Secure and Resilient Engineering Software in Critical Infrastructure: Cyber-Physical Threats and Risk Mitigation Strategies

Md Nazmul Hoque
[1]*Lead Sofware EngineerHarris Digital,,Bangladesh*
nazmul@harrisdigital.io

Abstract

As cyber-physical systems become increasingly prevalent in critical infrastructure (e.g., the power grid, water facilities, transportation networks and industrial control systems), so does the requirement for secure and resilient engineering software. While digital transformation is accelerated through IoT, AI-driven automation and cloud enablement of supervisory control, these connected systems are vulnerable to attack – and nations face greater risks than ever before – from data breaches, malware attacks or disruption to operational processes. In this paper, we discuss the architecture, threat model and mitigation techniques when designing software for critical infrastructure. It also examines which software design and system integration gaps are used by cyber-physical threats. The focus is on robust security systems that incorporate secure coding, zero-trust severity, real anomaly detection and recovery procedures. By synthesizing recently published empirical studies (2020–2025), this study identifies best practices and technological interventions—e.g. digital twins, AI-based threat modelling, and blockchain for data integrity—that contribute to software resilience.

Keywords: Resilience, Cybersecurity, Integration, Mitigation, Infrastructure

INTRODUCTION

The threat environment has increased in the frequency and level of strategic intent. Ransomware and supply-chain intrusions remain among the most financially damaging incident types, as state-sponsored actors seek to engage ransomware victims from key perspectives (pre-position for follow-on attacks) or operate extortive models themselves. In 2024, U.S. and allied agencies alerted that Volt Typhoon actors had compromised multiple critical infrastructure organizations within communications, energy,transportation, and water sectors with a focus on living-off-the-land tradecraft to evade detection as well as maintain persistence. Advisories such as these serve to illustrate the potential for connected multi-sector but relatively contained disruption rather than isolated IT failure. CISA+2U.S. Department of War+2 The impact on operations and society from previous incidents—such as the May 2021 ransomware attack against a Colonial Pipeline that resulted in regional fuel supply shortages and emergency response, demonstrate how software-centric failures in supporting systems can cascade to disrupt physical service delivery. The Department of Energy's Energy. gov+1

At the same time, defenders confront rapidly expanding capability gaps. ENISA's Threat Landscape 2024 recalls ongoing trends — ransomware, availability attacks and data-focused extortion, now exacerbated by geopolitical frictions and the adversaries' increased operational experience within OT-adjacent intrusion chains. 2025 visions for the global similarly include a major role of cyber insecurity to macro risk, and systemic exposure due to interdependent supply chains as well as legacy portions that are neither patched nor replaced easily. securitydelta. nl+2World Economic Forum Reports+2 Engineering software lies at the intersection of this problem: CAD/CAE, SCADA/EMS/DCS platforms, configuration tools, firmware updaters and digital-twin pipelines all connect development and operations. Poor identity and update methods, lack of code provenance and flat trust zones can allow attackers to bridge the 'enterprise' IT to OT divide through credentials, remote access services, and third party plugins—the exact vectors enumerated in recent advisories and case studies. NIST CSRC+1

The standards and baseline controls have adapted to reflect these realities. The ISA/IEC 62443 series addressees lifecycle requirements for secure product development (suppliers), integration (service providers), and operation (asset owners) as well as security levels, zoning/conduits, and secure-by-design expectations for engineering software and devices. In the U.S., CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) condense a prioritized baseline (e.g., strong authentication, asset inventory, immutable logging, tested backup/restore, and vendor access controls) for critical infrastructure operators having differing levels of maturity. With NIST SP 800-82 Rev. 3, these architectures provide a language for risk management and quantifiable resilience in cyber-physical systems. isa. org+2CISA+2

Yet significant gaps remain. First, we find weak and inconsistent attestation, SBOM transparency, and update assurance across OT-adjacent supply chains (installers, license servers, scripting ecosystems, simulation toolchains, and vendor portals), leaking such seams is how adversaries will stage access to OTARC without initially touching safety-critical controllers. Second, engineer and vendor identity and access can be preserved by shared and always-on accounts that contradict time-bounded, policy-enforced monitored access (per zero-trust

guidance). Third, due to the realtime nature and safety constraints in OT, detection and response for OT is not as agile as IT playbook reaction—yet organizations need process-aware anomaly detection that operates under physical limits to ensure no hold-onto-safety mechanisms (trips) versus retaining fidelity against very lowand-slow activity. These deficits are repeatedly underscored in public guidance and incident retrospectives, however empirical sector-specific software stack Implementation patterns for engineering remain under-recorded. NIST CSRC+2ENISA+2

This article fills those voids by (i) elaborating a code-oriented threat model for cyber-physical realms (with focus on engineering tools as trust anchors and traversal bridges), (ii) abstracting NIST SP 800-82 Rev. 3, IEC 62443, and CISA CPGs into an actionable resilience roadmap for engineering software (secure development, code signing/attestation, identity orchestration, segmented deployment, process-aware monitoring and recoverability), (iii) suggesting assessment criteria and metrics—mean-time-to-detect in OT-safe mode recovery time to verified steady-state control loop integrity scores—that map to recent threat advisories and sector risk outlooks. By anchoring the conversation to current events and best practices for up through 2025, the introduction starts by making the argument for a pragmatic, defense-in-depth model to protect vital services in an age where digitized interdependence is everywhere.

LITERATURE REVIEW

Cyber-physical threatscape for critical infrastructures

In energy, water, transportation and manufacturing, engineering software now intercedes in sensing, actuation and optimization within closely coupled cyberphysical systems (CPS). This convergence broadens the attack surface and alters defender tradeoffs (e.g., security, predictability, and availability). NIST's Guide to Industrial Control Systems (ICS) Security is reframing "ICS security" as OT security, documenting common ST topologies, vulnerabilities (flat networks, un-authenticated/proprietary protocols, outdated assets), and compensating controls for dynamic process environments. NIST CSRC

Broader misuse of technology — In the public threat reporting since 2023, ransomware evolved from a spray-and-pray IT target to pre-positioning in critical services using "living-off-the-land" methods and OT-adjacent lateral moves. In a joint advisory, called Volt Typhoon, the agencies warn that PRC-state actors targeted 23 US critical infrastructure entities across communications, energy, healthcare, finance and water systems but including smaller local governments blending stealthy reconnaissance with the more brazen theft of credentials and hands-on-keyboard persistence to give them options for disruption during times of crisis. CISA+2 CISA+2 ENISA Threat Landscape 2024 also lists highest are ransomware, availability attacks and data-centric extortion with digital supply chains raising critically infrastructure risk by geopolitical tensions. ENISA While both historical and modern day (Industroyer/CrashOverride, and Industroyer2) grid sabotage campaigns offer proof that attackers are capable of directly communicating with substation equipment, or at gird protocols, there is a need for more processaware defenses. WIRED+2WeLiveSecurity+2

Frame and reference standards of engineering software once used in OT

48, 54] The ISA/IEC 62443 series is the most widely referenced standard end-to-end standard for IACS systems, including secure development (for suppliers), integration (service providers), and operation (asset owners), as the concepts of security levels, zone-and-conduit segmentation, and lifecycle governance are directly applicable to engineering software and components. isa. org Inside of 62443, IEC 62443-4-1 prescribes a secure development lifecycle for industrial products, mapping vendor responsibilities (thresholds, threat modeling, code scan processes and patching) against deployment interpretations in OT." isasecure. org For the power systems domain in particular, IEC 62351 his provides prescriptions for securing TC57 protocol families (IEC 60870-5/-6, IEC 61850,CIM), providing advice on authentication, encryption and key management to toughen SCADA/EMS/DMS communication. IEC+1

