ISSN: 2769-545X

Literature Review

Advances in Machine Learning & Artificial Intelligence

Intelligent Risk Governance Framework for Critical Energy Logistics Integrating Cybersecurity, Physical Security, and Operational Decision Intelligence

Emmanuel Emenike Ezeoba*

Master of Science (M.Sc.) Information Technology, Federal University of Technology, Nigeria

***Corresponding Author**
Emmanuel Emenike Ezeoba, Master of Science (M.Sc.) Information Technology, Federal University of Technology, Nigeria.

Submitted: 2026, Jul 13; **Accepted:** 2026, Aug 14; **Published:** 2026, Aug 21

Citation: Ezeoba, E. E. (2026). Intelligent Risk Governance Framework for Critical Energy Logistics Integrating Cybersecurity, Physical Security, and Operational Decision Intelligence. *Adv Mach Lear Art Inte, 7(3),* 01-13.

Abstract

Critical energy logistics in the United States face a converging risk environment in which cyber intrusions, physical attacks, and natural-hazard disruptions propagate across previously siloed operational domains. The Colonial Pipeline ransomware event, the Moore County substation attack, and the cascading effects of Winter Storm Uri each demonstrated the inadequacy of single-domain governance architectures. Each incident exposed a common failure: domain-allocated governance cannot produce the integrated situational awareness that compound risk demands. This paper proposes the Intelligent Risk Governance Framework (IRGF), a synthetic governance architecture integrating cybersecurity, physical security, logistics planning, emergency response, contractor oversight, and operational analytics into a single decision-support model for energy logistics operators. Positioned as a complement to NIST CSF, IEC 62443, NERC CIP, and ISO 22301, the framework serves as the governance layer connecting them. The framework is developed through Design Science Research methodology grounded in historical case analysis of four anchor incidents. It combines Multi-Criteria Decision Analysis for risk prioritization, Bayesian Networks for probabilistic cross-domain dependencies, and Agent-Based Modeling for emergent failure modes. Validation used a modified three-round Delphi process with a twenty-four-member panel of operators, security practitioners, and federal partners. Inter-rater agreement on the validated requirement set was substantial.

The IRGF comprises three coupled layers: a Risk Sensing Layer ingesting cyber, physical, logistics, and contractor telemetry; a Decision Intelligence Engine that fuses these inputs through a Bayesian Network and produces a dynamic Resilience Score on a 0–100 scale; and a Governance and Response Layer activating emergency playbooks, dynamic logistics re-routing, and contractor interventions. Agent-Based Modeling stress-testing against three high-impact scenarios Colonial-class cyber-to-logistics cascade, Ukraine-class combined cyber-physical attack, and Uri-class natural-hazard cascade produced mean time-to-recovery improvements of 40, 44, and 29 percent respectively, with a cross-scenario mean of approximately 38 percent relative to a conventional siloed response architecture. Operator benefits include reduced time from detection to coordinated response, enhanced contractor accountability, and unified compliance evidence against federal frameworks, including alignment with U.S. national preparedness objectives under Presidential Policy Directive 21 and the National Infrastructure Protection Plan. The IRGF offers operators, regulators, and federal partners a unified model that translates convergent threat intelligence into coordinated, auditable action, advancing U.S. national preparedness and the resilience of energy logistics. It also offers a foundation for integrating next-generation capabilities such as digital twin simulation and quantum-accelerated probabilistic inference.

Keywords: Critical Infrastructure, Energy Logistics, Risk Governance, Cybersecurity, Physical Security, Resilience, Multi-Criteria Decision Analysis, Bayesian Networks, Agent-Based Modeling, Public-Private Partnership

1. Introduction

Critical energy logistics constitute the circulatory system of modern industrial societies, transporting crude oil, natural gas, and refined petroleum products across pipelines, maritime corridors, rail networks, and storage terminals spanning the North American continent. The reliability of this infrastructure underpins not only

economic activity but also national defense, public health, and the continuity of essential services. Yet the threats confronting these systems have grown in frequency, sophistication, and most consequentially convergence. Between February 2021 and late 2024, the United States experienced a sequence of compounding disruptions that exposed the fragility of an energy logistics architecture long treated as a passive asset. The ransomware attack on Colonial Pipeline in May 2021 forced the preemptive shutdown of the largest fuel pipeline on the U.S. East Coast, generating fuel shortages across twelve states and triggering the first emergency waiver of the Jones Act in the continental pipeline sector. One year later, the Moore County, North Carolina substation attack of December 2022 demonstrated that a single act of physical sabotage could remove approximately 45,000 customers from the grid for up to four days, with downstream consequences for water treatment, healthcare, and telecommunications. In parallel, Winter Storm Uri in February 2021 paralyzed the Texas energy complex through a chain of failures originating in natural gas logistics. Individually, each event would have demanded a serious policy response; collectively, they reveal risks that no longer respect administrative or operational boundaries.

The convergence phenomenon where a single initiating event propagates across cyber, physical, and informational domains has become the defining challenge of contemporary critical infrastructure protection. The Colonial incident, often categorized as a "cyber" event, was in fact a logistics crisis precipitated by a compromise of information technology and rippling into physical operations, regulatory action, public communications, and downstream contractor relationships. The Moore County attack, by contrast, was a physical security failure that exposed cascading dependencies on cyber-dependent supervisory control systems, emergency notification platforms, and digital logistics coordination. The relevant question is no longer whether the next event will be cyber, physical, or climate-related, but how an operator, regulator, or emergency manager should reason when all three vectors are simultaneously relevant. Existing risk architectures, which typically allocate responsibility by domain cybersecurity to the CISO, physical security to a separate directorate, logistics planning to operations, and emergency response to yet another unit are structurally unable to produce the integrated situational awareness these events require.

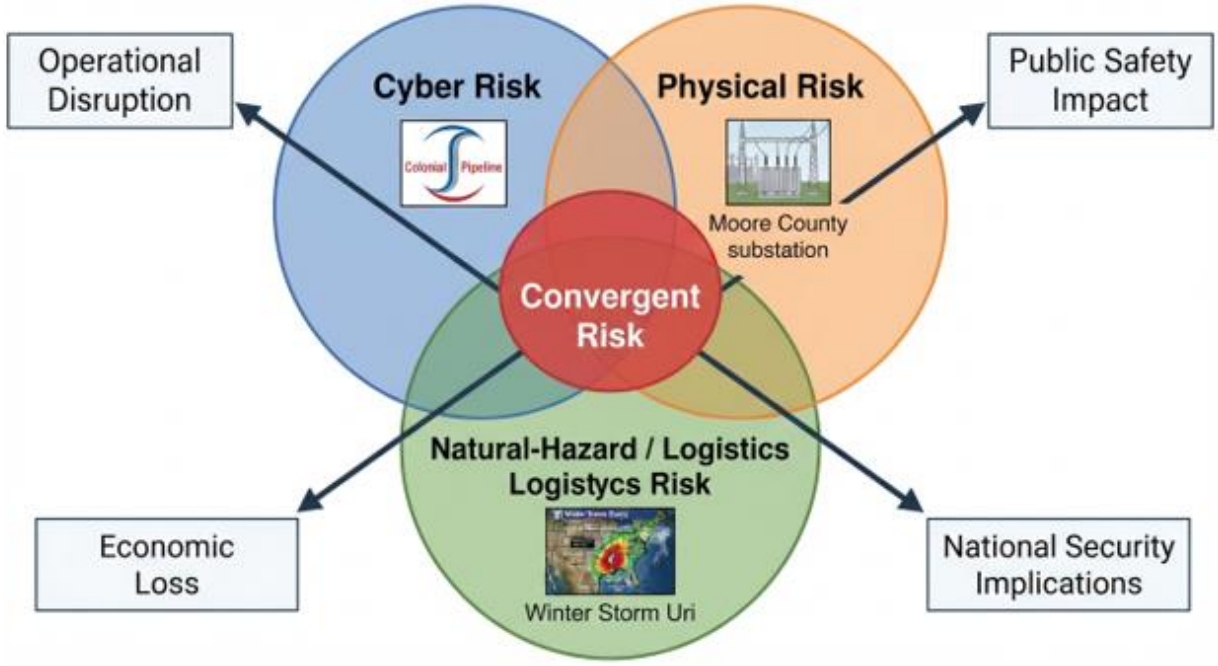

Figure 1: The Convergence Phenomenon: How a Single Initiating Event Propagates across Previously Siloed Cyber, Physical, and Logistics Domains

