ISSN: 2182-2069 / E-ISSN: 2182-2077

Exploring Secure SCADA Frameworks for Coastal Power Grids and Offshore Platforms

Rajendran Palanivelu[1*], and Yeshwanth Raj[2]

[1*]Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India.
rajendran.p@ametuniv.ac.in, https://orcid.org/0000-0001-5016-9742

[2]Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India.
yeswanthraj@ametuniv.ac.in, https://orcid.org/0009-0003-4467-3389

Received: May 14, 2025; Revised: June 30, 2025; Accepted: August 05, 2025; Published: August 30, 2025

Abstract

An integral part of a modern maritime infrastructure involves coastal grids as well as offshore power plants, both of which are remotely managed using SCADA systems. With the development of systems containing more hybrids of cloud and IoT technology, the risk for cybersecurity breaches continue to increase. This research looks into SCADA security frameworks with a special focus on coastal and offshore maritime constraints, which include but aren't limited to limited environments, isolation, real-time action requirements, and remote accessibility. Current frameworks are examined within the context of critical maritime asset protection focusing on existing gaps alongside contributory strong factors to asset damage capture. Through simulations and case studies, the effectiveness of various layered encryption approaches alongside anomaly detection and secure communication protocols are explored. This work aims to improve resilience against potential threats to SCADA-based coastal and offshore power systems while maintaining energy flow reliability alongside maritime safety. Recommendations are outlined to aid further augmentations of cyber crosshairs in maritime SCADA systems.

Keywords: SCADA Systems, Cybersecurity, Coastal Power Grids, Offshore Platforms, Maritime Infrastructure, Secure Communication, Critical Infrastructure Protection.

1 Introduction

Supervisory Control and Data Acquisition (SCADA) Systems are primary technologies utilized in the majority of processes; coastal power grid and offshore energy platforms are only two examples. They enable distributed infrastructure monitoring and real-time control from a central location, maintaining continuity and ensuring safety within critical environments. In maritime settings, SCADA systems perform subsea cable monitoring, turbine synchronization, and remote fault response for turbines in complex energy installations (Stouffer et al., 2015). There is little physical access to maritime energy structures, hence, the environmental conditions make maintaining SCADA operation integrity, availability, and security imperative (Pragadeswaran et al., 2024). Modern SCADA systems are no longer confined to proprietary settings, but rather exists as interconnected systems that use standard communication protocols, cloud computing, and the Industrial Internet of Things (IIoT) (Yan et al., 2012). While improving operational efficiency and scalability, this transition becomes a risk by exposing

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 437-448.
DOI: *10.58346/JISIS.2025.I3.030*

*Corresponding author: Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India.

SCADA systems to new cyber threats. In particular, coastal and offshore infrastructure becomes a target for cyber threat actors using remote access points, unsecured protocols, and software vulnerabilities (Galloway & Hancke, 2013).

In the context of maritime energy installations, the consequences of a cyberattack on SCADA systems could be catastrophic in nature including prolonged blackouts, ecological harm, and economic disruption. The ever evolving malware, such as the Stuxnet worm and the Ukraine power grid attack illustrate the profound damage sophisticated SCADA tailored malware can inflict on essential infrastructure (Makkada et al., 2024). These offshore and coastal systems are no exception as their heavy reliance on communication and automation renders them vulnerable to persistent advanced threats (Knowles et al., 2015). In coastal SCADA-enabled power plants and offshore facilities, current cybersecurity measures are inadequate. Many of these systems are still using old methods like Modbus and DNP3 with weak ciphering and validating protocols (Zhu et al., 2011). Even when firewalls and intrusion prevention systems are in place, attackers take advantage of zero-day exploits or escalate access through using stolen credentials (Cherdantseva et al., 2016). In addition, these technologies are rigid and static and thus are incapable of meeting changing cyberspace challenges in real-time (Karnouskos, 2011, Tan, et al. 2024).