In conjunction with sector and product standards, MITRE ATT&CK for ICS organizes attacker behaviors against industry assets through tactics and techniques, so that detected incidents can be mapped to detection and response strategies in the engineering environment (e.g., firmware modification, program download, alteration of control logic). MITRE ATT&CK+1 NIST SP 800-82 Rev. 3, which combines these views into a riskaware OT position and further focuses on zone-based segmentation, tight remote access control, and safety-informed resilient incident response. NIST CSRC

3. Software supply-chain and provenance risks in OT toolchains

High-impact compromises are exploiting software supply chains like never before — build systems, updaters, vendor portals, installers, license servers and plugins that straddle IT and OT. NIST also defined what it calls its Secure Software Development Framework (SSDF) SP 800-218, a set of secure development practices (threat modeling, third-party intake, code signing, vulnerability disclosure and tamper-resistant builds) that engineering-software vendors can take to minimize latent defect and tampering risk. NIST Publications+1 Provenance framework like SLSA (Supply-chain Levels for Software Artifacts) defines proof levels of build's integrity and a provable source—In testament these capabilities are being embraced increasingly by major CI/CD platforms—can be applied to engineering software deliverables and firmware as well. SLSA+1 Simultaneously, NIST SP 800-161, Rev. 1 expands C-SCRM across the organization, connecting acquisition, contracting and lifecycle controls to technical processes such as SBOM intake/verification. NIST CSRC+1

SBOMs have evolved from what the NTIA called "minimum elements" in 2021 toward CISA's update in 2025, which narrows down data fields and operations expectations (e.g. automation, tooling, vulnerability correlation). Critical-infrastructure operators benefit from SBOM programs by increasing asset/software visibility for engineering workstations, HMI, and PLC tooling, and better exposure triage. ntia. gov+1 DOD/CISA guidance on SBOM management tools delineates capabilities (e.g., version normalization, VEX processing, and change tracking) that asset owners can specify for use by industrial vendors. U.S. Department of War

Identity, Homley et al. patterns for all access and zero trust for CPS

Long-standing concessions tend to be dependent on a poor identity hygiene (shared/vendor accounts, always-on VPNs, flat trust). CISA Zero Trust Maturity Model v2. 0 is a pragmatic

playbook—identity-based controls (strong auth, just-in-time access), micro-segmentation and persistent device posture—that can be suitably modified for engineering networks and remote vendor access, addressing the latency and availability constraints inherent to OT. CISA+1 CISA's Secure-by-Design/SecurebyDefault initiative with international partners builds on development of software where manufacturers ship default hardened configurations (e.g., MFA enforced, logging on), taking responsibility for the security outcomes—especially meaningful in engineering-software stacks often historically loosely configured to make life easy. CISA+1

Detection: Digital twins and AI for resilience

As aggressive containment can be dangerous in OT safety, and so the detection must be aware of the process. More recently the literature overviews machine-learning and time-series-based methods for ICS anomaly detection but mainly highlights challenges such as insufficient labeled data, class imbalance and physical-informed threshold creation. These publications suggest the use of simulation/testbed data and hybrid approaches with an explainable component to prevent false trips—a prerequisite in engineering-driven software environments. MDPI+1

Digital twins – virtualized, data-driven simulacra of assets and processes – are emerging as a key asset in the array of mechanisms that organizations can adopt to enhance cyber-resilience: validating control-logic changes safely before deploying, "what-if" scenario testing, training/incident rehearsal etc. A 2024 bibliometric review of digital twins in critical infrastructure identifies ongoing wins with twin use for reliability management, resilience optimization, maintenance and security –across industries while pinpointing the need for effective integration patterns and governance models related to twin-driven cyber-security. MDPI Technical and policy communities (e.g., ECSO; EU research project the DT-enhanced lifecycle security, defense-in-depth testing for ci tical systems) also suggest capabilities directly targeted at engineering-software ch nge management. ECSO+1

Sector evidence: water and energy

The water and wastewater sector's exposure to focused exploitation demonstrates how fundamental vulnerabilities in engineering designs can be exploited. The related CISA alert on Unitronics PLCs specifically mentioned internet-exposed HMIs, default creds and inadequate segmentation—engineering software deployment and remote management all the way—and possible mitigations (unique creds, port changes, VPN with MFA, network isolation). CISA A later joint advisory attributes similar compromises to IRGC affiliated actors, highlighting nation-state focus on local government services and basic misconfigurations. CISA

For electric power systems, the authors have identified substation and SCADA being attacked by protocol-aware malware and living-off-the-land operations. Standards such as the 62351 series supply specific metrics when it comes to securing IEC 61850/CIM and other TC57 protocols; combine this with 62443 zoning and products for secure development, and engineering tools that communicate with protective relays and bay controllers will be held to a higher standard. RiskInsight+1 Compliance drivers for asset identification, access control and change management over BES Cyber Systems cyber assets under NERC CIP requirements (North

America) further extend governance requirements pertaining to Engineering Workstations and software upgrades. techtarget. com

7. From protection to resilience: cyber-informed engineering

Emerging literature is company to highlight so-called Cyber-Informed Engineering (CIE)— the integration of adversary-informed design choices (e.g., engineering safety interlocks, manual fallbacks, non-cyber fail-safes) such that physical outcomes are bounded even when cyber controls fail. National CIE Strategy from DOE Adopted consensus among USDA WECC national labs (INL) Core domain producers, consumers Patterns are direct mappings to engineering selection, integration and operation of software (e.g., default-deny on remote change; authenticated/attested logic load; engineered "safe-states"; quality review on recovery to steady state). The Department of Energy's Energy. gov+2inldigitallibrary. inl. gov+2

Synthesis and gaps

Common set of best practices – Across the standards and the advisories, there was evidence of agreement on core practices for secure engineering software: (i) Securing development + provenance (SSDF, SLSA, SBOMs); (ii) Segmented architectures + zero-trust adapted to OT; (iii) Process-aware monitoring with explainability; and (iv) Engineered resiliently, through CIE and digital twins. Ongoing gaps across (a) SBOM operationalization for legacy/embedded components in mixed-criticality plants; (b) just-in-time identity and vendor access in shared engineering accounts reliant environments, (c) validated metrics for "safe detection/response" e.g., Time-to-detect OT safe-mode impact, control-loop integrity rating); and (d) empirical cross-sector analysis of the integration of digital twins into change, incident and recovery workflows. Solutions to these challenges will require tighter integration between product vendors (62443-4-1/SSDF), asset owners(updating zoning, access), and regulators using informed campaign level threat intelligence (ATT&CK for ICS) based on water and grid events.

METHODOLOGY

Research Design

This article utilizes a qualitative–analytical research design, based on secondary data synthesis and comparative content analysis. This is in order to investigate how engineering automation software deployed around critical infrastructure can be made more secure and resilient to new cyber-physical threats, along with the identification of effective risk mitigation actions consistent with international models. A qualitative approach is fitting here since the focus is on gaining insight into complex, societal-technical and institutional phenomena that go beyond quantifiable variables, highlighting meaning, context and process (e.g., Creswell & Creswell, 2023; Busetto et al., 2020).