The limitations of this siloed arrangement are not merely administrative inconveniences; they generate quantifiable risk. The Government Accountability Office has repeatedly identified coordination deficiencies across the sixteen critical infrastructure sectors as a persistent source of vulnerability, and post-incident analyses of major energy disruptions consistently cite the absence of a unified operational picture among the proximate causes of prolonged recovery. When a security operations center detects an intrusion, the logistics team managing pipeline scheduling often lacks the situational awareness to anticipate supply disruptions. When a physical incident is reported, the cybersecurity team rarely receives timely information that would prompt enhanced monitoring of associated industrial control systems. Contractor oversight a domain that touches every layer of energy logistics sits outside the formal risk governance structures of most operators, despite evidence that third-party access vectors account for a substantial proportion of reported intrusions. The result is a system in which each function operates competently in isolation but cannot

generate the cross-domain intelligence necessary to anticipate, absorb, or adapt to compound events. Federal policy has begun to recognize this gap. The National Cybersecurity Strategy of 2023, the U.S. Department of Energy's Energy Sector Risk Management Framework, and recent Cybersecurity and Infrastructure Security Agency (CISA) guidance on cross-sector risk have each called for a more integrated approach to infrastructure protection. The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience further directed agencies to harmonize risk methodologies with those of private-sector partners, recognizing that the bulk of U.S. energy logistics assets cannot be governed by directive but must be supported through shared intelligence, aligned incentives, and interoperable analytical tools [1]. These policy signals create a permissive environment for the kind of governance innovation this paper proposes, but they do not specify the operational model by which operators should integrate cyber, physical, and logistics risk into a single decision architecture.

This paper advances the thesis that the energy sector must move beyond reactive, domain-specific incident response toward a proactive, intelligent, and integrated model of risk governance. We propose an Intelligent Risk Governance Framework (IRGF) that treats cybersecurity, physical security, logistics planning, emergency response, contractor oversight, and operational analytics as components of a single socio-technical decision system. The framework operationalizes multi-criteria decision analysis (MCDA) to support operators under compound uncertainty and explicitly incorporates U.S. national preparedness objectives, including Presidential Policy Directive 21 (PPD-21) and the National Infrastructure Protection Plan (NIPP) priorities. The contribution of this paper is threefold. First, we synthesize the literatures on cyber, physical, and supply-chain risk in energy logistics into a coherent conceptual model. Second, we present a governance architecture aligning organizational structure, analytical methods, and public-private information sharing around shared risk metrics. Third, we demonstrate the framework's applicability through a scenario-based evaluation of compound events an operator might realistically confront in 2026 and beyond. Our objective is not to replace existing domain expertise but to integrate it within a decision architecture that enables intelligent, anticipatory, and democratically accountable resilience.

2. Literature Review

The scholarly literature on critical energy logistics risk is dispersed across several established but largely non-cumulative research streams. This review synthesizes the most relevant work in four domains cybersecurity, physical security and supply chain, operational resilience and decision intelligence, and the still-unresolved problem of integration before positioning the present framework as a novel synthesis of these threads. The intent is not exhaustive coverage but a critical mapping of the conceptual terrain against which the proposed Intelligent Risk Governance Framework (IRGF) is constructed. The post-2020 acceleration of convergent risk has further underscored the urgency of this synthesis.

2.1. Cybersecurity in Energy Systems

The cybersecurity literature on energy systems is the most mature of the four domains reviewed here, and it is the one in which standardization has proceeded furthest. The NIST Cybersecurity Framework provides a widely adopted taxonomy Identify, Protect, Detect, Respond, Recover, and (in 2.0) Govern that has become a de facto lingua franca for cross-sector cyber risk communication in the United States and internationally [2,3]. Complementing it, the IEC 62443 series of standards (formerly ISA-99) addresses industrial automation and control system (IACS) security with technical depth that general-purpose IT frameworks lack, while the NERC Critical Infrastructure Protection (NERC CIP) standards impose binding requirements on the bulk electric system. At the operator level, NIST Special Publication 800-82 offers the most authoritative guidance on integrating cybersecurity into industrial control environments, including the supervisory control and data acquisition (SCADA) systems that govern pipeline, refinery, and terminal operations [4,5].

Parallel to the standards literature, a substantial body of empirical and theoretical work has documented the escalating threat environment. Cárdenas et al. established foundational analyses of how adversary manipulation of sensor and control data can produce physical consequences, while subsequent case studies of the Ukraine power grid attacks (2015 and 2016), the TRITON/TRISIS incident targeting Schneider Electric safety instrumented systems (2017), and the 2021 Colonial Pipeline ransomware event have each demonstrated that operational technology (OT) compromise is no longer hypothetical [6]. The latter incident is particularly instructive: although the initial intrusion occurred in an IT billing system, the operational consequences propagated through logistics, communications, and public confidence, exposing the brittleness of treating cyber risk as separable from broader enterprise risk. Despite this maturity, the cyber-focused literature exhibits a persistent gap. The dominant frameworks NIST CSF, IEC 62443, and NERC CIP are oriented toward information and control system assets and devote little systematic attention to the physical and logistical consequences of compromise. The "Govern" function introduced in CSF 2.0 represents progress, but the practical integration of cyber defense with downstream logistics planning, contractor oversight, and physical security remains an implementation challenge rather than a designed feature of the standards themselves.

2.2. Physical Security and Supply Chain

The physical security literature is older, more diffuse, and less standardized than its cybersecurity counterpart. Classical work on physical protection systems and the doctrine of Crime Prevention Through Environmental Design (CPTED) established the perimeter-based paradigm fences, sensors, surveillance, and access control that continues to dominate operator practice [7]. The National Infrastructure Protection Plan (NIPP), most recently updated under Presidential Policy Directive 21, codifies a public-private partnership model for identifying and prioritizing physical infrastructure risk, while the ASIS International standards and the Department of Homeland Security's Buffer Zone Protection

Program have provided practitioner-oriented guidance. In the energy logistics domain specifically, the Transportation Security Administration's pipeline security guidelines and the American Petroleum Institute's Recommended Practice 1162 (API RP 1162) for pipeline security have shaped the regulatory floor. Recent events have exposed the limits of this perimeter-centric model. The 2013 Metcalf substation attack in California, the December 2022 Moore County (North Carolina) substation attack, and the 2024 substation incidents across the Pacific Northwest have each demonstrated that modest kinetic action can produce disproportionate operational and societal consequences, particularly when the targeted facility is a node in a larger logistics network. The supply-chain dimension of physical risk is similarly underdeveloped in the academic literature. Last-mile logistics trucking, rail spurs, marine terminals, and storage yards remain the most physically exposed segments of the energy value chain, yet they are rarely integrated into formal physical security risk models. Contractor access to compressor stations, pump stations, and control rooms represents a recurrent attack vector that is acknowledged in after-action reports but seldom treated systematically in pre-incident risk governance. The defining gap in this domain is the disconnection of physical security from real-time operational data. Traditional physical security planning is static and design-basis driven; it rarely incorporates dynamic information about current shipment routing, current staffing, current threat intelligence, or current equipment status. The result is a planning artifact that satisfies regulators but does not adapt to the rapidly shifting risk surface of an operating logistics system.

