Applied Science, Computing and Energy, 2026, 4(6), 994-1007

Legal Liability for Artificial Intelligence-Assisted Nuclear Safety Decisions: A Comparative Assessment of Operator Responsibility, Regulatory Accountability, and Compensation for Nuclear Damage

Grace Ritsemwa Dallong-Opadotun

Received: 11 June 2026/Accepted: 17 August 2026/ Published: 24 August 2026

Abstract: *Artificial intelligence is moving into nuclear engineering and regulatory work through anomaly detection, predictive maintenance, document review, simulation, information retrieval, and decision support. The legal consequence is not that established responsibility disappears, but that decision-making becomes distributed across operators, regulators, software suppliers, data providers, and technical support organizations. This article examines how existing nuclear law should allocate responsibility when an AI-assisted decision contributes to unsafe operation, defective regulatory action, or nuclear damage. It uses doctrinal and comparative analysis of the Vienna Convention on Civil Liability for Nuclear Damage, selected national nuclear liability regimes, IAEA safety standards, emerging work in the nuclear sector on AI, and peer-reviewed scholarship on AI liability and nuclear law. Three legal questions are separated: operational responsibility for safety, public-law accountability for regulatory decisions, and civil compensation for nuclear damage. The analysis finds that AI should not displace the nuclear operator's prime responsibility for safety. Under channeled nuclear liability regimes, victims ordinarily claim against the operator without proving fault, while claims against suppliers are restricted, and operator recourse is limited. Defective AI may therefore alter technical causation without necessarily altering the victim-facing defendant. This makes contractual governance important: operators should preserve validation duties, audit rights, access to technical records, cybersecurity obligations, and express recourse clauses in the procurement of safety-significant AI. Where a regulator uses AI, statutory powers should remain attributable to authorized human officials; AI should support, not autonomously exercise, licensing, inspection or enforcement authority. Nigeria is a party to the 1963 Vienna Convention but not the 1997 Protocol or the Convention on Supplementary Compensation for Nuclear Damage. The article argues that AI provides an additional reason for Nigeria to review both nuclear liability modernization and nuclear digital-governance rules. A workable framework should preserve clear human and institutional responsibility while requiring traceability, validation, and reviewability across the AI decision chain.*

Keywords: *Artificial intelligence; Nuclear liability; Operator responsibility; Regulatory accountability; Nuclear damage; Human oversight; Nigeria; AI governance.*

Grace Ritsemwa Dallong-Opadotun
Department of Jurisprudence and International Law, Faculty of Law, National Open University of Nigeria
Email: ritsemwa500@gmail.com
https://orcid.org/0000-0002-6370-1483

1.0 Introduction

Artificial intelligence (AI) is increasingly relevant to nuclear energy because nuclear facilities generate large volumes of operational, maintenance, inspection, safety, and environmental data requiring rapid and accurate analysis. AI can support anomaly detection, predictive maintenance, simulation, information retrieval, document analysis, and technical decision-making. These capabilities are particularly valuable in complex or emergency conditions, where operators must interpret multiple interacting parameters within limited time. Karim and Muhammad-Sukki (2022) note that AI can

provide expert guidance and rapid access to extensive information in nuclear power plant operations, although AI failure may also create physical and safety risks. Thus, AI deployment in nuclear energy presents not only technological opportunities but also significant legal and governance questions.

The development of nuclear energy depends on appropriate infrastructure, technical expertise, reliable equipment, and effective knowledge management. Eddy (2024) emphasizes the importance of technological and institutional capacity for sustainable nuclear development, while Eddy and Uchenna (2025) highlight the role of reliable scientific infrastructure in supporting nuclear science. Similarly, Eddy *et al*. (2025) identify effective knowledge management as essential for maintaining nuclear expertise and supporting sustainable development in Nigeria. These factors are particularly relevant to AI because its reliability depends on the quality of data, software, hardware, human expertise, validation, cybersecurity, and institutional governance.

AI applications are already extending into nuclear safety and regulatory activities. Eddy (2026), for example, demonstrated the use of explainable AI for multimodal anomaly detection in nuclear power plants, highlighting its potential for improving safety and reliability. The OECD Nuclear Energy Agency (NEA) reported in 2026 that nuclear regulators from several countries were examining AI applications, including information retrieval, simulation, and regulatory processes, while emphasizing the continuing importance of human expertise (OECD Nuclear Energy Agency [NEA], 2026). The International Atomic Energy Agency (IAEA) has similarly identified AI-related issues in nuclear installation safety and regulatory decision-making as emerging areas requiring regulatory and technical consideration (IAEA, 2026).

The increasing use of AI raises a fundamental legal question: who is responsible when an AI-assisted nuclear decision contributes to harm? A conventional safety decision may be attributed to an operator or authorized official, whereas an AI-assisted decision may involve developers, software suppliers, system integrators, data providers, technical support organizations, operators, and regulators. Errors may result from defective software, inadequate data, inappropriate model selection, poor integration, insufficient validation, cybersecurity failures, or excessive reliance on AI recommendations. Consequently, responsibility may involve a network of technical and institutional actors.

The wider AI-liability literature recognizes this complexity. Giuffrida (2019) argues that delegation of decision-making to AI does not eliminate human or institutional responsibility. Porter *et al*. (2025) similarly conceptualize AI responsibility as a network involving different actors, events, and forms of responsibility. Ajakaye (2024), through a comparative analysis of United States and European approaches, identifies causation, foreseeability, negligence, risk classification, conformity assessment, and accountability as important issues in AI liability. Vellinga (2024) further observes that AI's opacity, autonomy, and complexity can create difficulties in establishing causation and obtaining compensation. However, these studies largely address AI liability generally rather than its interaction with the specialized legal framework governing nuclear damage.

