greater IT

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

environment that manages business process and data analytics. But it brings huge cybersecurity challenges: the priorities of security are different for SCADA systems and IT networks. IT networks ensure data confidentiality and integrity, but in SCADA systems, availability and real-time control are crucial, which, if not rightly handled, may lead to vulnerabilities being introduced.

As an example, it may expose the SCADA system to IT-based threats, such as malware or unauthorized access, that may lead to operational disruption. It follows that integration in the context of a SCADA system is even more challenging because the operational needs call for real-time activities. According to, a real-time capability for a Tier 1 SCADA system will ensure safety, efficiency, and reliability in infrastructure operation. The system requires low latency in communication to avoid delaying critical commands, high availability to reduce losses financially and risks to safety, and scalability for the operational needs. What's more, it needs to be done without sacrificing real-time performance, hence, the need to find that sweet spot between cybersecurity and operational requirements. This makes the challenge of securing Tier 1 SCADA systems very unique: how to keep reliability and responsiveness very high when faced with ever-evolving cyber threats.

3. IDENTIFICATION OF KEY VULNERABILITIES

Identifying vulnerabilities in SCADA systems is essential to developing robust cybersecurity strategies, especially given their critical role in Tier1 infrastructures. The integration of SCADA systems with enterprise IT networks introduces a wide array of potential attack vectors. In this section, we examine some of the most critical vulnerabilities, focusing on input validation, code quality, and patch management.

3.1 Vulnerabilities in Input Validation

This table highlights common input validation vulnerabilities in SCADA systems and their potential impacts.

Vulnerability	Description	Example	Impact
Improper Input Validation[9]	Failing to ensure data is properly formatted before entering the system.	Attackers input invalid control commands to manipulate the system's behaviour.	System malfunctions or unauthorized access.
Buffer Overflow[10]	Inserting more data than a system buffer can handle, leading to overwriting memory.	Malformed data injection triggers a buffer overflow, giving attackers control over the SCADA system.	System crashes, control hijacking, or data breaches.
SQL Injection[11]	Entering malicious SQL queries in input fields.	Injecting SQL commands into input fields to retrieve or modify sensitive data from the SCADA database.	Unauthorized data access, modification, or database corruption.
Command Injection[12]	Injecting malicious commands into a system input.	Attacker inputs shell commands through input fields, gaining unauthorized control over the system.	Remote command execution or system compromise.
Cross Site Scripting (XSS)[13]	Injecting malicious scripts into SCADA web interfaces.	Entering JavaScript code into web interfaces, affecting user or system data.	Session hijacking, data theft, or disruption of web-based interfaces.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

3.2 Poor Code Quality and Its Impact

This table highlights common poor code quality vulnerabilities in SCADA systems and their potential impacts.

Issue	Description	Example	Impact
Unsecured Communication Protocols[14]	Using outdated or weak protocols without encryption or authentication.	Legacy SCADA systems using unencrypted Modbus or DNP3 protocols for data transmission.	Exposure to data interception and man in the middle attacks.
Hardcoded Credentials[15]	Storing passwords or credentials directly in the code, making them easily discoverable.	Default or hardcoded login credentials embedded in SCADA software code.	Unauthorized access to the system, leading to security breaches.
Failure to Handle Edge Cases[16]	Inadequate code to handle uncommon but critical scenarios in control logic.	Missing error handling for unexpected sensor input ranges, causing system crashes or incorrect responses.	System instability, operational failure, or safety risks.
Memory Leaks[17]	Improper management of memory resources, leading to exhaustion over time.	Legacy code that doesn't release memory, causing the system to slow down or crash.	System downtime, performance degradation, or crashes.
Race Conditions[5]	Code that fails to properly synchronize access to shared resources.	Multiple processes attempting to modify shared variables simultaneously in SCADA control logic.	Unpredictable system behaviour or control failures.
Security Bypasses[17]	Flaws that allow bypassing security mechanisms due to poor coding practices.	Poor validation of access controls, allowing unauthorized users to modify control settings.	Unauthorized changes to critical infrastructure and control systems.
Proprietary Protocol Vulnerabilities[18]	Legacy protocols without modern security measures, exposing coding flaws.	SCADA systems relying on proprietary protocols vulnerable to reverse engineering.	Increased risk of attacks exploiting protocol weaknesses.

