Cybersecurity Risk Assessment of Critical Digital Assets in Nuclear Power Plant Instrumentation and Control Systems

Abimbola Olamide Ayotomiwa[1, *], **Toheeb Oluwaseun Adamolekun**[1]
[1]Department of Electrical and Computer Engineering,
North Carolina A&T State University, Greensboro, NC, USA
*Corresponding author: bimbolahan@gmail.com

https://doi.org/DOI: 10.56201/ijcsmt.vol.11.no8.2025.pg88.107

Abstract
The increasing digitalisation of nuclear power plant instrumentation and control systems has intensified the need to assess cybersecurity risks without compromising essential safety functions. This review examines how critical digital assets are identified, classified, and protected, with particular attention to vulnerabilities, credible attack pathways, consequence-based risk evaluation, and regulatory requirements. A structured narrative synthesis of scholarly research, international standards, regulatory guidance, and relevant industrial cybersecurity studies was undertaken to compare architectural characteristics, assessment techniques, and defensive practices. The review identifies safety-related controllers, instrumentation interfaces, engineering workstations, communication gateways, and operator monitoring systems as assets whose cybersecurity significance depends on functional dependencies and potential safety consequences. Findings indicate that conventional vulnerability scoring alone inadequately represents nuclear cyber risk. Function-based asset mapping, threat scenario analysis, probabilistic safety assessment, Bayesian modelling, and graded evaluation provide complementary perspectives, although limited incident evidence and uncertain adversarial behaviour restrict quantitative confidence. Defence-in-depth, network segmentation, controlled access, secure configuration management, anomaly monitoring, and validated incident response emerge as essential safeguards. Emerging artificial intelligence and digital-twin applications may strengthen detection and situational awareness, but require rigorous qualification before use in safety-critical environments. The review also identifies persistent challenges associated with legacy equipment, supply-chain dependencies, human factors, and differences in regulatory and organisational preparedness across nuclear programmes. It concludes that effective cybersecurity governance must integrate technical evidence with nuclear safety analysis rather than rely on compliance checklists alone. Recommended priorities include maintaining traceable asset inventories, validating protective boundaries, applying non-intrusive assessments, strengthening workforce competence, and developing transparent, uncertainty-aware methods for evaluating cyber-induced safety consequences throughout the facility operational lifecycle.

Keywords: *Nuclear Power Plants; Critical Digital Assets; Instrumentation and Control Systems; Cybersecurity Risk Assessment; Defence-in-Depth; Nuclear Safety.*

1. Introduction

1.1. Background of Nuclear Power Plant Cybersecurity

Cybersecurity has become an indispensable component of nuclear power plant safety and operational resilience, reflecting the increasing integration of digital technologies into instrumentation and control (I&C) infrastructures. Historically, nuclear facilities relied extensively on analogue control architectures, which provided relatively limited exposure to network-based intrusions. However, progressive digitalisation has introduced programmable logic controllers, distributed control systems, digital protection devices and interconnected monitoring platforms into critical plant operations. Although these technologies enhance diagnostic capabilities, operational precision and equipment reliability, they simultaneously create vulnerabilities requiring systematic cybersecurity evaluation. Ayodeji et al. (2023) establish that digital control networks, sensor interfaces, human interactions and supply-chain dependencies constitute potential pathways through which cyber threats may compromise nuclear operational integrity.

Unlike conventional information technology environments, nuclear I&C systems operate under stringent safety, reliability and real-time performance requirements. Their cybersecurity significance extends beyond information confidentiality to encompass the integrity of reactor protection signals, availability of essential control functions and prevention of unauthorised equipment manipulation. Consequently, successful cyber intrusions may introduce misleading measurements, disrupt protective responses or impair systems supporting safe reactor operation. The International Electrotechnical Commission (IEC) (2019) recognises these distinctive requirements through IEC 62645, establishing cybersecurity provisions applicable to programmable digital I&C systems while emphasising prevention, detection and response measures compatible with nuclear safety obligations.

The institutional development of nuclear cybersecurity reflects growing recognition that conventional physical protection arrangements cannot independently address digitally enabled threats. The U.S. Nuclear Regulatory Commission (2010), through Regulatory Guide 5.71, established guidance for implementing cybersecurity programmes that protect digital computers, communication systems and networks associated with safety, security and emergency preparedness functions. Its approach incorporates defence-in-depth, protective controls, digital asset assessment and continuing programme management, thereby linking cybersecurity responsibilities with established nuclear regulatory expectations.

From a risk assessment perspective, protecting critical digital assets requires evaluating both system vulnerabilities and the potential safety consequences of exploitation. Zhang and Kelly (2023) highlight the need for structured cyber risk assessment approaches capable of accommodating the operational characteristics of nuclear facilities. Such assessments must consider adversarial capabilities, system interdependencies, attack pathways, and consequences affecting reactor safety functions rather than relying exclusively on conventional enterprise cybersecurity indicators. African nuclear development introduces additional institutional considerations. Arinze, Longe, and Eneh (2020), examining nuclear cybersecurity from a Nigerian regulatory perspective, emphasise the relationship between digital system dependability, international security requirements and national regulatory preparedness. Similarly, Asare and Bonney (2025) identify cybersecurity governance, ageing software, insecure networks and organisational security culture as significant concerns for emerging nuclear programmes across Africa, particularly where advanced reactor technologies are contemplated.

Emerging research further demonstrates the increasing relevance of intelligent cybersecurity techniques for detecting complex threats within nuclear digital environments. Lezzi et al. (2025)

examine artificial intelligence applications for identifying vulnerabilities, analysing cyber risks and supporting protective countermeasures. Nevertheless, effective cybersecurity assessment remains dependent on accurate asset identification, credible threat modelling, safety-informed risk prioritisation and assurance that protective measures do not interfere with essential I&C functions. These considerations establish cybersecurity risk assessment as a fundamental requirement for protecting critical digital assets throughout nuclear power plant operational lifecycles.

1.2. Digital Transformation of Nuclear Instrumentation Systems

Digital transformation is reshaping nuclear power plant instrumentation and control (I&C) systems through the progressive replacement of analogue technologies with programmable, networked and data-driven architectures. These developments facilitate precise process regulation, continuous equipment monitoring and improved operational diagnostics. Nevertheless, introducing digitally interconnected components into safety-critical environments requires careful consideration of cybersecurity vulnerabilities, system reliability and functional independence. Hunton et al. (2023) demonstrate the importance of structured engineering assessments during safety-related I&C modernisation, particularly when evaluating technology readiness, integration requirements and implementation constraints within existing nuclear facilities.

Modern automation infrastructures increasingly incorporate programmable logic controllers, supervisory control and data acquisition systems and integrated engineering platforms. Sunday and Omoegun (2022) examine how Siemens Totally Integrated Automation environments facilitate coordinated programming, monitoring and industrial process management, illustrating the operational significance of interconnected control technologies. Similarly, Omoegun et al. (2024) establish that SCADA-based automation supports real-time information exchange, predictive analytics and enhanced supervisory capabilities, although expanding digital connectivity also necessitates appropriate cybersecurity safeguards.

