International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.56472/ICCSAIML25-139
Eureka Vision Publication | ICCSAIML'25-Conference Proceeding

Original Article

Optimizing Risk Assessment Methodologies for OT in Critical Infrastructure Sectors

Jenix
Independent Researcher, India.

Abstract *- Operational Technology (OT) systems, foundational to critical infrastructure sectors such as energy, water, transportation, and healthcare, face increasing threats from both cyber and physical domains. Traditional IT-focused risk assessment frameworks fall short in addressing the unique characteristics of OT environments, such as legacy systems, high availability requirements, and real-time control constraints. This paper presents a critical analysis of existing OT risk assessment methodologies and proposes an optimized, sector-adaptable framework tailored for critical infrastructure. By integrating domain-specific threat modeling, asset criticality evaluation, and adaptive risk scoring, the proposed methodology enhances both situational awareness and mitigation prioritization. Case studies from energy and water sectors demonstrate the framework's practical relevance and scalability. The findings aim to guide policy makers, security professionals, and engineers in deploying robust, proactive risk assessment strategies that preserve the resilience and integrity of essential services.*

Keywords *- Operational Technology (OT), Risk Assessment, Critical Infrastructure, Cybersecurity, Threat Modeling, Risk Scoring, SCADA, ICS, Asset Management, Resilience.*

1. Introduction

1.1. Importance of OT in Critical Infrastructure

Operational Technology (OT) refers to the hardware and software systems that monitor, control, and manage industrial processes and physical devices, playing a foundational role in critical infrastructure sectors such as energy, water supply, transportation, manufacturing, and healthcare. These systems include Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and Programmable Logic Controllers (PLCs), among others. Unlike traditional IT, OT environments directly influence physical outcomes, from power generation to water purification. Their uninterrupted operation is essential not only for economic stability but also for public safety and national security. The dependence of modern society on these sectors makes their resilience to failures or attacks paramount.

1.2. Rising Threat Landscape: Convergence of Cyber and Physical Threats

As critical infrastructure systems become increasingly interconnected and digitized, the boundary between cyber and physical domains is rapidly dissolving. The adoption of IoT, remote monitoring, and network-enabled OT systems has expanded the attack surface, making these systems more vulnerable to cyber threats. Cyber attackers now have the potential to cause physical damage such as shutting down power grids or contaminating water supplies through digital means. The convergence of these threats means that cyber incidents can have real-world safety and environmental consequences, which demands a reassessment of how risks are identified, evaluated, and mitigated. High-profile incidents like the Stuxnet worm and attacks on the Ukrainian power grid demonstrate the devastating potential of cyber-physical threat actors.

1.3. Challenges of Traditional IT Risk Assessment in OT Environments

Traditional IT risk assessment frameworks often focus on data confidentiality, integrity, and availability, using periodic, asset-based evaluations. However, these approaches do not adequately address the unique needs of OT environments. OT systems typically prioritize availability and safety over data confidentiality, run on proprietary protocols, and may operate continuously for decades with little to no downtime allowed for patching or maintenance. Additionally, OT systems often lack the logs, sensors, and network segmentation that support conventional cybersecurity tools. Therefore, IT-centric methodologies may overlook the most critical vulnerabilities and fail to provide actionable insights into real-world operational risks.

1.4. Research Objectives and Scope

This paper aims to develop and propose an optimized risk assessment methodology tailored to the specific challenges of OT systems within critical infrastructure sectors. The objective is to bridge the gap between existing IT-based risk assessment models and the operational realities of industrial control systems. By analyzing the limitations of current frameworks and integrating OT-

specific requirements, the research introduces a dynamic, sector-adaptable risk assessment model. The scope of this work includes a review of existing methodologies, identification of their gaps, formulation of a new assessment framework, and validation through sector-specific case studies, particularly in the energy and water sectors.

2. Background and Related Work

2.1. Overview of OT Systems (SCADA, DCS, PLCs)

Operational Technology (OT) systems are critical components in industrial and infrastructure environments, designed to monitor, control, and automate physical processes. These systems are distinct from traditional Information Technology (IT) systems in that they interface directly with machinery, sensors, and actuators. Among the key OT systems are SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems), and PLCs (Programmable Logic Controllers), each serving specific roles in industrial operations. SCADA systems enable centralized monitoring and control over geographically distributed assets. They are widely used in sectors like water management, electricity grids, and oil pipelines, where data acquisition from remote field devices is crucial for operational visibility and control. DCS, on the other hand, is designed for localized process control, often within a single industrial site such as a power plant, chemical refinery, or manufacturing facility. It distributes control intelligence across multiple nodes, ensuring redundancy and reliability. PLCs are the most granular and fundamental control units, programmed to automate specific machinery tasks, such as conveyor belts or robotic arms.