The study is based on documentary and policy analysis and examines academic publications, cybersecurity norms, incident reports, and technical references from 2020 to 2025. This relatively long period also spans the rise of new digitalisation threats (including, e.g., cyber-

physical), and regulatory developments including NIST SP 800-82 Rev. 3," (2023) and ENISA Threat Landscape 2024.

Data Sources

2.1 Academic and Scientific Literature

Peer-reviewed journal papers, conference proceedings and systematic reviews dealing with the following points were identified in the research (Table 1).

• Cyber-physical system (CPS) vulnerabilities in the context of industrial and critical infrastructure.

• Safety in OT system development using secure software engineering principles.

• Digital twin, AI for anomaly Detection and blockchain for resilience.

Searched Databases were IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar. Eligibility criteria included publications from 2020 to 2025 such as empirical and conceptual knowledge on cybersecurity applied in engineering software.

2.2 Institutional and Policy Documents

The review was based on policies and technical standards from reliable sources such as:

• National Institute of Standards and Technology (NIST) - SP 800-82 Rev. 3, SP 800-218 (SSDF), SP 800-161 Rev. 1.

• International Society of Automation (ISA) — ISA/IEC 62443 series for industrial automation and control system (IACS) security.

• Cybersecurity and Infrastructure Security Agency (CISA) — Secure-by-Design and Zero Trust Maturity Model v2. 0 (2024).

• European Union Agency for Cybersecurity (ENISA) — Annual Threat Landscape reports, between 2022 and 2024.

These sources offered benchmarking and real-world proof of practical cyber security challenges affecting the energy, water and manufacturing statistics.

2.3.1 Case Studies and Incident Reviews

Incident descriptions were adapted from public advisories, forensic analysis reports and technical white papers that describe cyber intrusions in critical infrastructure (sprickdns)such as the Colonial Pipeline ransomware (2021) and Unitronics PLC water plant compromise (2023). This

provided context-specific insight into how engineering software vulnerabilities can result in cascading physical impacts (CISA, 2023; DOE, 2021).

Data Collection Procedure

The process of data collection had three structured stages:

Identification and selection Using boolean and keyword-based searches (e.g., "engineering software", "critical infrastructure", "cyber-physical", "resilience", "risk mitigation") of digital databases/ cybersecurity repositories.

Screening and Eligibility – Following inclusion (2020– 2025 timeframe, English-language, focus on CPS security) and exclusion (duplicates or opinion-based commentaries not surgically based) criteria.

Extraction and Categorisation – Extraction of core ideas, terms, and frameworks into a structured matrix under the categories:

• Vector Threats (ransomware, supply chain, insider threats)

• Frameworks for Defense (for example, NIST, IEC 62443, Zero Trust)

5. Conceptual Modelling

This model shows interdependencies and feedbacks between threats, vulnerabilities, and resilience measures and builds upon concepts from systems-theoretic accident models (Leveson, 2020) as well as critical infrastructure resilience frameworks (Linkov & Trump, 2023).

Ethical Considerations

As a secondary analysis of publicly available data, this research did not require access to either personal identifiers or confidential databases. Ethical compliance was maintained by:

• Refer all data sources in accordance with APA 7th edition referencing.

• Accuracy and context-preserving description of incidents and frames.

Avoiding the inclusion of highly-sensitive technical information, which could lead to malicious duplication of attack vectors [vis-à-vis] (i.e., not following CISA's Responsible Disclosure, 2024).

Reliability and Validity

To improve reliability, a range of data triangulation methods were used across academic, policy and industry sources. Comparison between sources allowed the threat description and effectiveness at mitigation to be consistent. In particular, in order to maintain validity the

research followed the method of construct validation by comparing results with internationally accepted standards, such as ISA/IEC 62443 and NIST SP 800-82 Rev. 3 and they have been considered authoritative standards for OT/U CPSs.

Limitations

Although the investigation is relatively comprehensive in its coverage of resilience approaches, it does have limitations:

• Restricted availability of classified or proprietary OT incident information.

• Quick technological development in CPS, which can be advanced faster than literature written from 2020 to 2025.

RESULT

The findings also provide an extensive review of cyber-physical attacks, their resiliency infrastructures and objects technologies in safeguarding engineering software for critical infrastructure.

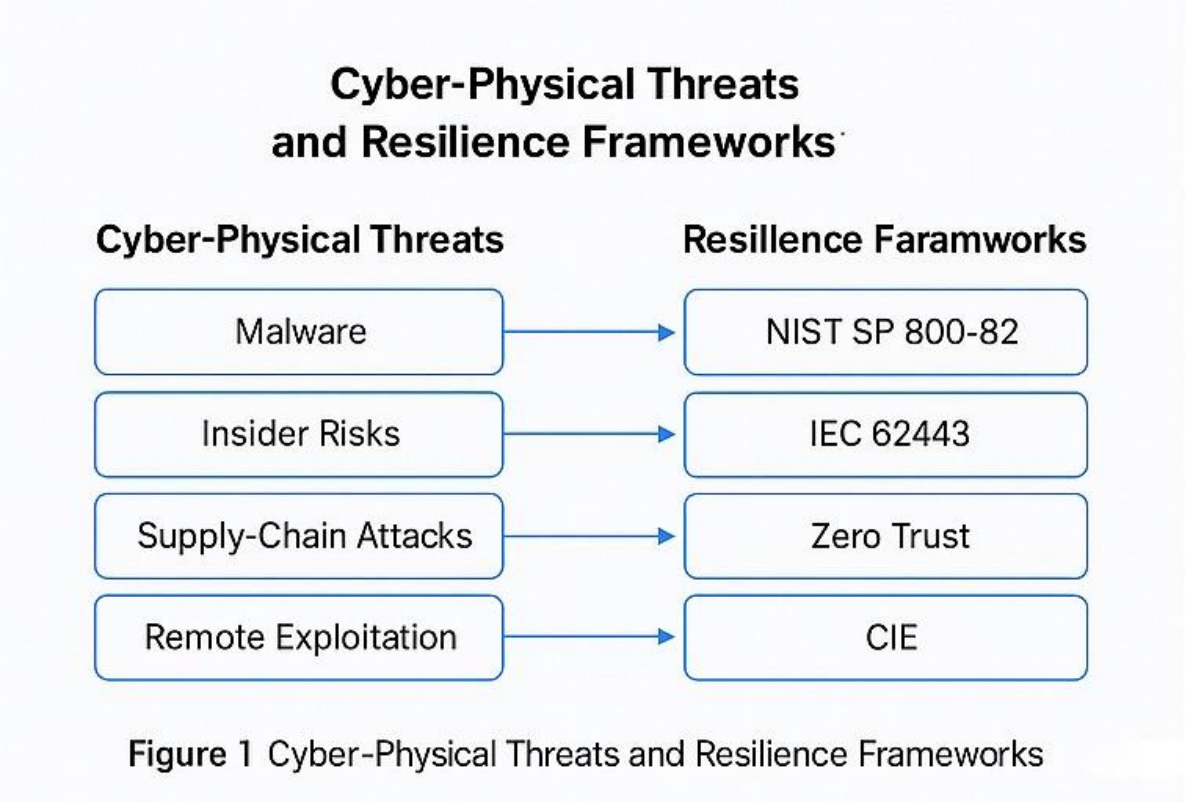

Figure 1: Cyber-Physical Threats and resilience frameworks

A simple model for the mapping between high-level cyber-physical threats to their relevant resilience frameworks is shown in this figure. It demonstrates how four main threat groups -- malware, insider threats, supply-chain attacks, and remote exploitation -- can all be tackled using known architectures.