Nuclear liability law presents a distinctive legal context. International nuclear liability regimes generally channel liability for nuclear damage to the operator of the nuclear installation and impose liability without requiring victims to establish ordinary fault or negligence. They also provide rules concerning financial security, compensation, jurisdiction, and the types of compensable damage (IAEA, n.d.). This structure is intended to facilitate predictable and effective compensation while providing legal certainty for operators, suppliers, insurers, governments, and potential victims. The result is an important distinction between technical causation and legal responsibility: an AI developer or supplier may contribute technically to an accident, while the operator may remain the legally responsible party for

compensating victims. Karim and Muhammad-Sukki (2022) identify this issue as insufficiently tested in the context of AI-related nuclear damage.

A further distinction is required between operator safety responsibility, regulatory accountability, and civil compensation. The use of AI does not necessarily transfer the operator's primary responsibility for nuclear safety to the AI developer or software provider. Operators must still ensure appropriate selection, validation, monitoring, maintenance, and supervision of safety-significant AI systems. Conversely, where regulators employ AI for licensing, inspection, compliance monitoring, or enforcement, the central issues include statutory authority, human review, transparency, traceability, procedural fairness, and judicial or administrative review. These issues differ from questions concerning compensation for nuclear damage.

Despite increasing research on AI liability, nuclear safety, and nuclear liability, these areas remain insufficiently integrated. Existing AI scholarship examines attribution, causation, explainability, and compensation (Ajakaye, 2024; Porter *et al*., 2025; Vellinga, 2024), while nuclear-law frameworks establish specialized principles of operator responsibility and channelled liability (IAEA, n.d.). Research on AI in nuclear facilities demonstrates its potential for safety and operational applications (Eddy, 2026; Karim & Muhammad-Sukki, 2022), but limited attention has been given to how AI-assisted nuclear decisions interact simultaneously with operator responsibility, regulatory accountability, and civil compensation. This constitutes the principal knowledge gap addressed by the present study.

The issue is particularly relevant to Nigeria, which is a party to the 1963 Vienna Convention on Civil Liability for Nuclear Damage and continues to develop its nuclear science, infrastructure, technical capacity, and knowledge-management systems (IAEA, n.d.; Eddy, 2024; Eddy *et al*., 2025). As AI becomes increasingly relevant to nuclear operations and regulatory processes, Nigeria and other emerging nuclear jurisdictions require legal frameworks capable of accommodating AI without weakening established principles of nuclear safety and victim compensation.

Accordingly, this study aims to comparatively examine how existing nuclear liability and regulatory frameworks allocate legal responsibility when AI contributes to nuclear safety decisions, regulatory actions, or nuclear damage. It addresses three questions: (1) who remains responsible for operational nuclear safety when AI contributes to a safety-significant decision; (2) how should public-law accountability operate when regulators use AI; and (3) how should victims be compensated when an AI-related failure contributes to nuclear damage? The study is significant because it provides a framework for clarifying responsibility among nuclear operators, regulators, AI developers, suppliers, and other technical actors. It also highlights the importance of human oversight, validation, traceability, cybersecurity, auditability, and contractual recourse for safety-significant AI. For Nigeria, the analysis provides a basis for considering how nuclear liability modernization and emerging AI-governance requirements can develop together while preserving clear institutional responsibility and effective compensation for nuclear damage.

2.0 Materials and Methods

2.1 Doctrinal and Comparative Legal Method

This study employs a doctrinal and comparative legal research methodology. The doctrinal analysis examines the Vienna Convention on Civil Liability for Nuclear Damage, relevant IAEA explanatory materials and Safety Standards, Nigeria's treaty status, and selected national nuclear liability legislation. The comparative component examines Canada, the United Kingdom, and the United States to identify how different legal systems allocate responsibility for nuclear safety, nuclear

damage, and compensation. The analysis is supplemented by peer-reviewed literature on nuclear liability, AI liability, AI governance, and AI applications in nuclear energy, including Giuffrida (2019), Heffron *et al*. (2016), Karim and Muhammad-Sukki (2022), Cha (2024), Henson (2024), and Klebanov and Lizikova (2025).

The jurisdictions and sources were selected because they provide relevant examples of operator-focused nuclear liability, regulatory responsibility, and emerging approaches to AI-related accountability. Primary legal materials are treated as the principal sources for determining applicable legal rules, while scholarly literature and institutional publications are used to interpret, contextualize, and critically examine those rules.

The study is prospective rather than case-based. It does not assume the existence of an established judicial precedent concerning AI-caused nuclear damage where such precedent has not been identified. No reported Nigerian judicial decision was identified in the legal and institutional sources reviewed that directly addresses nuclear damage resulting from AI-assisted decision-making. The study therefore examines how existing legal principles would apply if AI became materially involved in a nuclear safety or regulatory decision. Where the law remains unsettled, the analysis identifies the uncertainty and distinguishes established legal rules from interpretive or prospective arguments.