3.3 Inadequate Patch Management Practices

This table highlights the risks and complications associated with inadequate patch management in SCADA systems, underscoring the importance of balancing security updates with operational continuity.

Challenge	Description	Example	Impact
Delayed Patching[19]	Patches are postponed to avoid operational disruptions in critical real time systems.	Security vulnerabilities remain unpatched due to concerns over interrupting vital SCADA operations.	Increased risk of exploitation of known vulnerabilities.
Lack of Automated Patching[20]	Absence of automated tools leads to reliance on manual patching processes.	SCADA systems require manual updates, introducing potential for human error in applying patches.	Patch delays, misconfigurations, and increased exposure to attacks.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Operational Constraints[21]	Patching must be carefully planned to avoid downtime, limiting opportunities for updates.	SCADA operators hesitate to apply patches during periods of high operational activity or critical tasks.	Prolonged exposure to security risks and potential system instability.

4. ASSESSMENT OF EXISTING SECURITY MECHANISMS

The Chart synthesises threats affecting different vendors and components in the industrial systems. The company that has the largest number of overall vulnerabilities is Siemens with 61, these vulnerabilities are, for the most part, located in PLCs. Schneider Electric ranked second with 42 vulnerabilities, of which most of them affected HMIs. Currently, Rockwell Automation has 17 vulnerabilities with majority of them relevant to networks. A total of 20 vulnerabilities are recorded in Advantech's products with most of the vulnerabilities found in their HMIs and PLCs. There are 12 vulnerabilities for ABB and 12 for Allen Bradley both of which are distributed among various sections of the software components. Honeywell again presents fewer vulnerabilities than the other two with estimates of 4, Mitsubishi with 2 and General Motors with 1.

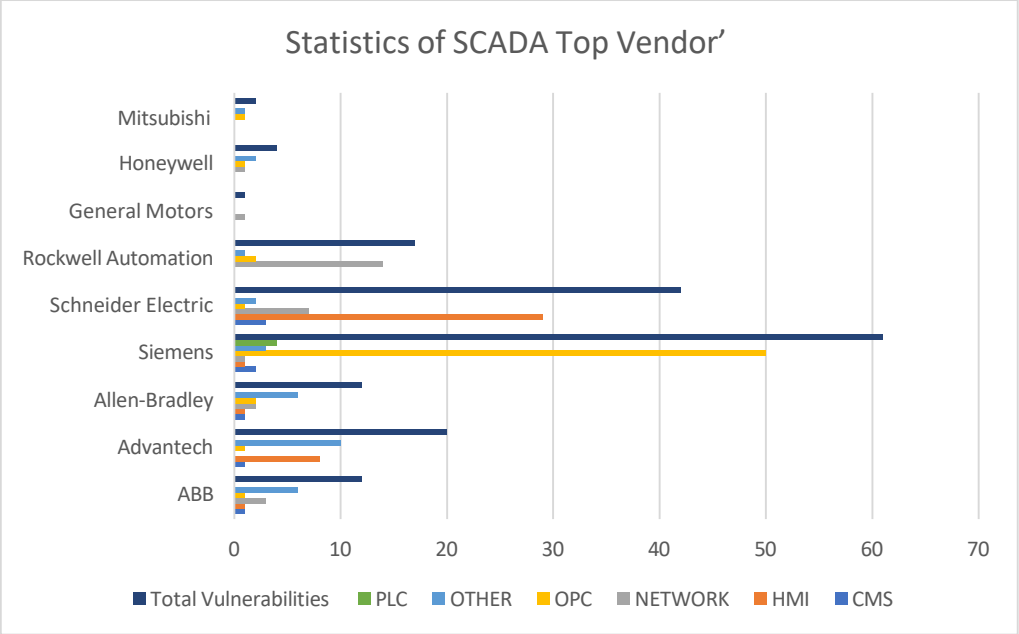


Chart1: Statics of SCADA Top Vendors

Some of the vulnerabilities are categorized as Content Management Systems (CMS), Human Machine Interfaces (HMI), Networking, OPC, and PLC systems. To protect SCADA systems from the new generation of threats, several protective measures have been adopted across the industries. However, operations of these mechanisms are challenging due to diverse characteristics of SCADA systems, which sometimes depicts the fundamental weaknesses of these mechanisms. This section reviews the traditional security control measures of firewalls, encryption standards and access control measures with reference to their applicability to SCADA specific vulnerabilities.