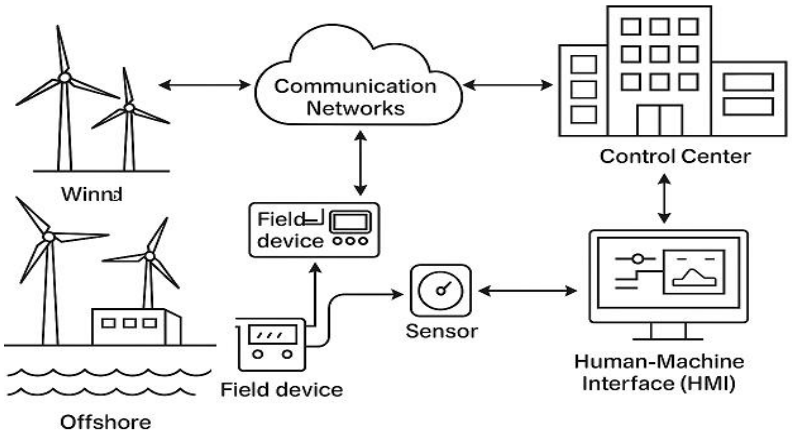

Figure 1: SCADA Architecture for Maritime Coastal and Offshore Energy Systems

This SCADA (Supervisory Control and Data Acquisition) system maritime specialization for coastal power plants and offshore energy platforms is displayed in the figure (Figure 1) above. It illustrates key elements which consist of field devices like RTUs (Remote Terminal Units), sensors, and actuators installed onboard ships and offshore facilities. These units communicate with control centers situated onshore or on-board a central command ship through secure communication networks. Such networks sometimes utilize satellite or marine radio links. The control centers equipped with data servers and firewalls monitoring and supporting system integrity implement HMIs (Human-Machine Interfaces) for decision-making. With this configuration, it is possible to collect, monitor, and control critical maritime infrastructure in real-time. It shows the value of reliable and secure communication systems especially in remote and always hostile marine surfaces.

Even though international frameworks for the security of industrial control systems exist—like NIST SP 800-82 and ISA/IEC 62443— they are not fully integrated into maritime practice (Bhamare et al, 2020). Coastal and offshore infrastructures need cybersecurity frameworks that address their particular operational challenges, such as limited data throughput, significant delays, and minimal personnel presence. A singular SCADA security strategy tailored to these environments is ineffective. This

research focuses on developing secure SCADA systems for coastal power generation and offshore platforms. This study seeks to determine the impact of applying layered security techniques: encryption and confidential communications, intrusion detection, automated response systems, and others to layered security architectures (Nithyalakshmi et al., 2021). Performance assessments will be conducted through simulations and modeling, measuring response time, uptimes, resilience to certain actions, and overall system durability amid various potential attacks (Zhu & Basar, 2015). The results should help develop effective adaptive maritime cybersecurity implementations. This work helps in forming resilient and robust SCADA systems capable of contending with the diverse threats posed to the maritime domain. These frameworks will enable safe access to coastal and offshore energy infrastructure by integrating the maritime domains' specific needs with modern technology.

2 Background

The significance of SCADA systems is particularly prevalent in the industrial infrastructure industry concerning energy distribution and offshore power generation. These systems are fundamental in servicing the remote monitoring and control functions of turbines, substations, transformers, and offshore platforms (Boyes, 2015). SCADA systems are essential for a remote operator to control electrical loads, recognize faults, and keep system functionality within difficult and dynamic solutions such as coastal grids and offshore installations (Gungor et al., 2011).

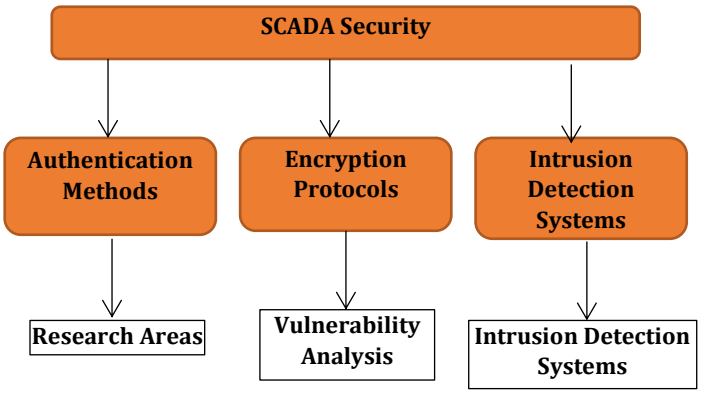

Figure 2: Review on SCADA Security

The figure 2 provides a relatively simple overview of the primary areas of scholarly research undertaken on securing SCADA systems with respect to three domains: Authentication Methods, Encryption Protocols, and Intrusion Detection Systems. Authentication Methods addresses the measures that restrict access to the system, preventing the intrusion by users and devices that have not been granted access. Encryption Protocols is discussed concerning vulnerability analysis, focusing on securing data that is being sent or received against interception and alteration. Intrusion Detection Systems (IDS) are studied for their capacity to detect and respond to incursable hostile acts within the SCADA networks. Together these components exemplify the areas of emphasis of academic and applied research directly or indirectly aimed at strengthening the SCADA architectures utilized in critical infrastructure.

The components that constitute sophisticated SCADA systems are HRIs, RTUs, PLCs, along with a collective or central server or master station (Verma & Reddy, 2025). These components are networked with one another through industrial standard such as Modbus, DNP3 or IEC 60870-5-104, most of which were designed long before the security was a consideration (Cardenas et al., 2008). Hence, SCADA infrastructures have low resiliency to a wide range of cyber risks including but not limited to: unauthorized access, data alteration, man-in-the-middle, and denial-of-service attacks (Kumar & Patel,

2014). The IIOT integration and shift to cloud-based SCADA systems have greatly increased the potential cybersecurity risk (Hammad et al., 2022).

