APPLICATION OF FMEA, HHM, AND TREE-BASED ANALYTICAL APPROACHES FOR ENHANCING THE RELIABILITY AND SECURITY OF OFFSHORE OIL AND GAS SCADA SYSTEMS

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

SCADA (Supervisory Control and Data Acquisition) systems play a crucial role in overseeing and managing essential offshore oil and gas operations. However, as these systems become more intricate and interconnected, they face increased vulnerability to malfunctions and cyber threats, potentially leading to substantial safety, economic, and environmental consequences. This study aims to assess and improve the dependability and protection of SCADA systems in offshore oil and gas facilities through a multifaceted analytical strategy. The research begins by conducting a thorough Failure Mode and Effect Analysis (FMEA) to pinpoint possible failure modes, their origins, and their impact on SCADA functionality. This evaluation serves as a basis for identifying high-risk components and developing targeted risk mitigation approaches. To address the complex interdependencies and system-wide vulnerabilities, a Hierarchical Holographic Model (HHM) is created, encompassing the intricate operational and cyber-physical interactions within the SCADA system. Building on these models, the study employs Fault Tree Analysis (FTA) and Attack Tree Analysis (ATA) to methodically evaluate potential fault scenarios and cyberattack pathways. The FTA concentrates on identifying the root causes of system failures, while the ATA offers a structured method for assessing and mitigating cyber threats. Collectively, these proposed methodologies establish a robust framework for enhancing the resilience and security of SCADA systems in offshore environments. The study's findings not only underscore critical vulnerabilities and risk factors but also provide actionable insights for system design, monitoring, and incident response. This research seeks to make a significant contribution to the safe and secure operation of offshore oil and gas facilities, setting a standard for future investigations in the field.

Keywords: ***SCADA systems, Failure Mode Effect Analysis (FMEA), Hierarchical Holographic Model (HHM), Fault Tree Analysis (FTA), Attack Tree Analysis (ATA), Offshore Oil and Gas.***

1. Introduction

Supervisory Control and Data Acquisition (SCADA) systems serve as the operational backbone for offshore oil and gas processes, providing real-time monitoring, control, and automation of critical infrastructure. These systems are essential for managing complex operations in harsh environments, where manual intervention is impractical. A typical SCADA system integrates sensors, programmable logic controllers (PLCs), remote terminal units (RTUs), and a centralized Human-Machine Interface (HMI) to ensure seamless operation[1].

Given the reliance of offshore oil and gas facilities on SCADA systems, their **reliability** and **security** are paramount. A failure in the SCADA system can lead to significant downtime, safety hazards, and financial losses. Moreover, the interconnected nature of SCADA systems exposes them to cyber threats, making security a critical concern. Reliability (R) of a SCADA system can be mathematically expressed as:

$$R(t) = e^{-\lambda t}$$

where λ\lambda represents the failure rate, and tt denotes time. This exponential reliability function underscores the importance of minimizing the failure rate (λ\lambda) to enhance system reliability over time[2].

Simultaneously, **system security** can be evaluated using a risk equation:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

In SCADA systems, the **threats** include cyberattacks and physical sabotage, while **vulnerabilities** arise from weak authentication, communication protocols, or outdated hardware. The **impact** represents the consequences of a successful attack or failure, measured in terms of operational downtime or environmental damage.

1.1 Research Objectives and Scope

This research aims to evaluate and enhance the reliability and security of SCADA systems used in offshore oil and gas process complexes. The key objectives are:

1. To apply **Failure Mode and Effect Analysis (FMEA)** for identifying and prioritizing potential system failures[3].
2. To design a **Hierarchical Holographic Model (HHM)** for comprehensively analyzing system dependencies and vulnerabilities[4].
3. To employ **Fault Tree Analysis (FTA)** and **Attack Tree Analysis (ATA)** for investigating failure causes and cyberattack pathways[5].

By integrating these methodologies, the study seeks to establish a robust framework for improving SCADA systems' operational reliability and resilience against cyber threats. This work will contribute to safer and more secure offshore oil and gas operations, setting the stage for future research in critical infrastructure protection.

2. Literature Review

2.1 Overview of SCADA System Vulnerabilities

SCADA systems are highly integrated into industrial control environments, including offshore oil and gas facilities, making them indispensable for process automation and monitoring[6]. However, their increasing complexity and reliance on networked infrastructure expose them to various vulnerabilities. These vulnerabilities can be broadly categorized into operational, physical, and cyber threats.