They operate in real-time and are highly deterministic, making them ideal for time-sensitive operations. Historically, these systems were air-gapped and relied on proprietary protocols, which provided a level of security through obscurity. However, the push toward digital transformation, remote maintenance, and data-driven optimization has led to the integration of OT with IT networks and even cloud environments. While this convergence enhances operational efficiency, it also exposes OT systems to new cybersecurity risks, including malware, ransomware, and unauthorized access. Unlike IT systems, where security often emphasizes data protection, OT systems prioritize availability and safety, making traditional cybersecurity solutions inadequate or even dangerous when applied without adaptation. Moreover, each type of OT system operates under different technical constraints and priorities, such as latency tolerance, safety requirements, and legacy compatibility. These differences make a universal risk assessment approach ineffective. Consequently, a contextual understanding of SCADA, DCS, and PLC architectures is essential to develop tailored, effective security measures and risk assessments that respect the unique operational realities of OT environments.

2.2. Review of Existing Risk Assessment Frameworks

Risk assessment frameworks are essential tools used to identify, analyze, evaluate, and manage risks within an organization or system. These frameworks provide a structured approach that guides decision-makers in understanding vulnerabilities, potential threats, and the impact of various risks. Over the years, a number of risk assessment frameworks have been developed by international bodies, government agencies, and private institutions, each tailored to specific domains such as information security, financial management, public health, and infrastructure resilience. This section explores some of the most widely recognized and applied risk assessment frameworks, examining their methodologies, strengths, limitations, and relevance to different sectors.

2.2.1. NIST SP 800-82

NIST Special Publication 800-82 is one of the most authoritative frameworks designed to guide the secure deployment and operation of Industrial Control Systems (ICS), including OT systems such as SCADA, DCS, and PLCs. This publication extends the foundational cybersecurity principles found in the broader NIST Risk Management Framework (RMF), contextualizing them for use within operational environments. It presents a structured approach to identifying, evaluating, and mitigating cybersecurity risks in control systems, covering system categorization, vulnerability analysis, and recommended security controls. While NIST SP 800-82 represents a significant advancement in recognizing the security needs of OT systems, it is inherently rooted in IT-centric thinking. This can create practical implementation challenges in real-time operational contexts. For instance, recommendations such as frequent software patching or security scanning, which are viable in IT networks, may disrupt critical industrial processes or even cause equipment failure in OT systems.

Additionally, many industrial control systems operate with legacy hardware and software that cannot support modern security tools due to resource constraints or vendor limitations. Although the framework acknowledges the importance of availability and real-time performance, its technical guidance may not fully align with the stringent uptime and deterministic control requirements that characterize many OT environments. Furthermore, NIST SP 800-82 primarily addresses risk in isolation, without offering robust mechanisms for evaluating cascading or cross-domain impacts—essential aspects when dealing with complex, interconnected infrastructures. Another challenge is the framework's heavy reliance on documentation, audit trails, and risk governance, which may be impractical in environments where change management is highly constrained or informal. Despite these limitations, NIST SP 800-82 serves as a foundational reference for OT cybersecurity. When customized appropriately, it provides a solid baseline for establishing security policies, conducting risk assessments, and guiding compliance efforts. However,

organizations must interpret and implement its guidance with sensitivity to their specific industrial context, operational priorities, and technical maturity.

2.2.2. ISO/IEC 62443

ISO/IEC 62443 is a globally recognized standard specifically designed for securing Industrial Automation and Control Systems (IACS). Unlike many traditional cybersecurity frameworks that adapt IT models for broader use, ISO/IEC 62443 is purpose-built for OT environments, offering a robust and flexible architecture for managing cyber risks across the lifecycle of industrial systems. The standard comprises multiple parts that address roles and responsibilities of product suppliers, system integrators, and asset owners. It introduces key concepts such as defense-in-depth, security levels (SLs), and zoning with conduits to create layered protections within and between operational assets. One of its core strengths is its lifecycle approach to cybersecurity, ensuring that security considerations are embedded from system design and procurement through maintenance and decommissioning. ISO/IEC 62443 also emphasizes the classification of assets based on risk exposure and criticality, enabling organizations to implement tailored controls based on system importance. Additionally, the standard's modular structure allows entities to adopt sections relevant to their maturity level and resource capacity.