These technological improvements enhance operational efficiency and scalability, but they come with new vulnerabilities due to heightened dependence on online and interconnected systems (Humayed et al., 2017). Such vulnerabilities are critical in offshore scenarios where remotely located machinery cannot be accessed physically. Their associated threat response times can lead to a system's security being compromised (Alcaraz & Zeadally, 2015, Cárdenas, A. A., 2018). SCADA system security faces many difficulties, the most prominent being the aging foundational components mesh with new IT requirements (Mthembu & Dlamini, 2024). Under certain conditions, older appliances can be stripped of almost all processing capabilities (e.g. required for encryption or anomaly detection) giving them easy abuse exploitable (Knowles et al., 2015). In addition, SCADA systems were originally built to function with efficiency, not security in mind, and many systems still operate without requiring authentication, authorization, or encryption (Stouffer et al., 2015; Mohankumar et al., 2024). SCADA systems have been the focus of numerous studies attempting to find their inherent vulnerabilities and suggest means of mitigating them. These include network segmentation, protocol whitelisting, behavioral intrusion detection systems, and secure boot mechanisms (Karnouskos, 2011; Liu & Tang, 2024). Real-time operations anomaly detection and data integrity assurance through the implementation of blockchain and machine learning has also been explored (Yang et al., 2019; Chinnasamy, 2024; Dhivya et al., 2023). There is still much work to be done in these fields as their adoption continues to be limited by the implementation intricacies, the need to suspend the system, or downtime which is seldom permissible in critical infrastructures (Cherdantseva et al., 2016). The ongoing work also includes the refinement of policies and governance for SCADA system security that include custom-tailored access control models, incident response procedures, and threat modeling focused on maritime and coastal energy infrastructure specific vulnerabilities (Zografopoulos et al., 2021; Tan et al., 2024). Additional efforts towards standardization such as ISA/IEC 62443 and NIST SP 800-82 have offered suggestions for fortifying the cybersecurity frameworks within industrial control environments, but the sector-wide compliance is still maturing (Khurana et al., 2010).In conclusion, SCADA systems are essential for the coastal power grid and offshore platform management, but they are still susceptible to cyber-attacks due to outdated protocols, hybrid integration with contemporary systems, and minimal physical surveillance in remote locations (Anny Leema et al., 2024; Whitmore & Fontaine, 2024). It is necessary to redefine policies and governance alongside technological investment in SCADA systems to address domain-specific challenges. Innovations in resilient security models are critically important to maintain secure and continuous power systems servicing maritime regions.

3 Secure SCADA Frameworks

In the domain of coastal power grids and offshore platforms, securing SCADA systems necessitates a multi-faceted approach tailored to the specific threats these systems confront. Given their role in remotely monitoring and managing critical infrastructure, SCADA systems must defend against unauthorized access, information leakage, and interruption of service through cyberattacks. Usually SCADA is implemented in conjunction with a multi-layer framework consisting of secure user verification, restricted communication access, and threat mitigation tools including firewalls, virus scanners, and security cameras.

3.1 Measures for Authentication and Access Control

Access control and authentication are the major domains of a secured SCADA framework. Cybercriminals leverage poor authentication protocols, out-of-the-box defaults, and oversights within authentication schemes. Consequently, significant consideration has to be put into passwords and user verification. SCADA systems ought to be configured so that Multi-Factor Authentication (MFA) is mandatory especially in scenarios where logins require more than just a user ID and password. Device and user permissions need to follow the Russian policy and not go beyond the minimal necessary functions required to carry out their tasks so as to mitigate the consequences of a compromised account. Additionally, centralized systems for managing identities can improve security over user access and make auditing easier. These systems can automatically enforce security policies, terminate access in a timely manner when roles change, and track users for suspicious activities. For remote SCADA systems, which are prevalent in offshore facilities, Virtual Private Networks (VPNs) and some Secure Gateway Devices offer controlled, authenticated access points that restrict system interactions to valid user interfaces.

3.2 Encryption Methods for the Transmission of Information

The data traveling within SCADA networks can be intercepted, modified, and spoofed. To safeguard against these threats, encryption must be applied to every communication channel in the system. With end-to-end encryption, data is protected from the point of generation in a field device to processing by a control center. Data confidentiality and integrity can be preserved over unauthenticated networks using encryption methods like Transport Layer Security (TLS) and IPsec to encapsulate data packets. In these covert computations, such as along coastal grids and adept offshore platform systems, the application of lightweight cryptography can be warranted owing to low processing capacity. Furthermore, silos of unused data like configuration “cfg” files and logging files should be encrypted to avert unauthorized access when there is a physical breach of the storage device. Also, the frameworks of encryption strategies are useful but only when appropriate protections are applied, which include effective key management practices such as periodic rotation and the safeguarding of sensitive keys.

3.3 Intrusion Detection and Prevention Systems

Surveillance or Intrusion Detection and Prevention System (IDPS) plays an essential role in improving the overall security posture of SCADA networks. IDPS are used to observe network and system activity to detect possible security threats in real time. Signature-based detection techniques identify predefined set of threats using a constituent known as attack signature databases, while anomaly-based detection marks behavior that deviates from set standards, thereby proving helpful in identifying zero-day and insider attacks. There is a need to optimize the operational requirements productivity IDPS solutions deployment in a SCADA Systems like industrial systems which require low latency, high availability, and the bare minimum of false positives. Maximization of threat visibility can be achieved through network segmentation and sensor placement in important regions within the network architecture. Also, IDPS integrated with automated response systems can take immediate action to neutralize threats, for example by containing devices perceived to be dangerous or cutting off access to harmful traffic.