4.1 Firewall Configurations and Their Limitations

This table outlines the limitations of firewall configurations in SCADA networks, emphasizing the need for more specialized and adaptable security measures to complement firewalls.

Table3: Firewall Limitations Glance

Firewall Limitation	Description	Example	Impact

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Need for Open Communication[22]	SCADA systems require open communication channels, limiting the strictness of firewall rules.	Firewalls must allow continuous data flow for operations, making it hard to block suspicious activity.	Increased vulnerability to unauthorized access or data manipulation.
Static Configurations[23]	Firewall rules are rarely updated to adapt to new threats in SCADA systems.	A firewall configured with outdated rules fails to block a new type of attack exploiting open ports.	Exposure to emerging threats and attacks on critical infrastructure.
Inability to Handle SCADA Protocols[23]	Traditional firewalls struggle to understand and filter SCADA specific protocols.	A firewall fails to detect malicious traffic in protocols like Modbus or DNP3 due to lack of protocol awareness.	Reduced ability to block attacks specifically targeting SCADA communication.

4.2 Encryption Protocols and Their Challenges in SCADA

Challenge	Description	Example	Impact
Legacy System Compatibility[24]	Many older SCADA systems lack support for modern encryption standards like AES or TLS.	Legacy SCADA systems struggle to integrate AES or TLS encryption due to outdated hardware and software.	Increased vulnerability to attacks due to lack of encryption.
Real time Performance Impact[24]	Encryption overhead, especially from protocols like AES256 or RSA, may introduce latency, affecting real time data processing.	Implementing AES256 encryption slows down Modbus data transmission, disrupting real time control operations.	Decreased system performance and operational inefficiencies.
Incompatibility with SCADA Protocols[24]	Common encryption protocols like SSL/TLS may not be compatible with SCADA specific protocols such as Modbus or DNP3.	SSL/TLS is incompatible with older SCADA protocols like Modbus, forcing the use of unencrypted transmissions.	Exposure to man in the middle (MITM) attacks or data interception.
Use of Weak Encryption Methods[25]	Legacy systems may rely on outdated or weak encryption like DES or 3DES due to compatibility issues.	SCADA systems use deprecated encryption algorithms like DES or 3DES, which are easily broken by modern attackers.	Increased risk of cryptographic attacks and system compromise.
Poor Key Management[25]	Hardcoded or static keys used with encryption protocols such as RSA or AES weaken the security of encrypted communications.	RSA keys are hardcoded into SCADA firmware, making them vulnerable to reverse engineering and exploitation.	Key exposure leads to unauthorized decryption and system breaches.

To address these challenges, SCADA systems need more granular and dynamic access control mechanisms, including multifactor authentication (MFA) and automated logging of access attempts. These measures will help ensure that only authorized users can make critical changes to SCADA operations, improving both security and resilience.

5. DEVELOPMENT PHASES IN CYBER RISK ASSESSMENT

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Cyber risk assessment involves a series of systematic steps aimed at identifying, analysing, and mitigating security risks. In model development, these phases help build a framework to quantify, assess, and manage these risks in a structured manner.