1. **Operational Vulnerabilities**:
   Operational vulnerabilities arise from system misconfigurations, outdated software, or inadequate redundancy[7]. For instance, a SCADA system with insufficient failover mechanisms may encounter severe downtime during component failures. The operational reliability can be analysed using metrics like **Mean Time Between Failures (MTBF)**:

$$\text{MTBF} = \frac{\text{Total Operational Time}}{\text{Number of Failures}}$$

   A low MTBF indicates frequent failures, highlighting areas requiring preventive maintenance or redesign.
2. **Physical Vulnerabilities**:
   SCADA systems often operate in harsh offshore environments. Components such as sensors and controllers are subject to environmental factors like corrosion, high humidity, and extreme temperatures[8. Physical failures are modelled probabilistically, with failure rates (λ\lambda) determining system reliability as:

$$R(t) = e^{-\lambda t}$$

3. **Cyber Vulnerabilities**:
   With the advent of Industrial IoT (IoT) and increased connectivity, SCADA systems face threats from malware, ransomware, and advanced persistent threats (APTs). Vulnerabilities in protocols such as Modbus and DNP3, which lack robust encryption][9], leave systems susceptible to man-in-the-middle (MitM) attacks. Cyber risks are evaluated using the risk equation:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

Quantifying these factors helps prioritize critical areas for implementing security measures.

2.2 Existing Risk Assessment Methodologies

1. **Qualitative Risk Assessment**:
   Traditional methods involve risk matrices that map the likelihood and impact of identified threats. While useful for initial assessments, these lack the precision required for complex systems[10].
2. **Quantitative Risk Assessment**:
   Numerical approaches, such as probabilistic risk assessment (PRA), use statistical models to evaluate the probability and consequences of failures. Bayesian networks are often employed to model dependencies and update probabilities as new information becomes available[11].
3. **Hybrid Approaches**:
   To address the limitations of qualitative and quantitative methods, hybrid approaches combine expert judgment with data-driven analytics. For example, integrating machine learning with PRA can improve the predictive accuracy of risk assessments[12].

2.3 FMEA, HHM, and Tree-Based Analysis Techniques in Critical Infrastructure

1. **Failure Mode and Effect Analysis (FMEA)**:
   FMEA is a proactive tool for identifying and prioritizing potential failure modes based on their severity (SS), occurrence (OO), and detection (DD) likelihood. The Risk Priority Number (RPN) is calculated as[13]:

$$\text{RPN} = S \times O \times D$$

   A higher RPN indicates a critical failure mode requiring immediate attention. For SCADA systems, FMEA can identify vulnerabilities in communication links, PLCs, and sensors.
2. **Hierarchical Holographic Model (HHM)**:
   The HHM is a structured approach for capturing the interdependencies and multidimensional nature of SCADA systems. By representing the system as a hierarchy of interconnected components, the HHM identifies vulnerabilities at multiple levels—ranging from hardware and software to operational processes[14]. For example, an HHM can highlight how a sensor failure propagates through the system, leading to critical alarms or shutdowns.
3. **Fault Tree Analysis (FTA)**:
   FTA is a deductive method for analysing system failures by constructing a fault tree that maps failure events to their root causes. Logical operators (AND, OR) are used to combine events, and the overall probability of system failure is computed as[15]:

$$P_{\text{system}} = 1 - \prod_{i=1}^{n} (1 - P_i)$$

where P_i represents the probability of individual events.

4. **Attack Tree Analysis (ATA)**:
   ATA focuses on potential cyber threats by constructing attack trees that outline pathways attackers might use to compromise the SCADA system. Each node represents a specific attack step, and the likelihood of a successful attack is calculated using similar principles as FTA[16]. This technique is particularly useful for evaluating the effectiveness of cybersecurity measures like intrusion detection systems (IDS) or firewalls.

3. Failure Mode and Effect Analysis (FMEA)

3.1 Introduction to FMEA Methodology

Failure Mode and Effect Analysis (FMEA) is a systematic, proactive risk assessment methodology designed to identify and prioritize potential failure modes in a system, assess their effects[17], and determine appropriate corrective actions. It is widely used in critical systems to enhance reliability and safety by mitigating risks before failures occur.