In their totality, these measures offer a multi-faceted approach to security designed for SCADA systems deployed in maritime and coastal regions. To adequately protect sensitive infrastructure and information systems, like SCADA, sustains, complex and multi functional driven systems are paramount. Technologies need to be backed up not only for sophisticated advanced persistent threats, but also for generic DoS type attacks. There is a need to address the focus towards `Risk assessment,

prevention and mitigation system information`. In deploying competing systems, responding effectively becomes a matter of existing within a sustained trusted security system, together with multi-system multi-layer defense technologies that are sophisticated enough to face aerial assaults masterminded by entities advanced persistent with undeterred will.

4 Case Studies

The practical use of secure SCADA systems in coastal and offshore settings illuminates certain best practices alongside problems that are often encountered. These studies illustrate the impact of integrating technology, enforcing policies, and organizational efforts towards defending critical infrastructure from cyberattacks.

4.1 Striking Examples in Power Grids of the Coast

An example of successful implementation is the secure SCADA system deployed in the Texas Gulf Coast Power Grid servicing the heterogeneous industrial and civilian coastal infrastructure. Due to rising cyber threat concerns, utility operators upgraded their legacy SCADA architecture systems by adding end-to-end encryption, multi-factor authentication, and redundant communication channels. The addition of intrusion detection derparture systems configured for industrial control systems was a game changer in detecting anomalous behavior in real time towards enhancing their detection capabilities. This change improved network resilience while achieving compliance with NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) regulatory requirements. The secure SCADA protocol implementation enabled real-time data sharing across geographically dispersed coastline wind farms integrated into Denmark’s national grid. Encryption alongside strong identity management frameworks mitigated unauthorized access to remote monitoring stations, while adaptive firewalls coupled with continuous network monitoring neutralized threats before they were able to compromise operations. These protocols have greatly helped in maintaining the uninterrupted power supply and the integrity of the data across the system.

4.2 Denmark: Challenges in Securing Offshore Platforms

Offshore platforms are faced with unique technical and logistical challenges when securing SCADA systems. For example, the North Sea oil platforms operate in bandwidth constrained remote and harsh environments with limited maintenance windows. Many offshore platforms still depend on legacy SCADA systems that do not include basic features such as access control or encryption. Implementing modern cybersecurity tools poses disruption risks for mission-critical systems and complex engineering is required to seamlessly integrate them into older systems. Yet another critical personal awareness training challenge persists. Most offshore teams rotate frequently, and ensuring each member is trained on the relevant protocols is all but impossible. In addition, access to the systems, either physically by authorized individuals or malicious outsiders, has to be controlled very strictly which is logistically challenging due to the isolation of offshore locations. Security breaches in the past have provided stark lessons that have shaped SCADA security across maritime infrastructure. An illustrative example is the 2010 cyber intrusion case where an oil company’s offshore control system was breached. The incident revealed blatant shortcomings in firewall configurations and password policies. In this case, the attackers were found to have remote access through a wireless bridge used for monitoring that was not secured. This event led to the renewed scrutiny of wireless elements in SCADA architecture and greater implementation of secure encrypted channels for communication.

Another case concerned the partial service disruption of an offshore wind farm control network after a phishing attack. Although the malware did not cause any physical harm, it highlighted the potential destructive capability of human-factor vulnerabilities to bypass otherwise secure systems. So far more focus on workforce cyber security training and role playing for better organizational resilience has been emphasized.These case studies highlight the need for a multi-faceted security approach within SCADA frameworks. As much as technology is critical, lasting resilience is as dependent on policies, end-user activity, system auditing, and proactive defense measures for incidents. Design and operational frameworks for SCADA systems, both coastal and offshore, need to incorporate lessons from these practical case studies to effectively protect vital infrastructure in the face of shifting realities and emerging threats.

