International Journal of Information Security (2026) 25:26
https://doi.org/10.1007/s10207-025-01201-1

REGULAR CONTRIBUTION

Risk impact pathway analysis (RIPA): A dynamic risk assessment framework for interdependent critical infrastructures

Fatimah Faraji[1] · Haralambos Mouratidis[1] · Abdullah Al Zakwani[2]

Received: 31 October 2025 / Accepted: 22 December 2025

Abstract

Critical Infrastructures (CI) are increasingly interdependent, forming complex dependency networks where disruptions can propagate across sectors and amplify systemic risk. Conventional risk assessment methods are limited by evaluating components in isolation and neglecting how interdependencies shape cascading exposure. This paper introduces the Risk Impact Pathway Analysis (RIPA) framework–a dynamic, dependency-aware risk assessment model that explicitly traces and quantifies risk propagation pathways within interdependent CI systems. RIPA incorporates three key propagation factors: Linkage Intensity (LI), measuring dependency strength; Resilience (RE), acting as a risk shield; and Criticality, functioning as a risk amplifier. Unlike traditional methods focused solely on initial risk (R_0), RIPA calculates Total Systemic Risk, revealing hidden high-risk nodes and propagation routes. The framework is validated through a multi-sector case study of the LAMAD-LLC integrated infrastructure system, demonstrating its applicability and effectiveness. Results demonstrate that incorporating interdependency criteria into risk assessment reveals significant hidden vulnerabilities, with certain infrastructure components exhibiting risk increases compared to traditional single-point assessments. This amplification effect illustrates how failures or vulnerabilities propagate through interconnected systems, creating compound risks not captured by conventional methods. Sensitivity analysis reveals that resilience enhancement interventions achieve approximately twice the risk reduction compared to equivalent modifications in either criticality scores or linkage intensity parameters. These findings validate RIPA's capacity to provide a pathway-centric, topology-aware understanding of systemic exposure, enabling more targeted and effective infrastructure risk management strategies than traditional approaches.

Keywords Systemic risk · Cascading failures · Critical infrastructure protection · Dynamic risk assessment · Interdependency analysis · Resilience · criticality

1 Introduction

CI, such as power grids, communications networks, and water supplies, form the supporting pillars of modern society [1–4]. Over the past decade, these systems have become increasingly interconnected and reliant on advanced cyber-physical technologies, creating a dense web of interdependencies[1, 4, 5]. While this interconnectedness has delivered substantial efficiency gains, it has also introduced a critical vulnerability–systemic risk. Systemic risk is defined not by the failure of a single, isolated component, but by the potential for that initial failure to trigger catastrophic cascading effects across multiple sectors[1, 5, 6].

The 2017 NotPetya cyberattack exemplifies this danger. Initially targeting Ukrainian systems through a compromised software update, the attack rapidly cascaded globally within hours–crippling Maersk's entire worldwide shipping network, paralysing manufacturing facilities across Europe and the United States, disrupting healthcare systems, and causing over $10 billion in damages [7, 8]. The attack exploited IT-OT interdependencies to propagate from administrative networks into operational control systems, demonstrating

✉ Fatimah Faraji
ff23395@essex.ac.uk

Haralambos Mouratidis
h.mouratidis@essex.ac.uk

Abdullah Al Zakwani
abdullah.alzakwani@lamad.om

[1] Institute for Analytics and Data Science (IADS), School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK

[2] Executive Director Innovation and Analytics Expert, LAMAD, LLC, Oman

Published online: 07 January 2026

how a single cyber intrusion can trigger cascading failures throughout interconnected critical infrastructures. Due to the intricate dependencies within and between sectors, localised disruptions can propagate unpredictably, leading to widespread, multi-system collapses with devastating societal and economic consequences. Understanding and managing the dependencies that create these pathways for systemic risk is therefore a paramount challenge in modern infrastructure protection [7, 8].

Extensive research has been conducted on CI risk assessment, employing diverse methodologies including network-based models, simulation frameworks, and formula-based approaches. However, a fundamental challenge remains: how to quantitatively model risk propagation through complex, multi-factor dependency networks in a way that captures the conditional dynamics of cascading failures [4]. As detailed in Section 2, existing approaches exhibit systematic limitations in pathway-level quantification, propagation dynamics, and resilience integration–leading to underestimation of systemic exposure and ineffective mitigation prioritisation.

Given these critical gaps in existing methodologies, this study addresses the following research questions:

RQ1: How can cascading effects in critical infrastructure systems be quantified to capture both the probability and intensity of risk propagation across interdependent components?

RQ2: To what extent do cascading interdependencies amplify risk levels compared to traditional single-point risk assessments that consider components in isolation?

RQ3: Which factors (initial risk, linkage intensity, resilience, or criticality) have the greatest influence on cascade propagation patterns and systemic risk levels?