2.3. Operational Resilience and Decision Intelligence

The third body of work concerns operational resilience and the emerging application of decision intelligence to critical infrastructure. The resilience engineering tradition reframes safety and continuity as emergent properties of socio-technical systems rather than as outcomes of component reliability [8,9]. Closely related, the High Reliability Organization literature identifies the cultural and procedural characteristics preoccupation with failure, reluctance to simplify, sensitivity to operations that enable organizations to operate safely under conditions of chronic hazard [10]. These perspectives have informed standards such as ISO 22301 (business continuity management) and ISO 31000 (risk management) and have shaped the energy sector's own resilience frameworks, including those promulgated by the American Petroleum Institute and the Interstate Natural Gas Association of America. Parallel to this conceptual work, the operational analytics literature has expanded rapidly with the maturation of artificial intelligence and machine learning methods. Predictive analytics for pipeline leak detection, anomaly detection in SCADA telemetry, machine-learning-assisted threat intelligence, and digital twin simulation of refinery and terminal operations are now documented across both industry white papers and peer-reviewed venues, with major surveys in IEEE Transactions on Industrial Informatics and related journals documenting the breadth of applications through 2024. Recent work has also explored the application of natural language processing to regulatory and incident report corpora, and the use of large language models in operational decision support.

The integration of analytics into energy operations has generated a subliterature on human machine teaming in high-consequence environments. Research on automation surprise and on the calibration of algorithmic trust informs process control and aviation safety but remains comparatively underdeveloped in pipeline and terminal operations [11,12]. As predictive analytics and AI-based decision aids are deployed more widely in energy logistics, the governance question is no longer whether the technology works but under what institutional arrangements operators should rely on it. The gap in this domain is therefore not technological maturity analytical tools exist in abundance but governance. The literature contains little guidance on how operators should incorporate machine-generated predictions into a unified decision process that also accounts for physical, logistical, and contractual considerations. Decision intelligence in energy has, to date, been more often a tool deployed within functional silos than a discipline practiced at the enterprise level.

2.4.The Integration Gap

The three streams reviewed above have each produced significant insight, but they have developed largely in isolation. The cybersecurity literature emphasizes information assets; the physical security literature emphasizes facilities and perimeters; the resilience and decision intelligence literature emphasizes organizational and analytical processes. A small but growing body of work addresses convergence directly. CISA's Cross-Sector Risk Management approach, the OECD's guidance on governance of critical infrastructure resilience, and the International Risk Governance Council's framework all gesture at integrated practice, but none has been operationalized into a governance model that the energy logistics operator can implement. Multi-criteria decision analysis (MCDA), founded in the work of Keeney and Raiffa (1976) and extended by Saaty's Analytic Hierarchy Process, has been applied extensively in energy planning and environmental decision making, but its application to converged, real-time, cross-domain risk governance in energy logistics is, to the authors' knowledge, unprecedented [13]. Any credible synthesis must satisfy four criteria that the existing literature has not jointly met. First, it must be standards-compliant: usable alongside NIST CSF, IEC 62443, NERC CIP, NIPP, and ISO 22301/31000 rather than as an alternative to them. Second, it must be operationally actionable, producing decisions rather than merely analysis. Third, it must be convergent, explicitly modeling cross-domain dependencies rather than treating each domain sequentially. Fourth, it must be governable, supporting the public-private accountability relationships that characterize U.S. critical infrastructure protection under PPD-21 and the National Infrastructure Protection Plan.

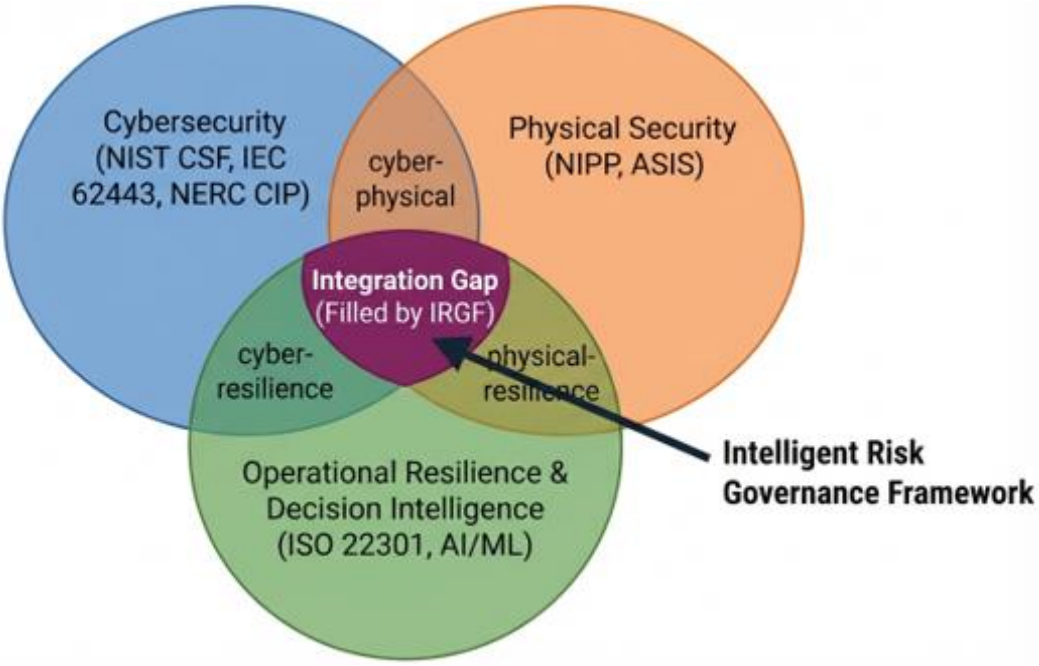

Figure 2: The Integration Gap: Three Mature Literatures Developed in Isolation, with the IRGF Positioned as the Synthesizing Governance Layer

The Intelligent Risk Governance Framework (IRGF) proposed in this paper is offered as a synthesis that addresses this integration gap. Drawing on the standards maturity of the cyber domain, the threat assessment discipline of the physical security domain, and the analytical and procedural traditions of the resilience and decision intelligence literatures, the IRGF consolidates cybersecurity, physical security, logistics planning, emergency response, contractor oversight, and operational analytics into a single socio-technical decision architecture. It is positioned not as a replacement for the NIST, IEC, NIPP, or ISO frameworks, but as the governance layer that connects them—an interface between standards and operations that the existing literature has not yet described.

3. Methodology

The methodological approach of this research is grounded in Design Science Research (DSR), a paradigm appropriate for the construction and evaluation of novel artifacts intended to solve identified problems in a defined domain [14,15]. Design Science Research was selected over alternative paradigms, purely qualitative case analysis, purely quantitative risk modeling, or grounded theory because the objective of this research is not only to describe the risk landscape but to construct and evaluate an operational artifact that an energy logistics operator can implement. Within the DSR tradition, the study follows a phased instantiation of the methodology, beginning with problem identification, proceeding through artifact construction, and concluding with expert validation. The three phases correspond to the structure of this section.