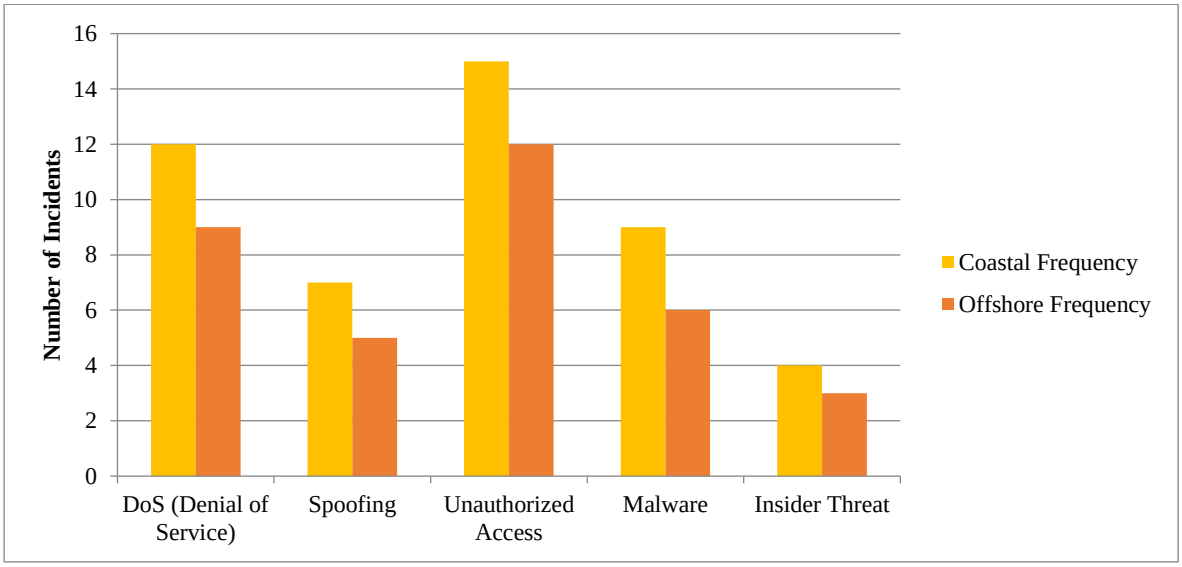

Figure 3: Frequency of Cyber Incidents by Type (Coastal vs Offshore)

In coastal power grids alongside offshore platforms, their cyber incident frequency was recorded and is compared in the same diagram (Figure 3). Five particularly common incidents are paralelled: Denial of Service (DoS), Spoofing, Unauthorized Access, Malware, and Insider Threats. An important observation is that in both contexts, coastal grids in particular, cyber incidents of Unauthorized Access seem to occur at unignorable rates. Close numbers of DoS attacks also occur, especially in coastal setups that face high network exposure. Incidents like Insider Threats and Spoofing, although appearing as rarer, still pose an enduring threat. These observations show that as compared to offshore platforms, coastal systems become increasingly targeted for cyber attacks, suggesting the necessity for specific protective measures depending on the working atmosphere. The comparison of operational downtime in hours (before and after the implementation of security measures) over the four scenarios (Case A to Case D) is presented in Figure 4. The graph clearly indicates that in all cases, downtime increased somewhat after security implementation—this is interesting. Reasonably, this may be due to extra authentication, access control, and monitoring systems that enhance cybersecurity but may also cause delays in recovering operations or dealing with incidents. Case B is particularly noteworthy because, as mentioned, it had the highest increase in downtime, which might mean there was some poorly integrated subsystem or he had complex problems to deal with. Nevertheless, although the downtime is higher, suboptimal as it may be, this is fine because of the high level of system resilience and threat mitigation improvement achieved. Figure 5 depicts the cost breakdown of cybersecurity incidents in maritime and coastal SCADA systems. Recovery costs take up the largest segment at 35%, illustrating the costs

incurred in restoring systems, data, and services after an attack. The cumulative impact of trust and reputation consequences esteems data loss and reputation damage as significant, each accounting for 25%. Equipment damage comprises the remaining 15%, illustrating the tangible hardware losses linked with certain cyber threats. This breakdown illustrates that beyond the immediacy of technical restoration, cybersecurity incidents have enduring repercussions spanning operational, reputational, and infrastructural domains.