Evidence from Africa further demonstrates the practical application of programmable technologies within nuclear environments. Obeng et al. (2021) investigate a programmable logic controller-based pneumatic transfer system for Ghana Research Reactor-1, applying failure mode and effect analysis to evaluate equipment reliability and potential operational consequences. This illustrates the importance of incorporating systematic dependability assessments into nuclear automation upgrades. Emerging digital transformation initiatives also encompass digital twins, intelligent monitoring and advanced analytical models. Sharma et al. (2022) explain that digital twins integrate physical-system information with computational representations to support monitoring, simulation and predictive decision-making. Within nuclear I&C environments, such capabilities offer opportunities for identifying abnormal operating conditions and assessing equipment performance.

1.3. Cybersecurity Threats and Nuclear Safety Implications

Cybersecurity threats to nuclear power plant instrumentation and control (I&C) systems represent a distinctive safety concern because malicious interference with digital assets can propagate into physical processes. Threats include unauthorised configuration changes, compromised maintenance devices, malicious software, manipulated sensor readings and denial of essential control services. Their significance depends on whether compromised functions can undermine protective barriers, operator decisions or safe plant shutdown.

The U.S. Nuclear Regulatory Commission (2024) requires protection of digital systems supporting safety, security and emergency preparedness, including equipment whose compromise could

impair these functions. This regulatory emphasis establishes that cyber risk assessment must identify critical digital assets according to their potential consequences rather than technological sophistication alone. Rowland, Maccarone, and Clark (2023) distinguish damage to digital information from physical harm arising through unsafe control actions. Their information harm framework demonstrates why altered setpoints or misleading displays warrant evaluation against plant operating conditions, safeguards, and operator responses. Complementing this perspective, Shin et al. (2021) apply integrated safety–security analysis to a simulated nuclear condensate system, illustrating how attack scenarios can be traced through control interactions to hazardous outcomes. African regulatory experience reinforces the importance of institutional preparedness. The Nigerian Nuclear Regulatory Authority (2024) describes collaborative training addressing cybersecurity and physical protection at nuclear facilities, indicating recognition of their interdependence. In South Africa, the National Nuclear Regulator (2015) specifies controls for critical digital assets alongside incident response, protective separation, and safeguards against cybersecurity measures adversely affecting plant functions.

1.4. Review Objectives, Scope, and Research Significance

This review critically examines cybersecurity risk assessment practices associated with critical digital assets in nuclear power plant instrumentation and control (I&C) systems, emphasising their implications for operational integrity, regulatory compliance, and nuclear safety. Its primary objective is to evaluate how evolving digital architectures influence cybersecurity exposure and determine the effectiveness of existing approaches for identifying, analysing, and prioritising vulnerabilities within safety-critical nuclear environments. Particular attention is directed towards understanding the relationships between cyber threats, digital asset criticality, system interdependencies, and potential consequences for essential reactor protection functions.

The review encompasses digital instrumentation architectures, critical asset identification, cybersecurity threat characteristics, vulnerability assessment methodologies, and risk evaluation frameworks applicable to nuclear facilities. It further examines established regulatory requirements, defence-in-depth principles, access control mechanisms, network segmentation, and cybersecurity monitoring strategies. Emerging technological developments, including artificial intelligence, digital twins, and advanced intrusion detection capabilities, are considered alongside implementation challenges involving legacy infrastructure, system qualification, workforce preparedness, and evolving adversarial capabilities.Methodologically, the study adopts a structured, literature-based analytical approach, synthesising relevant scholarly publications, regulatory guidance, international standards, and established cybersecurity frameworks without undertaking experimental penetration testing or plant-specific vulnerability assessments. Its significance lies in strengthening understanding of how cybersecurity assessments can support nuclear safety objectives while accommodating technological modernisation. By identifying methodological limitations, regulatory considerations, and emerging research priorities, the review provides an evidence-informed foundation for improving risk-based decision-making, prioritising protective investments, and developing resilient cybersecurity strategies for nuclear I&C systems across established and emerging nuclear programmes.

2. Critical Digital Assets in Nuclear Systems

2.1. Architecture of Nuclear Instrumentation and Control Systems

Nuclear instrumentation and control (I&C) systems comprise interconnected sensing, processing, communication, and actuation components responsible for monitoring reactor conditions,

regulating operational processes, and executing essential safety functions. These systems continuously acquire information concerning neutron flux, temperature, pressure, coolant flow, and equipment performance to support automated control and operator decision-making. Their architecture prioritises reliability, redundancy, functional independence, and protection against failures capable of compromising reactor safety. Model-driven engineering approaches facilitate systematic architectural specification, verification, and integration of safety and cybersecurity requirements throughout system development (Ouni et al., 2021). Nuclear I&C architectures generally distinguish safety-related protection systems from operational control and supervisory functions. Reactor protection systems detect abnormal conditions and initiate protective responses, while process control systems maintain routine operating parameters. Effective architectural separation is essential to prevent disturbances within non-safety systems from affecting critical protection functions. Nevertheless, software dependencies and common-because failures can undermine redundant configurations, necessitating comprehensive architectural assessment and independent verification (Zhang et al., 2023). At the instrumentation level, sensors, signal-conditioning modules, and digital controllers convert physical reactor measurements into actionable operational information. FPGA-based instrumentation offers specialised processing capabilities for neutron flux monitoring, demonstrating the importance of dependable measurement acquisition and signal verification (Ibrahim et al., 2020). Similarly, reliability assessments of semiautomated research reactor monitoring systems illustrate how systematic failure analysis supports component evaluation and architectural improvements (Obeng et al., 2025). Digital human–machine interfaces provide operators with integrated process displays, alarms, and supervisory controls. Although digitalisation enhances information accessibility, interface complexity can introduce cognitive demands affecting situational awareness and operational responses (Porthin, Liinasuo & Kling, 2020). Emerging condition-monitoring technologies further support equipment assessment and operational diagnostics. Vibration-based monitoring demonstrates the potential of integrated sensors for identifying equipment abnormalities (Omoegun et al., 2023), while digital twin applications in electrical substations offer transferable concepts for equipment modelling and fault detection (Shittu et al., 2023). Collectively, these architectural developments underscore the importance of reliable instrumentation, functional segregation, cybersecurity safeguards, and intelligent monitoring in protecting critical nuclear digital infrastructure.

2.2. Identification and Classification of Critical Digital Assets

Identification and classification of critical digital assets (CDAs) constitute fundamental requirements for cybersecurity risk assessment within nuclear power plant instrumentation and control (I&C) systems. These activities establish which programmable devices, communication interfaces, computing platforms, and supporting digital components require protection because their compromise could adversely affect nuclear safety, security, or emergency preparedness. Effective identification therefore extends beyond conventional equipment inventories to examine functional dependencies, system connectivity, and potential consequences arising from malicious interference. The International Atomic Energy Agency (IAEA) (2021) advocates a systematic, function-oriented approach to identifying sensitive digital assets and establishing graded cybersecurity protection according to their operational significance.

Asset identification ordinarily begins by establishing essential plant functions and tracing their implementation through interconnected systems, subsystems, and individual digital components. Reactor protection controllers, safety-related monitoring equipment, engineering workstations,

communication gateways, and associated software configurations must be examined according to their contributions to protected functions. Joo, Seo, and Suh (2017) demonstrate the practical significance of function-based asset identification in research reactor nuclear instrumentation, highlighting the importance of identifying system boundaries and relevant digital components before determining cybersecurity protection requirements. Classification requires distinguishing nuclear safety classifications from cybersecurity criticality. Although safety classification reflects the importance of equipment to nuclear safety functions, cybersecurity criticality additionally considers attack exposure, interdependencies, and the consequences of unauthorised manipulation. Lee and Lee (2024) demonstrate how technical assessment methodologies can support more efficient evaluation of digital assets performing nuclear safety functions, potentially reducing unnecessary assessment burdens without weakening essential protection.