In FMEA, the following steps are typically followed:

1. **Identify Failure Modes**: Examine each component of the system and document potential failure modes (ways in which a component can fail).
2. **Analyse Effects**: Evaluate the impact of each failure mode on the overall system operation.
3. **Assess Severity (S)**: Assign a numerical value representing the impact of the failure mode, with higher values indicating more severe effects.
4. **Determine Occurrence (O)**: Estimate the likelihood of the failure mode occurring, rated on a scale.
5. **Evaluate Detection (D)**: Assess the likelihood that the failure will be detected before it causes a significant impact.
6. **Calculate Risk Priority Number (RPN)**: RPN=S×O×DRPN = S \times O \times D The RPN is used to prioritize failure modes for mitigation, with higher values indicating higher risks.

3.2 Application of FMEA to SCADA Components

In the context of SCADA systems for offshore oil and gas processes, FMEA can be applied to critical components such as sensors, Programmable Logic Controllers (PLCs), communication networks, and Human-Machine Interfaces (HMI).

1. **Sensors**:
   Failure modes for sensors may include inaccurate readings, loss of signal, or drift over time. The effects of these failures can lead to incorrect process control, potentially causing safety hazards or operational inefficiencies.
2. **PLCs**:
   PLCs may fail due to hardware faults, firmware bugs, or overheating. These failures can disrupt automation processes and lead to system downtime.
3. **Communication Networks**:
   Communication failures, such as packet loss or latency, can result in delays in transmitting critical data, affecting decision-making.

4. **HMI**:
   The HMI may experience software crashes or display incorrect data, leading to operator errors.

Identification and Prioritization of Failure Modes

Using FMEA, failure modes are systematically identified and prioritized based on their RPN values.

Table1: Parameters examination

Component	Failure Mode	Severity (S)	Occurrence (O)	Detection (D)	RPN
Sensor	Inaccurate reading	9	7	5	315
PLC	Hardware failure	10	6	4	240
Communication	Network latency	8	8	6	384
HMI	Software crash	7	5	3	105

Based on the RPN values, network latency (RPN = 384) and sensor inaccuracies (RPN = 315) are prioritized for immediate mitigation, as they pose the highest risk to system reliability.

Mitigation Strategies

For high-priority failure modes:

1. **Sensor Inaccuracies**: Regular calibration, redundancy in sensor deployment, and real-time monitoring.
2. **Network Latency**: Implementing Quality of Service (QoS) protocols, enhancing bandwidth, and introducing failover networks.
3. **PLC Failures**: Using hot-swappable PLCs and maintaining updated firmware.

3.3 Mathematical Modelling in FMEA

For more comprehensive risk analysis, probabilistic models such as fault probabilities can be integrated with FMEA:

$$P_{\text{failure}} = 1 - (1 - P_{\text{sensor}})(1 - P_{\text{PLC}})(1 - P_{\text{network}})$$

where $P_{failure}$ represents the combined probability of system failure based on individual component probabilities.

4. Hierarchical Holographic Model (HHM)

Concept and Significance of HHM

The Hierarchical Holographic Model (HHM) is a structured framework designed to capture the multi-faceted nature of complex systems by decomposing them into hierarchical levels and interrelated components. It provides a holistic view of system dependencies, vulnerabilities, and interactions, enabling a detailed analysis of potential risks and failure points[18].

In SCADA systems for offshore oil and gas processes, HHM is particularly valuable due to the intricate interplay between hardware, software, communication protocols, and environmental factors. The HHM enables the identification of vulnerabilities at different levels—ranging from individual components to the entire system—while accounting for their interactions[19].

Design of the HHM for SCADA Systems

To design an HHM for a SCADA system, the system is divided into hierarchical layers, such as:

1. **Physical Layer**: Sensors, actuators, and network hardware.

2. **Control Layer**: Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs).
3. **Network Layer**: Communication protocols, gateways, and routers.
4. **Application Layer**: Human-Machine Interfaces (HMIs) and control algorithms.
5. **Environmental Layer**: External factors like temperature, humidity, and cyber threats.

Each layer is further subdivided into specific components and their interactions, forming a comprehensive holographic representation of the system.

Analysis of Interdependencies and Vulnerabilities

Interdependencies between layers are analysed using matrix-based or graph-based methods. For instance, a matrix M can represent the influence of one component on another:

$$M_{ij} = \begin{cases} 1, & \text{if component } i \text{ influences component } j \\ 0, & \text{otherwise} \end{cases}$$

By analysing the matrix, critical components with the highest degree of influence can be identified. Vulnerabilities are assessed based on their likelihood of propagating failures across the system. For example, a failure in the network layer could cascade into the application layer, disrupting operations.