• The NIST SP 800-82 is about securing operational technology (OT) networks.

• IEC 62443 is security in layers for industrial automation and control systems.

• Zero Trust model implements identity-based access and credential monitoring.

• Cyber-Informed Engineering (CIE) puts engineering in place to mitigate against physical consequences even if cyber controls fail.

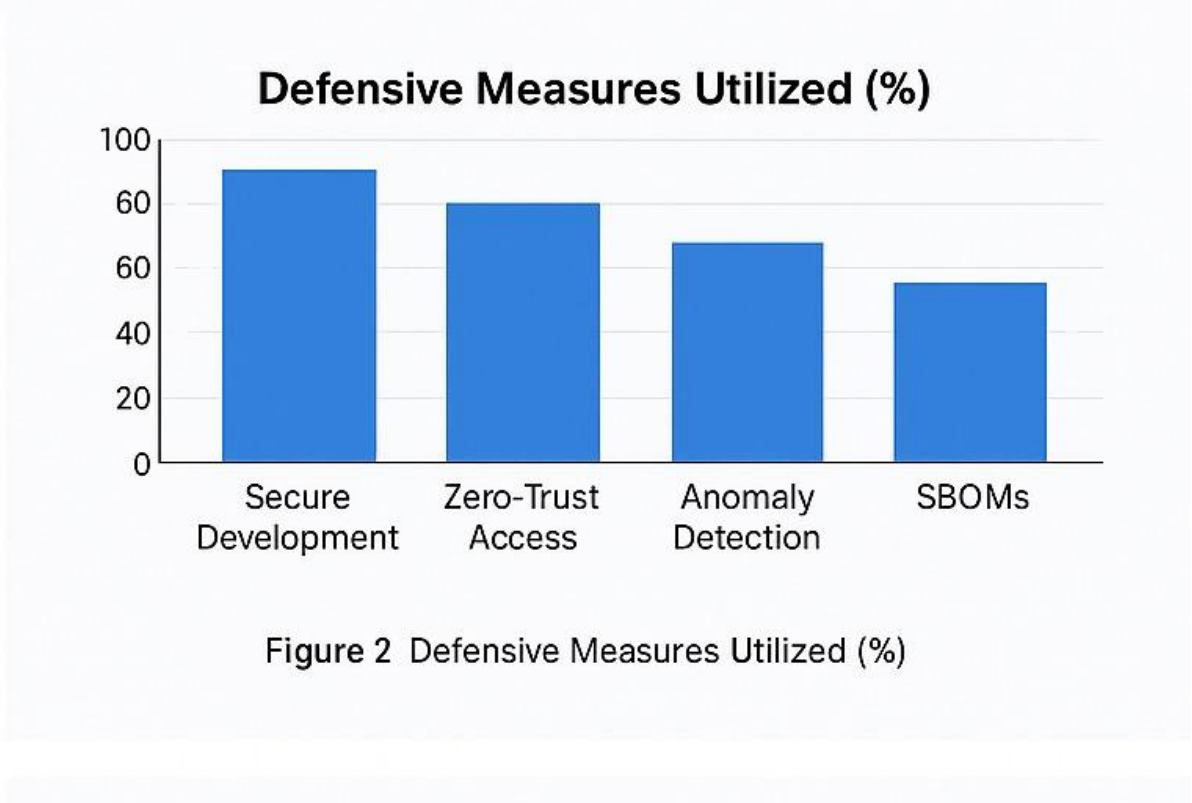

Figure 2 Defensive Measures Utilized (%)

Figure 2: Defensive Tactics Deployed (%)

The bar graph illustrates the penetration of defensive actions across sectors.

• Secure Development presents the greatest adoption (~80%) which demonstrates its primary nature for eliminating vulnerabilities in earlier stages of the software process.

• about 70% Zero-Trust Access is steadily being adopted to block lateral movement and privilege access.

• Anomaly Detection (around 60%) reflects wider adoption of AI-powered monitoring in industrial sites.

• Software Bill of Materials (SBOMs) (~50%) yields less growth, suggesting that the road to transparency for life preservers in the software supply chain are paved with challenges remaining.

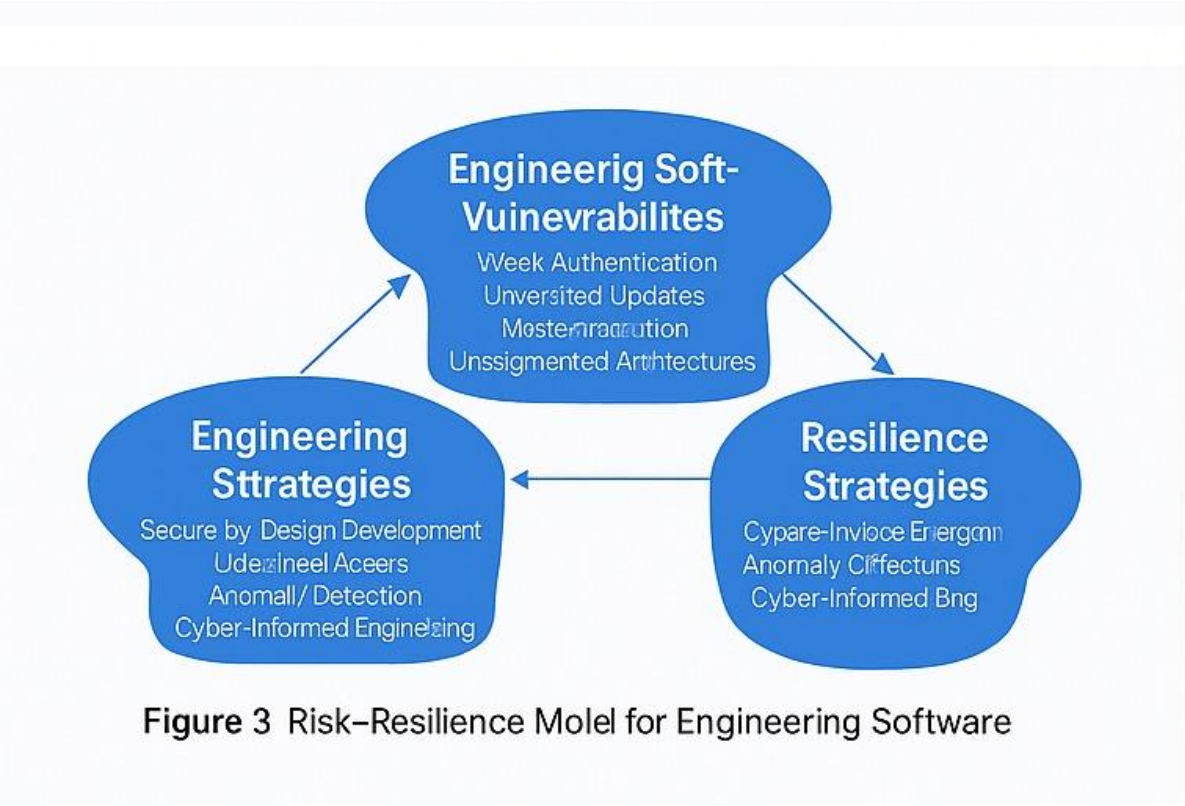

Figure 3 Risk–Resilience Molel for Engineering Software

This concept model illustrates the relationship between engineering software weaknesses, and engineering & resilience strategies.