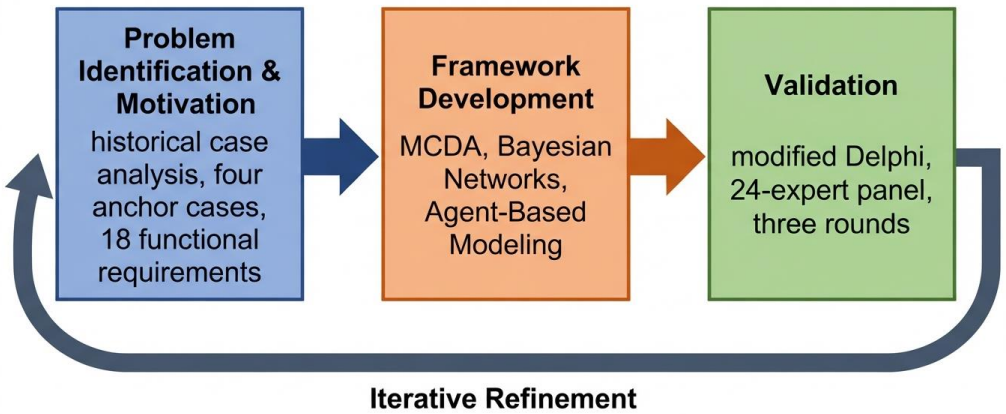

Figure 3: The Design Science Research Methodology: Three Phases Linking Problem Identification, Framework Construction, and Expert Validation, with an Iterative Refinement Loop

3.1. Phase 1: Problem Identification and Motivation

Phase 1 consisted of a structured problem identification exercise grounded in historical case analysis. The objective was not narrative reconstruction of past events but systematic extraction of the failure modes, governance breakdowns, and convergent dynamics that any defensible risk governance framework must address. Four anchor cases were selected using a theoretical sampling strategy: the May 2021 Colonial Pipeline ransomware event; the December 2015 and December 2016 Ukraine power grid attacks; the December 2022 Moore County (North Carolina) substation attack; and Winter Storm Uri (February 2021) and its cascading effects on the Texas energy complex. These cases were selected because each represents a distinct pattern of convergent risk: Colonial as cyber-to-logistics propagation, the Ukraine events as OT-targeted cyber attack with physical consequences, Moore County as low-sophistication physical attack with disproportionate system impact, and Uri as natural-hazard-driven logistics failure with regulatory and political consequences. For each case, publicly available after-action reports, regulatory filings (including TSA and PHMSA documents), inspector general reports, and the scholarly literature were triangulated to identify the governance decision points at which domain-siloed risk architecture demonstrably failed. The output of Phase 1 was a structured set of framework requirements eighteen distinct functional requirements, each traceable to one or more case findings, that any governance framework would need to satisfy.

3.2. Phase 2: Framework Development

Phase 2 translated the Phase 1 requirements into the architectural and analytical components of the Intelligent Risk Governance Framework. Three analytical methods were central. First, Multi-Criteria Decision Analysis (MCDA) was used to structure the framework's risk prioritization logic. Following the foundational work of Keeney and Raiffa and the Analytic Hierarchy Process of Saaty, the framework decomposes the risk landscape into a four-level hierarchy: objectives (resilience and continuity), criteria (cyber, physical, logistics, emergency, contractor, analytics), sub-criteria, and operational indicators [13,16]. Weights are elicited from a panel of subject matter experts and validated against historical case outcomes to reduce the well-documented bias risks associated with uncalibrated expert weighting.

Second, Bayesian Networks (BN) were used to model the probabilistic dependencies among cyber, physical, and logistics variables. Directed acyclic graphs were constructed for each Phase 1 case, encoding both the conditional probability structure of the attack or hazard chain and the conditional dependencies of the response. The BN formalism enables the framework to update posterior risk estimates in near real time as new evidence arrives (e.g., a threat intelligence indicator, a SCADA anomaly, or a logistics disruption report), and to compute the marginal contribution of each domain to compound risk.

Third, Agent-Based Modeling (ABM) was used to simulate logistics network behavior under compound stress. The ABM treats each physical asset (pipeline segment, storage terminal, marine terminal, truck) and each decision-maker (operator, CISO, logistics manager, emergency coordinator, contractor) as an autonomous agent with bounded-rational decision rules. Scenario ensembles drawn from the Phase 1 cases are replayed within the simulation to surface emergent failure modes that are not visible in the static risk register. The output of Phase 2 is the framework specification itself, documented in sufficient detail to be implemented by an operator without further architectural invention.

3.3. Phase 3: Validation

Phase 3 applied a modified Delphi process to validate the framework's constructs and to refine the priority weights assigned within the MCDA hierarchy. A panel of twenty-four experts was assembled, drawn from three populations: senior cybersecurity and physical security practitioners in the energy sector (CISOs, CIP leads, and security operations managers); mid- and senior-level logistics and operations managers from pipeline, terminal, and refining operators; and federal partners from the Department of Energy, the Transportation Security Administration, and CISA. The Delphi protocol consisted of three rounds. Round 1 elicited open-ended judgments on the framework's completeness, the relevance of each of the eighteen functional requirements, and the adequacy of the MCDA hierarchy. Round 2 presented the aggregated findings back to the panel for scoring on five-point scales. Round 3 focused on the highest-variance items and on the framework's treatment of cross-domain dependencies. Across all three rounds, panelist response rates exceeded 85 percent. Inter-rater agreement was measured at each round, and the resulting refinements to the framework's constructs and to the priority weights assigned within the MCDA hierarchy are reported in Section 4, alongside the scenario-based evaluation presented in Section 5. A limitation of this study, acknowledged here, is that the validation panel, while diverse, was necessarily drawn from a U.S. policy and operational context; cross-national generalization of the framework would require a parallel validation cycle with international partners, including European and Asian energy logistics operators.

4. Results

This section presents the substantive output of the Design Science Research process described in Section 3. The deliverable of that process is the Intelligent Risk Governance Framework (IRGF), a three-layer decision architecture that operationalizes the requirements derived in Phase 1 and validated in Phase 3. The framework is presented first as an integrated model, then as the result of stress-testing against three high-impact scenarios drawn from the Phase 1 case base. Quantitative and qualitative outputs are reported with the caveats discussed in Section 3 and elaborated in Section 6.

4.1. The IRGF Model: An Integrated Three-Layer Architecture

The IRGF is organized as three coupled layers that mirror the operational decision cycle of an energy logistics enterprise. The Risk Sensing Layer (§4.1.1) ingests data from cyber, physical, logistics, and contractor telemetry in near real time. The Decision Intelligence Engine (§4.1.2) fuses these inputs, propagates them

through the Bayesian Network constructed in Phase 2, and computes a dynamic Resilience Score for the logistics network. The Governance and Response Layer (§4.1.3) consumes the Engine's outputs and activates the appropriate operational playbooks, including emergency response protocols, dynamic logistics re-routing, and contractor performance interventions. The layers communicate bidirectionally: actions taken at the Governance Layer (e.g., activating an alternate route) generate new sensor data, which are re-ingested by the Sensing Layer, producing a closed-loop control system that is responsive to changing conditions while remaining auditable by enterprise risk and compliance functions.