Table 1. Illustrative classification of critical digital assets in nuclear I&C systems

Digital asset category	Primary function	Illustrative cybersecurity priority	Principal assessment considerations
Reactor protection controllers	Initiate automatic protective actions	Highest	Integrity, independence, availability
Safety-related sensors and interfaces	Acquire essential process measurements	Highest	Signal integrity, measurement reliability
Engineering workstations	Configure and maintain controllers	High	Privileged access, configuration integrity
I&C communication gateways	Exchange operational information	High	Network boundaries, authorised data flows
Operator monitoring interfaces	Display plant conditions and alarms	High, function-dependent	Information integrity, operator awareness
Plant data historians	Record operational measurements	Moderate, function-dependent	Data integrity, connectivity, recovery
Maintenance diagnostic devices	Support testing and troubleshooting	High when connected to protected systems	Portable access, software integrity

Source: Author's synthesis of the functional and cybersecurity assessment principles discussed in this review. Priorities are illustrative rather than prescribed regulatory classifications; actual assignments require plant-specific safety and cybersecurity assessment.

Cybersecurity classification must also consider the potential propagation of disturbances across interconnected operational environments. Shittu, Olagunju, and Shittu (2024) examine cyber-physical resilience in digital electrical infrastructure, illustrating the importance of assessing interconnected monitoring and protection components. Within nuclear facilities, such dependencies require particular scrutiny when supporting equipment provides access to protected systems. Risk-informed classification further demands attention to consequence severity. Son et al. (2025) integrate security control assessments with probabilistic safety indicators, demonstrating how cyber-related functional impairments can inform relative risk prioritisation. Comparable considerations arise in emerging nuclear programmes, where Ameyaw, Emi-Reynolds and Abrefah (2025) examine interconnected cyber-physical hazards within Ghana's proposed nuclear infrastructure.

Maintaining accurate classifications requires periodic reassessment following equipment modifications, software upgrades, and changes in system connectivity. Tomažič, Nelson, and Šeruga (2024) emphasise the importance of verifying asset identification, security controls, and regulatory compliance through structured inspections. Accordingly, classification records should remain traceable to plant functions, documented system boundaries, and evidence supporting each asset's assigned protection requirements.

2.3. Cybersecurity Vulnerabilities and Potential Attack Pathways

Cybersecurity vulnerabilities within nuclear power plant instrumentation and control (I&C) systems arise from the interaction of programmable devices, communication infrastructures, software dependencies, and operational procedures. These vulnerabilities are particularly significant because nuclear facilities depend on reliable digital functions for process monitoring, reactor protection, and operational decision-making. Potential threats include malicious software, unauthorised configuration changes, credential compromise, false-data injection, and disruption of communication services. Kim et al. (2020) demonstrate that systematically classifying cyberattacks according to their characteristics, targets, and potential consequences provides an essential foundation for understanding cybersecurity exposure within nuclear digital environments. Interconnected control architectures introduce vulnerabilities through engineering workstations, supervisory networks, maintenance interfaces, and data exchange mechanisms. Inadequate authentication, outdated software, insufficient network separation, and insecure communication protocols can increase opportunities for unauthorised interference. Opara et al. (2022) examine secure data exchange architectures in SCADA-controlled power systems, highlighting the importance of protecting information integrity and communication reliability across industrial control infrastructures.

The increasing convergence of information technology and operational technology further complicates cybersecurity risk management. Malatji, Marnewick, and von Solms (2022) identify technical capabilities, organisational preparedness, and coordinated security governance as important considerations for strengthening critical infrastructure resilience. Within nuclear environments, these concerns extend to managing external connectivity, third-party maintenance activities, and potential compromise of supporting digital assets.

Attack pathways may develop through interconnected components when weaknesses in access controls or system configuration permit unauthorised activity to reach operational networks. Lee et al. (2022) demonstrate how formalised attack patterns can support the identification of potential exploitation scenarios and inform appropriate cybersecurity countermeasures. Such approaches facilitate systematic examination of vulnerable interfaces without assuming that every compromised component provides direct access to reactor protection systems.

Cybersecurity threats become especially consequential when digital manipulation affects the behaviour of physical equipment. Zhang and Coble (2020) investigate cyberattack detection techniques for nuclear equipment, illustrating the importance of identifying anomalous operational information before compromised measurements influence control decisions.

Furthermore, interfaces connecting safety-related and security-related systems demand careful architectural evaluation. Busquim e Silva et al. (2021) demonstrate the relevance of cybersecurity assessment frameworks for examining vulnerabilities and potential consequences associated with digital interfaces in nuclear facilities.

Insider threats introduce additional complexities because authorised personnel may possess legitimate access to sensitive equipment and configuration functions. Campos and Alamaniotis

(2021) examine internal cyberattacks and forensic detection methods, emphasising the importance of recognising suspicious activities within nuclear operational environments. Consequently, comprehensive vulnerability assessment must consider technical weaknesses, human interactions, system interdependencies, and existing protective barriers while evaluating credible pathways through which cybersecurity incidents could compromise critical digital assets and nuclear safety functions.

3. Cybersecurity Risk Assessment Methods and Frameworks

3.1. Threat Identification and Vulnerability Assessment Techniques

Threat identification and vulnerability assessment are fundamental components of cybersecurity risk evaluation within nuclear power plant instrumentation and control (I&C) systems. These processes systematically examine potential adversaries, exploitable weaknesses, digital asset dependencies, and conditions under which malicious activities could compromise essential operational functions. Unlike conventional information technology assessments, nuclear cybersecurity evaluations must account for safety classifications, equipment availability, deterministic control requirements, and consequences associated with compromised protection systems. Eggers (2023) emphasises integrating cybersecurity considerations throughout digital I&C engineering to recognise potential vulnerabilities before they become embedded in safety-critical architectures. Threat identification commonly incorporates asset inventories, security architecture reviews, adversarial scenario development, and historical incident analysis. Han, Lee, and Seong (2022) propose an operating-experience-based approach using Bayesian updating to estimate cyber threat frequencies, demonstrating how documented events can contribute to structured assessments despite uncertainties surrounding nuclear cybersecurity data.

System-theoretic assessment provides another important technique for examining interactions between controllers, sensors, operators, and protective equipment. Son, Song, and Lee (2023) apply safety-oriented threat scenario identification and security control evaluation to prioritise cyber risks according to functional consequences. This approach enables analysts to investigate hazardous control interactions rather than concentrating exclusively on individual software weaknesses. Formal architectural modelling further supports vulnerability identification by establishing system boundaries, communication pathways, and security requirements. The International Electrotechnical Commission (IEC) (2023) describes modelling approaches applicable to digital I&C architectures, including asset grouping, security zones, and verification of information exchange restrictions. Complementarily, Jung et al. (2023) examine technical security control assessment as a means of determining whether implemented safeguards adequately address identified cyber threats.