RQ4: How can risk mitigation strategies be optimised by incorporating cascade dynamics, and what is the relative effectiveness of different intervention approaches?

To address these limitations, this paper proposes the RIPA framework–a dynamic, dependency-aware risk assessment model that explicitly traces and quantifies risk propagation pathways within interdependent CI systems. RIPA differentiates between two primary forms of risk: Initial Risk (R_0) inherent to an individual node, and Propagated Risk (Rpro) transmitted through the network. The core of our contribution is a novel method for quantifying this propagated risk through explicit modelling of three key, modulating dimensions: the source and destination nodes' resilience capacities, the multi-criteria intensity of their connection, and the destination node's criticality. Specifically:

- **Linkage intensity (LI):** Multi-criteria measure of dependency strength.
- **Resilience:** Active risk shield at source and destination nodes.
- **Criticality (CDE):** Risk amplification factor for systemically important nodes.

Unlike traditional methods focused solely on R_0, RIPA computes the *Total Systemic Risk*, revealing systemic hot spots invisible to conventional approaches. The framework employs a Breadth-First Search (BFS) algorithm to systematically explore all propagation pathways and introduces a *Pathway Impact Score (PIS)* for prioritising high-risk cascades.

By integrating these factors, RIPA enables more systematic risk appraisal, prioritising elements based on both inherent exposure and their capacity to trigger or contribute to cascading failures. This paper presents the complete RIPA framework, validates it through a real-world multi-sector case study (LAMAD-LLC, 21 nodes, 33 dependencies), demonstrates that resilience provides approximately twice the risk reduction of other factors and that RIPA-guided strategies outperform conventional approaches by 78%, and provides practical recommendations for resilience planning in interconnected infrastructures.

The remainder of this paper is structured as follows: Section 2 reviews related work and identifies research gaps; Section 3 presents the RIPA framework; Section 5 describes the case study application; Section 5 analyses results and discusses implications; Section 6 provides practical recommendations; and Section 7 concludes.

2 Related work

The challenge of ensuring the resilience of CI in the face of cascading failures has been a focal point of extensive [9]. Our proposed RIPA framework builds upon a rich body of work in CI modelling, interdependency analysis, and impact assessment. This section reviews the foundational literature, highlights established methodologies, and identifies the specific gaps that RIPA is designed to address.

2.1 Methodologies for modelling CI interdependencies

A significant portion of the literature is dedicated to developing models that can represent the complex web of interdependencies within and between CIs. The work by Iturriza et al. [10] provides a comprehensive overview of this landscape through a systematic literature review, classifying various modelling methodologies such as system dynamics, agent-based models, and network-based models. This foundational work highlights the diversity of available approaches and underscores that the choice of methodology is contingent on specific research goals.

Within these broad categories, specific techniques range from detailed simulations to formal mathematical models. On the simulation front, Grafenauer et al. [11] present a framework built in OMNeT++ that uses stochastic processes and Markov chains to visualise the uncertain and time-dependent nature of failure propagation. In contrast, Gueye et al. [12] pursue a more abstract, mathematical approach, developing a matrix-based model that characterises cascades solely through operations on the network's adjacency matrix. These studies provide the essential tools for representing CIs as interconnected systems, but they often focus on the structure of failure rather than the dynamic, multi-faceted nature of risk.

2.2 Assessing the impact and propagation of cascades

Moving beyond simply modelling connections, a crucial subset of research focuses on quantifying the impact of cascading failures. Grounding the discussion in reality, Gong et al. [13] conducted a multi-case analysis of 12 historical disasters, providing empirical data on the most frequent cascading pathways and confirming that electric power is the most pivotal initiator of failures. This empirical evidence underscores the critical need for models that can accurately represent these observed high-frequency pathways.

To formalise the analysis of such events, Zuccaro et al. [14] contribute a theoretical model that deconstructs a cascade into its "elementary bricks" (Hazard, Exposure, Vulnerability) and introduces the concept of dynamic vulnerability, where the susceptibility of an element increases as it is hit by successive events in a chain. Complementing this, other researchers have used network science to develop quantitative models. Wang et al. [15], for instance, use a physics-inspired, betweenness-based model to measure the damage from various attack types using concrete topological metrics. While powerful, such purely topological models often overlook other critical operational factors, such as the intrinsic resilience of an asset or its strategic importance.

This drive for actionable assessment has led to the development of several practical modelling frameworks. For instance, Rehak et al. [16] introduced the Cascading Impact Assessment (CIA) Method, which provides a structured, formula-based approach for quantifying the spread of impacts. Their method is notable for explicitly modulating impact intensity by the Resilience Level of the dependent sector. Similarly, Helminen and Hakkarainen [17] proposed their own practical modelling approach aimed at assessing cascading effects, further highlighting the research trend towards creating usable tools for practitioners. The application of such frameworks is demonstrated in a case study by Brabcova et al. [18], where concepts like "Resilience" and "Linkage Intensity" are operationalised with scorable sub-criteria. These practical, formula-based approaches serve as a foundational step toward the more comprehensive, multi-factor risk propagation model proposed in our RIPA framework.