2.2 Analytical Framework: Responsibility, Accountability, and Compensation

The analysis is organized around three distinct but interconnected concepts: responsibility, accountability, and compensation. *Responsibility* refers primarily to the legal and institutional duty to ensure the safe operation of a nuclear installation. *Accountability* concerns the legality, transparency, reviewability, and attribution of decisions made by public regulatory authorities. *Compensation* concerns the legal allocation of financial responsibility for recognized nuclear damage following a nuclear incident.

These concepts are related but are not legally interchangeable. An operator may retain responsibility for nuclear safety even where a regulator has approved a particular technology or safety system. Conversely, a regulator may be accountable for an unlawful licensing, inspection, or enforcement decision without becoming the operator liable for nuclear damage. Similarly, an AI developer or software supplier may contribute technically to a failure while the applicable nuclear liability regime channels the victim's compensation claim to the nuclear operator.

The analytical framework therefore distinguishes technical causation from legal responsibility. AI may complicate the technical and evidentiary chain linking an incident to particular actors, but the presence of AI does not automatically alter established categories of operator responsibility, regulatory accountability, or nuclear compensation. This distinction provides the basis for assessing whether existing nuclear liability regimes can accommodate AI-assisted decision-making without creating uncertainty regarding the party responsible for safety or compensation.

2.3 Comparative Analytical Procedure

The comparative analysis examines each jurisdiction against common legal dimensions: (i) the allocation of primary responsibility for nuclear safety; (ii) the basis and scope of operator liability; (iii) the treatment of suppliers and third parties; (iv) financial security and compensation mechanisms; (v) regulatory responsibility and reviewability; and (vi) the potential implications of AI-assisted decision-making. The findings are then compared with the international framework and Nigeria's existing treaty position to identify areas of legal continuity, uncertainty, and possible regulatory development.

3.0 Results and Discussion

3.1 AI-assisted nuclear decisions as socio-technical decisions

AI should not be treated as an isolated technological actor in nuclear decision-

making. A safety-significant AI system operates within a broader socio-technical arrangement involving data selection, model development, validation, software interfaces, cybersecurity, operating procedures, human review, and organizational decisions. Consequently, the safety and legal implications of an AI-assisted decision depend not only on the model's performance but also on how the system is developed, validated, deployed, monitored, and used.

The importance of reliability, safety, transparency, and human oversight is recognized in contemporary AI governance. Tabassi (2023) identifies validity, reliability, safety, accountability, transparency, and explainability as important characteristics of trustworthy AI, while the Organisation for Economic Co-operation and Development (OECD, 2024) emphasizes transparency, robustness, safety, accountability, and traceability in its AI Principles. These principles are particularly relevant to nuclear applications because an AI system that performs satisfactorily under controlled conditions may nevertheless become unsafe if it operates outside its validated environment or if its limitations are not understood by human users.

For legal analysis, AI use in nuclear activities can be viewed at four levels. The first involves information retrieval or summarization; the second involves prediction or classification, such as identifying equipment degradation; the third involves recommending a safety or regulatory action; and the fourth involves executing an action with limited immediate human intervention. As the authority and potential consequences of an AI system increase, the need for formal qualification, independent validation, controlled updates, traceable records, and meaningful human intervention also increases. This graded approach is consistent with the broader emphasis on risk-based AI governance and the nuclear safety principle of applying controls proportionate to safety significance (IAEA, 2016c; Tabassi, 2023).

3.2 The Operator's Prime Responsibility for Safety

The IAEA's fundamental safety framework places primary responsibility for safety on the person or organization responsible for a facility or activity. Regulatory approval does not transfer this responsibility from the operator (IAEA, 2006, 2016a). This principle remains applicable when AI is incorporated into operational decision-making.

Accordingly, an operator should not avoid responsibility merely because a safety-related decision was based on an AI recommendation. The relevant legal and safety inquiry should include whether the operator selected an appropriate system, defined its authorized application, verified and validated its performance, controlled model and data changes, provided competent human review, monitored performance, and maintained appropriate fallback arrangements. These are organizational decisions that remain within the operator's responsibility even where the AI system is supplied by a third party.

Karim and Muhammad-Sukki (2023) similarly identify difficulties in applying existing liability principles to AI-related failures in nuclear power plants, while concluding that existing nuclear liability and tort principles provide an important starting point. Klebanov and Lizikova (2025) likewise emphasize that AI applications in nuclear energy require legal adaptation while retaining the established nuclear regulatory framework.

The principle of operator responsibility also supports nuclear safety culture. If responsibility were routinely transferred to software suppliers whenever AI was involved, operators could potentially treat automated recommendations as substitutes for independent safety judgment. Maintaining clear operator responsibility therefore preserves the principle that AI should function within an established safety-management system rather than replace the operator's institutional duty.

3.3 Civil Liability: Channeling, Strict Liability, and Victim Compensation

The Vienna Convention establishes a specialized system for compensation for nuclear damage in which liability is principally channelled to the operator of the nuclear installation (Vienna Convention on Civil Liability for Nuclear Damage, 1963; IAEA, 2007). The regime is designed to facilitate compensation without requiring victims to establish ordinary negligence on the part of the operator. This approach recognizes that nuclear accidents can involve technically complex chains of events involving operators, suppliers, contractors, and other organizations.

Heffron *et al*. (2016) identify channeling as a central feature of the international nuclear liability regime. Its practical importance becomes even clearer in an AI environment. An AI-related nuclear incident could involve a software developer, data provider, system integrator, equipment manufacturer, operator, and technical support organization. Requiring victims to establish separate fault claims against each actor could undermine the objective of providing predictable and accessible compensation.