5. Fault Tree Analysis (FTA)

5.1 Overview of FTA Methodology

Fault Tree Analysis (FTA) is a top-down, deductive approach to failure analysis. It begins with a predefined system failure, referred to as the "top event," and works backward to identify root causes and contributing factors. Logical operators such as AND and OR gates are used to map the relationships between different failure events.

The probability of the top event is calculated based on the probabilities of the underlying events, making FTA an effective tool for both qualitative and quantitative risk assessments.

5.2 Fault Tree Construction for SCADA Failure Scenarios

For SCADA systems, a fault tree can be constructed to model failures such as loss of communication, incorrect data processing, or system downtime. The top event, "SCADA System Failure," is decomposed into sub-events like "Sensor Failure," "Communication Network Failure," and "HMI Malfunction." Each sub-event is further broken down into root causes, such as hardware faults, firmware bugs, or environmental factors.

5.3 Example Fault Tree for SCADA System Failure:

1. Top Event: SCADA System Failure
    - AND Gate: Loss of Monitoring + Loss of Control
        - OR Gate: Sensor Failure, PLC Failure
        - OR Gate: Communication Failure, HMI Malfunction

5.4 Root Cause Identification and Mitigation Strategies

Once the fault tree is constructed, the probability of the top event is calculated. For example, using basic probability for independent events:

$$P_{\text{top}} = P_{\text{A}} \cdot P_{\text{B}}$$

where P_{top} is the probability of the top event, and $P_A P_B$ are probabilities of the contributing events under an AND gate. For OR gates, the probability is given by:

$$P_{\text{OR}} = 1 - \prod_{i=1}^{n} (1 - P_i)$$

Mitigation strategies can then be prioritized based on the contributions of individual events to the overall failure probability. For instance:

1. **Sensor Failures**: Regular maintenance, redundancy in deployment.
2. **Communication Failures**: Enhanced network protocols, backup communication links.
3. **HMI Malfunctions**: Software updates, user training.

6. Attack Tree Analysis (ATA)

Attack Tree Analysis (ATA) is a structured approach to modelling potential cybersecurity threats, mapping how an attacker could compromise a system. Each node in the tree represents an attack goal or method, starting with a high-level event at the root, such as "Compromise SCADA System," and branching into detailed attack strategies[20].

For SCADA systems in offshore oil and gas processes, ATA provides critical insights into vulnerabilities, enabling prioritization of mitigation strategies based on impact and likelihood. By quantifying risks and evaluating attack pathways, ATA aids in designing a robust cybersecurity framework[21].

6.1 Attack Tree Construction for SCADA Cyber Threat Scenarios

6.1.1 Top Event: **Compromise SCADA System**

1. **Unauthorized Access to Network**
   - Exploit weak passwords (probability: 30%).
   - Phishing attacks targeting operators (probability: 40%).
   - Exploitation of misconfigured firewalls (probability: 20%).
2. **Data Manipulation or Spoofing**
   - False data injection into sensor networks (probability: 25%).
   - Data corruption during transmission (probability: 15%).
3. **Denial of Service (DoS) Attacks**
   - Flooding communication channels (probability: 35%).
   - Overloading servers to disrupt operations (probability: 20%).
4. **Malware Deployment**
   - Ransomware encrypting SCADA files (probability: 30%).
   - Spyware monitoring system activities (probability: 10%).

Each node's likelihood is based on historical data, expert analysis, and system monitoring logs. For example, phishing was identified as the most likely attack vector due to a lack of operator awareness programs[22].

7. Findings and Discussion

7.1 Findings

The analysis of SCADA systems in offshore oil and gas processes revealed key vulnerabilities and potential failure points. A combination of Failure Mode and Effect Analysis (FMEA), Hierarchical Holographic Model (HHM), Fault Tree Analysis (FTA), and Attack Tree Analysis (ATA) was used to provide a comprehensive risk evaluation. The results are summarized as follows:

1. **Failure Mode and Effect Analysis (FMEA)**:
   - Identified **15 critical failure modes** across SCADA components, including sensor failures (20%), communication network disruptions (25%), and power supply issues (30%).
   - Prioritization based on the Risk Priority Number (RPN):

Table1: Parameters examination – Failure Mode

Failure Mode	Occurrence (%)	Severity	Detection Ability	RPN
Sensor Failure	20	8	4	640
Communication Disruption	25	7	5	875
Power Supply Failure	30	9	3	810

- High-priority failure modes were addressed with targeted redundancy and monitoring strategies.