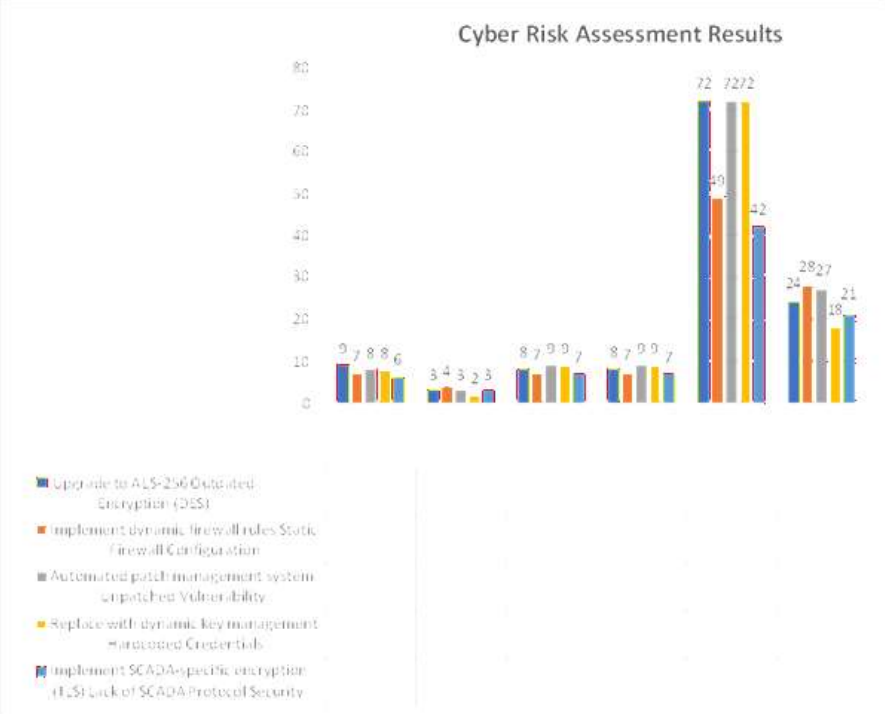
Fig Development Phases of Cyber Risk Assessment

- Risk Identification: Detect and document potential security threats and vulnerabilities within the system. Aim to create a comprehensive list of all possible risks that could impact the organization's assets.
- Risk Analysis: Analyze identified risks to understand their nature, causes, and potential impact. Assess both the likelihood of each risk occurring and the severity of its consequences.
- Risk Prioritization: Prioritize risks based on their potential impact and likelihood. Focus resources and efforts on the most critical risks that require immediate attention.
- Risk Mitigation Strategies: Develop and implement strategies and controls to address the prioritized risks. Design measures to reduce the likelihood of risk occurrence and minimize the impact if the risk materializes.
- Model Development and Testing: Build and refine a risk assessment model based on the identified risks and mitigation strategies. Test the model to ensure its effectiveness and reliability in assessing and managing risks.
- Continuous Monitoring and Updating: Continuously monitor the risk environment and the effectiveness of implemented controls. Regularly update the risk assessment model to adapt to new threats and changes in the risk landscape.

5.1 Cyber Risk Assessment Results

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Likelihood (1-10)	Likelihood (Post-Mitigation)	Impact (1-10)	Impact (Post-Mitigation)	Risk Score (Pre-Mitigation)	Risk Score (Post-Mitigation)
9	3	8	8	72	24
7	4	7	7	49	28
8	3	9	9	72	27
8	2	9	9	72	18
6	3	7	7	42	21



- ✓ **Upgrade to AES256:** Replacing outdated DES encryption with AES256 significantly reduces the risk. The likelihood of exploitation decreases from 9 to 3, and the overall risk score improves from 72 to 24, though the impact remains the same at 8.
- ✓ **Implement Dynamic Firewall Rules:** Updating static firewall configurations to dynamic rules lowers the likelihood of a firewall breach from 7 to 4. Despite no change in impact, the risk score reduces from 49 to 28, reflecting improved security.
- ✓ **Automated Patch Management System:** Introducing an automated patch management system decreases the likelihood of unpatched vulnerabilities from 8 to 3. Although the impact remains at 9, the risk score is significantly reduced from 72 to 27.
- ✓ **Replace with Dynamic Key Management:** Switching from hardcoded credentials to dynamic key management greatly lowers the likelihood of exposure from 8 to 2. This change reduces the risk score from 72 to 18, even though the impact remains high at 9.
- ✓ **Implement SCADA Specific Encryption (TLS):** Applying TLS encryption specifically for SCADA systems decreases the likelihood of a security breach from 6 to 3. The risk score improves from 42 to 21, with no change in the impact score of 7.

6. CONCLUSION

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

From the findings of this study, a lot of information on the security risks and challenges pertaining to Tier-1 SCADA systems have been discovered particularly in enterprise environments. Analysing SCADA components and their related threats one can conclude that these systems or components of them can be affected by a big number of threats ranging from the improper input validation to the usage of outdated encryption. If they are not addressed properly, they result in the following adverse effects on the systems and operations: unauthorized access, system failure, and disruptions of continuity. The first major observation established from the research is the expansion in the attack vector due to interfacing with SCADA systems with the larger IT systems. This has brought about new forms of risks like buffer overflows, SQL injections and Code flaws like hard coded credentials as well as poor patch management. These issues make reference to the importance of stronger cybersecurity measures than can cope with present risks as well as those emerging in the future.