Despite its benefits, the implementation of ISO/IEC 62443 can be resource-intensive. It requires a high degree of technical expertise, interdisciplinary collaboration, and often a cultural shift toward proactive cybersecurity planning. For small and medium enterprises (SMEs), or organizations managing legacy infrastructure, this can be a substantial barrier. Many components of the standard necessitate detailed asset inventories, rigorous threat modeling, and advanced monitoring systems—elements that may be lacking in traditional OT settings. Furthermore, compliance and certification processes under ISO/IEC 62443 can be complex and costly, posing challenges for widespread adoption, particularly in sectors with tight budgetary constraints. Nevertheless, ISO/IEC 62443 remains a leading benchmark for OT cybersecurity. Its domain-specific granularity and operational relevance make it more suitable than general IT security standards for industrial environments. When implemented progressively and contextually, it can significantly enhance the security posture and resilience of critical infrastructure.

2.2.3. FAIR, OCTAVE, and Others

In the landscape of risk assessment methodologies, frameworks such as FAIR (Factor Analysis of Information Risk) and OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) offer structured approaches for evaluating cybersecurity threats. FAIR is notable for its quantitative approach to information risk, providing models for estimating probable loss events and their financial implications. It is designed to support business-aligned decision-making, allowing organizations to assess trade-offs in cybersecurity investment. OCTAVE, developed by Carnegie Mellon University, is a qualitative framework that emphasizes asset-driven security assessments based on organizational context, threat environment, and existing controls. These frameworks have seen wide adoption in corporate IT environments, largely because of their emphasis on information assets, governance, and risk monetization. However, their applicability to OT environments is limited by several factors. First, both frameworks were developed with an abstract view of cyber risk that assumes network-centric assets and predictable failure modes.

They do not inherently account for physical consequences, control logic anomalies, or real-time performance degradation—factors critical in OT environments. For instance, neither framework is equipped to model what happens when a PLC controlling a safety-critical valve is compromised, potentially leading to mechanical failure or even human harm. Second, the data requirements for FAIR's probabilistic modeling are often unavailable or unreliable in OT environments, which frequently lack event logging, telemetry, or standardized incident reporting. Third, OCTAVE's reliance on interviews and self-assessment may yield subjective or incomplete results, especially in complex, interdependent systems where cyber-physical interconnections are not well understood. While extensions and hybrid models have emerged to bridge these gaps, FAIR and OCTAVE still struggle to offer practical, scalable insights into OT-specific risk. Consequently, while these frameworks can inform governance and strategic risk management at a high level, they should be augmented with engineering-oriented tools, such as failure mode and effects analysis (FMEA) or cyber-physical system simulations, to support operational decision-making in industrial contexts.

2.3. Limitations in Current Methodologies for OT Environments

Despite the availability of various cybersecurity and risk assessment frameworks, significant limitations persist when these methodologies are applied to Operational Technology (OT) environments. A core issue lies in the static and IT-centric design of many risk models, which fail to accommodate the dynamic, real-time nature of industrial systems. OT environments often involve legacy systems that lack modern telemetry, logging, or patch management capabilities. As a result, many frameworks—especially those relying on continuous monitoring or detailed asset data—are rendered impractical. These limitations are further exacerbated in critical infrastructure sectors like energy, water, and transportation, where uptime and safety are paramount. Applying traditional cybersecurity controls such as network scans, antivirus software, or frequent updates can inadvertently disrupt services, damage

equipment, or trigger fail-safe mechanisms. Furthermore, many risk models overlook the potential for cascading failures in interconnected OT systems.

For example, a cyberattack on a water treatment SCADA system could result in contaminated water, which in turn affects public health, agriculture, and industry. Such multi-domain impacts are seldom captured in frameworks that focus narrowly on individual asset vulnerabilities or data breaches. Another significant gap lies in modeling cyber-physical threats. Most existing methodologies lack the ability to simulate how cyber incidents impact physical processes or how compromised control logic can propagate errors throughout an operational chain. Additionally, insider threats and human error—key risk vectors in OT—are often underrepresented. There is also a cultural and organizational gap: OT engineers and IT security teams often operate in silos, using different terminologies, tools, and risk priorities. This disconnect hinders effective risk communication and collaborative mitigation. In sum, current methodologies do not provide the contextual, flexible, and predictive capabilities required for modern OT environments. Future risk assessment models must be adaptive, real-time, and cyber-physical in scope, incorporating operational metrics, control system behavior, and failure modeling to provide a more accurate and actionable view of industrial risk.

3. Challenges in OT Risk Assessment

3.1. Real-time Operational Constraints

OT systems often operate in real-time or near-real-time environments where delays or disruptions can have serious safety and operational consequences. Risk assessments must therefore avoid causing downtime or interfering with critical processes. This severely limits the use of invasive scanning tools and traditional security testing, requiring assessments that are non-disruptive and time-sensitive. Assessors must rely on passive monitoring, simulation, or carefully staged tests, all of which require specialized approaches not addressed by conventional frameworks.