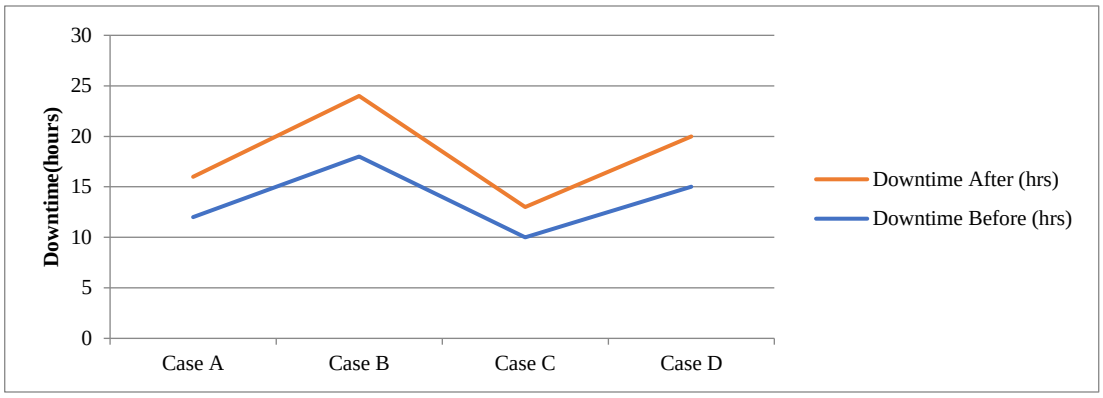

Figure 4: Operational Downtime Before and After Security Implementation

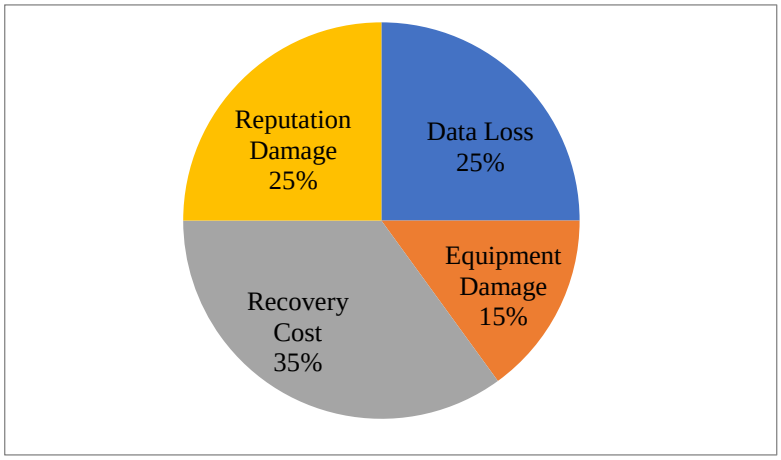

Figure 5: Cost Breakdown of Cybersecurity Incidents

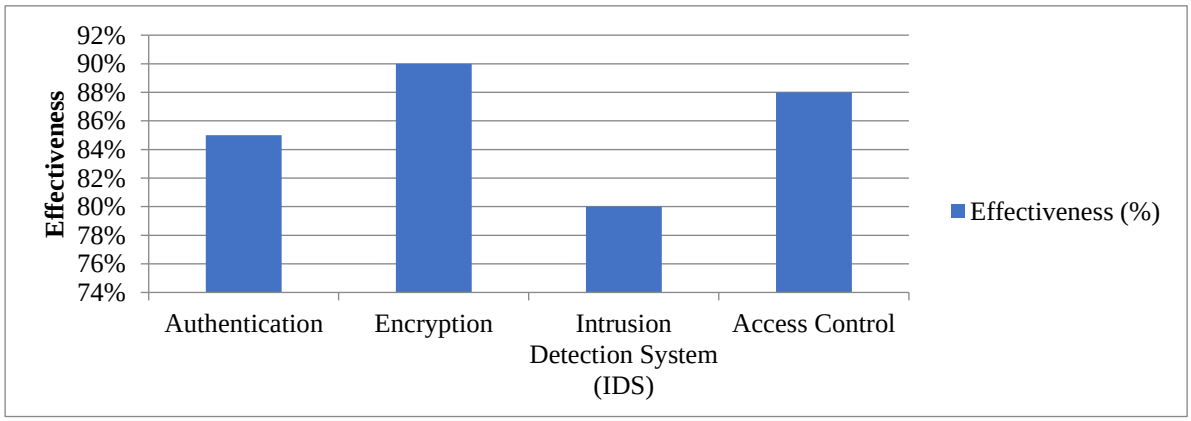

Figure 6: Effectiveness of Security Measures Across Case Studies

Figure 6 showcases how effective each security measure is across different case studies in SCADA systems for coastal power grids and offshore platforms. It also demonstrates the rank each measure holds. In this case, Encryption is the most effective measure with 90% being the rate attributed to it, proving its value within guarding the data in transmission. Access control measures comes in a close second at 88% which further emphasizes its role in the deterrence of intrusion. Authentication guarantees user's identity before granting system access which puts its usefulness at a solid 85%. While still serving a very essential purpose, Intrusion Detection Systems (IDS) do show relatively lesser effectiveness at 80%. This lackluster performance could stem from the sophistication underlying advanced threat detection. This comparison furthers the understanding of the different magnitudes each security measure has on the cyber security fortification of SCADA systems.

5 Recommendations

5.1 Most Effective Approaches for Safeguarding SCADA Systems

The protection of SCADA systems in coastal grids and offshore power stations starts with ever-deepening policies, that is, a defense-in-depth approach which is a multi-layered security strategy with barriers such as physical controls, access to the equipment, network segmentation, Strong credentials, monitoring in real-time, and others. Implementation of Zero Trust Architecture (ZTA) policies that stipulate verifying every user, and system no matters them being inside or out of the walls enhances fortification of the system. Basic system maintenance using patch management techniques takes care of symmetry gaps that would be misused by attackers especially using old systems. As bypassing security containment of modern systems become easer, stronger employee handbook policies and training sessions with materials focusing on exposure to social engineer tactics and safe access methods used on remote systems are mandatory on a periodic basis. Forming and mantainment of tested responsive actions to cyberattacks ensures swift containment allows speedy recovery while minimizing operational disruption.

5.2 Fusion of Security Components with Pre-Existing SCADA Systems

The most significant challenge with incorporating security into pre-existing SCADA systems is with older infrastructure which lacks a cybersecurity framework. The first step involves developing an asset inventory alongside a risk assessment, critical for prioritizing security improvements relative to risks associated with the SCADA assets. Encryption routers and protocol gateways that allow communication between outdated devices and modern networks can be strategically placed to enforce monitoring and covert control. VLANs along with industrial firewalls should be deployed to fence-off SCADA systems from more extensive IT networks, minimizing chances of lateral movement attacks. In the absence of confidentiality supporting native encryption, confidentiality can be granted using wrapper protocols or tunneling methods. Furthermore, integrating security tools assists organizations in acquiring logs, detecting intrusions, and responding to them in a timely manner which enhances the security of old SCADA systems.