Table 2. Threat identification and vulnerability assessment techniques for nuclear I&C systems

Assessment technique	Principal application	Expected assessment output
Critical asset inventory	Identify safety-relevant digital components	Verified asset register
Threat scenario modelling	Examine credible malicious activities	Documented threat scenarios
Configuration assessment	Identify insecure system settings	Configuration weakness report
Communication pathway analysis	Examine network interfaces and boundaries	Exposure and dependency map
System-theoretic analysis	Identify unsafe control interactions	Safety-relevant threat scenarios
Security control evaluation	Assess safeguard effectiveness	Control effectiveness findings
Passive monitoring and log analysis	Identify anomalous system activities	Indicators requiring investigation
Controlled simulation testing	Examine possible functional consequences	Validated assessment evidence

Source: Author's synthesis of the assessment principles presented in the cited literature. Techniques require plant-specific authorisation and safety controls.

Human and organisational vulnerabilities also require systematic consideration. Arinze et al. (2022) examine insider-threat concerns within Nigeria's nuclear security arrangements, identifying organisational preparedness and personnel awareness as important assessment considerations. Similarly, Saidu, Suleiman, and Akpan (2021) discuss broader cybersecurity challenges in Nigeria, supporting the relevance of security awareness and institutional capability development.

Regional threat intelligence can supplement technical assessment by identifying recurring incident characteristics. Pieterse (2021) analyses South African cyber incidents and highlights the importance of understanding evolving threat exposure, institutional vulnerabilities, and prevention capabilities.

3.2. Risk Quantification and Consequence-Based Evaluation Models

Risk quantification in nuclear power plant instrumentation and control (I&C) systems provides a systematic basis for evaluating cybersecurity threats according to their potential operational and safety consequences. Unlike conventional cybersecurity scoring, nuclear risk models must consider how malicious interference with critical digital assets influences protective functions, accident progression, and plant safety margins. Quantification therefore involves integrating threat characteristics, system vulnerabilities, control effectiveness, and consequence severity. Park and Lee (2019) demonstrate that probabilistic safety assessment (PSA) can identify the relative importance of cyberattack scenarios by evaluating their effects on safety-related equipment and plant risk indicators. Consequence-based assessment commonly employs fault trees, event trees, Bayesian networks, and probabilistic modelling to represent dependencies between digital component failures and adverse operational outcomes. Shin, Son and Heo (2017) integrate Bayesian networks with event-tree analysis to evaluate cybersecurity risks associated with nuclear I&C systems, demonstrating how conditional relationships can support assessments of protective

system vulnerabilities. Such methodologies are particularly valuable when direct cybersecurity experimentation could interfere with essential reactor functions.

Contemporary models increasingly incorporate adversarial behaviour and exploitation difficulty alongside consequence severity. Park and Lee (2020) develop a quantitative framework combining Bayesian belief networks and PSA to examine cyberattack scenarios according to their relative difficulty and potential nuclear safety implications. Similarly, Maccarone and Cole (2022) employ Bayesian game theory to represent strategic interactions under uncertainty, providing an analytical basis for evaluating defensive decisions against adaptive adversaries.

Table 3. Illustrative risk quantification and consequence-based evaluation models for nuclear I&C cybersecurity

Evaluation model	Principal assessment variables	Application to critical digital assets	Major limitation
Probabilistic safety assessment	Failure probabilities, accident sequences, safety consequences	Evaluates safety significance of compromised digital functions	Cyberattack probabilities are difficult to establish
Bayesian network analysis	Conditional probabilities and system dependencies	Models uncertainty and interconnected vulnerabilities	Sensitive to assumptions and prior probabilities
Event-tree analysis	Initiating events and protective system responses	Examines potential cyber-induced accident progression	Requires credible scenario definitions
Fault-tree analysis	Component failures and logical dependencies	Identifies combinations affecting protective functions	Limited representation of evolving adversarial behaviour
Bayesian game theory	Attacker strategies, defender decisions, uncertainty	Supports security resource allocation	Depends on assumptions about adversarial incentives
Graded risk assessment	Asset criticality, exposure, consequence severity	Prioritises protection according to functional importance	May produce qualitative or ordinal rankings

Source: Author's synthesis of established nuclear cybersecurity and probabilistic risk assessment methodologies. The models are illustrative analytical approaches rather than interchangeable regulatory requirements.

The applicability of graded approaches extends to research reactor environments. Vechgama et al. (2024) develop a cybersecurity risk analysis framework for a TRIGA reactor computational system, illustrating how protection requirements can be differentiated according to system importance and identified vulnerabilities. In Ghana, Abrefah and Ameyaw (2024) investigate PSA importance measures for a research reactor, demonstrating how quantitative indicators can identify safety-significant components and support prioritisation.

Consequence modelling also has implications for emergency preparedness. Perryman (2008) examines risk-informed emergency planning at South Africa's Koeberg Nuclear Power Station, demonstrating how probabilistic and deterministic assessments can inform protective action requirements.

Organisational considerations remain relevant when interpreting numerical risk estimates. Falemi et al. (2024) propose integrating workforce capabilities and operational analytics within enterprise risk management, providing a conceptual basis for incorporating human and institutional factors into broader risk governance.

3.3. Regulatory Standards and Risk Assessment Frameworks

Regulatory standards and risk assessment frameworks provide the institutional and technical foundations for safeguarding critical digital assets within nuclear power plant instrumentation and control (I&C) systems. Their principal purpose is to establish consistent requirements for identifying cybersecurity threats, evaluating potential consequences, implementing protective controls, and demonstrating compliance throughout the nuclear facility lifecycle. Unlike conventional cybersecurity governance, nuclear regulatory approaches must reconcile information security objectives with stringent requirements for functional independence, deterministic performance, and reactor safety. The International Atomic Energy Agency (IAEA) (2021) advocates a coordinated national computer security regime incorporating defined responsibilities, threat assessment, graded protection, and regulatory oversight.

International standards provide complementary mechanisms for implementing these requirements. The International Electrotechnical Commission (IEC) (2019) establishes provisions for coordinating cybersecurity and nuclear safety, particularly where security controls could adversely influence protective system performance. Such coordination requires cybersecurity measures to undergo appropriate engineering evaluation before implementation within safety-related digital environments. The broader industrial cybersecurity framework IEC 62443-3-2 provides structured procedures for defining system boundaries, establishing security zones and conduits, evaluating vulnerabilities, and determining target security levels. Its application to nuclear environments requires alignment with sector-specific safety obligations and licensing requirements (IEC, 2020).

Table 4. Comparative regulatory standards and cybersecurity risk assessment frameworks for nuclear I&C systems

Standard or framework	Primary regulatory or technical focus	Application to nuclear critical digital assets
IAEA NSS No. 42-G	National nuclear computer security governance	Threat assessment, graded protection, regulatory responsibilities
IEC 62859	Nuclear safety and cybersecurity coordination	Compatibility of security measures with safety functions
IEC 62443-3-2	Industrial control system risk assessment	Security zones, conduits, vulnerability assessment
NIST SP 800-82 Rev. 3	Operational technology cybersecurity	Asset protection, access control, monitoring and risk reduction
COBIT and ITIL	IT governance and service management	Accountability, auditability and organisational control
National cybercrime legislation	Criminalisation and investigation of cyber offences	Supporting legal and enforcement environment
Consequence-based security assessment	Risk-informed security prioritisation	Protection proportional to credible nuclear safety consequences

Source: Author's synthesis of the regulatory and technical frameworks examined in this section. The instruments have different legal statuses and are not universally interchangeable or mandatory across jurisdictions.