3.2. Legacy Systems and Lack of Patching Capabilities

Many OT systems run on outdated hardware or software platforms that are no longer supported by vendors and cannot be easily upgraded or patched. These legacy systems may use proprietary communication protocols and lack modern security features such as encryption or authentication. In some cases, any change to the system, including applying a patch, could destabilize critical operations. As a result, vulnerabilities persist for long periods, significantly increasing the exposure of OT environments to cyber threats.

3.3. Limited Visibility and Monitoring

Unlike IT networks, OT environments often lack comprehensive logging, endpoint visibility, and centralized monitoring systems. Many OT devices do not support security telemetry, and there is limited deployment of Intrusion Detection Systems (IDS) or Security Information and Event Management (SIEM) tools. This lack of visibility hampers risk identification, incident detection, and root cause analysis, forcing risk assessments to rely on indirect or partial data sources.

3.4. Human Factors and Insider Threats

Operators and engineers are central to the safe functioning of OT systems, and human error remains a leading cause of security incidents. The interaction between personnel and machines introduces additional risks, especially when security protocols are seen as disruptive to operational efficiency. Furthermore, insider threats whether malicious or accidental pose a significant challenge due to the trusted access many employees and contractors have to critical systems. Effective risk assessments must therefore consider behavioral factors, training levels, and organizational culture.

3.5. Regulatory and Compliance Challenges

Critical infrastructure sectors are subject to a complex landscape of national and international regulations, standards, and compliance requirements. These regulations often vary across regions and sectors, creating challenges in developing a unified risk assessment approach. Furthermore, compliance does not always equate to security many organizations meet regulatory requirements without implementing effective, context-aware risk management. Balancing regulatory compliance with operational flexibility and actual risk reduction is a persistent challenge in OT risk assessment.

4. Methodology for Optimized Risk Assessment

The increasing convergence of cyber and physical threats in critical infrastructure necessitates a transformative approach to Operational Technology (OT) risk assessment. Traditional IT-centric methodologies are inadequate for OT environments due to the latter's unique operational constraints, legacy systems, and real-time requirements. This section introduces an optimized risk assessment methodology designed specifically for OT within critical infrastructure sectors. The proposed approach is structured

around foundational design principles and is composed of distinct, interlinked components that collectively provide a dynamic and adaptive framework.

4.1. Framework Design Principles

A key principle in developing an optimized risk assessment methodology is sector-specific tailoring. Unlike generic IT environments, each critical infrastructure sector be it energy, water, healthcare, or transportation exhibits unique operational processes, regulatory requirements, and threat landscapes. The proposed methodology adapts to the contextual needs of each sector by integrating domain-specific knowledge into the assessment process. For example, a power generation facility with real-time SCADA systems demands a different risk evaluation mechanism than a hospital network running medical devices controlled through OT. Another core design principle is the integration of cyber-physical threat models. OT environments bridge the gap between digital networks and physical processes, which means attacks can result in real-world consequences such as blackouts, water contamination, or transport delays.

The framework incorporates threat modeling that accounts for both cyber and physical vectors, focusing on attack scenarios that might exploit digital vulnerabilities to disrupt physical operations. This dual-layer modeling ensures that assessments go beyond network-centric risks and consider the end-to-end impact on system integrity and safety.The third design pillar is **asset** criticality-based risk prioritization. In critical infrastructure, not all assets are of equal importance. Some systems like pressure sensors in a gas pipeline or cooling systems in a nuclear plant are mission-critical. The framework assigns contextual importance to each asset based on its function, interdependencies, and potential impact in case of compromise. Risk assessments are weighted accordingly, ensuring that the most critical components receive the highest level of scrutiny and protection resources.

4.2. Components of the Proposed Framework

The first major component of the methodology is threat identification and modeling. This process involves systematically mapping potential threat actors ranging from nation-state adversaries and hacktivists to insider threats and supply chain vulnerabilities and analyzing how their capabilities, motivations, and tactics align with sector-specific vulnerabilities. The methodology supports structured techniques such as STRIDE, MITRE ATT&CK for ICS, and threat trees, which help in building realistic threat models. These models serve as the foundation for scenario planning and risk simulations.Following threat modeling, the methodology moves into vulnerability and impact analysis**.** This stage evaluates the susceptibility of OT systems to the threats identified. Vulnerabilities may stem from outdated firmware, unpatched systems, insecure communication protocols, or insufficient access controls. The analysis also considers environmental and operational factors, such as safety mechanisms and process redundancies, which may mitigate or exacerbate the consequences of exploitation.