AI therefore introduces an important distinction between technical causation and legal responsibility. A software supplier may have developed a defective model, a data provider may have supplied erroneous information, or an integrator may have improperly configured the system. Nevertheless, under a channeled nuclear liability regime, those contributions may be relevant to causation and recourse without necessarily making each contributor a primary defendant in a victim's nuclear-damage claim.

The channeling principle does not mean that suppliers have no legal significance. Ram Mohan (2014) demonstrates, in the context of India's nuclear liability framework, that supplier liability and recourse can affect incentives, insurance arrangements, and risk allocation throughout the nuclear supply chain. Ram Mohan (2019) further demonstrates the importance of interpreting nuclear liability and recourse provisions within the specific statutory and international framework rather than applying ordinary tort assumptions automatically. These observations are relevant to AI suppliers because their technical contribution may be significant even where direct victim-facing nuclear liability remains channelled to the operator.

3.4 Recourse Against AI Suppliers and Contractual Governance

Under the Vienna framework, operator recourse against other parties is subject to specified conditions, including circumstances provided for by contract and intentional acts or omissions (IAEA, 2007). An operator procuring safety-significant AI should therefore not assume that ordinary supplier liability will automatically provide compensation or reimbursement following a nuclear incident.

AI procurement contracts should identify the validated function and authorized operating conditions of the system and preserve evidence required for safety assessment and incident investigation. Relevant contractual provisions should address model and data provenance, training and validation documentation, configuration control, cybersecurity, notification of material software or model changes, defect reporting, access to relevant logs, incident cooperation, business continuity, and retention of technical records. Where permitted by the applicable nuclear liability regime, contracts should also expressly address recourse and indemnification.

The importance of careful contractual drafting follows from the limited nature of recourse under nuclear liability law. Ram Mohan (2019) emphasizes that nuclear channeling and statutory recourse must be interpreted within the applicable legal framework rather than through ordinary tort principles. Consequently, AI procurement contracts should identify the governing nuclear liability regime, define the conduct and losses covered by contractual recourse, and coordinate contractual obligations with

insurance and financial-security arrangements.

Contractual allocation, however, should not be confused with the operator's public-law safety responsibility. The operator remains responsible for determining whether an AI system is suitable for a particular nuclear application and for ensuring that its use remains consistent with applicable safety requirements. Supplier obligations provide additional contractual controls and remedies without automatically transferring the operator's regulatory responsibility.

3.5 Comparative National Nuclear Liability Regimes

Comparative national legislation demonstrates that operator-focused liability and financial protection are implemented through different legal structures.

Canada's *Nuclear Liability and Compensation Act* establishes operator-focused liability for specified nuclear damage, provides for liability without proof of fault, restricts recourse, and requires financial security (**Canada, 2015**). The United Kingdom's *Nuclear Installations Act 1965* establishes statutory liability associated with licensed nuclear sites and their operators (**United Kingdom, 1965**). In the United States, the Price-Anderson framework provides financial protection for public liability associated with commercial nuclear activities through insurance and industry-supported compensation arrangements (**United States Nuclear Regulatory Commission, 2021**).

These systems are not identical and should not be treated as a single uniform model. Their common feature is the effort to establish predictable mechanisms for compensating nuclear damage without requiring victims to pursue ordinary fault claims against multiple participants in a complex nuclear supply chain. Heffron *et al*. (2016) similarly identify legal certainty and effective compensation as important functions of the international nuclear liability framework.

The emergence of AI does not eliminate this rationale. Proprietary software, distributed data services, cloud dependencies, and common AI platforms may make technical causation more difficult to reconstruct. Maintaining a clear compensation defendant therefore remains important, while contractual, regulatory, and insurance mechanisms can address the conduct of upstream technology suppliers.

3.6 Nigeria's Treaty Position and Domestic Implications

Nigeria acceded to the 1963 Vienna Convention on Civil Liability for Nuclear Damage in 2007. The IAEA Office of Legal Affairs records Nigeria as a party to the Convention but not to the 1997 Protocol to Amend the Vienna Convention, the Joint Protocol linking the Vienna and Paris regimes, or the Convention on Supplementary Compensation for Nuclear Damage (CSC) (International Atomic Energy Agency, Office of Legal Affairs, 2026).

The 1997 Protocol updated important aspects of the Vienna liability framework, while the CSC established an additional international compensation mechanism for qualifying states (Protocol to Amend the Vienna Convention on Civil Liability for Nuclear Damage, 1997; Convention on Supplementary Compensation for Nuclear Damage, 1997). These instruments therefore provide useful benchmarks for considering the adequacy of existing national arrangements as nuclear technology and supply chains become more complex.

Nigeria's *Nuclear Safety and Radiation Protection Act No. 19 of 1995* established the domestic framework for nuclear safety and radiation protection and provided for the Nigerian Nuclear Regulatory Authority (Federal Republic of Nigeria, 1995). The sources reviewed for this study do not establish a Nigerian judicial precedent specifically addressing AI-assisted nuclear harm or comprehensively defining the contractual exposure of AI suppliers following a nuclear incident. These limitations should be treated as areas of legal uncertainty rather than as grounds for assuming a particular legal outcome. The Nigerian position therefore creates a basis for

examining nuclear liability modernization alongside emerging AI governance. If Nigeria expands nuclear-energy activities or adopts advanced digital technologies within nuclear applications, questions concerning supplier recourse, financial security, cybersecurity, digital evidence, and long-term record retention may become increasingly important. Any consideration of the 1997 Vienna Protocol or CSC should consequently assess not only compensation and jurisdiction but also the implications of contemporary technology supply chains.