Risk assessment frameworks additionally emphasise the relationship between cybersecurity controls and operational requirements. Stouffer et al. (2023) provide guidance for identifying operational technology vulnerabilities and selecting protective measures compatible with system availability and safety constraints. Consequently, nuclear cybersecurity evaluations must accommodate equipment qualification, maintenance restrictions, and the limitations of intrusive security testing. Regulatory compliance also requires appropriate selection of risk assessment methodologies. Setianingsih et al. (2021) examine cybersecurity assessment approaches applicable to nuclear facilities, identifying defence-in-depth, safety–security integration, and probabilistic assessment as essential considerations when evaluating regulatory suitability.

National regulatory environments introduce further distinctions. South Africa (2020), through its Cybercrimes Act, establishes a broader legislative framework addressing cyber-related offences and supporting enforcement. Although not a nuclear-specific licensing instrument, this legislation provides relevant national legal context for cybersecurity governance.

Organisational compliance mechanisms likewise contribute to sustained cybersecurity implementation. Fadero et al. (2018) examine COBIT and ITIL governance frameworks within Nigerian institutions, demonstrating the relevance of accountability, audit practices, and structured technology management to regulatory compliance. Emerging regulatory approaches increasingly favour consequence-informed security arrangements. Ion and Llambias (2024) examine risk-based and security-by-design practices across selected nuclear jurisdictions, emphasising proportionate protection based on credible adverse consequences. Such approaches encourage regulatory consistency while preserving flexibility for advanced reactors and evolving digital architectures.

4. Cybersecurity Risk Mitigation and Defense Strategies

Cybersecurity risk mitigation within nuclear power plant instrumentation and control (I&C) systems requires an integrated defence strategy that preserves essential safety functions while reducing opportunities for malicious interference. Effective protection combines preventive, detective, responsive, and recovery-oriented measures, supported by systematic risk assessment and continuous security assurance. Mohan et al. (2024) emphasise the significance of incorporating cybersecurity into nuclear facility design, operational governance, and supply-chain management, recognising that technological safeguards must complement established nuclear safety arrangements. Defence-in-depth constitutes a fundamental protection principle, involving multiple independent security barriers across critical digital assets, communication networks, and administrative processes. Network segmentation, restricted connectivity, secure configuration management, and controlled maintenance access reduce opportunities for unauthorised interactions between operational and safety-related systems. Access governance further requires authentication, accountability, and periodic verification of privileges. Goncalves (2023) demonstrates the importance of evaluating access-control effectiveness through measurable security performance and residual-risk considerations.

Cryptographic protection offers additional safeguards for sensitive information and authorised communications. Shittu and Nabil (2023) demonstrate how attribute-based encryption enables differentiated information access according to defined user attributes. Such principles can inform protection of nuclear engineering records and maintenance information, provided implementation respects system qualification and operational constraints.

Distributed verification technologies also present opportunities for strengthening information integrity. Shittu et al. (2021) examine blockchain-based transactions within renewable microgrids, illustrating potential applications of traceable records and decentralised verification. However,

introducing comparable mechanisms into nuclear environments requires rigorous evaluation of computational overhead, interoperability, and safety implications.

Detection capabilities remain essential because preventive safeguards cannot eliminate every credible threat. Chaudhary et al. (2024) investigate anomaly detection techniques for nuclear operational data, demonstrating how analytical monitoring can support identification of abnormal system behaviour. Similarly, Ayodeji et al. (2024) develop an attention-based detection model for simulated cyberattacks affecting small modular reactor digital control systems, highlighting opportunities for intelligent monitoring of compromised sensor information.

Cybersecurity resilience additionally requires dependable response and recovery arrangements. Yoo et al. (2025) investigate self-healing control strategies against false-data injection attacks, combining anomaly detection with corrective control mechanisms in a simulated pressurised water reactor environment. These findings illustrate emerging possibilities for maintaining operational stability during cyber disturbances, although deployment within licensed safety systems would require extensive verification and regulatory acceptance.

5. Implementation Challenges and Future Research Directions

Cybersecurity risk mitigation within nuclear power plant instrumentation and control (I&C) systems requires coordinated preventive, detective, responsive, and recovery-oriented measures that preserve operational integrity and nuclear safety. Effective defence strategies must address vulnerabilities associated with critical digital assets, communication networks, software configurations, and authorised personnel. Clark and Rowland (2021) establish that nuclear cybersecurity defence-in-depth should integrate risk-informed asset prioritisation, protective barriers, and consequence assessment to reduce the likelihood that malicious digital interference compromises essential plant functions. Network segmentation, controlled system interfaces, restricted privileges, and secure configuration management constitute important preventive safeguards. These measures limit unnecessary communication between systems and reduce opportunities for unauthorised access. Dzobo, Tivani, and Mbatha (2024) examine cybersecurity challenges affecting the interconnected energy infrastructure in South Africa, highlighting the importance of resilient communication architectures and coordinated security measures.

Continuous monitoring strengthens defensive capabilities by identifying abnormal operational behaviour before disturbances escalate. Sunday and Omoegun (2022) examine sensor-based fault detection in automated equipment, demonstrating the relevance of continuous data acquisition and analytical monitoring for identifying operational anomalies. Within nuclear environments, comparable techniques can support anomaly identification when implemented through appropriately validated, non-intrusive monitoring arrangements.

Emerging artificial intelligence applications further extend cybersecurity monitoring capabilities. Shittu and Shittu (2024) investigate AI-enabled digital twins for predictive maintenance and operational optimisation, illustrating how computational representations and operational data can support fault identification. Their underlying principles may inform nuclear cybersecurity monitoring, although safety-critical applications require rigorous verification and compatibility assessments. Incident response represents another essential component of nuclear cybersecurity resilience. Lee et al. (2022) develop a decision-oriented cyberattack response planning model incorporating plant safety margins and alternative defensive actions. Such approaches can improve understanding of response priorities while ensuring that protective interventions do not inadvertently undermine reactor safety.

Organisational preparedness remains equally significant. Akhigbe, Falemi and Akin-Oluyomi (2024) examine employee readiness during technological adoption, emphasising workforce competence, structured training, and institutional adaptability. Nuclear cybersecurity programmes consequently require personnel familiarisation, access accountability, coordinated incident exercises, and established procedures for managing security-related modifications.

Broader infrastructure experience also demonstrates the consequences of inadequate cybersecurity governance. Timcke, Gaffley, and Rens (2023) examine cyber vulnerabilities affecting South Africa's Transnet, illustrating how organisational weaknesses and interconnected digital infrastructures can contribute to operational disruption.

Conclusion

This review examined the cybersecurity risks associated with critical digital assets in nuclear power plant instrumentation and control systems, establishing how digital modernisation influences exposure, safety assurance, and regulatory obligations. Its objectives were addressed through a synthesis of system architectures, asset identification principles, threat pathways, assessment methodologies, and protective strategies. The analysis demonstrates that cyber risk cannot be judged solely by software vulnerabilities or network accessibility; its significance depends on the functions an asset supports, the credibility of attack scenarios, and the potential consequences for reactor safety. A central finding is that reliable asset classification requires tracing digital dependencies across sensors, controllers, engineering workstations, communication interfaces, and human–machine systems. Defence-in-depth, functional independence, controlled connectivity, and secure configuration management remain essential, but their effectiveness depends on continuous verification. Probabilistic safety assessment, Bayesian modelling, scenario analysis, and graded risk evaluation provide complementary decision tools. Nevertheless, limited incident data, uncertain adversarial behaviour, and complex interdependencies constrain the precision of quantitative estimates. Regulatory standards offer necessary direction, although compliance alone does not establish operational resilience.