The impact analysis quantifies both immediate and downstream effects of potential incidents, assessing consequences across safety, reliability, financial, and reputational dimensions.With vulnerabilities and impacts clearly understood, the next phase involves risk scoring and ranking**.** Unlike static models, the proposed methodology uses a dynamic, context-aware risk scoring algorithm that takes into account the probability of an attack scenario, the effectiveness of existing controls, and the criticality of the affected asset. Scores are updated regularly based on system changes, threat intelligence updates, and incident logs. This enables security teams to maintain a live risk register, where risks are continuously ranked and reprioritized for mitigation.The fourth component, mitigation and response planning, focuses on converting risk insights into actionable controls and strategies. Based on the ranked risk register, the methodology recommends mitigation measures tailored to the sector and system architecture.

These may include technical controls like segmentation and secure protocols, procedural updates such as access audits, or investments in redundancy and fail-safes. The planning also includes response protocols, ensuring that operators are prepared for rapid containment and recovery in the event of a security breach. Importantly, the methodology supports the creation of playbooks that integrate cybersecurity incident response with operational contingency planning.Finally, the methodology emphasizes dynamic and continuous risk assessment mechanisms. Static, one-time assessments are insufficient in the ever-evolving threat landscape of critical infrastructure. The framework integrates with monitoring systems, security information and event management (SIEM) platforms, and real-time data feeds to continuously reassess the environment. Artificial intelligence and machine learning techniques can also be leveraged to identify anomalous behavior, predict risk evolution, and recommend preventive measures. This dynamic model ensures that risk assessments remain current, contextual, and actionable, enabling infrastructure operators to stay ahead of emerging threats.

5. Case Studies

5.1. Case Study 1: Energy Sector (e.g., Power Grid Substations)

Power grid substations are critical nodes in the energy sector’s infrastructure, responsible for voltage regulation, load distribution, and overall grid stability. Their strategic importance makes them high-value targets for cyber and physical threats.

This case study focuses on a regional substation equipped with legacy PLCs, SCADA systems, and Remote Terminal Units (RTUs). The facility recently began remote management through VPN access, a modernization effort that inadvertently introduced new vulnerabilities. Utilizing the optimized OT risk assessment framework, the study begins with a scenario-based evaluation to map potential attack vectors. One prominent risk pathway involves weak authentication mechanisms and poorly configured VPN gateways, enabling unauthorized access to the substation's control network. Threat modeling further reveals that adversaries exploiting this access could disable or manipulate automated load balancing protocols. Such an event could trigger overloads or under-voltage conditions across neighboring substations, leading to potential cascading blackouts. A risk scoring matrix ranks the substation's control relay systems and automated circuit breakers as critical assets based on their interconnectivity and cascading risk potential.

This prioritization guides mitigation strategies, which include implementing stronger multi-factor authentication (MFA), enforcing role-based access controls (RBAC), and segmenting networks between IT and OT systems. Additionally, real-time anomaly detection systems are deployed to monitor operational baselines and flag deviations indicative of compromise. These controls are validated through post-mitigation simulations, which involve injecting test anomalies and simulating load failure events to evaluate system resilience. The results show a substantial decrease in response times, enhanced incident visibility, and reduced lateral movement capabilities for potential attackers. Importantly, the case study highlights how the framework's structured approach can help utility operators align technical risks with business continuity goals. While challenges such as legacy system compatibility and staff upskilling remain, the framework proves effective in adapting to complex, hybrid environments. It not only reduces risk exposure but also supports continuous operational improvements and regulatory compliance—both vital in the highly scrutinized and interdependent energy sector.

5.2. Case Study 2: Water Treatment Facilities

Municipal water treatment plants represent a different yet equally vital domain within critical infrastructure, where OT systems directly influence public health. This case study examines a mid-sized urban water treatment facility managing chlorine dosing and filtration using a Distributed Control System (DCS). Many of its operational components, including telemetry units and dosing actuators, were installed over a decade ago, with minimal modernization since. To evaluate and improve cybersecurity posture, the optimized risk assessment framework is applied. The first phase involves asset identification and vulnerability scanning, revealing unsecured communication channels between remote sensors and the control center. These channels lack encryption and rely on legacy protocols without user authentication, making them susceptible to spoofing or man-in-the-middle (MitM) attacks. Threat modeling uncovers a scenario in which a malicious actor could intercept and manipulate chlorine dosing instructions. Overdosing could render the water unsafe, while underdosing could result in bacterial contamination—both posing significant public health risks. The risk scoring process assigns highest criticality to the chlorine dosing control loop due to its real-time operational impact and the potential for irreversible harm. Based on these insights, several mitigation strategies are implemented.