3.7 Regulatory Accountability When the Regulator Uses AI

The legal position of a nuclear regulator differs from that of a nuclear operator. Nuclear civil liability conventions primarily address compensation for nuclear damage and do not transform a regulatory licensing or inspection decision into operation of the nuclear installation. When regulators use AI to retrieve information, screen applications, prioritize inspections, or assist technical assessment, the principal legal issues therefore concern statutory authority, procedural fairness, transparency, reason-giving, and reviewability.

The NEA's work on regulatory AI use emphasizes the importance of appropriate governance and continuing human expertise rather than treating AI as an autonomous regulatory authority (Nuclear Energy Agency [NEA], 2026). Similarly, the European Union's Regulation (EU) 2024/1689 emphasizes human oversight for high-risk AI systems within its scope (European Union, 2024). Although the EU framework does not automatically apply to Nigerian nuclear regulation, its governance principles provide a useful comparative reference.

A nuclear regulator using AI should therefore identify permissible and restricted applications of AI. The administrative record should, where material to the decision, preserve relevant inputs, model versions, outputs, human review, and reasons for the final decision. Where AI materially contributes to a licensing or enforcement decision, the regulatory framework should provide mechanisms for addressing factual or legal errors without allowing proprietary system design to prevent meaningful review.

Human oversight should be substantive rather than merely formal. A regulatory official who simply approves an AI-generated recommendation without considering the underlying technical basis may not have exercised meaningful independent judgment. AI should therefore support, rather than replace, legally authorized regulatory decision-making.

3.8 Causation and Evidence in AI-Assisted Incidents

Strict or absolute operator liability reduces the importance of proving negligence but does not eliminate the need to establish legally recognized nuclear damage and the required causal connection to a nuclear incident. AI may complicate factual reconstruction because outputs can depend on datasets, model versions, software dependencies, updates, and external services.

An evidentiary audit trail should therefore be treated as an important component of safety governance. Records should identify the approved model version, validated use case, relevant input data, material outputs, uncertainty information where applicable, human review, overrides, software or model updates, and cybersecurity incidents. Record-retention arrangements should also reflect the potentially long latency of some radiological injuries and applicable limitation periods.

Giuffrida (2019) identifies the difficulty of allocating liability where humans remain involved in AI decision-making. In the nuclear context, the appropriate response is not to eliminate human responsibility but to ensure that the decision chain remains reconstructable. Traceability can help establish whether an AI system operated outside its approved purpose, whether contrary evidence was ignored, whether a model update had been validated, or whether a regulator relied on an AI-generated summary without adequate review. Such evidence may become relevant to regulatory enforcement, contractual recourse, insurance,

and judicial review even where civil nuclear liability remains channelled to the operator.

3.9 Nuclear Law as a Reference Point for AI Liability

Nuclear liability has attracted attention in broader AI-liability scholarship because both fields can involve activities capable of producing severe consequences. Henson (2024) considers whether strict liability and insurance mechanisms associated with nuclear activities could provide lessons for catastrophic AI risks. Cha (2024) similarly examines lessons that international AI governance may derive from the IAEA's nuclear safety framework.

The analogy, however, has limits. Nuclear installations are licensed, geographically identifiable, and subject to extensive safety and regulatory controls. AI systems can be copied, modified, and deployed across many sectors and jurisdictions. AI-related harms can also extend beyond physical injury to economic, informational, or other forms of harm. Nuclear liability principles therefore cannot simply be transferred wholesale to general AI regulation.

Within nuclear facilities, however, the relationship is more direct because an AI system becomes part of an already regulated nuclear activity. The appropriate approach is therefore to integrate AI-specific requirements—such as validation, traceability, cybersecurity, data governance, and human oversight—into existing nuclear safety and liability structures rather than replacing those structures.

3.10 Proposed Allocation of Legal Responsibility

Table 1 summarizes the proposed allocation of legal responsibility among the principal actors involved in AI-assisted nuclear safety governance. It distinguishes the continuing safety responsibility of the nuclear operator from the regulatory accountability of the competent authority, the contractual and technical responsibilities of AI suppliers and technical support organizations, and the financial-security role of insurers or other financial guarantors.

As shown in Table 1, the use of AI does not automatically transfer the operator's primary responsibility for nuclear safety to technology suppliers or other third parties. Instead, AI-specific controls, including validation, human oversight, configuration management, cybersecurity, traceability, contractual recourse, and financial security, should operate within the existing allocation of nuclear safety and liability responsibilities.

The framework presented in Table 1 is proposed as an analytical and governance model rather than as a statement that every identified control is presently required by international or Nigerian law. Its purpose is to demonstrate how established nuclear responsibility principles can be applied to AI-assisted decision-making while preserving clear accountability across the technology and regulatory chain.

Table 1. Proposed allocation of responsibility in AI-assisted nuclear safety governance

Actor	Proposed legal allocation and AI-specific controls
Nuclear operator/licensee	Retains primary responsibility for facility or activity safety and remains the principal victim-facing party where liability is channelled to the operator. Controls should include qualification and validation, human authorization, configuration management, audit records, fallback arrangements, contractual recourse, and financial security.
Regulatory body	Remains responsible for the lawful, independent, transparent, and reviewable exercise of statutory powers. AI assistance should not transfer operator safety responsibility to the regulator. The regulator should define permitted AI uses, require appropriate human review, preserve decision records, and maintain review or appeal mechanisms.