The review further identifies important implementation challenges involving legacy equipment, software qualification, personnel competence, supply-chain access, and the integration of emerging monitoring technologies. Artificial intelligence and digital twins offer opportunities for earlier anomaly recognition and improved situational awareness, but their deployment must not introduce unacceptable complexity or interfere with safety functions.

Accordingly, nuclear operators should maintain function-based digital asset inventories, prioritise assessments according to credible safety consequences, enforce independently verified security boundaries, and conduct periodic non-intrusive evaluations. Regulators and industry organisations should promote transparent risk criteria, targeted workforce training, secure procurement practices, and evidence-based incident learning. Future research should validate cybersecurity assessment models against representative nuclear configurations and investigate uncertainty, common-cause digital failures, and safe integration of intelligent detection systems. These measures would strengthen accountable, proportionate protection throughout the operational lifecycle.

References

Abrefah, R.G. and Ameyaw, F. (2024) 'Quantifying safety significance: An in-depth analysis of importance measures in Level 1 PSA for the VVR 10-MW water-water research reactor', Nuclear Science and Engineering, 198(10), pp. 2038–2050. DOI: 10.1080/00295639.2023.2284454.

Akhigbe, R., Falemi, A. and Akin-Oluyomi, O.T. (2024) 'An advanced framework for technology adoption that supports employee readiness in modern organizations', International Journal of Advanced Multidisciplinary Research and Studies, 4(1), pp. 1637–1659. DOI: 10.62225/2583049X.2024.4.1.5344.

Ameyaw, F., Emi-Reynolds, B. and Abrefah, R. (2025) 'Multi-hazard risk assessment in probabilistic safety analysis: An integrated framework for Ghana's nuclear infrastructure', Safety and Reliability, published online 11 November. DOI: 10.1080/09617353.2025.2575707.

Arinze, U.C., Longe, O.B. and Eneh, A.H. (2020) 'Regulatory perspective on nuclear cyber security: The fundamental issues', International Journal of Nuclear Security, 6(1), Article 3. DOI: 10.7290/ijns060103.

Arinze, U.C., Sambo, I., Edward, N. and Okonkwo, I. (2022) 'Tackling potential insider threat in nuclear and radiological facilities and Nigeria's nuclear security architecture: Tools, preventive and protective measures', International Conference on the Safety and Security of Radioactive Sources: Accomplishments and Future Endeavours, Vienna, Austria, 20–24 June. International Atomic Energy Agency. Available at: https://conferences.iaea.org/event/262/contributions/21282/.

Asare, E. and Bonney, J.A. (2025) 'Nuclear and cyber security in Africa: Current and future risks', Proceedings of the Institute of Nuclear Materials Management Annual Meeting. Institute of Nuclear Materials Management. Available at: https://resources.inmm.org/annual-meeting-proceedings/nuclear-and-cyber-security-africa-current-and-future-risks.

Ayodeji, A., Di Buono, A., Pierce, I. and Ahmed, H. (2024) 'Wavy-attention network for real-time cyber-attack detection in a small modular pressurized water reactor digital control system', Nuclear Engineering and Design, 424, Article 113277. DOI: 10.1016/j.nucengdes.2024.113277.

Ayodeji, A., Mohamed, M., Li, L., Di Buono, A., Pierce, I. and Ahmed, H. (2023) 'Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors', Progress in Nuclear Energy, 161, Article 104738. DOI: 10.1016/j.pnucene.2023.104738.

Busquim e Silva, R.A., Piqueira, J.R.C., Cruz, J.J. and Marques, R.P. (2021) 'Cybersecurity assessment framework for digital interface between safety and security at nuclear power plants', International Journal of Critical Infrastructure Protection, 34, Article 100453. DOI: 10.1016/j.ijcip.2021.100453

Campos, B.M. and Alamaniotis, M. (2021) 'Review of internal cyber attacks in nuclear facilities and an artificial neural network model for implementing internal cyberforensics', Nuclear Technology and Radiation Protection, 36(2), pp. 128–138. DOI: 10.2298/NTRP2102128C.

Chaudhary, A., Han, J., Kim, S., Kim, A. and Choi, S. (2024) 'Anomaly detection and analysis in nuclear power plants', Electronics, 13(22), Article 4428. DOI: 10.3390/electronics13224428.

Clark, A.J. and Rowland, M.T. (2021) Safety and Security Defense-in-Depth for Nuclear Power Plants. SAND2021-14591. Albuquerque, NM: Sandia National Laboratories. DOI: 10.2172/1832309.

Dzobo, O., Tivani, L. and Mbatha, L. (2024) 'A review on cybersecurity for distributed energy resources: Opportunities for South Africa', Journal of Infrastructure, Policy and Development, 8(15), Article 8631. DOI: 10.24294/jipd8631.

Eggers, S.L. (2023) 'Cyber risk considerations for nuclear digital I&C systems', in Risk-Informed Methods and Applications in Nuclear and Energy Engineering: Modeling, Experimentation, and Validation. Amsterdam: Elsevier, pp. 55–72. DOI: 10.1016/B978-0-323-91152-8.00003-X.

Fadero, S., Oyesiji, S.O., Nwakamma, S. and Jooda, D. (2018) 'IT governance frameworks (COBIT/ITIL) and their impact on regulatory compliance in Nigerian insurance firms', IRE Journals, 2(5), pp. 478–496. DOI: 10.64388/IREV2I5-1722619.

Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2024) 'A conceptual enterprise risk management model that integrates HR strategy with operational analytics', International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), pp. 1730–1753. DOI: 10.54660/.IJMRGE.2024.5.6.1730-1753.

Goncalves, D.P. (2023) 'Security access control effectiveness design', South African Journal of Industrial Engineering, 34(3), pp. 84–96. DOI: 10.7166/34-3-2954.

Han, S.M., Lee, C. and Seong, P.H. (2022) 'Estimating the frequency of cyber threats to nuclear power plants based on operating experience analysis', International Journal of Critical Infrastructure Protection, 37, Article 100523. DOI: 10.1016/j.ijcip.2022.100523.

Hunton, P., England, R., Herrell, D., Lawrie, S. and Samselski, M. (2023) 'Safety-related instrumentation and control pilot upgrade: Initial scoping phase implementation and lessons learned', Nuclear Technology, 209(3), pp. 366–376. DOI: 10.1080/00295450.2022.2053808.

Ibrahim, M.I., Zaky, M.M., Hassan, M.H. and Nagy, M. (2020) 'Development of neutron flux measurement module for research reactors based on FPGA. Part-1-Model development and generic verification', Alexandria Engineering Journal, 59(6), pp. 4107–4120. DOI: 10.1016/j.aej.2020.07.016.

International Atomic Energy Agency (IAEA) (2021) Computer Security Techniques for Nuclear Facilities. IAEA Nuclear Security Series No. 17-T (Rev. 1). Vienna: International Atomic Energy Agency. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf.

International Atomic Energy Agency (IAEA) (2021) Computer Security for Nuclear Security. IAEA Nuclear Security Series No. 42-G. Vienna: International Atomic Energy Agency. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.