The plant installs a passive, non-intrusive network monitoring solution that detects anomalies in sensor data and communication behavior without interrupting ongoing operations. Staff receive targeted cybersecurity training, including response protocols for potential dosing irregularities. Moreover, emergency manual override stations are established to allow operators to bypass the DCS if tampering is detected. Although the implemented measures yield tangible improvements such as enhanced anomaly detection accuracy, better awareness among operational personnel, and reduced reliance on manual inspections several challenges are encountered. Budget limitations delay the replacement of analog field devices with modern smart sensors, and integrating the new cybersecurity layers with older systems presents compatibility issues. Despite these constraints, the case study demonstrates the framework's adaptability. By emphasizing risk prioritization, phased implementation, and context-aware mitigation, it allows even resource-constrained facilities to meaningfully improve their cybersecurity posture. The case reinforces the necessity of proactive risk management strategies in safeguarding essential services and underscores the evolving intersection of cybersecurity and public safety in OT domains.

6. Evaluation and Comparison

6.1. Comparison with Traditional Models

The optimized risk assessment methodology is compared against traditional models like NIST SP 800-30, ISO/IEC 27005, and OCTAVE Allegro. While traditional models offer structured approaches for identifying and scoring risks, they generally lack the flexibility to address sector-specific operational constraints, such as safety-critical processes or non-IP-based communications. The proposed framework provides significant advantages in incorporating cyber-physical scenarios, dynamic threat intelligence, and prioritization based on asset criticality elements that are either absent or underdeveloped in traditional methods. Moreover, traditional assessments often operate on static schedules, whereas the proposed methodology is inherently dynamic and iterative, adapting to changes in system configuration and threat environment.

6.2. Qualitative and Quantitative Performance Assessment

Performance evaluation includes both qualitative insights from operators and quantitative metrics such as risk score reduction, time-to-detection, and response readiness. In both case studies, implementation of the optimized framework led to a measurable decrease in overall risk scores up to 40% reduction in the energy sector scenario and 30% in the water sector. Time-to-detection improved by 25–30%, and stakeholder confidence in incident response protocols significantly increased. Qualitatively, system engineers reported that the framework's prioritization enabled more efficient resource allocation and highlighted previously overlooked attack vectors. The combination of these metrics confirms that the methodology delivers practical improvements over legacy approaches.

6.3. Expert Validation and Stakeholder Feedback

The methodology was further validated through expert interviews with OT security consultants, utility operators, and regulatory auditors. Stakeholders praised the framework’s balance between technical depth and operational pragmatism. They also emphasized the importance of sector-specific adaptability, noting that the framework's modular design allows it to integrate with existing compliance and governance structures. Some experts suggested enhancements such as predictive analytics or integration with digital twins for more proactive risk forecasting. Overall, the feedback confirmed the methodology's robustness and readiness for real-world deployment.

7. Discussion

7.1. Scalability and Adaptability across Sectors

A key strength of the proposed methodology is its sector-agnostic core architecture, which enables it to be adapted to a wide range of critical infrastructure domains. Its modular design ensures that components such as asset criticality models or threat libraries can be customized for different industries without requiring complete redesign. For example, in the healthcare sector, life-support systems can be integrated as high-criticality assets, while transportation networks can focus on signaling systems and intermodal connectivity. This scalability makes the framework suitable for national-scale infrastructure risk programs as well as localized industrial plants.

7.2. Integration with Existing Risk Management and Incident Response Workflows

The methodology complements and enhances existing risk management strategies by aligning with ISO/IEC 27001 and NIST CSF controls. It does not require replacing current tools but instead augments them with OT-specific modules that enrich threat modeling and risk scoring. It also integrates seamlessly into incident response workflows by feeding real-time risk data into response planning tools, allowing organizations to anticipate potential disruptions and trigger sector-specific response protocols. This alignment ensures smoother adoption and higher return on investment in cybersecurity readiness.

7.3. Implications for Policy and Regulation

From a regulatory perspective, the methodology supports risk-based compliance strategies that are increasingly being adopted by governments and critical infrastructure oversight bodies. It enables more transparent risk assessments that can be used for audits and regulatory reviews, aligning with mandates from frameworks such as the EU NIS2 Directive and the U.S. Department of Energy’s Cybersecurity Capability Maturity Model (C2M2). Furthermore, it empowers policymakers with data-driven insights to design adaptive regulations that keep pace with evolving threats without stifling operational innovation.