AI/software supplier	May contribute to technical causation but ordinarily does not become the victim-facing defendant for nuclear damage where liability is channelled to the operator. Contracts should address warranties, validation evidence, cybersecurity, defect reporting, audit access, incident cooperation, and applicable recourse.
Technical support organization	Provides technical expertise without displacing the legal responsibility of the operator or regulator. Competence, documented assumptions, conflict controls, and traceable technical advice should be maintained.
Insurer/financial guarantor	Provides financial security within the applicable nuclear compensation arrangement. Underwriting may consider safety-significant AI, common software dependencies, cybersecurity, governance controls, validation evidence, and access to incident records.

3.11 Insurance, Financial Security, and Correlated AI Failure

Nuclear liability regimes connect legal responsibility with financial security so that funds are available when nuclear damage occurs. This relationship is particularly relevant to AI because software can create correlated risks. A single AI model, software library, data dependency, or update could potentially be used across several systems or facilities, creating the possibility of common-cause failures.

Existing nuclear compensation arrangements address catastrophic risks through operator insurance, financial security, and, in some jurisdictions, pooled or supplementary funding. The United States Price-Anderson framework provides an example of industry-supported financial protection, while Canadian legislation establishes statutory financial-security requirements (Canada, 2015; United States Nuclear Regulatory Commission, 2021).

The introduction of AI may require insurers and financial guarantors to consider additional information, including whether the system is safety-significant, the extent of human intervention, validation evidence, dependence on common third-party models, cybersecurity controls, update procedures, and incident logging. These factors may inform financial-risk assessment without transferring responsibility for nuclear safety from the regulator or operator to the insurer.

Supplier concentration also creates potential systemic risk. Where multiple operators depend on the same AI platform, contractual indemnity may have limited practical value following a systemic defect if the supplier lacks sufficient assets or insurance. Operators should therefore not treat contractual recourse as a substitute for statutory financial security, while regulators should consider common software dependencies when evaluating digital safety.

3.12 Human Oversight Must Be Operational, Not Nominal

Human oversight should involve more than placing a person at the end of an automated workflow. Effective oversight requires sufficient time, competence, authority, and access to relevant information for the reviewer to understand and, where necessary, reject an AI recommendation. If a human operator lacks access to relevant data or is unable to challenge an automated recommendation, human involvement may become merely formal.

For safety-significant applications, procedures should specify the evidence that a reviewer must examine, circumstances requiring independent verification, how uncertainty should be communicated, and when the system should revert to a safe or conservative state. Training should cover model limitations and recognized failure modes rather than focusing only on interface operation. These principles are consistent

with the emphasis on leadership and management for safety in the IAEA framework (IAEA, 2016b) and with risk-based AI governance (Tabassi, 2023; European Union, 2024).

The same principle applies to regulatory authorities. A licensing or inspection officer should retain sufficient independence to evaluate AI-generated information rather than simply endorse it. The final statutory decision should remain attributable to the authorized official or institution, with adequate records demonstrating the basis for the decision.

3.13 A Graded Legal Framework for Safety-Significant AI

The pathway presented in Fig. 1 provides the basis for a graded framework in which the level of regulatory control increases according to the safety significance, autonomy, and potential consequences of the AI application.

A workable governance framework should distinguish AI applications according to their safety significance. An administrative text-search system used to retrieve regulatory information should not be subject to exactly the same requirements as an AI system that recommends reactor shutdown or predicts degradation of a safety-significant component.

Relevant criteria include the potential consequence of error, degree of autonomy, time available for human intervention, ease of independent verification, and reversibility of the decision. For lower-significance applications, conventional information-security and quality controls may be adequate. AI systems supporting safety assessment or maintenance prioritization should require documented validation, performance monitoring, version control, and competent human review. Systems capable of initiating or materially controlling safety functions should require substantially stronger qualification, assurance, fallback, and regulatory controls.