International Electrotechnical Commission (IEC) (2019) Nuclear power plants: Instrumentation, control and electrical power systems: Cybersecurity requirements. IEC 62645:2019. 2nd edn. Geneva: International Electrotechnical Commission. Available at: https://webstore.iec.ch/en/publication/32904.

International Electrotechnical Commission (IEC) (2019) Nuclear Power Plants: Instrumentation and Control Systems: Requirements for Coordinating Safety and Cybersecurity. IEC 62859:2016+AMD1:2019 CSV. Geneva: International Electrotechnical Commission. Available at: https://webstore.iec.ch/en/publication/65893.

International Electrotechnical Commission (IEC) (2020) Security for Industrial Automation and Control Systems: Part 3-2: Security Risk Assessment for System Design. IEC 62443-3-2:2020. Geneva: International Electrotechnical Commission. Available at: https://webstore.iec.ch/en/publication/30727.

International Electrotechnical Commission (IEC) (2023) Nuclear Power Plants: Instrumentation and Control Systems: Use of Formal Security Models for I&C Security Architecture Design and Assessment. IEC TR 63415:2023. Geneva: International Electrotechnical Commission. Available at: https://webstore.iec.ch/en/publication/71453.

Ion, R. and Llambias, J.M. (2024) 'A brief assessment of regulatory requirements/expectations on consequence-based security and security-by-design approaches in select regulatory jurisdictions', Proceedings of the Canadian Nuclear Society Annual Conference, 2024. Canadian Nuclear Society. Available at: https://proceedings.cns-snc.ca/index.php/pcns/article/view/7710.

Joo, S., Seo, S.M. and Suh, Y.S. (2017) 'Identification of critical digital assets for nuclear instrumentation system in research reactor', International Symposium on Future I&C for Nuclear Power Plants (ISOFIC 2017). Available at: https://www.kns.org/files/int_paper/paper/ISOFIC_2017_10/ISOFIC-2017-Sungmoon-JOO.pdf.

Jung, D., Shin, J., Lee, C., Kwon, K. and Seo, J.T. (2023) 'Cyber security controls in nuclear power plant by technical assessment methodology', IEEE Access, 11, pp. 15229–15241. DOI: 10.1109/ACCESS.2023.3244991.

Kim, S., Heo, G., Zio, E., Shin, J. and Song, J.G. (2020) 'Cyber attack taxonomy for digital environment in nuclear power plants', Nuclear Engineering and Technology, 52(5), pp. 995–1001. DOI: 10.1016/j.net.2019.11.001.

Lee, C., Han, S.M., Chae, Y.H. and Seong, P.H. (2022) 'Development of a cyberattack response planning method for nuclear power plants by using the Markov decision process model', Annals of Nuclear Energy, 166, Article 108725. DOI: 10.1016/j.anucene.2021.108725.

Lee, M., Kwon, H. and Yoon, H. (2022) 'Compliance-driven cybersecurity planning based on formalized attack patterns for instrumentation and control systems of nuclear power plants', Security and Communication Networks, 2022, Article 4714899. DOI: 10.1155/2022/4714899.

Lee, S.W. and Lee, J.H. (2024) 'Improving the efficiency of cybersecurity risk analysis methods for nuclear power plant control systems', Journal of the Korea Institute of Information Security and Cryptology, 34(3), pp. 537–552. DOI: 10.13089/JKIISC.2024.34.3.537.

Lezzi, M., Martino, L., Damiani, E. and Yeun, C.Y. (2025) 'A systematic literature review on AI-based cybersecurity in nuclear power plants', Journal of Cybersecurity and Privacy, 5(4), Article 79. DOI: 10.3390/jcp5040079.

Maccarone, L.T. and Cole, D.G. (2022) 'Bayesian games for the cybersecurity of nuclear power plants', International Journal of Critical Infrastructure Protection, 37, Article 100493. DOI: 10.1016/j.ijcip.2021.100493.

Malatji, M., Marnewick, A.L. and von Solms, S. (2022) 'Cybersecurity capabilities for critical infrastructure resilience', Information and Computer Security, 30(2), pp. 255–279.

Mohan, P., Glantz, C., Landine, G., Gourisetti, S.N. and Motkuri, R.K. (2024) 'Cybersecurity and nuclear facilities', in Kapur, S.P., Rajagopalan, R.P. and Wueger, D. (eds.) The Challenges of Nuclear Security. Cham: Palgrave Macmillan. DOI: 10.1007/978-3-031-56814-5_7.

National Nuclear Regulator (2015) Guidance on the Implementation of Cyber or Computer Security for Nuclear Facilities. Regulatory Guide RG-0014, Revision 0. Centurion, South Africa: National Nuclear Regulator. Available at: National Nuclear Regulator RG-0014.

Nigerian Nuclear Regulatory Authority (2024) USDOE Partners NNRA on Cybersecurity of Nuclear Facilities in Nigeria. Abuja: Nigerian Nuclear Regulatory Authority. Available at: NNRA official publication.

Obeng, H.K., Amponsah-Abu, E.O., Nayrko, B.J.B., Edziah, R., Gasu, P.D. and Ampong, A.G. (2021) 'Failure mode and effect analysis for a programmable logic controller-based control unit for a miniature neutron source reactor pneumatic transfer system', Journal of Electrical and Computer Engineering, 2021, Article 7653857. DOI: 10.1155/2021/7653857.

Obeng, H.K., Edziah, R. and Amponsah-Abu, E.O. (2025) 'Reliability analysis for a new semiautomated control and monitoring system for GHARR-1 MNSR using failure modes, effects, and criticality analysis', Journal of Electrical and Computer Engineering, 2025(1), Article 4692754. DOI: 10.1155/jece/4692754.

Omoegun, G.O., Sunday, E.A., Essien, M.A. and Oluokun, O.A. (2023) 'Vibration-based condition monitoring of rotating machinery using LabVIEW', International Journal of Scientific Research in Civil Engineering, 7(6), pp. 82–108. DOI: 10.32628/IJSRCE237529.

Omoegun, G.O., Sunday, E.A., Essien, M.A. and Oluokun, O.A. (2024) 'Implementing smart automation solutions in medium-scale industries using SCADA systems', International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(5), pp. 1207–1231. DOI: 10.32628/CSEIT241061242.

Opara, I.S., Shittu, M.A., Adeniji, I.O. and Shittu, H. (2022) 'Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems', IRE Journals, 6(3), pp. 359–380. DOI: 10.64388/IREV6I3-1714041.

Ouni, B., Aussagues, C., Dhouib, S. and Mraidha, C. (2021) 'Model-driven architectural framework towards safe and secure nuclear power reactors', Sensors, 21(15), Article 5136. DOI: 10.3390/s21155136.

Park, J.W. and Lee, S.J. (2019) 'Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants', Nuclear Engineering and Technology, 51(1), pp. 138–145. DOI: 10.1016/j.net.2018.09.009.

Park, J.W. and Lee, S.J. (2020) 'A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence', Annals of Nuclear Energy, 142, Article 107432. DOI: 10.1016/j.anucene.2020.107432.

Perryman, L.J. (2008) 'Risk-informed emergency planning requirements for Koeberg Nuclear Power Station', International Journal of Risk Assessment and Management, 8(1–2), pp. 80–93. DOI: 10.1504/IJRAM.2008.016143.