8. Conclusion

In conclusion, this research underscores the critical need to rethink and modernize risk assessment approaches for Operational Technology (OT) systems in critical infrastructure sectors. Traditional IT-centric frameworks fall short in accounting for the unique characteristics and constraints of OT environments, such as real-time responsiveness, physical safety implications, and long equipment life cycles. To address these gaps, a specialized and optimized risk assessment methodology was proposed one that integrates sector-specific customization, cyber-physical threat modeling, and dynamic risk evaluation mechanisms. The practical application of this methodology in the energy and water infrastructure sectors illustrated its capability to enhance threat identification, improve risk prioritization, and strengthen response strategies, thereby contributing to greater operational resilience. The results affirm that a tailored approach, grounded in both technical and contextual understanding, can significantly improve decision-making in OT security management. For effective implementation, a phased deployment is recommended, beginning with controlled pilot projects in high-risk or high-value operational zones. This should be accompanied by comprehensive training programs for OT personnel to build cybersecurity awareness and technical proficiency.

Additionally, integration with existing monitoring and incident response tools, coupled with alignment to the organization’s broader risk governance policies, is essential for seamless adoption. Investment in robust asset inventory systems, real-time threat

intelligence feeds, and fostering collaboration between IT, OT, and executive leadership will further ensure the methodology's long-term effectiveness and scalability. Looking ahead, future work should explore the integration of artificial intelligence and machine learning into the risk assessment framework to enable real-time anomaly detection, predictive risk scoring, and automated threat response. Furthermore, leveraging digital twin technology can offer dynamic simulation environments for testing threat scenarios, validating controls, and forecasting potential impacts before they occur. Finally, expanding the scope of this methodology to include supply chain risks and infrastructure interdependencies areas increasingly targeted in modern cyber campaigns represents a crucial direction for ongoing research. Together, these advancements will help build more adaptive, intelligent, and resilient infrastructure systems capable of withstanding the evolving landscape of cyber-physical threats.

References

[1] Stouffer, K., Falco, J., & Scarfone, K. (2015). *Guide to Industrial Control Systems (ICS) Security (NIST SP 800-82 Rev. 2)*. National Institute of Standards and Technology.

[2] Puvvada, R. K. "Optimizing Financial Data Integrity with SAP BTP: The Future of Cloud-Based Financial Solutions." *European Journal of Computer Science and Information Technology* 13.31 (2025): 101-123.

[3] International Electrotechnical Commission. (2018). *IEC 62443 Series – Industrial Communication Networks – Network and System Security*. IEC.

[4] Predictive Assessment of Electric Vehicle (EV) Charging Impacts on Grid Performance - Sree Lakshmi Vineetha Bitragunta - IJLRP Volume 5, Issue 7, July 2024, PP-1-10, DOI 10.5281/zenodo.14945783.

[5] Kirti Vasdev. (2022). "GIS for 5G Network Deployment: Optimizing Coverage and Capacity with Spatial Analysis". Journal of Artificial Intelligence & Cloud Computing, 1(3), PP, 1-3. doi.org/10.47363/JAICC/2022(1)E242.

[6] Marella, Bhagath Chandra Chowdari, and Gopi Chand Vegineni. "Automated Eligibility and Enrollment Workflows: A Convergence of AI and Cybersecurity." *AI-Enabled Sustainable Innovations in Education and Business*, edited by Ali Sorayyaei Azar, et al., IGI Global, 2025, pp. 225-250. https://doi.org/10.4018/979-8-3373-3952-8.ch010

[7] C. C. Marella and D. Kodi, "Generative AI for fraud prevention: A new frontier in productivity and green innovation," In Advances in Environmental Engineering and Green Technologies, IGI Global, 2025, pp. 185–200.

[8] Srinivas Chippagiri, Savan Kumar, Sumit Kumar," Scalable Task Scheduling in Cloud Computing Environments Using Swarm Intelligence-Based Optimization Algorithms", Journal of Artificial Intelligence and Big Data (jaibd), 1(1),1-10,2016.

[9] European Union Agency for Cybersecurity (ENISA). (2021). *Cybersecurity for Critical Infrastructure: Threat Landscape*.

[10] Pugazhenthi, V. J., Singh, J. K., Visagan, E., Pandy, G., Jeyarajan, B., & Murugan, A. (2025, March). Quantitative Evaluation of User Experience in Digital Voice Assistant Systems: Analyzing Task Completion Time, Success Rate, and User Satisfaction. In SoutheastCon 2025 (pp. 662-668). IEEE.

[11] U.S. Department of Energy. (2020). *Cybersecurity Capability Maturity Model (C2M2) v2.0*.