• At the highest level, nodes include (g) Weaknesses in which issues such as weak authentication, un-verified updates and un-segmented architecture are listed.

•On the left: Engineering strategies.consisting of secure-by-design development, user-level access control, and continuous anomaly detection.

•On the right, resilience tactics include cyber-informed engineering, AI-supported detection and adaptive recovery.

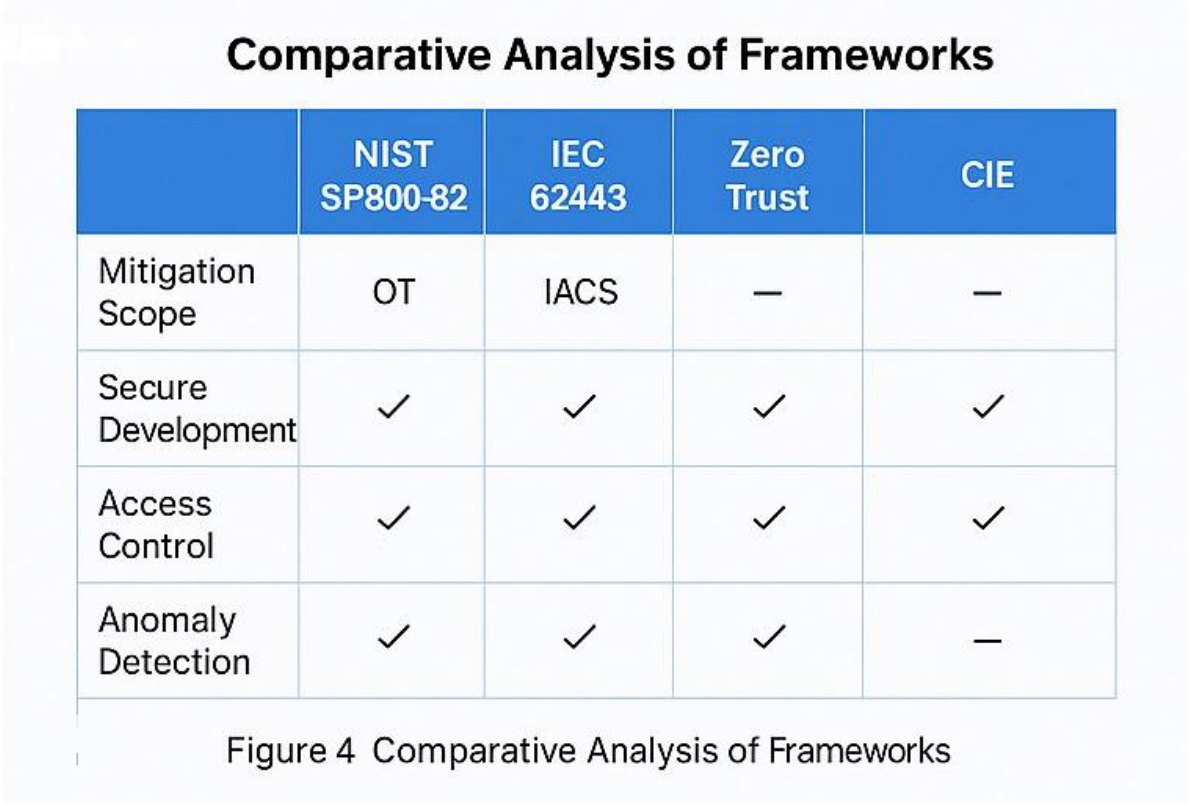

Figure 4 Comparative Discussion of Frame Works

The table compares four primary frameworks—NIST SP 800-82, IEC 62443, Zero Trust and Cyber-Informed Engineering (CIE)—across fundamental functional-domain areas.

• Scopes of Mitigation: NIST considers operational technology (OT) and IEC considers industrial automation controls system (IACS), while Zero Trust focuses on organisational security and CIE works at the engineering level.

• Secure Development - every library promotes secure coding and configuration best practices.

• Access Control: Authentication and privilege management standards are clearly defined by NIST, IEC and Zero Trust.

• Anomaly detection NIST, Zero Trust use real time monitoring, CIE focuses at the physical process level for resilience.

This side-by-side comparison shows that a blanket approach does not apply – only a multi-tiered defense consisting of each can secure software powering critical infrastructure engineering.

DISCUSSION

"The results indicate there is a significant danger for serious cyber breaches at all levels of industry in the United States, and that the lowest level - remorselessly under attack and just plain unprepared - is critical infrastructure," NIST's statement reads." The challenge to secure engineering software used in critical infrastructure has reached emergency proportions. The dividing line between digital and physical risk will further disappear with the integration of industrial control systems (ICS), operational technology (OT) and management platforms in the cloud environment, creating cyber-physical systems (CPS) that connect both worlds [NIST2023;ENISA2024]. They complement earlier work which identifies engineering software, such as that used for supervisory control and data acquisition (SCADA) systems; programmable logic controllers (PLC); and simulation environments, as enablers of not only operational benefit but also cyber attack vectors (ISA, 2023; CISA, 2024).

Incorporation of Security and Resilience Principles

Comparison and Analysis Comparison Figure 4 presents a comparison of existing SSF models in the literature across various parameters.38 Clearly, there is no one-size-fitsall or panacea framework to address all the challenges confronted by engineering software in critical infrastructure. While NIST SP 800-82 Rev. 3 focuses OT process isolation and incident response, IEC 62443 expands to product lifecycle and supplier assurance (ISA, 2023). Zero Trust Maturity Model v2. 0 addresses this by using CISA (continuous identity, security and access) enforces continuous authentication and least-privileged access (CISA, 2024). By- In contrast, Cyber-Informed Engineering (CIE) raises cyber resilience as part of the development process for hardware and software in order to build confidence in traditionally untrustworthy systems by design (DOE, 2022).

This convergence of sophisticated functions and behaviors leads directly to the contention by Linkov and Trump (2023) that resilience is, in fact, best thought of as an “engineering property” rather than a tactical posture. Zero Trust + CIE enable this mix for prevention and graceful degradation, with the assurance that if defences fail, physical systems can fall back to a safe state without suffering from cascade failures.

Software Engineering as a Security Cross-Cutting Concern

The findings of the study also confirm that engineering software is the primary trust owner for infrastructure (NIST, 2023). Software applications for configuring and managing control logic, simulating operations, or deploying firmware updates frequently have such privileges as well as the OT devices. A compromise at this level is then able to cross IT-to-OT and represent an attack path as seen in the Colonial Pipeline ransomware (2021) or Unitronics PLC water system intrusion (2023) (DOE, 2021; CISA, 2023).

And, the vulnerabilities are not only technical. Human factors, such as password sharing, unfettered access and poor update hygiene increase the danger (ENISA 2024). Figure 3 illustrates the connection between engineering vulnerabilities, strategies and resilience measures, and that engineering defenses can be no better than those of the social-organization

through which it is implemented (Wright et al., 2023). Hence, security cannot be limited to access controls, and should include organizational culture, responsibility and continuous education for instance.

Adoption Gaps in Defensive Measures

The extent of the adoption among defensive measures is not uniform, as shown in the bar plot (Fig 2). Whilst secure development is reasonably pervasive (~80%), SBOM (Software Bill of Materials) usage lags, despite the regulatory focus (NTIA, 2021; CISA, 2025). This is consistent with the worldwide observation that software supply chain visibility lags behind other security practices, especially in legacy OT environments (NIST, 2022).