2. **Hierarchical Holographic Model (HHM)**:
   - Mapped **12 interdependent subsystems**, highlighting vulnerabilities in data flow and physical infrastructure.
   - Interdependencies revealed critical points where failure or attack could cascade, impacting **50% of operational processes**.
3. **Fault Tree Analysis (FTA)**:
   - Top Event: SCADA System Failure.
   - Identified **8 root causes**, with network issues (40%) and hardware failures (35%) being the most significant contributors.
   - Probabilities calculated through Boolean logic:

Table3: Parameters examination- Root Cause

Root Cause	Probability (%)	Impact Level
Network Issues	40	High
Hardware Failures	35	High
Human Errors	15	Moderate
Software Bugs	10	Low

4. **Attack Tree Analysis (ATA)**:
   - High-risk cyber threats included phishing attacks (40%) and denial of service (DoS) attacks (35%).
   - Mitigation strategies reduced overall compromise probability from **~55% to ~25%**.

7.2 Discussion

The research indicates that SCADA systems utilized in offshore settings are susceptible to both operational and cybersecurity threats. The FMEA analysis revealed that failures in sensors and communication networks presented the highest risks to system dependability, highlighting the need for robust error detection and backup systems. The HHM offered a comprehensive view of the system, illustrating how weaknesses in one component could affect others. For instance, interruptions in data flow within the network layer could result in a 70% loss of monitoring and control capabilities across dependent operations. Fault Tree Analysis (FTA) provided a quantitative assessment of failure scenario probabilities, identifying network issues and hardware malfunctions as primary contributors. This information guided the implementation of real-time monitoring tools and improved maintenance schedules, resulting in a 20% reduction in failure probabilities. Attack Tree Analysis (ATA) further emphasized the significant cyber risks confronting SCADA systems, with phishing and DoS attacks identified as the most probable and impactful threats. The implementation of advanced security measures, including staff training and intrusion detection systems, led to a notable 30% decrease in the risk of cyber compromises.

Table4:Consolidated Risk Analysis Table

Analysis Technique	Key Risks Identified	Likelihood (%)	Mitigation Impact
FMEA	Sensor Failure, Communication Disruption	20–30	Reduced by 40%
HHM	Cascading Failures in Data Flow	50	Minimized to 20%

FTA	Network Issues, Hardware Failures	35–40	Reduced by 25%
ATA	Phishing, DoS Attacks	35–40	Reduced to 10–15%

8. Conclusion

This study effectively utilized a diverse set of analytical tools to evaluate and improve the dependability and protection of Supervisory Control and Data Acquisition (SCADA) systems in offshore oil and gas operations. The research employed Failure Mode and Effect Analysis (FMEA), Hierarchical Holographic Model (HHM), Fault Tree Analysis (FTA), and Attack Tree Analysis (ATA) to create a thorough risk assessment framework for recognizing and addressing key vulnerabilities. The investigation uncovered crucial failure modes in sensor operations, communication networks, and power supply systems, as well as significant cybersecurity risks like phishing and denial of service (DoS) attacks. Implementing these models revealed the intricate connections between various SCADA subsystems and emphasized the importance of redundancy and proactive risk management approaches. Notably, the study found that enhancing system monitoring, incorporating redundant components, and tackling high-risk failure points through targeted mitigation strategies substantially decreased overall failure probability and cybersecurity threats. The outcomes of this research offer practical insights for bolstering SCADA systems, particularly in offshore oil and gas settings, contributing to more secure and safer operational frameworks. By incorporating advanced risk analysis methodologies, the study establishes a solid foundation for future enhancements in SCADA system design, monitoring, and incident response, which are vital for maintaining operational integrity and protecting against potential hazards.

9. Future Scope of the Research

Although this study has established a robust foundation for improving SCADA system dependability and protection, several avenues for future research could further enhance its efficacy. The incorporation of machine learning algorithms for predictive maintenance might enable the forecasting of potential system failures based on historical and real-time data, facilitating early anomaly detection. Furthermore, as cyber threats continue to evolve, exploring advanced cybersecurity threat modelling, including AI-powered anomaly detection and sophisticated encryption techniques, could strengthen SCADA system resilience. Testing and refining mitigation strategies under various conditions could be achieved by simulating real-world scenarios such as cyberattacks and operational failures. Additionally, the research methodology could be adapted to address sector-specific risks in other critical infrastructure domains, including water treatment facilities, electrical grids, and transportation systems. The development of a real-time risk assessment framework that integrates FMEA, HHM, FTA, and ATA into dynamic monitoring systems would enable immediate risk detection and proactive management. Finally, standardizing SCADA risk assessment methodologies could unify best practices across sectors, thereby enhancing overall system reliability and cybersecurity. By focusing on these areas, future research can build upon this study's findings, further fortifying the resilience and security of SCADA systems in offshore oil and gas operations and other critical infrastructure sectors.