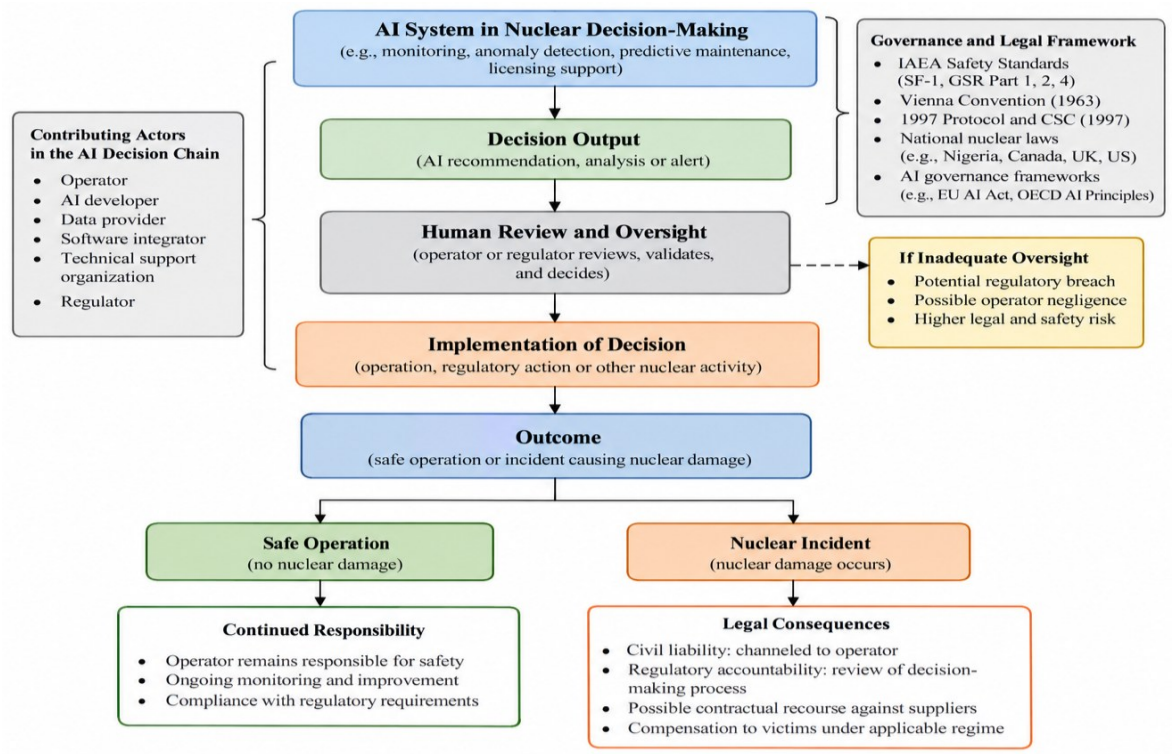

Fig. 1: Figure 1. Legal Responsibility Pathway for AI-Assisted Nuclear Safety Decisions.

This graded approach is consistent with the IAEA's emphasis on graded safety assessment and management of safety (IAEA, 2016b, 2016c) and with risk-based AI governance

approaches (Tabassi, 2023; European Union, 2024). The nuclear sector should nevertheless retain sector-specific requirements because nuclear safety involves specialized concepts such as defense in depth, licensing, safety assessment, and clearly assigned responsibility.

4.0 Conclusion

The integration of artificial intelligence (AI) into nuclear safety decision-making provides important opportunities for improved monitoring, prediction, diagnosis, and regulatory support, but it also introduces complex questions concerning legal responsibility, accountability, causation, evidence, and compensation. This study demonstrates that the use of AI does not, by itself, alter the established principle that the nuclear operator bears primary responsibility for the safety of the facility or activity. Even where safety-related decisions are supported by AI, the operator remains responsible for appropriate system selection, validation, deployment, monitoring, human oversight, and controlled modification.

The analysis further establishes that nuclear civil liability and regulatory accountability are distinct but interconnected issues. Under established nuclear liability principles, liability is generally channelled to the operator to facilitate effective compensation for nuclear damage. Consequently, an AI developer, software supplier, data provider, or system integrator may contribute technically to an incident without necessarily becoming the primary victim-facing defendant. AI therefore affects the technical and evidentiary dimensions of causation more directly than it changes the fundamental structure of nuclear liability. Contractual arrangements remain important for allocating commercial risks, preserving evidence, facilitating technical cooperation, and establishing legally permissible recourse, but they cannot transfer the operator's statutory safety responsibility.

The study also finds that the use of AI by nuclear regulatory authorities creates additional public-law accountability requirements. Regulatory decisions supported by AI should remain subject to meaningful human oversight, transparency, reason-giving, procedural fairness, and appropriate review mechanisms. Accordingly, AI governance should address not only post-incident liability but also responsibility throughout the design, deployment, supervision, and review of AI-supported decisions.

For Nigeria, the 1963 Vienna Convention provides an important foundation for nuclear civil liability, while the limited legal treatment of AI-related nuclear harm indicates a need for further regulatory development. Nigeria should therefore integrate AI governance with nuclear safety, liability, cybersecurity, evidence management, and regulatory oversight. A clear and adaptive framework would enable the benefits of AI to be realized while preserving identifiable legal responsibility when AI-assisted nuclear decisions fail.

Five recommendations follow from the doctrinal and comparative analysis.

First, Nigerian nuclear regulation should expressly provide that the use of AI or automated decision-support systems does not displace the operator's primary responsibility for nuclear safety. Suppliers and contractors may have contractual obligations, but the licensee should remain responsible for ensuring that AI is safely integrated into nuclear operations.

Second, the Nigerian Nuclear Regulatory Authority should consider developing a graded regulatory framework for AI and machine-learning applications. The framework should identify safety-significant uses and establish requirements for validation, model-change control, cybersecurity, human oversight, record retention, and incident reporting. It should distinguish AI used in nuclear operations from lower-risk administrative AI used by regulatory personnel.

Third, procurement of safety-significant AI should be treated as both a technical and legal risk-allocation process. Contracts should preserve access to technical documentation, model and data provenance, validation

evidence, audit records, defect notifications, incident information, continuity arrangements, and applicable recourse mechanisms. These provisions should operate consistently with the applicable nuclear liability regime.

Fourth, Nigeria should periodically review its nuclear civil-liability framework and treaty position in light of developments in nuclear technology and digital supply chains. The 1963 Vienna Convention, the 1997 Protocol to Amend the Vienna Convention, and the Convention on Supplementary Compensation for Nuclear Damage provide relevant international benchmarks for considering compensation, jurisdiction, financial security, and cross-border nuclear liability (Vienna Convention on Civil Liability for Nuclear Damage, 1963; Protocol to Amend the Vienna Convention on Civil Liability for Nuclear Damage, 1997; Convention on Supplementary Compensation for Nuclear Damage, 1997).