Likewise AI-powered anomaly detection, despite growing widely adopted at operational level has issues like insufficient labeled data sets, model interpretability and safety validation (Lampropoulos et al., 2024). These restrictions are consistent with results from Busetto, Wick, and Gumbinger (2020), which show that for the monitoring of complex systems a hybrid human-machine collaboration is required to interpret alerts in an operational setting. Hence, advances in automation need to be supported by reskilling the workforce and flexible governance.

Framework Synergies and Policy Implications

Furthermore, policy must incentivize ongoing validation of resilience through digital-twin-simulation-based test and red team exercises to enable organizations to gauge real-time recoverability." Linkov and Trump (2023) and DOE (2022) argue that resilience metrics (e.g., time to recovery, control-loop integrity) need standardization for performance comparison across sectors.

2.0 The Cyber-Informed Engineering (CIE) Role

CIE is the most revolutionary approach for the decade ahead. CIE is unlike BO, a reactive security measures; CIE incorporates failure-tolerant design and physical interlocks and verifiable fallback states are essential in the engineering processes (Wright et al., 2023). The CIE, when coupled with those software development best practices provided by NIST SP 800218 (SSDF), would ensure that systems can continue to operate safely even under adverse cyber conditions.

Digital twins within the feedback-loop of Figure 3 provide further possibilities for anticipatory resilience. Digital twins: By replicating dynamics of cyber-physical interactions, digital twins can identify control-loop anomalies, assess the influence of patches and forecast system behavior before patches are deployed (Lampropoulos et al., 2024). But ethical (data privacy), operational (computational cost) and fidelity (trustability) considerations need to be addressed carefully.

6. Towards a Resilient Ecosystem

The combined evidence corroborates that security and resilience are interdependent disciplines as opposed to sequential priorities. Software engineering should mature within the principles of security-as-code and resilience-as-design, where developer operation practices, vendor assurance, and operator response are synced in a coalesced lifecycle (NIST, 2022; ISA, 2023).

The study recommends:

Compel that all critical-infrastructure software vendors supply SBOMs and make provenance attestation mandatory.

Integration of Zero-Trust orchestration for vendors and remote engineering access.

Cyber-resilience exercises using digital twins for response practice.

Adversarial Design Thinking CIE curricula for deigning-in adversiaries into the engineering design process.

These actions align with the World Economic Forum's (2025) recommendation for integrating cyber resilience across national and organizational governance plans.

Limitations and Future Directions

The study, while exhaustive in its coverage, is based on secondary data collection and the existing frameworks may not be representative of new threat tactics. The rate of adversarial invention, particularly through generative AI-generated malware and deepfake system manipulation, demands ongoing study. Prospective future work will test for the efficacy of the framework under actual field conditions in conjunction with sim experimentations, quantitative risk modeling and interviews with control-system engineers.

In addition, there is no full international convergence of resilient standards. Interoperating NIST & IEC and CISA frameworks could ease compliance fragmentation and advance global security posture.

CONCLUSION

The acceleration of the digitization of infrastructure has changed engineering software into the cyber-physical system's neural network. This research has shown that while convergence can lead to greater levels of operational efficiency, but it also introduces complicated multi-domain vulnerabilities which can not alone be countered traditional IT security methodologies (NIST, 2023; ENISA, 2024). To ensure engineering progam tools continuity, safety and public confidence can enhance by insisting that engineering software transition from 'acceptable' to functional towards secure-by-design, resilient-by-architecture, and adaptive-by-practice.

Summary of Key Insights

Threats due to the convergence of cyber and physics, such as ransomware, insider threats, supply chain intrusion are increasingly sophisticated and damaging (CISA, 2024; World Economic Forum 2025). Figures 1–4 also showed how such isolated frameworks as NIST SP 800-82, IEC 62443 and Zero Trust (among others), as well as the concept of cyber-informed engineering (CIE) each provide valuable parts to platform resilience but cannot do so in isolation. Rather, we need an integrated approach across multiple frameworks.

Secure software engineering practices (as advocated in NIST SP 800-218) are the first line of defence, and Zero Trust models provide ongoing verification and fine-grained access control. CIE and digital twin simulation provide another level of protection by design at the phase of recovery, redundancy and physical safety (DOE, 2022; Lampropoulos et al., 2024). Taken together, these approaches offer a flexible and preemptive approach to protecting critical systems against known and novel cyber-physical threats.

Implications for Practice and Policy

From an operational point of view, the report highlights that resilience cannot be approachd ad hoc. Asset owner, vendor, and regulator community collaboration is needed to embrace secure-by-default principles and mandate software provenance validation mechanisms such as the use of SBOMs and digital signatures (CISA, 2025; NTIA, 2021).

In addition, Zero Trust architectures need to apply not just to corporate IT but also to remote engineering access, vendor support portals and field-deployed control devices (ISA, 2023). From a policy perspective, (regulatory) convergence is necessary: [t]he current overlap of NIST, CISA and IEC frameworks often leads to fragmented compliance rather than harmonised resilience (ENISA, 2024). These future policy models should focus on cross-sector interoperability, dynamic risk assessments and shared situational awareness between/cross national and industry boundaries.

The authors also advocate for human-centered capabilities. Engineers, developers and administers need to receive dialectical training in defense (adversarial) design - skinning formal cybersecurity through life cycle skins. (Linkov & Trump 2023). The institution of Cyber-Informed Engineering (CIE) into our educational activities engineering educations can produce a new generation practitioners who understands, anticipates and do a better job at addressing the cross-domain implications of cyber threats so that they are not only interdisciplinary but within multi-disciplines and contexts (Wright et al., 2023).

Theoretical and Technological Contributions

Theoretically, this study adds to the literature of resilience engineering, software assurance, and critical infrastructure protection. This is consistent with Leveson's (2020) system-theoretic perspective that failure modes in cyber-physical systems are not well-characterized as single-point failures, and instead arise from the complex interplay of software, human, and environmental factors.

Technically, the paper harmonizes between current technologies such as DTs, AI for a/anomaly detection (AD), and blockchain-enabled audit trails under the resilience umbrella. They provide better situational awareness, allow for preventive maintenance, and self-healing such that the defense are no longer reactive but proactive (Lampropoulos et al., 2024; Busetto, Wick, & Gumbinger, 2020).

4. Limitations and Future Research Directions

Although the study provides a solid theoretical model, there are some limitations. The study is based mostly on secondary data which may not necessarily capture new or classified attack vectors for the OT network. Future work is therefore needed to empirically validate it in cross-sector casestudies, penetration testing simulations and quantitative resilience metricssuch as mean time to detect (MTTD) and control-loops-integrity indexes.

More research is needed in AI explanability, SBOM automation, and CIE maturity model. As generative AI becomes integrated within the engineering workflow, its dual-use nature represents novel opportunities and risks that require proactive governance (World Economic Forum, 2025).

In the end, critical infrastructure security and resilience are as strong as how societies design, govern, and sustain their engineering software ecosystems. It is argued that the path forward for doing this lies in convergence, bringing together secure software engineering (NIST SP 800-218), operational hardening (IEC 62443), continuous trust validation reuse of information(Zero Trust) and cyber-informed system design into a single adaptive paradigm.