5.3 Believed Future Research Directions

As new threats arise, use of SCADA systems needs to be constantly fortified. One promising field is Artificial Intelligence (AI) as well as Machine Learning (ML) which can be used in the identification of threats. These technologies have the ability to track activity on the SCADA network and identify anomalies associated with potential intrusions. Another area of development is the use of blockchain

technology to safeguard transactional information in SCADA frameworks, making trustless and permanent records readily accessible. The impact of 5G networks will have to examined alongside edge computing with SCADA systems further developed for remote offshore platforms with limited bandwidth. There is also the consideration of quantum computing which could make current encryption systems undergo changes. This highlights the need for strong investigation and formulation of post quantum cryptographic algorithms for control industrial systems. Lastly, cyber attacks can now be simulated and evaluate security measures using SCADA without risking physical assets undergoing any assault through the use of Digital twins.

6 Conclusion

This study was concerned with the construction and practical implementation of secure SCADA frameworks for coastal power plants and offshore power platforms. An examination of existing systems, common vulnerabilities, and contemporary cybersecurity solutions indicates the need for a more advanced comprehensive layered defense strategy in the current threat landscape. Furthermore, essential findings accentuate the need for more stringent controls to be applied, including but not limited to, strong authentication methods, encrypted communications, and advanced intrusion detection systems at the borders of intelligent SCADA systems for both new and legacy installations. Secure SCADA frameworks should not be integrated within control systems as a SCADA upgrade. Rather, they are equally, if not more important, for the operational safety, structural integrity, and efficient performance of the maritime energy infrastructure. Because of the geography and harsh operating environment of these systems, the impact of a cyberattack poses great negative results to public safety, environmental safeguard, and national energy security. Secure frameworks have proved their effectiveness in a number of case studies which strengthens the idea that the control systems stand to benefit from additional protective measures. The energy sector along with government authorities face significant issues concerning their operations. With the infusion of modern technologies, both of these sectors need to work together to implement security measures, nurture industry standards, and even support the development of new technologies such as AI threat detection systems and quantum computing encryption systems that are invulnerable to attacks. Policies should also be developed to cover the particular complexities posed by SCADA systems located in maritime or coastal regions, ensuring that infrastructure protection is proactive and resilient to future cyber attacks. Ultimately, the study supports the notion that controlling access to SCADA systems is a requirement, not in preventing access, but to protect the core operational systems involved in managing energy resources along coastal and offshore areas.

References

[1] Alcaraz, C., & Zeadally, S. (2015). Critical control system protection in the 21st century. *Computer*, 48(5), 74–83. https://doi.org/10.1109/MC.2013.69

[2] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *computers & security*, *89*, 101677. https://doi.org/10.1016/j.cose.2019.101677

[3] Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Research challenges for the security of control systems. *HotSec*, *5*(15), 1158.

[4] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, 1-27. https://doi.org/10.1016/j.cose.2015.09.009

[5] Chinnasamy. (2024). A Blockchain and Machine Learning Integrated Hybrid System for Drug Supply Chain Management for the Smart Pharmaceutical Industry. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(2), 29-40.

[6] Dhivya, S., Devashree, S., & Manosigan, C. (2023). Fake Product Identification Using Blockchain. *International Journal of Advances in Engineering and Emerging Technology*, *14*(2), 15-22. https://erlibrary.org/erl/ijaeet/article/view/ERL-231037

[7] Galloway, B., & Hancke, G. P. (2012). Introduction to industrial control networks. *IEEE Communications surveys & tutorials*, *15*(2), 860-880. https://doi.org/10.1109/SURV.2012.071812.00124

[8] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. *IEEE transactions on Industrial informatics*, *7*(4), 529-539. https://doi.org/10.1109/TII.2011.2166794

[9] Hammad, A. J., Al-Mashhadani, R. A. I. H., & Naama, L. T. A. (2022). The Impact of Strategic Human Resources Tools on Enhancing Human Competencies-An Exploratory Study for a Sample of Workers in the Salah Al-Din Education Directorate. *International Academic Journal of Organizational Behavior and Human Resource Management*, *9*(1), 23-36. https://doi.org/10.9756/IAJOBHRM/V9I1/IAJOBHRM0903

[10] Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802-1831. https://doi.org/10.1109/JIOT.2017.2703172

[11] Karnouskos, S. (2011, November). Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society* (pp. 4490-4494). IEEE. https://doi.org/10.1109/IECON.2011.6120048

[12] Khurana, H., Hadley, M., Lu, N., & Frincke, D. A. (2010). Smart-grid security issues. *IEEE Security & Privacy*, *8*(1), 81-85. https://doi.org/10.1109/MSP.2010.49

[13] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80. https://doi.org/10.1016/j.ijcip.2015.02.002