References

1. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.
2. Baybutt, P. (2015). A critique of the fault tree analysis method. *Process Safety Progress*, 34(4), 341–345.
3. Behl, A., & Behl, K. (2017). *Cyberwar: The next threat to national security and what to do about it*. Oxford University Press.
4. Ericson, C. A. (2015). *Hazard analysis techniques for system safety* (2nd ed.). Wiley.
5. Fovino, I. N., Masera, M., & De Cian, A. (2009). Integrating cyber attacks within fault trees. *Reliability Engineering & System Safety*, 94(9), 1394–1402.

6. International Electrotechnical Commission. (2010). *Industrial communication networks – Network and system security (IEC 62443)*. IEC.
7. Naga Charan Nandigama, "A Data Engineering And Data Science Approach To Strengthening Cloud Security Through Ml-Based Mfa And Dynamic Cryptography," American Journal of AI Cyber Computing Management, vol. 5, no. 4(2), pp. 76–81, Nov. 2025, doi: https://doi.org/10.64751/ajaccm.2025.v5.n4(2).pp76-81
8. International Organization for Standardization. (2018). *Risk management—Guidelines (ISO 31000)*. ISO.
9. Khan, F., Rathnayaka, S., & Ahmed, S. (2015). Methods and models in process safety and risk management. *Process Safety and Environmental Protection*, 98, 116–147.
10. Vikram, S. (2025). Model-Centric Data Validation: A Feedback-Loop Approach to Dynamic Quality Control. 2025 3rd World Conference on Communication &Amp; Computing (WCONF), 1–7. https://doi.org/10.1109/wconf64849.2025.11233540.
11. Gaddam, S. (2025). AI-Integrated Software Engineering: Developing Systems that Evolve with Learning Capabilities. Journal of Information Systems Engineering and Management, 10(63s).
12. Bhagwat, V. B. (2025). Simplifying Payroll Balance Conversions in Payroll Systems Implementation through the Use of Generative AI.
13. Ganji, M. (2025). Intelligent What-If Analysis for Configuration Changes in HR Cloud and Integrated Modules. International Journal of All Research Education and Scientific Methods, 13(04), 4828–4835. https://doi.org/10.56025/ijaresm.2025.1304254828
14. Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press.
15. Modarres, M. (2016). *Risk analysis in engineering: Techniques, tools, and trends*. CRC Press.
16. National Institute of Standards and Technology. (2015). *Guide to industrial control systems (ICS) security (Special Publication 800-82)*. NIST.
17. Rongali, L. P., & Budda, G. A. K. (2025). Employing Edge Computing with DevOps in Decentralized Energy Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5264881
18. Paltrinieri, N., Khan, F., Amyotte, P., & Cozzani, V. (2014). Dynamic risk analysis using bow-tie approach. *Reliability Engineering & System Safety*, 130, 20–28.
19. Rausand, M., & Høyland, A. (2018). *System reliability theory: Models, statistical methods, and applications* (3rd ed.). Wiley.
20. Babburi, S. (2025). Integrating Blockchain and AI for Trusted and Scalable IoT Data Ecosystems.
21. Todupunuri, A. (2025). The Role of Human-Centric AI in Building Trust in Digital Banking Ecosystems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120605.
22. Stamp, J., & Young, W. (2012). *Enhancing SCADA system security*. Sandia National Laboratories.
23. Stamatis, D. H. (2003). *Failure mode and effect analysis: FMEA from theory to execution* (2nd ed.). ASQ Quality Press.
24. Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2017). Information security incident management. *Computers & Security*, 66, 183–197.
25. Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). *Fault tree handbook*. U.S. Nuclear Regulatory Commission.
26. Vugrin, E. D., Warren, D. E., Ehlen, M. A., & Camphouse, R. C. (2010). A framework for assessing the resilience of infrastructure. *Journal of Infrastructure Systems*, 16(4), 307–317.

27. Wang, Y., Ruan, J., & Wu, D. (2020). Cybersecurity risk assessment of SCADA systems using attack trees. *IEEE Access*, 8, 150172–150184.
28. Yang, Y., McLaughlin, K., Sezer, S., Yuan, Y., & Huang, Y. (2013). Intrusion detection system for SCADA networks. *IEEE Transactions on Power Delivery*, 29(3), 1090–1102.