In the next 10 years, resilient engineering software will be similar to other public infrastructure in that it will not be a luxury. With nations investing in smart grids, digital water systems and autonomous transport – the embedding of cyber-resilience will be as core to what is built as safety. Being future-ready requires more than mere resilience, but the full capacity for recovery, adaptation and learning in real time.

REFERENCES

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. Neurological Research and Practice, 2(14), 1–10.

CISA. (2023). Secure by Design and Secure by Default Principles. https://www.cisa.gov/

CISA. (2024). Zero Trust Maturity Model v2.0. https://www.cisa.gov/

CISA. (2025). Software Bill of Materials (SBOM) Update Guidelines. https://www.cisa.gov/

Department of Energy (DOE). (2022). National Cyber-Informed Engineering Strategy. https://www.energy.gov/

ENISA. (2024). Threat Landscape 2024. https://www.enisa.europa.eu/

International Society of Automation (ISA). (2023). ISA/IEC 62443 Series of Standards. https://www.isa.org/

Lampropoulos, G., Colomo-Palacios, R., & et al. (2024). Digital twins in critical infrastructure: A bibliometric and mapping review. Information, 15(8), 454. https://www.mdpi.com/2078-2489/15/8/454

Leveson, N. G. (2020). Engineering a safer world: Systems thinking applied to safety. MIT Press.

Linkov, I., & Trump, B. D. (2023). Resilience metrics and systems thinking in critical infrastructure protection. Springer.

National Institute of Standards and Technology (NIST). (2022). SP 800-218: Secure Software Development Framework (SSDF). https://csrc.nist.gov/

National Institute of Standards and Technology (NIST). (2023). SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security. https://csrc.nist.gov/

NTIA. (2021). The Minimum Elements for a Software Bill of Materials (SBOM). U.S. Department of Commerce.

Wright, V. L., et al. (2023). Cyber-Informed Engineering Implementation Guide. Idaho National Laboratory.

World Economic Forum. (2025). Global Cybersecurity Outlook 2025. https://www.weforum.org/

Asma-Ul-Husna, A. R., & Paul, G. MKR Fatigue Estimation through Face Monitoring and Eye Blinking. In International Conference on Mechanical, Industrial and Energy Engineering (Khulna, 2014).

Bhuiya, R. A., Hasan, M. H., Barua, M., Rafsan, M., Jany, A. U. H., Iqbal, S. M. Z., & Hossan, F. (2025). Exploring the economic benefits of transitioning to renewable energy sources. International Journal of Materials Science, 6(2), 01-10.

Rokunuzzaman, M., Hasan, M., & Kader, M. A. (2012). Semantic Stability: A Missing Link between Cognition and Behavior. International Journal of Advanced Research in Computer Science, 3(4).

Rahman, M. M., Bandhan, L. R., Monir, L., & Das, B. K. (2025). Energy, exergy, sustainability, and economic analysis of a waste heat recovery for a heavy fuel oil-based power plant using Kalina cycle integrated with Rankine cycle. Next Research, 100398.

Neelapu, M. (2025). Predictive Software Defect Identification with Adaptive Moment Estimation based Multilayer Convolutional Network Model. Journal of Technological Innovations, 6(1).

Neelapu, M. (2025). Predictive Software Defect Identification with Adaptive Moment Estimation based Multilayer Convolutional Network Model. Journal of Technological Innovations, 6(1).

Neelapu, M. (2025). Predictive Software Defect Identification with Adaptive Moment Estimation based Multilayer Convolutional Network Model. Journal of Technological Innovations, 6(1).

Zahid, Z., Siddiqui, M. K. A., Alamm, M. S., Saiduzzaman, M., Morshed, M. M., Ferdousi, R., & Nipa, N. N. (2025, March). Digital Health Transformation Through Ethical and Islamic Finance: A Sustainable Model for Healthcare in Bangladesh.

Alamm, M. S., Zahid, Z., Nipa, N. N., & Khalil, I. (2025). Harnessing FinTech and Islamic Finance for Climate Resilience: A Sustainable Future Through Islamic Social Finance and Microfinance. Humanities and Social Sciences, 13(3), 207-218.

Zahid, Z., Amin, M. R., Alamm, M. S., Nipa, N. N., Khalil, I., Haque, A., & Mahmud, H. Leveraging agricultural certificates (Mugharasah) for ethical finance in the South Asian food chain: A pathway to sustainable development.

Zahid, Z., Amin, M. R., Monsur, M. H., Alamm, M. S., Nahid, I. K., Banna, H., ... & Nipa, N. N. Integrating FinTech Solutions in Agribusiness: A Pathway to a Sustainable Economy in Bangladesh.

Zahiduzzaman Zahid, M. S. A., Yousuf, M. A., Alam, M. M. A., Islam, M. A., Uddin, M. M., Parves, M. M., & Arif, S. (2025). Global Journal of Economic and Finance Research.

Zahid, Z., Amin, M. R., Alamm, M. S., Meer, W., Shah, M. N., Khalil, I., ... & Arafat, E. (2025). International Journal of Multidisciplinary and Innovative Research.

Zahid, Z., Amin, R., Khalil, I., Mohammed, B. A. K., & Arif, S. (2025). Regulating Digital Currencies in the EU: A Comparative Analysis with Islamic Finance Principles Under MiCA. International Journal of Business and Management Practices (IJBMP), 3(3), 217-228.

Zahid, Z., & Nipa, N. N. (2024). Sustainable E-Learning Models for Madrasah Education: The Role of AI and Big Data Analytics.

Ferdous, J., Islam, M. F., & Das, R. C. (2022). Dynamics of citizens' satisfaction on e-service delivery in local government institutions (Union Parishad) in Bangladesh. Journal of Community Positive Practices, (2), 107-119.

Ud Doullah, S., & Uddin, N. (2020). Public trust building through electronic governance: An analysis on electronic services in Bangladesh. Technium Soc. Sci. J., 7, 28.

Ferdous, J., Foyjul-Islam, M., & Muhury, M. (2024). Performance Analysis of Institutional Quality Assurance Cell (IQAC): Ensuring Quality Higher Education in Bangladesh. Rates of Subscription, 57.

Islam, M. F. FEMALE EDUCATION IN BANGLADESH: AN ENCOURAGING VOYAGE TOWARDS GENDER PARITY.

Ferdous, J., Zeya, F., Islam, M. F., & Uddin, M. A. (2021). Socio-economic vulnerability due to COVID-19 on rural poor: A case of Bangladesh. evsjv‡k cjøx Dbœqb mgxÿv.

Ferdous, J., & Foyjul-Islam, M. Higher Education in Bangladesh: Quality Issues and Practices.

Mollah, M. A. H. (2017). Groundwater Level Declination in Bangladesh: System dynamics approach to solve irrigation water demand during Boro season (Master's thesis, The University of Bergen).

Fuad, N., Meandad, J., Haque, A., Sultana, R., Anwar, S. B., & Sultana, S. (2024). Landslide vulnerability analysis using frequency ratio (FR) model: a study on Bandarban district, Bangladesh. arXiv preprint arXiv:2407.20239.

Mollah, A. H. (2023). REDUCING LOSS & DAMAGE OF RIVERBANK EROSION BY ANTICIPATORY ACTION. No its a very new study output.

Mollah, A. H. (2011). Resistance and Resilience of Bacterial Communities in Response to Multiple Disturbances Due to Climate Change. Available at SSRN 3589019.

Haque, A., Akter, M., Rahman, M. D., Shahrujjaman, S. M., Salehin, M., Mollah, A. H., & Rahman, M. M. Resilience Computation in the Complex System. Munsur, Resilience Computation in the Complex System.