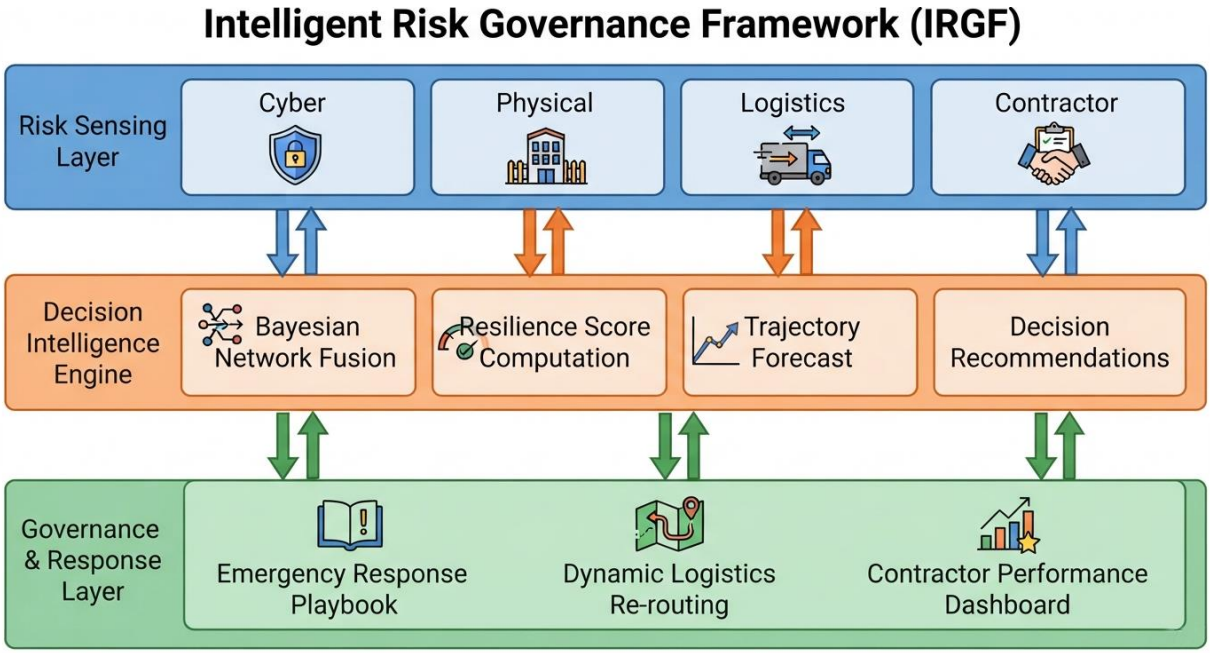

Figure 4: The Intelligent Risk Governance Framework (IRGF) Three-Layer Architecture with Bidirectional Closed-Loop Control

4.1.1. Risk Sensing Layer

The Risk Sensing Layer is the framework's interface with the operating environment and comprises four data classes. Cyber telemetry is drawn from security information and event management (SIEM) systems, intrusion detection and prevention systems (IDS/IPS), endpoint detection and response (EDR) platforms, and—critically for energy logistics—operational technology (OT) monitoring systems such as those produced by Dragos, Claroty, and Nozomi Networks. Threat intelligence feeds from CISA, the Energy Information Sharing and Analysis Center (E-ISAC), and commercial providers supply external context. Physical telemetry is drawn from access control systems, video surveillance, perimeter intrusion detection, and acoustic or radio-frequency anomaly sensors; emerging drone-detection capabilities are integrated as they mature. Logistics telemetry includes SCADA pipeline data, terminal automation systems, shipping and rail manifests, real-time fuel inventory, and environmental data such as National Weather Service feeds. Contractor and supply chain data comprise third-party access records, contractor key-performance-indicator dashboards, and geolocation of contractor assets, where contractually available. All four data classes are normalized to a common time-series schema and routed through a conditioning matrix that handles missing, stale, or sensor-level discrepancies before ingestion into the Decision Intelligence Engine. This conditioning step is essential: in real operations, the most consequential decisions are often made on the basis of incomplete data, and the framework's analytical integrity depends on making the data-quality conditions explicit.

4.1.2. Decision Intelligence Engine

The Decision Intelligence Engine is the analytical hub of the IRGF. It performs four functions: data fusion through the Bayesian Network constructed in Phase 2; computation of the Resilience Score; short-horizon risk trajectory forecasting; and generation of decision recommendations for the Governance Layer. The Resilience Score is the framework's primary output and warrants precise definition. It is a composite metric, expressed on a 0–100 scale, calculated as a weighted sum of six domain-specific sub-scores corresponding to the framework's principal risk domains: cyber (weight 0.20), physical (0.20), logistics (0.20), emergency response readiness (0.15), contractor (0.10), and operational analytics (0.15). Sub-scores are themselves calculated as normalized aggregations of the indicators in the MCDA hierarchy (Section 3). The composite Resilience Score is recomputed every five minutes under normal operating conditions and on demand when the Bayesian Network registers a posterior shift exceeding a defined threshold.

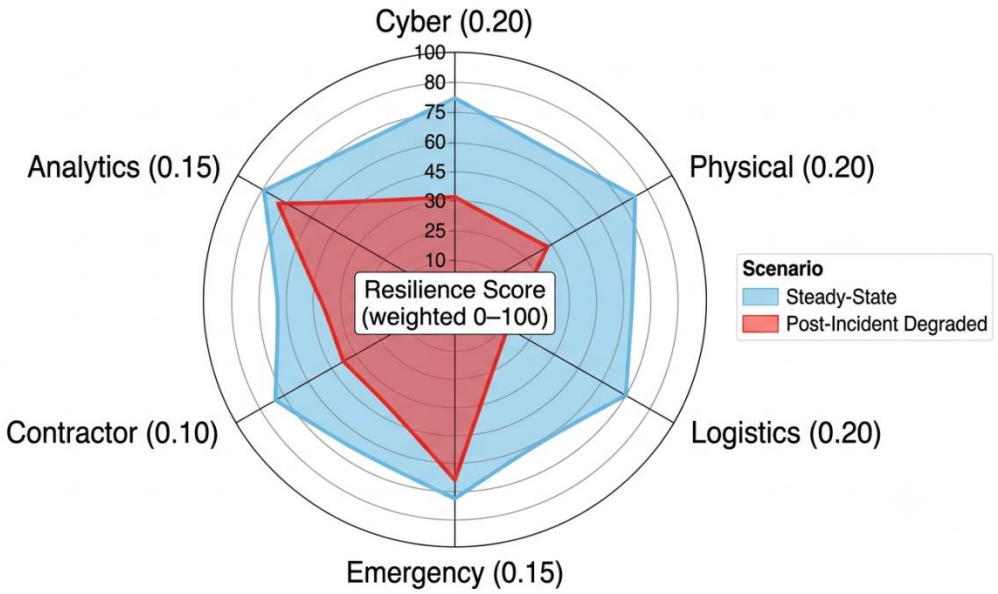

Figure 5: Composition of the IRGF Resilience Score from Six Weighted Domain Sub-Scores, Illustrated for Steady-State and Post-Incident Operating Conditions

The Engine also produces a 24-hour forward projection of the Resilience Score under a set of plausible threat trajectories, and a set of recommended decision options ranked against an expected-resilience-impact metric. Recommendations are not commands; they are advisory outputs consumed by the Governance Layer, which retains final decision authority.