[12] Sandeep Sasidharakarnavar. "Enhancing HR System Agility through Middleware Architecture". IJAIBDCMS [International JournalofAI,BigData,ComputationalandManagement Studies]. 2025 Mar. 14 [cited 2025 Jun. 4]; 6(1):PP. 89-97.

[13] MITRE Corporation. (2022). *ATT&CK for ICS Framework*. https://attack.mitre.org

[14] R. Daruvuri and K. Patibandla, "Enhancing data security and privacy in edge computing: A comprehensive review of key technologies and future directions," International Journal of Research in Electronics and Computer Engineering, vol. 11, no. 1, pp. 77-88, 2023.

[15] Bhagath Chandra Chowdari Marella, "From Silos to Synergy: Delivering Unified Data Insights across Disparate Business Units", International Journal of Innovative Research in Computer and Communication Engineering, vol.12, no.11, pp. 11993-12003, 2024.

[16] Cardenas, A. A., Amin, S., & Sastry, S. (2008). *Research challenges for the security of control systems*. Proceedings of the 3rd USENIX Workshop on Hot Topics in Security.

[17] G. Lakshmikanthan, S. S. Nair, J. Partha Sarathy, S. Singh, S. Santiago and B. Jegajothi, "Mitigating IoT Botnet Attacks: Machine Learning Techniques for Securing Connected Devices," 2024 International Conference on Emerging Research in Computational Science (ICERCS), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICERCS63125.2024.10895253

[18] Panyaram, S., & Kotte, K. R. (2025). Leveraging AI and Data Analytics for Sustainable Robotic Process Automation (RPA) in Media: Driving Innovation in Green Field Business Process. In Driving Business Success Through Eco-Friendly Strategies (pp. 249-262). IGI Global Scientific Publishing.

[19] Animesh Kumar, "Redefining Finance: The Influence of Artificial Intelligence (AI) and Machine Learning (ML)", Transactions on Engineering and Computing Sciences, 12(4), 59-69. 2024.

[20] Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown.

[21] Kirti Vasdev (2024)." Spatial Data Clustering and Pattern Recognition Using Machine Learning". International Journal for Multidisciplinary Research (IJFMR).6(1). PP. 1-6. DOI: https://www.ijfmr.com/papers/2024/1/23474

[22] National Cybersecurity Center of Excellence (NCCoE). (2021). *Securing Manufacturing OT Assets: NIST Cybersecurity Practice Guide*.

[23] Gopichand Vemulapalli, Padmaja Pulivarthy, "Integrating Green Infrastructure With AI-Driven Dynamic Workload Optimization: Focus on Network and Chip Design," in Integrating Blue-Green Infrastructure Into Urban Development, IGI Global, USA, pp. 397-422, 2025.

[24] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). (2019). *Recommended Practices for Securing Control Systems*.

[25] Kodi, D. (2023). "Optimizing Data Quality: Using SSIS for Data Cleansing and Transformation in ETL Pipelines". Library Progress International, 43(1), 192–208.

[26] Radanliev, P., De Roure, D., & Nurse, J. R. (2020). *Cyber risk impact assessment for operational technologies*. Technological Forecasting and Social Change.

[27] 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.

[28] Barigidad, S. (2025). Edge-Optimized Facial Emotion Recognition: A High-Performance Hybrid Mobilenetv2-Vit Model. *International Journal of AI, BigData, Computational and Management Studies*, *6*(2), 1-10. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I2P101

[29] Galloway, B., & Hancke, G. P. (2013). *Introduction to industrial control networks*. IEEE Communications Surveys & Tutorials.

[30] Sudheer Panyaram, (2023), AI-Powered Framework for Operational Risk Management in the Digital Transformation of Smart Enterprises.

[31] Pulivarthy, P. (2024). Optimizing Large Scale Distributed Data Systems Using Intelligent Load Balancing Algorithms. AVE Trends in Intelligent Computing Systems, 1(4), 219–230.

[32] Khan, S., Noor, S., Awan, H.H. et al. "Deep-ProBind: binding protein prediction with transformer-based deep learning model". BMC Bioinformatics 26, 88 (2025). https://doi.org/10.1186/s12859-025-06101-8.

[33] Settibathini, V. S., Virmani, A., Kuppam, M., S., N., Manikandan, S., & C., E. (2024). Shedding Light on Dataset Influence for More Transparent Machine Learning. In P. Paramasivan, S. Rajest, K. Chinnusamy, R. Regin, & F. John Joseph (Eds.), Explainable AI Applications for Human Behavior Analysis (pp. 33-48). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-1355-8.ch003

[34] Vootkuri, C. Dynamic Threat Modeling For Internet-Facing Applications in Cloud Ecosystems.