The work also stressed the development of a methodical approach to the assessment of cyber risks and generation of risk models. As we can observe following the phases of risk identification, risk analysis, risk prioritization and risk mitigation, model testing, and risk monitoring the organization can achieve a stronger framework. In addition, improving the strength of encryption, using dynamic Firewalls, and automating patch management were demonstrated to lower the risks associated with vulnerability exploitation thus enhancing the total security of the system.

In conclusion, it is imperative to note that it is impossible to solve the cybersecurity problems of SCADA systems at once but only to approach the problem comprehensively by defining the concrete risks, finding the ways to minimize these risks and implementing permanent surveillance over the situation. It is therefore possible to develop dynamic SCADA specific security that can readily enhance the protection of these important infrastructures through better encryption, real-time threat response and improved patch management. Therefore, the findings of this research point to the importance of continued assessment and improvement of security measures to counter the present and the future security risks.

7. FUTURE SCOPE OF THE RESEARCH

Future papers can review the actual use of artificial intelligence and/or machine learning algorithms to monitor threat activity and perform real-time reactions in SCADA systems. Over time, the threats change, and thus, there could be improvements in the employment of the methods of proactive security all the time leading to fast identification of the potential attacks. Further, exploring the adoption of block chain technology for valid and time-tested communication in sincerity of SCADA networks could also help in protecting the integrity of data. Other areas for future research can also be expected to direct solutions towards creating highly sophisticated encryption approaches that are capable of evolving in real-time in response to threats that may develop in the future. Further, research on 5G and edge computing influence on SCADA security could reveal how these technologies can enhance their elements' reliability. All in all, further research is needed to build better Strong-AI extensible, and effective cybersecurity solutions for securing the SCADA systems in an environment that is gradually expanding with more complex interconnectivity.

8. REFERENCES

1. K. Raghunandan, Supervisory Control and Data Acquisition (SCADA), in Introduction to Wireless Communications and Networks, Textbooks in Telecommunication Engineering. Springer, Cham, 2022, pp. 531-553. doi: 10.1007/978-3-030-92188-0_16.

2. S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," Computers & Security, vol. 70, pp. 436-454, 2017. doi: 10.1016/j.cose.2017.06.010.

3. D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1942-1976, third quarter 2020. doi: 10.1109/COMST.2020.2987688.

4. A. S. Mohammed, P. Reinecke, P. Burnap, O. Rana, and E. Anthi, "Cybersecurity challenges in the offshore oil and gas industry: an industrial cyber-physical systems (ICPS) perspective,"