2.3 The specific challenge of cyber-induced cascading effects

While many models are agnostic to the cause of failure, a growing body of work recognises that the integration of Cyber-Physical Systems (CPS) into CIs presents a unique and increasingly potent threat. This thinking has been extended to specific industrial domains, such as in the work by Fu et al. [19], who developed a detailed cascading failure model for Cyber-Manufacturing Systems (CMS). Their model highlights the tight coupling between a physical communication network and a service (production) network, demonstrating that failures in one can directly trigger catastrophic cascades in the other.

Moving from theory to practice, Palleti et al. [20] provide a crucial experimental investigation of these phenomena. By launching cyber-attacks on an interconnected water treatment and distribution testbed, they demonstrate how a cyber event in one system can induce tangible, physical cascading effects in another. This adversarial context is further explored by Chaoqi et al. [21], who use game theory to analyse the strategic interaction between an attacker and a defender, incorporating the cascade effect directly into the game's payoff structure. This highlights that an intelligent attacker will strategically target nodes that are not just vulnerable, but that are also positioned to trigger the most significant cascading failures.

The latest research in this area leverages Artificial Intelligence to manage increasing cybersecurity complexity. Islam et al. [22] introduced a dynamic cybersecurity risk management (d-CSRM) framework that integrates a hybrid AI model–combining linear regression and deep learning–to continuously assess risk based on evolving parameters such as vulnerability exploitation likelihood (EPSS) and asset dependencies. A notable strength of this work is the inclusion of Explainable AI (XAI) methods, such as SHAP and LIME, which enhance transparency and trust in model predictions. However, while the d-CSRM framework effectively addresses dynamic and temporal aspects of risk, it remains primarily focused on individual and cascading vulnerabilities rather than on the broader systemic interdependencies across infrastructures. This limitation suggests the need for approaches capable of quantifying and propagating risk through complex, multi-layered networks of assets and services–an area where models such as RIPA can further extend the understanding of systemic and propagated risk dynamics.

2.4 Standards and guidelines for critical infrastructure risk assessment

In addition to the scientific literature, risk assessment in critical infrastructures is framed by several international standards and guidelines. ISO 31000:2018 provides high-level principles and a generic process for risk management applicable to any type of organisation, covering the identification, analysis, evaluation, treatment, monitoring, and communication of risks. Building on these principles, ISO/IEC 27005:2022 and related information security standards offer detailed guidance for managing information security risks, supporting the implementation of ISO/IEC 27001 through structured processes for identifying, analysing, evaluating, and treating information security risks [23–25].

In the cyber-physical domain, the ISA/IEC 62443 series focuses on the security of industrial automation and control systems (IACS) and operational technology. It defines a risk-based, lifecycle-oriented approach to identifying critical assets, setting security levels (SL 1-4), and applying defence-in-depth controls for industrial control systems and critical infrastructure. Similarly, the NIST Risk Management Framework, particularly NIST SP 800-30 Rev. 1, specifies a structured methodology for conducting information security risk assessments, guiding organisations through the identification of threats, vulnerabilities, likelihood, impact, and prioritisation of risks. NIST SP 800-39 extends this to enterprise-level risk management with a multi-tiered approach (organizational, mission/business process, and information system levels)[26, 27].

These standards and guidelines provide process-level and governance-level frameworks for how risk assessments should be organised, documented, and integrated into organisational decision-making. However, they typically remain agnostic regarding specific modelling techniques for representing interdependencies among infrastructures, tracing impact pathways across multiple network layers, and quantitatively estimating systemic and cascading effects. For example, ISO 31000 and ISO/IEC 27005 describe *what steps to perform* in a risk assessment but do not prescribe *how* to conduct multi-layer network modelling of cross-sector dependencies or compute pathway-based propagated risk metrics. Similarly, while IEC 62443 acknowledges the concept of zones and conduits to represent functional groupings and communication channels, it does not provide mathematical formulations for quantifying risk propagation through these connections or for calculating cumulative systemic exposure[28, 29].

Positioning RIPA within Standards-Based Frameworks. The proposed Risk Impact Pathway Analysis (RIPA) approach is intended to be complementary to these frameworks. It operationalises the "risk analysis" and "risk assessment" phases defined in the standards by providing: (i) an explicit representation of interdependent critical infrastructures as a multi-layer network, (ii) a quantitative pathway-based model of risk propagation and cascading effects incorporating linkage intensity, resilience, and criticality as dynamic factors, and (iii) infrastructure-specific metrics—including propagated risk (R_{pro}), total systemic risk (R_{total}), and Pathway Impact Scores (PIS)—that enable prioritisation of systemic vulnerabilities beyond individual asset risks. In this sense, RIPA can be embedded within the risk assessment stage of ISO 31000 / ISO/IEC 27005 / IEC 62443 / NIST SP 800-30 compliant processes as an analytical engine that yields detailed, system-level and cross-sector insights not specified by the standards themselves.