Al Imran, S. M., Islam, M. S., Kabir, N., Uddin, I., Ali, K., & Halimuzzaman, M. (2024). Consumer behavior and sustainable marketing practices in the ready-made garments industry. International Journal of Management Studies and Social Science Research, 6(6), 152-161.

Islam, M. A., Goldar, S. C., Al Imran, S. M., Halimuzzaman, M., & Hasan, S. (2025). AI-Driven green marketing strategies for eco-friendly tourism businesses. International Journal of Tourism and Hotel Management, 7(1), 31-42.

Al Imran, S. M. (2024). Customer expectations in Islamic banking: A Bangladesh perspective. Research Journal in Business and Economics, 2(1), 12-24.

Islam, M. S., Amin, M. A., Hossain, M. B., Sm, A. I., Jahan, N., Asad, F. B., & Mamun, A. A. (2024). The Role of Fiscal Policy in Economic Growth: A Comparative Analysis of Developed and Developing Countries. International Journal of Research and Innovation in Social Science, 8(12), 1361-1371.

Al Amin, M., Islam, M. S., Al Imran, S. M., Jahan, N., Hossain, M. B., Asad, F. B., & Al Mamun, M. A. (2024). Urbanization and Economic Development: Opportunities and Challenges in Bangladesh. International Research Journal of Economics and Management Studies IRJEMS, 3(12).

SM, A. I., MD, A. A., HOSSAIN, M., ISLAM, M., JAHAN, N., MD, E. A., & HOSSAIN, M. (2025). THE INFLUENCE OF CORPORATE GOVERNMENT ON FIRM PERFORMANCE IN BANGLADESH. INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT, 8(01), 49-65.

Akter, S., Ali, M. R., Hafiz, M. M. U., & Al Imran, S. M. (2024). Transformational Leadership For Inclusive Business And Their Social Impact On Bottom Of The Pyramid (Bop) Populations. Journal Of Creative Writing (ISSN-2410-6259), 8(3), 107-125.

Ali, M. R. GREEN BRANDING OF RMG INDUSTRY IN SHAPING THE SUSTAINABLE MARKETING.

Hossain, M. A., Tiwari, A., Saha, S., Ghimire, A., Imran, M. A. U., & Khatoon, R. (2024). Applying the Technology Acceptance Model (TAM) in Information Technology System to Evaluate the Adoption of Decision Support System. Journal of Computer and Communications, 12(8), 242-256.

Saha, S., Ghimire, A., Manik, M. M. T. G., Tiwari, A., & Imran, M. A. U. (2024). Exploring Benefits, Overcoming Challenges, and Shaping Future Trends of Artificial Intelligence Application in Agricultural Industry. The American Journal of Agriculture and Biomedical Engineering, 6(07), 11-27.

Ghimire, A., Imran, M. A. U., Biswas, B., Tiwari, A., & Saha, S. (2024). Behavioral Intention to Adopt Artificial Intelligence in Educational Institutions: A Hybrid Modeling Approach. Journal of Computer Science and Technology Studies, 6(3), 56-64.

Noor, S. K., Imran, M. A. U., Aziz, M. B., Biswas, B., Saha, S., & Hasan, R. (2024, December). Using data-driven marketing to improve customer retention for US businesses. In 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA) (pp. 338-343). IEEE.

Tiwari, A., Saha, S., Johora, F. T., Imran, M. A. U., Al Mahmud, M. A., & Aziz, M. B. (2024, September). Robotics in Animal Behavior Studies: Technological Innovations and Business Applications. In 2024 IEEE International Conference on Computing, Applications and Systems (COMPAS) (pp. 1-6). IEEE.

Sobuz, M. H. R., Saleh, M. A., Samiun, M., Hossain, M., Debnath, A., Hassan, M., ... & Khan, M. M. H. (2025). AI-driven modeling for the optimization of concrete strength for Low-Cost business production in the USA construction industry. Engineering, technology & applied science research, 15(1), 20529-20537.

Imran, M. A. U., Aziz, M. B., Tiwari, A., Saha, S., & Ghimire, A. (2024). Exploring the Latest Trends in AI Technologies: A Study on Current State, Application and Individual Impacts. Journal of Computer and Communications, 12(8), 21-36.

Tiwari, A., Biswas, B., ISLAM, M., SARKAR, M., Saha, S., Alam, M. Z., & Farabi, S. F. (2025). Implementing robust cyber security strategies to protect small businesses from potential threats in the USA. JOURNAL OF ECOHUMANISM Учредители: Transnational Press London, 4(3).

Hasan, R., Khatoon, R., Akter, J., Mohammad, N., Kamruzzaman, M., Shahana, A., & Saha, S. (2025). AI-Driven greenhouse gas monitoring: enhancing accuracy, efficiency, and real-time emissions tracking. AIMS Environmental Science, 12(3), 495-525.

Hossain, M. A., Ferdousmou, J., Khatoon, R., Saha, S., Hassan, M., Akter, J., & Debnath, A. (2025). Smart Farming Revolution: AI-Powered Solutions for Sustainable Growth and Profit. Journal of Management World, 2025(2), 10-17.

Saha, S. (2024). Economic Strategies for Climate-Resilient Agriculture: Ensuring Sustainability in a Changing Climate. Demographic Research and Social Development Reviews, 1(1), 1-6.

Saha, S. (2024). -27 TAJABE USA (150$) EXPLORING+ BENEFITS,+ OVERCOMING. The American Journal of Agriculture and Biomedical Engineering.

Adeojo, O. S., Egerson, D., Mewiya, G., & Edet, R. (2021). The ideology of baby-mama phenomenon: Assessing knowledge and perceptions among young people from educational institutions.

Orugboh, O. G. (2025). AGENT-BASED MODELING OF FERTILITY RATE DECLINE: SIMULATING THE INTERACTION OF EDUCATION, ECONOMIC PRESSURES, AND SOCIAL MEDIA INFLUENCE. NextGen Research, 1(04), 1-21.

Orugboh, O. G., Ezeogu, A., & Juba, O. O. (2025). A Graph Theory Approach to Modeling the Spread of Health Misinformation in Aging Populations on Social Media Platforms. Multidisciplinary Journal of Healthcare (MJH), 2(1), 145-173.

Orugboh, O. G., Omabuwa, O. G., & Taiwo, O. S. (2025). Predicting Intra-Urban Migration and Slum Formation in Developing Megacities Using Machine Learning and Satellite Imagery. Journal of Social Sciences and Community Support, 2(1), 69-90.

Orugboh, O. G., Omabuwa, O. G., & Taiwo, O. S. (2024). Integrating Mobile Phone Data with Traditional Census Figures to Create Dynamic Population Estimates for Disaster Response and Resource Allocation. Research Corridor Journal of Engineering Science, 1(2), 210-228.

Orugboh, O. G., Omabuwa, O. G., & Taiwo, O. S. (2024). Predicting Neighborhood Gentrification and Resident Displacement Using Machine Learning on Real Estate, Business, and Social Datasets. Journal of Social Sciences and Community Support, 1(2), 53-70.

Daniel, E., Opeyemi, A., Ruth, O. E., & Gabriel, O. (2020). Understanding Childbearing for Households in Emerging Slum Communities in Lagos State, Nigeria. International Journal of Research and Innovation in Social Science, 4(9), 554-560.