Fifth, AI-assisted regulatory decisions should remain subject to established principles of public-law accountability. Each statutory decision should remain attributable to an authorized official or institution, preserve sufficient reasons and relevant records, permit meaningful human intervention, and remain subject to applicable review or appeal mechanisms. AI should support technical and administrative analysis without becoming an independent source of statutory authority.

5.0 References

Canada. (2015). Nuclear Liability and Compensation Act, S.C. 2015, c. 4, s. 120, as amended.

Cha, S. (2024). Towards an international regulatory framework for AI safety: lessons from the IAEA's nuclear safety regulations. Humanities and Social Sciences Communications, 11, 506. https://doi.org/10.1057/s41599-024-03017-1

Convention on Supplementary Compensation for Nuclear Damage. (1997). Adopted 12 September 1997; entered into force 15 April 2015.

European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

Federal Republic of Nigeria. (1995). Nuclear Safety and Radiation Protection Act No. 19 of 1995, Cap N142 Laws of the Federation of Nigeria 2004.

Giuffrida, I. (2019). Liability for AI decision-making: Some legal and ethical considerations. Fordham Law Review, 88, 439-456.

Heffron, R.J., Ashley, S.F. & Nuttall, W.J. (2016). The global nuclear liability regime post Fukushima Daiichi. Progress in Nuclear Energy, 90, 1-10. https://doi.org/10.1016/j.pnucene.2016.02.019

Henson, R. (2024). "I Am Become Death, the Destroyer of Worlds": Applying strict liability to artificial intelligence as an abnormally dangerous activity. Temple Law Review, 96, 349-391.

International Atomic Energy Agency (IAEA). (2006). Fundamental Safety Principles. IAEA Safety Standards Series No. SF-1. Vienna: IAEA.

International Atomic Energy Agency (IAEA). (2007). The 1997 Vienna Convention on Civil Liability for Nuclear Damage and the 1997 Convention on Supplementary Compensation for Nuclear Damage: Explanatory Texts. Vienna: IAEA.

International Atomic Energy Agency (IAEA). (2016a). Governmental, Legal and Regulatory Framework for Safety. IAEA Safety Standards Series No. GSR Part 1 (Rev. 1). Vienna: IAEA.

International Atomic Energy Agency (IAEA). (2016b). Leadership and Management for Safety. IAEA Safety Standards Series No. GSR Part 2. Vienna: IAEA.

International Atomic Energy Agency (IAEA). (2016c). Safety Assessment for Facilities and Activities. IAEA Safety Standards Series No. GSR Part 4 (Rev. 1). Vienna: IAEA.

International Atomic Energy Agency, Office of Legal Affairs. (2026). Country

Factsheet: Nigeria, Federal Republic of. Treaty status database.

Karim, R. & Muhammad-Sukki, F. (2023). Artificial Intelligence (AI) in the nuclear power plants: Who is liable when AI fails to perform. In F. Taghizadeh-Hesary & D. Zhang (Eds.), The Handbook of Energy Policy (pp. 587-607). Springer. https://doi.org/10.1007/978-981-19-6778-8_27

Klebanov, L.R. & Lizikova, M.S. (2025). Artificial Intelligence in nuclear energy: Legal challenges and international cooperation in the search of approaches to regulation. RUDN Journal of Law, 29(2), 494-508. https://doi.org/10.22363/2313-2337-2025-29-2-494-508

Marchant, G.E. & Buckwald, J. (2026). Private standards as liability shields: A pro-innovation artificial intelligence regulatory approach for states. Minnesota Journal of Law, Science & Technology, 27(1), 61. https://doi.org/10.24926/15529541.3916

Nuclear Energy Agency (NEA). (2026). NEA explores regulatory use of artificial intelligence. OECD Nuclear Energy Agency, 17 April 2026.

Organisation for Economic Co-operation and Development (OECD). (2024). OECD AI Principles, updated 2024.

Protocol to Amend the Vienna Convention on Civil Liability for Nuclear Damage. (1997). Adopted 12 September 1997; entered into force 4 October 2003.

Ram Mohan, M.P. (2014). Placing the Indian civil nuclear liability regime in context: The extent of supplier's liability. Journal of Risk Research, 17(1), 121-139. https://doi.org/10.1080/13669877.2013.822922

Ram Mohan, M.P. (2019). Which interpretational route will the Supreme Court of India follow when faced with the contentious Civil Liability for Nuclear Damage Act, 2010? Statute Law Review, 40(3), 249-265. https://doi.org/10.1093/slr/hmy007

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

United Kingdom. (1965). Nuclear Installations Act 1965, c. 57, as amended.

United States Nuclear Regulatory Commission. (2021). The Price-Anderson Act: 2021 Report to Congress—Public Liability Insurance and Indemnity Requirements for an Evolving Commercial Nuclear Industry. NUREG/CR-7293.

Vienna Convention on Civil Liability for Nuclear Damage. (1963). Adopted 21 May 1963; entered into force 12 November 1977.

Compliance with Ethical Standards

Declaration

Ethical Approval

Not Applicable

Competing interests

The author declares no known competing financial interests.

Funding

No external funding was received for this doctrinal and comparative legal research.

Author's Contribution

The author conceived the study, conducted the legal and comparative analysis, verified the sources, and prepared the manuscript.