[14] Leema, A. A., Balakrishnan, P., & Jothiaruna, N. (2024). Harnessing the power of web scraping and machine learning to uncover customer empathy from online reviews. *Indian Journal of Information Sources and Services*, *14*(3), 52-63. https://doi.org/10.51983/ijiss-2024.14.3.08

[15] Liu, X., & Tang, A. (2024). A Communication Application Design Framework based on Mesh Network Architecture for Folk Song Dissemination. *International Journal of Communication Networks and Information Security*, *16*(2), 91-107. https://doi.org/10.58346/JOWUA.2024.I4.004

[16] Makkada, V., & Rai, I. (2024). Case Study: Cyber-attack on Ukrainian Power Grid. In *Information Technology Security and Risk Management* (pp. 18-24). CRC Press.

[17] Mohankumar, M., Balamurugan, K., Singaravel, G., & Menaka, S. R. (2024). A Dynamic Workflow Scheduling Method based on MCDM Optimization that Manages Priority Tasks for Fault Tolerance. *International Academic Journal of Science and Engineering*, *11*(1), 09-14. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1102

[18] Mthembu, T., & Dlamini, L. (2024). Thermodynamics of Mechanical Systems Principles and Applications. *Association Journal of Interdisciplinary Technics in Engineering Mechanics*, *2*(3), 12-17. https://ajitem.org/index.php/journal/article/view/EM23003

[19] Nithyalakshmi, V., Sivakumar, R., & Sivaramakrishnan, A. (2021). Automatic Detection and Classification of Diabetes Using Artificial Intelligence. *International Academic Journal of Innovative Research*, *8*(1), 1-5. https://doi.org/10.9756/IAJIR/V8I1/IAJIR0801

[20] Stouffer, K., Falco, J., & Scarfone, K. (2015). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16.

[21] Tan, W., Sarmiento, J., & Rosales, C. A. (2024). Exploring the Performance Impact of Neural Network Optimization on Energy Analysis of Biosensor. *Natural and Engineering Sciences*, *9*(2), 164-183. https://doi.org/10.28978/nesciences.1569280

[22] Verma, N., & Reddy, A. (2025). The Demographic Consequences of Urbanization: A Study of Changes in Family Structure and Household Composition. *Progression journal of Human Demography and Anthropology*, 1-7.

[23] Whitmore, J., & Fontaine, I. (2024). Techniques for Creating, Extracting, Separating, and Purifying Food and Feed Using Microalgae. *Engineering Perspectives in Filtration and Separation*, 28-33. https://filtrationjournal.com/index.php/epfs/article/view/EPFS24505

[24] Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE communications surveys & tutorials*, *14*(4), 998-1010. https://doi.org/10.1109/SURV.2012.010912.00035

[25] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal*, *4*(5), 1250-1258. https://doi.org/10.1109/JIOT.2017.2694844

[26] Zhu, B., Joseph, A., & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing* (pp. 380-388). IEEE. https://doi.org/10.1109/iThings/CPSCom.2011.34

[27] Zhu, Q., & Basar, T. (2015). Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems Magazine*, *35*(1), 46-65. https://doi.org/10.1109/MCS.2014.2364710

Authors Biography

Captain P. Rajendran A Master Mariner and Nautical Visionary, with an unshakable command forged over 28 years at sea, Captain P. Rajendran stands as a stalwart of maritime excellence. Having sailed across the globe on a wide spectrum of merchant vessels — including bulk carriers, general cargo ships, container vessels, Ro-Ro ships, and offshore support vessels. He was spent onboard Dynamic Positioning (DP) vessels and various supply ships, where he executed high-risk deep-sea towing and other operations with precision and expertise. Captain Rajendran has also contributed to maritime education and governance as an External Examiner for GP Rating Examinations (conducted by BEST Mumbai for the Southern Region) and for Second Mate Oral Examinations under the Directorate General of Shipping, MMD. In July 2013, he dropped anchor at AMET University, bringing his vast sea knowledge ashore. Since then, he has been passionately mentoring cadets in various subjects of Nautical Science. His core competencies include: Meteorology, Oceanography, Marine Environmental Science, Chart Work, Cargo Handling and Stowage, Rules of the Road, Ship Operation Technology in last 12 years shaping the next generation of mariners. For the past three years, he has been steering the department as Head of the Department and Course In-Charge, upholding academic standards while infusing real-world maritime acumen into the curriculum. Captain P. Rajendran's journey is not just one of sailing across oceans — it is one of navigating futures, building competence, and embodying the true spirit of a mariner.

Capt. Yeshwanth Raj, Studied ta Don Bosco High School, Chennai till Matric Exam and Pre university at MCC, Chennai. Joines Training ship Dufferin for Merchant navy training 1970 to 72. Served at sea from 1975 to 2000 in various ascending capacities and had command experience for 20 years. Took to training of cadets joining AMET University from 2000 to date. Currently serving as professor of practise. Also serving as External examiner for conducting Masters, Mates, Ratings examinations. Member of Company of Master Mariners.