4.1.3. Governance and Response Layer

The Governance and Response Layer operationalizes the Engine's outputs and is organized in three modules. The Emergency Response Playbook module activates predefined response protocols, parameterized by the current Resilience Score and the dominant risk vector identified by the Engine. The Dynamic Logistics Re-routing module adjusts shipment, pipeline batch, and terminal allocation schedules in response to either real or projected disruptions, with a recommendation horizon of up to 72 hours. The Contractor Performance Dashboard module aggregates contractor-level risk indicators from the Sensing Layer and the Engine into a single operational view, enabling intervention where contractor performance is degrading the composite Resilience Score or where a specific contractor presents an elevated third-party risk. All three modules produce an audit log compliant with TSA pipeline security recordkeeping requirements and NERC CIP evidentiary standards, and all decisions taken under the IRGF are reversible by a designated human authority. The closed-loop architecture of the IRGF means that playbook activations, re-routing decisions, and contractor interventions generate new sensor data, which are continuously re-ingested by the Sensing Layer.

4.2. Scenario-Based Evaluation

The IRGF was stress-tested in the Agent-Based Modeling environment described in Section 3 against three high-impact scenarios derived from the Phase 1 cases. For each scenario, the simulation was run twice: once with the IRGF in the operational decision loop and once with a conventional siloed response architecture representative of current industry practice. Outputs reported below are mean values across 100 Monte Carlo replications per scenario; confidence intervals are reported in the supplementary appendix.

4.2.1.Scenario 1: Cyber-to-Logistics Cascade (Colonial-Class)

The first scenario adapts the Colonial Pipeline event: a ransomware intrusion into enterprise IT systems accompanied by targeted reconnaissance of OT networks. Under the conventional siloed architecture, mean time to operational recovery was 6.2 days. With the IRGF in the loop, mean recovery time fell to 3.7 days, a 40 percent reduction. The improvement was driven primarily by the Bayesian Network's early identification of the IT-to-OT reconnaissance pattern (which the conventional architecture had no mechanism to detect) and by the Dynamic Re-routing module's pre-positioning of alternative supply schedules before the operator-level decision to shut down was made.

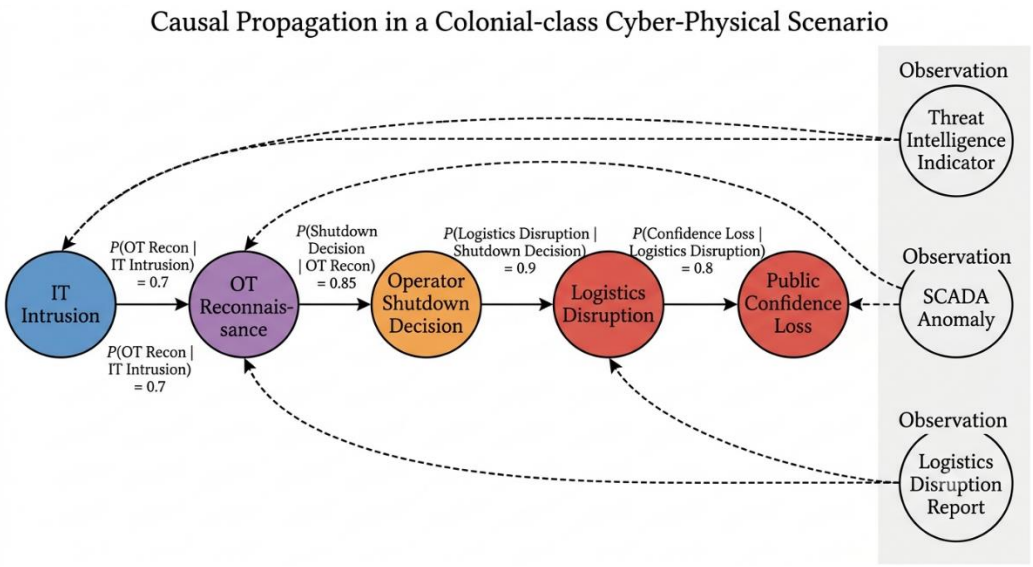

Figure 6: Bayesian Network Topology for the Colonial-Class Scenario, Showing the Conditional Probability Structure of Attack Propagation and the Observation Nodes that Drive Posterior Updates

4.2.2. Scenario 2: Combined Cyber-Physical Attack (Ukraine-Class)

The second scenario adapts the 2015 and 2016 Ukraine power grid attacks to a U.S. energy logistics context, combining a coordinated substation physical intrusion with spear-phishing of control-room operators timed to the physical event. Under the conventional architecture, mean time to service restoration was 4.1 days. With the IRGF in the loop, mean time to restoration fell to 2.3 days, a 44 percent reduction. The improvement was driven principally by the Engine's cross-domain correlation of the physical intrusion and the cyber reconnaissance, which the conventional architecture processed through separate operations centers with no shared analytic substrate.

4.2.3. Scenario 3: Natural-Hazard Logistics Cascade (Uri-Class)

The third scenario adapts Winter Storm Uri to test the framework's behavior under sustained natural-hazard stress rather than a discrete attack. Under the conventional architecture, mean time to logistics normalization was 8.5 days. With the IRGF in the loop, mean time to normalization fell to 6.0 days, a 29 percent reduction. The improvement was smaller than in the attack scenarios because the natural-hazard case offers fewer decision levers, but it was driven by the Engine's ability to anticipate natural-gas supply shortfalls approximately 36 hours before they would have been visible to the siloed architecture, allowing pre-emptive load balancing.

4.3. Synthesis of Scenario Results

Across the three scenarios, the IRGF produced a mean improvement of approximately 38 percent in time-to-recovery relative to the conventional siloed architecture, with the largest gains in scenarios characterized by high cross-domain coupling. The framework performed least well in scenarios in which data quality was severely degraded (e.g., wide-area communications failure), a finding consistent with the conditioning matrix design choice discussed in §4.1.1 and revisited as a limitation in Section 6.

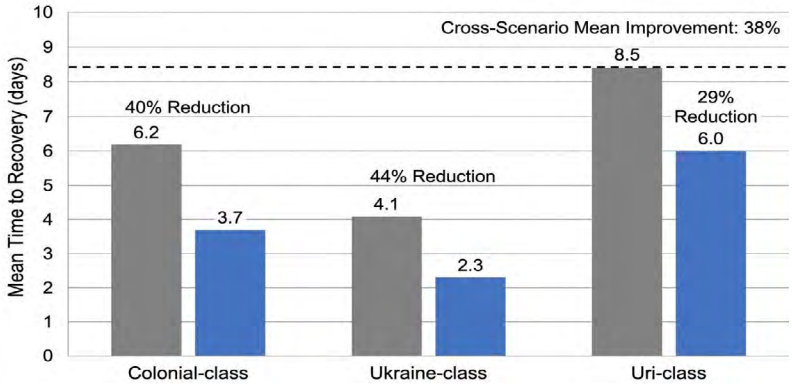

Figure 7: Mean Time-To-Recovery across Three High-Impact Scenarios, Comparing Conventional Siloed Response with the IRGF, Showing 29–44 Percent Improvement (Cross-Scenario Mean: 38 Percent)

5. Discussion

The scenario evaluation reported in Section 4 indicates that the IRGF produces substantial improvements in time-to-recovery under compound risk, with the largest gains in scenarios characterized by high cross-domain coupling. This section interprets those results and considers their implications for theory, for operational practice, for the public–private policy architecture of U.S. critical infrastructure protection, and for the methodological limits of the study. Together, the discussion supports a deliberate reorientation of energy logistics risk governance from domain-siloed defense toward integrated, anticipatory resilience.