Pieterse, H. (2021) 'The cyber threat landscape in South Africa: A 10-year review', The African Journal of Information and Communication, 28, pp. 1–21. DOI: 10.23962/10539/32213.

Porthin, M., Liinasuo, M. and Kling, T. (2020) 'Effects of digitalization of nuclear power plant control rooms on human reliability analysis: A review', Reliability Engineering & System Safety, 194, Article 106415. DOI: 10.1016/j.ress.2019.03.022.

Rowland, M.T., Maccarone, L.T. and Clark, A.J. (2023) 'Using the information harm triangle to identify risk-informed cybersecurity strategies for instrumentation and control systems', Nuclear Technology, 209(3), pp. 471–487. DOI: 10.1080/00295450.2022.2087841.

Saidu, I.R., Suleiman, T. and Akpan, U.E. (2021) 'The challenges of security threat in Nigeria cyberspace', FUDMA Journal of Sciences, 5(1), pp. 193–201. DOI: 10.33003/fjs-2021-0501-554.

Setianingsih, L.S., Pulungan, R., Putra, A.E., Wibowo, M.E. and Syarip (2021) 'Risk assessment methods for cybersecurity in nuclear facilities: Compliance to regulatory requirements', International Journal of Advanced Computer Science and Applications, 12(9). DOI: 10.14569/IJACSA.2021.0120979.

Sharma, A., Kosasih, E., Zhang, J., Brintrup, A. and Calinescu, A. (2022) 'Digital twins: State of the art theory and practice, challenges, and open research questions', Journal of Industrial Information Integration, 30, Article 100383. DOI: 10.1016/j.jii.2022.100383.

Shin, J., Choi, J.G., Lee, J.W., Lee, C.K., Song, J.G. and Son, J. (2021) 'Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed', Nuclear Engineering and Technology, 53(10), pp. 3319–3326. DOI: 10.1016/j.net.2021.04.031.

Shin, J., Son, H. and Heo, G. (2017) 'Cyber security risk evaluation of a nuclear I&C using BN and ET', Nuclear Engineering and Technology, 49(3), pp. 517–524. DOI: 10.1016/j.net.2016.11.004.

Shittu, H. and Nabil, M. (2023) 'Smart supply chain management with attribute-based encryption access control', Proceedings of the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 198–204. DOI: 10.1109/CCWC57344.2023.10099268.

Shittu, H., Olagunju, F. and Shittu, M. (2024) 'Cyber physical resilience in digital substations: IoT-enabled adaptive protection for secure DER integration', International Journal of Science, Architecture, Technology and Environment, 1(3). DOI: 10.63680/ijsate032532.08.

Shittu, H.A. and Shittu, M.A. (2024) 'AI-powered digital twins for predictive maintenance and operational optimization of renewable energy systems', International Journal of Science, Architecture, Technology and Environment, 1(7), pp. 151–163. DOI: 10.63680/ijsate0324085.011.

Shittu, H.A., Shittu, M.A., Adeleke, O.J. and Adedokun, O.J. (2021) 'Blockchain-based energy trading models for peer-to-peer renewable microgrids', International Journal of Research in Electrical and Electronics Engineering, 4(3), pp. 1–19. DOI: 10.34218/IJREEE_04_03_001.

Shittu, M.A., Shittu, H., Adeleke, O.J. and Adedokun, O.J. (2023) 'Digital twin modeling for real-time monitoring and fault detection in smart substations', International Journal of Industrial Engineering Research and Development, 14(2), pp. 25–44. DOI: 10.34218/IJIERD_14_02_003.

Son, K.S., Song, J.G. and Lee, J.W. (2023) 'Development of the framework for quantitative cyber risk assessment in nuclear facilities', Nuclear Engineering and Technology, 55(6), pp. 2034–2046. DOI: 10.1016/j.net.2023.03.023.

Son, K.S., Song, J.G., Hahm, I. and Lee, J.W. (2025) 'Quantifying cyber risk: A model for evaluating safety impacts of cyber threats on NPPs', Nuclear Engineering and Technology, 57(10), Article 103675. DOI: 10.1016/j.net.2025.103675.

South Africa (2020) Cybercrimes Act 19 of 2020. Pretoria: Government of South Africa. Available at: https://www.gov.za/documents/cybercrimes-act-19-2020-english-afrikaans-01-jun-2021-0000.

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A. and Thompson, M. (2023) Guide to Operational Technology (OT) Security. NIST Special Publication 800-82, Revision 3. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-82r3.

Sunday, E.A. and Omoegun, G.O. (2022) 'Automation of process control systems using Siemens TIA Portal: A case study approach', International Journal of Scientific Research in Mechanical and Materials Engineering, 6(5), pp. 30–55. Available at: https://ijsrmme.com/IJSRMME18210.

Sunday, E.A. and Omoegun, G.O. (2022) 'Smart fault detection in HVAC systems using sensor-based monitoring', International Journal of Scientific Research in Science, Engineering and Technology, 7(4), pp. 380–403. Reported DOI: 10.32628/IJSRSET229473.

Timcke, S., Gaffley, M. and Rens, A. (2023) 'The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet', The African Journal of Information and Communication, 32. DOI: 10.23962/ajic.i32.16949.

Tomažič, S., Nelson, T. and Šeruga, T. (2024) 'Conducting cybersecurity regulatory inspections at nuclear facilities', International Journal of Computer Applications, 186(12), pp. 17–24. DOI: 10.5120/ijca2024923510.

U.S. Nuclear Regulatory Commission (2010) Cyber Security Programs for Nuclear Facilities. Regulatory Guide 5.71. Washington, DC: U.S. Nuclear Regulatory Commission. Available at: https://www.nrc.gov/cdn/nmss/pdf/regguide571.pdf.

U.S. Nuclear Regulatory Commission (2024) 'Protection of digital computer and communication systems and networks', Code of Federal Regulations, Title 10, Part 73, §73.54. Washington, DC: U.S. Government Publishing Office. Available at: 10 CFR §73.54, 2024 Edition.

Vechgama, W., Dararutana, C., Pechrak, A., Wetchagarun, S., Sasawattakul, W. and Silva, K. (2024) 'Development of cyber risk analysis framework for core computational system of TRIGA reactor using graded approach', Annals of Nuclear Energy, 197, Article 110281. DOI: 10.1016/j.anucene.2023.110281.

Yoo, S., Mohler, G. and Zhang, F. (2025) 'Self-healing control of nuclear power plants under false data injection attacks', Nuclear Science and Engineering, 199(1), pp. 162–175. DOI: 10.1080/00295639.2024.2372520.

Zhang, F. and Coble, J. (2020) 'Robust localized cyber-attack detection for key equipment in nuclear power plants', Progress in Nuclear Energy, 128, Article 103446. DOI: 10.1016/j.pnucene.2020.103446.

Zhang, F. and Kelly, K. (2023) 'Overview and recommendations for cyber risk assessment in nuclear power plants', Nuclear Technology, 209(3), pp. 488–502. DOI: 10.1080/00295450.2022.2092356.

Zhang, H., Bao, H., Shorthill, T. and Quinn, E. (2023) 'An integrated risk assessment process of safety-related digital I&C systems in nuclear power plants', Nuclear Technology, 209(3), pp. 377–389. DOI: 10.1080/00295450.2022.2076486.