ACM Transactions on Cyber-Physical Systems (TCPS), vol. 6, no. 3, pp. 1-27, 2022. doi: 10.1145/3548691.
5. A. Abou el Kalam, "Securing SCADA and critical industrial systems: From needs to security mechanisms," International Journal of Critical Infrastructure Protection, vol. 32, p. 100394, 2021. doi: 10.1016/j.ijcip.2020.100394.
6. M. Sverko and T. G. Grbac, "Complex Systems - Network Component Security of SCADA Systems," in 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2021, pp. 1630-1635. doi: 10.23919/MIPRO52101.2021.9596701.
7. Y. Cherdantseva, P. Burnap, S. Nadjm-Tehrani, and K. Jones, "A Configurable Dependency Model of a SCADA System for Goal-Oriented Risk Assessment," Applied Sciences, vol. 12, no. 10, p. 4880, 2022. doi: 10.3390/app12104880.
8. M. Sverko, T. G. Grbac, and M. Mikuc, "SCADA Systems With Focus on Continuous Manufacturing and Steel Industry: A Survey on Architectures, Standards, Challenges and Industry 5.0," IEEE Access, vol. 10, pp. 109395-109430, 2022. doi: 10.1109/ACCESS.2022.3211288.
9. R. J. Thomas and T. Chothia, "Learning from Vulnerabilities - Categorising, Understanding and Detecting Weaknesses in Industrial Control Systems," in Computer Security, S. Katsikas, Ed., Cham: Springer, 2020, pp. 109-128. doi: 10.1007/978-3-030-64330-0_7.
10. M. Mesbah, M. S. Elsayed, A. D. Jurcut, and M. Azer, "Analysis of ICS and SCADA Systems Attacks Using Honeypots," Future Internet, vol. 15, no. 7, p. 241, 2023. doi: 10.3390/fi15070241.
11. J. -M. Lee and S. Hong, "Keeping Host Sanity for Security of the SCADA Systems," IEEE Access, vol. 8, pp. 62954-62968, 2020. doi: 10.1109/ACCESS.2020.2983179.
12. W. Alsabbagh, S. Amogbonjaye, D. Urrego, and P. Langendörfer, "A Stealthy False Command Injection Attack on Modbus based SCADA Systems," in 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2023, pp. 1-9. doi: 10.1109/CCNC51644.2023.10059804.
13. G. E. Rodríguez, J. G. Torres, P. Flores, and D. E. Benavides, "Cross-site scripting (XSS) attacks and mitigation: A survey," Computer Networks, vol. 166, p. 106960, 2020. doi: 10.1016/j.comnet.2019.106960.
14. Q. S. Qassim, N. Jamil, M. R. Z'aba, and W. A. W. Kamarulzaman, "Assessing the cyber- security of the IEC 60870-5-104 protocol in SCADA system," International Journal of Critical Infrastructures, vol. 16, no. 2, pp. 91-106, 2020. doi: 10.1504/IJCIS.2020.107242.
15. G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, and J. Benjamin, "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," IEEE Access, vol. 9, pp. 165295-165325, 2021. doi: 10.1109/ACCESS.2021.3133348.
16. B. S. Brad, M. Murar, G. Vlad, E. Brad, and M. Popanton, "Lifecycle Design of Disruptive SCADA Systems for Waste-Water Treatment Installations," Sustainability, vol. 13, no. 9, p. 4950, 2021. doi: 10.3390/su13094950.
17. C.-M. Mathas, C. Vassilakis, N. Kolokotronis, C. C. Zarakovitis, and M.-A. Kourtis, "On the Design of IoT Security: Analysis of Software Vulnerabilities for Smart Grids," Energies, vol. 14, no. 10, p. 2818, 2021. doi: 10.3390/en14102818.
18. S. V. B. Rakas, M. D. Stojanović, and J. D. Marković-Petrović, "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems," IEEE Access, vol. 8, pp. 93083-93108, 2020. doi: 10.1109/ACCESS.2020.2994961.
19. J. Biswas et al., "Reliability assessment of patched SCADA EMS/DMS servers through similarity matching," in 2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), New Orleans, LA, USA, 2022, pp. 1-5. doi: 10.1109/ISGT50606.2022.9817486.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

20. B. Babayigit and M. Abubaker, "Industrial Internet of Things: A Review of Improvements Over Traditional SCADA Systems for Industrial Automation," IEEE Systems Journal, vol. 18, no. 1, pp. 120-133, March 2024. doi: 10.1109/JSYST.2023.3270620.
21. D. Upadhyay, M. Zaman, R. Joshi, and S. Sampalli, "An Efficient Key Management and Multi-Layered Security Framework for SCADA Systems," IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 642-660, March 2022. doi: 10.1109/TNSM.2021.3104531.
22. A. Ara, "Security in Supervisory Control and Data Acquisition (SCADA) based Industrial Control Systems: Challenges and Solutions," in IOP Conference Series: Earth and Environmental Science, vol. 1026, no. 1, p. 012030, 2022. doi: 10.1088/1755- 1315/1026/1/012030.
23. A. Kumar, B. Bhushan, A. Malik, and R. Kumar, "Protocols, Solutions, and Testbeds for Cyber-Attack Prevention in Industrial SCADA Systems," in Internet of Things and Analytics for Agriculture, Volume 3, P. K. Pattnaik, R. Kumar, and S. Pal, Eds. Singapore: Springer, 2022,
pp. 307-327. doi: 10.1007/978-981-16-6210-2_17.
24. A. C. F. Chan and J. Zhou, "Toward Safe Integration of Legacy SCADA Systems in the Smart Grid," in Applied Cryptography and Network Security Workshops. ACNS 2022, J. Zhou, Ed., Cham: Springer, 2022, pp. 324- 341. doi: 10.1007/978-3-030-94215-1_23.