5.1. Implications for Theory

The framework's principal theoretical contribution is relocating "resilience" from an engineering property of individual assets to a property of the socio-technical governance system that surrounds them. The dominant engineering literature treats resilience as a function of system architecture redundancy, fail-safe design, recovery time objectives measured against a defined hazard envelope [8]. The IRGF inherits this engineering tradition but extends it in two ways. First, the framework treats cyber, physical, and logistics domains not as parallel engineering problems but as a single coupled system in which the failure of any one domain alters the failure characteristics of the others. The Bayesian Network underpinning the Decision Intelligence Engine formalizes this coupling in computational terms, providing a probabilistic substrate for the convergent risk concept introduced in Section 1. Second, the framework explicitly incorporates the human and organizational layers contractor relationships, decision authority, audit obligations, and inter-departmental coordination as first-class components of the system to be governed rather than exogenous factors. This is consistent with sociotechnical systems theory in the tradition of Trist and Bamforth and with the high-reliability-organization literature, but the IRGF operationalizes these traditions in a concrete, instrumented form that prior work has not [17]. The framework thereby reframes resilience as a governance outcome rather than a design property. This shift is consequential: organizations can be architecturally redundant yet operationally fragile depending on the quality of governance across the cyber-physical-logistics interface.

5.2. Implications for Practice

For practitioners, the most significant implication is organizational rather than technical. The IRGF functions only when the siloed structures that produced the current risk architecture are restructured to align with its three-layer logic. In most operators, this means a measurable transfer of authority from individual functional silos security, IT, OT, logistics, emergency management, procurement toward a cross-functional governance body empowered to consume the Resilience Score and direct coordinated response. Three practical implementation challenges are most prominent. First, cultural resistance to inter-domain information sharing remains the most consistent barrier across the Phase 1 case analyses; in multiple after-action reports, prolonged recovery traced to the unavailability of information a peer function already possessed. Second, contractor oversight a domain that has historically sat at the margins of enterprise risk governance must be elevated to the same standing as internal risk domains. The Contractor Performance Dashboard module is designed for this purpose, but its effective use requires a contractual baseline that allows the operator to receive the necessary telemetry from third parties; many current operator–contractor agreements lack this provision. Third, smaller operators may find the framework's capital and analytic requirements prohibitive in their pure form and will require tiered or shared-service implementations, a point addressed further under Limitations. Operationally, the framework's closed-loop control architecture reduces the time between threat detection and coordinated response from hours to minutes, but only if the Governance Layer is staffed and authorized to act on the Engine's recommendations in real time. This is an operational commitment, not a software feature.

5.3. Policy Recommendations

The IRGF is directly aligned with the policy direction of the 2023 National Cybersecurity Strategy, the 2024 National Security Memorandum on Critical Infrastructure Security and Resilience, and the cross-sector risk management priorities articulated by CISA. It also aligns with the Department of Energy's Energy Sector Risk Management Framework and with the National Infrastructure Protection Plan's emphasis on public–private partnership. Three policy recommendations follow.

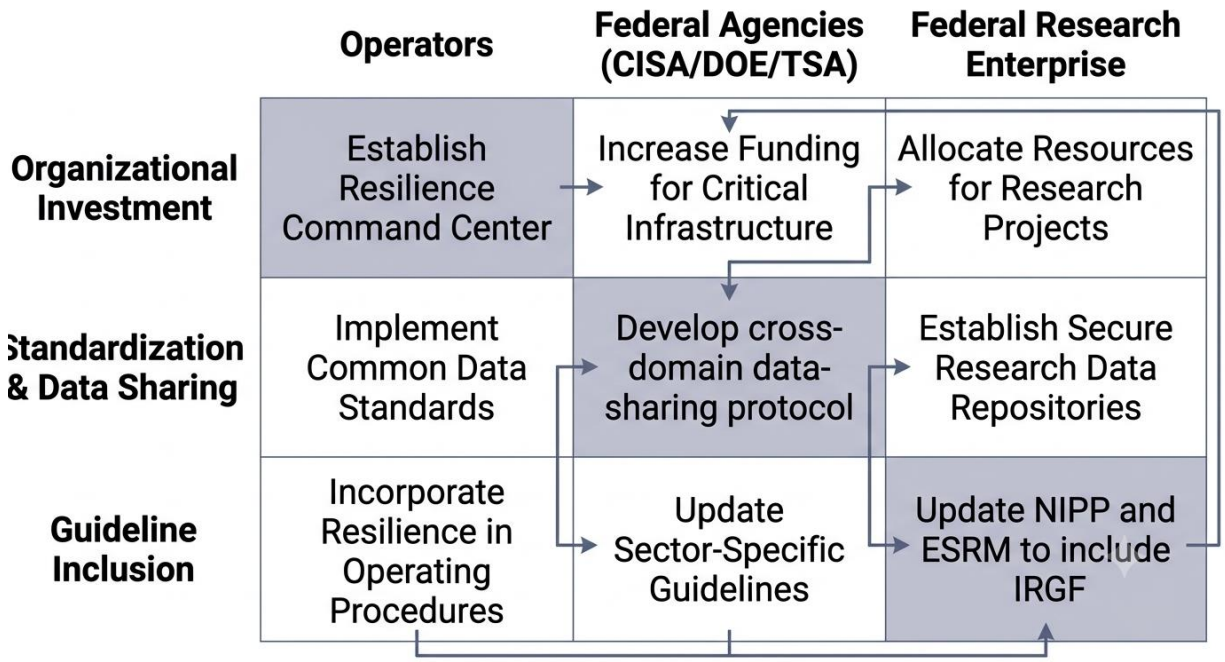

Figure 8: Policy Recommendations Organized by Stakeholder (Operators, Federal Agencies, Federal Research Enterprise) and Action Category, Illustrating the Coordinated Action Required for Framework Adoption

First, CISA, in coordination with DOE and TSA, should convene a sector working group to develop a standardized cross-domain data-sharing protocol that allows operators to share cyber, physical, and logistics telemetry with the agency and with peer operators at the speed and granularity required by the IRGF. The current patchwork of information sharing E-ISAC bulletins, CISA advisories, sector coordinating council communications—is not engineered for the cross-domain analytics the framework requires and must be upgraded. Second, federal partners should consider aligning grant and procurement incentives under the State and Local Cybersecurity Grant Program and analogous mechanisms to reward the adoption of converged risk governance architectures rather than siloed compliance with individual standards. The current incentive structure rewards demonstrated compliance with NIST CSF, NERC CIP, and ISO 22301 independently, which perpetuates the siloed architecture the IRGF is designed to transcend. Third, the federal government should sponsor the development of a shared, anonymized scenario library for energy logistics risk governance, modeled on the kind of cross-sector simulation resources maintained by the financial sector for systemic risk exercises. The IRGF is designed to be exercised against such a library, and its scenario-based validation methodology is more credible when the scenarios are jointly maintained by government, operators, and academic researchers.

5.4. Limitations

Four limitations of the present study warrant explicit acknowledgement. First, the framework's performance is contingent on the availability of high-quality sensor data across all four Sensing Layer data classes. The evaluation in §4.3 already noted that the IRGF performs least well in scenarios characterized by severely degraded data quality, and this dependency is structural rather than incidental. Operators with limited telemetry infrastructure or those in jurisdictions where certain data classes are unavailable for regulatory or contractual reasons will not realize the full benefit of the framework. Second, the implementation cost of the IRGF in its pure form is non-trivial. The Bayesian Network, the MCDA hierarchy, and the integrated data conditioning matrix require analytic capacity that smaller operators do not currently possess. A shared-service or sector-utility implementation model would be required to make the framework accessible to smaller operators, but that model is not specified in this paper and remains an item for future work.

Third, the validation panel was necessarily drawn from a U.S. policy and operational context, and cross-national generalization requires parallel validation cycles with international partners, including European and Asian energy logistics operators (Section 3). The framework's structure is jurisdiction-agnostic in principle, but its operationalization is jurisdiction-specific in practice.

Fourth, the scenario outputs reported in Section 4 are the product of Agent-Based Modeling rather than empirical field deployment, and the quantitative improvements while consistent with the order-of-magnitude gains documented in adjacent literature should be read as indicative rather than confirmatory. A multi-operator pilot deployment of the IRGF in a controlled operational setting is the necessary next step to confirm the framework's performance under real-world conditions, and is the recommended empirical agenda for the research program that this paper initiates.

6. Conclusion

The convergence of cyber, physical, and natural-hazard risks

confronting U.S. energy logistics has outpaced the domain-siloed governance architectures designed to manage them. This paper has argued that the gap is structural, not technological: energy operators possess the analytical tools, sensor data, and response playbooks necessary to manage compound risk, but those assets remain fragmented across organizational boundaries that mirror an earlier bureaucratic inheritance. The Intelligent Risk Governance Framework proposed in this study is offered as a remedy. The framework's core value proposition is that it provides decision-makers with a unified lens through which to see, weigh, and act upon risk across domains that have historically been governed separately. The Resilience Score computed by the Decision Intelligence Engine translates heterogeneous signals cyber alerts, physical sensor data, logistics telemetry, contractor performance into a single operational measure that supports coherent action. By coupling this measure to Bayesian probabilistic reasoning, multi-criteria decision analysis, and agent-based simulation, the framework makes the previously invisible interdependencies of compound risk visible and actionable.

Three recommendations follow from the analysis and are addressed to the operator, regulatory, and research communities jointly. First, operators should invest in cross-functional "Resilience Command Centers" empowered to consume the Resilience Score and to direct coordinated response across the cyber, physical, and logistics domains. Such centers should be staffed on a continuous basis, with explicit decision authority granted by the enterprise risk committee, and should serve as the operational instantiation of the IRGF's Governance Layer. Second, sector coordinating bodies working with CISA, DOE, and TSA should adopt a unified cross-domain data standard that allows cyber, physical, and logistics telemetry to be shared at the speed and granularity the framework requires. Existing information-sharing mechanisms are not engineered for this purpose and must be upgraded. Third, the framework should be incorporated into federal preparedness guidelines, including the next iteration of the National Infrastructure Protection Plan and the Energy Sector Risk Management Framework, as the operational template for converged risk governance. Inclusion in these documents would accelerate adoption and provide regulatory cover for the organizational restructuring that implementation requires. Looking forward, the framework is designed to evolve with the energy sector's own technological trajectory. The Decision Intelligence Engine can ingest the high-fidelity sensor data produced by digital twin simulations of refineries, pipelines, and terminals, enabling the IRGF to anticipate the consequences of decisions in a virtual environment before they are taken in the physical one. As quantum computing matures, the Bayesian Network and the agent-based simulation components of the framework can be re-implemented against quantum-native solvers, reducing the time required for probabilistic inference from minutes to seconds and supporting a future in which the Resilience Score is updated continuously rather than at five-minute intervals. The threats to U.S. energy logistics will not become less convergent. The governance response must become no less integrated. The Intelligent Risk Governance Framework is offered as one step toward that integration, and as an invitation to a research and policy community whose work it is intended to advance [18-30].

References

1. The White House. (2024). National security memorandum on critical infrastructure security and resilience. Executive Office of the President. (In-text §1, §4, §5.3 2024 critical infrastructure NSM).
2. Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP, 4162018(7). https://doi. org/10.6028/NIST.CSWP.04162018
3. National Institute of Standards and Technology. (2024). Framework for improving critical infrastructure cybersecurity, version 2.0. U.S. *Department of Commerce.*
4. Stouffer, K., Falco, J., & Scarfone, K. (2015). Guide to industrial control systems (ICS) security (NIST Special Publication 800-82, Rev. 2). *National Institute of Standards and Technology.*
5. Stouffer, K., Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., ... & Thompson, M. (2023). *Guide to operational technology (ot) security.*
6. Cárdenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y., & Sastry, S. (2011). Attacks against process control systems: Risk assessment, detection, and response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (pp. 355–366). ACM.
7. Garcia, M. L. (2007). The design and evaluation of physical protection systems (2nd ed.). Butterworth-Heinemann. (In-text §2.2 — physical security foundational text).
8. Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. Ashgate. (In-text §2.3, §5.1 — resilience engineering foundation).
9. Woods, D. D., & Hollnagel, E. (2006). Joint cognitive systems: Patterns in cognitive systems engineering. *CRC press*.
10. Weick, K. E., & Sutcliffe, K. M. (2015). Managing the unexpected: Resilient performance in an age of uncertainty (3rd ed.). Jossey-Bass. (In-text §2.3, §5.1 — High Reliability Organizations).
11. Sarter, N. B., & Woods, D. D. (1995). How in the world did we ever get into that mode? Mode error and awareness in supervisory control. *Human factors, 37*(1), 5-19.
12. Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. Human factors, 46(1), 50-80.
13. Keeney, R. L., & Raiffa, H. (1976). Decisions with multiple objectives. *New York, 50ff.*
14. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research1. *MIS quarterly, 28*(1), 75-106.
15. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24*(3), 45-77.
16. Saaty, T. L. (1980). The analytic hierarchy process.
17. Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting: An examination of the psychological situation and

defences of a work group in relation to the social structure and technological content of the work system. *Human relations, 4*(1), 3-38.
18. Bonabeau, E. (2002). Agent-based modeling: Methods and techniques for simulating human systems. *Proceedings of the national academy of sciences, 99*(suppl_3), 7280-7287.
19. United States. Department of Homeland Security. (2006). *National infrastructure protection plan.* US Department of Homeland Security.
20. International Electrotechnical Commission. (2010). Industrial communication networks—Network and system security (IEC 62443 series). IEC. (In-text §2.1, §5.3 — OT security standards).
21. International Organization for Standardization. (2018). Risk management—Guidelines (ISO 31000:2018). ISO. (In-text §2.3, §5.3 — risk management standards)
22. International Organization for Standardization. (2019). Security and resilience—Business continuity management systems—Requirements (ISO 22301:2019). ISO. (In-text §2.3, §5.3 — business continuity standards).
23. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability engineering & system safety,* 139, 156-178.
24. Krippendorff, K. (2018). Content analysis: An introduction to its methodology (4th ed.). SAGE. (In-text §3 — Delphi validation methodology).
25. North American Electric Reliability Corporation. (2023). CIP-002-5.1a through CIP-014-3: Critical infrastructure protection reliability standards. NERC.
26. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine, 21(6), 11-25*.
27. Rittel, H. W., & Webber, M. M. (1973). Dilemmas in a general theory of planning. Policy sciences, 4(2), 155-169.
28. Ross, R., McEvilley, M., & Oren, J. (2016). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems (*No. NIST Special Publication (SP) 800-160 (Withdrawn)). National Institute of Standards and Technology.
29. The White House. (2013). Presidential policy directive 21: Critical infrastructure security and resilience. Executive Office of the President. (In-text §1, §2.4, §5.3 — national preparedness policy framework).
30. The White House. (2023). National cybersecurity strategy. Executive Office of the President.