2.5 The need for dynamic and context-aware risk analysis

A key limitation of traditional modelling is its static nature. This is powerfully critiqued by Hempel et al. [30], who argue that the criticality of a component is not a fixed property but is dynamic and relational, changing as a crisis evolves. This concept of "dynamic criticality" reveals a fundamental flaw in static risk models. This view is broadened by Pescaroli and Nones [31], who frame cascading events as a core feature of our "global interconnected system" and call for moving beyond simplistic analogies to understand cascades as the activation of latent "vulnerability paths."

This need for a dynamic and contextual understanding extends beyond the technical systems to the human and organisational ones. Heino et al. [32]examine the chaotic operational environment that emerges during severe CI disruptions, arguing that major crises break down conventional administrative structures and force diverse stakeholders into new, unforeseen collaborative roles. Their work highlights that a purely technical view of interdependencies is insufficient. Together, these critiques call for a new generation of holistic frameworks that can capture the dynamic nature of criticality and the complex, non-linear propagation of interconnected risk–precisely the gap that our RIPA framework is designed to address.

2.6 Summary of research gaps

In summary, the literature reveals a clear evolution from static, structural models towards more dynamic and context-aware frameworks for analysing cascading risks. Research has successfully established various modelling methodologies, developed theoretical and quantitative approaches for impact assessment, and highlighted the unique challenges posed by cyber-physical systems and intelligent adversaries. Multi-criteria dependency frameworks have been applied in related networked domains such as fog computing resource allocation [33], demonstrating the broader applicability of

trust-based and multi-factor evaluation approaches. However, our review identifies a significant gap: there is no single, comprehensive framework that synthesises these elements by explicitly and quantitatively modelling the propagation of risk using a multi-factor approach that includes dynamic variables like resilience and criticality. While some formula-based methods exist, they often overlook the amplifying effect of criticality or are not explicitly tailored to the nuances of cyber-physical threats.

Therefore, this paper introduces the RIPA framework to address these limitations. RIPA makes two key contributions: (1) It operationalises a novel, formula-based method to calculate propagated risk that explicitly integrates the mitigating effect of resilience and the amplifying effect of criticality as core, quantifiable variables. (2) It adopts a pathway-centric view, allowing for the prioritisation and detailed analysis of entire risk chains rather than just individual components, thereby providing a more holistic and systemic assessment of cyber risk.

3 RIPA framework

This section details the proposed RIPA framework, a multi-stage framework for modelling and quantifying the propagation of cyber risk in interconnected CI systems (see Figure 1). The framework is structured into four sequential stages, each corresponding to a section below. Stage 1 covers component and link-level assessment 3.2; Stage 2 presents the dynamic risk propagation engine 3.3. Stage 3 explains system-level aggregation 3.4, and Stage 4 demonstrates practical application and decision-making 4. Before describing the calculation stages, we first define the foundational standards, key concepts, and modelling assumptions that underpin the framework. The key terms and definitions are summarised in Table 1.

3.1 Foundational standards and assumptions

The RIPA framework is grounded in common security knowledge bases and standards to support a rigorous threat and risk assessment process. This approach enables the asset-threat-vulnerability model to be fed with legitimate, industry-recognised data sources.

The primary knowledge bases used are:

- Common Platform Enumeration (CPE): A standardised format used to identify and classify software, platforms, and other IT assets, enabling consistent mapping across different tools and environments [34].
- Common Weakness Enumeration (CWE): A comprehensive catalogue of software and hardware weakness types, used to identify and categorise design flaws, coding errors, or implementation faults [35].
- Common Vulnerabilities and Exposures (CVE): A widely recognised list of publicly disclosed cybersecurity vulnerabilities. Each CVE entry is associated with a Common Vulnerability Scoring System (CVSS) score, which provides a numerical value reflecting its severity. To account for the real-world likelihood of exploitation, which CVSS does not fully capture, we also incorporate the Exploit Prediction Scoring System (EPSS)[36].

The framework operates under the following considerations:

- Threat Scope: We consider only cyber threats that arise from malicious attempts to gain unauthorised access to a network or system.
- Threat Mapping: The primary threats considered for nodes are deliberate attacks and human errors, which are mapped to specific vulnerability categories.

3.2 Individual risk assessment

Before the dynamic propagation of risk across the network can be modelled, the initial risk profile of each individual node must first be quantified. This is achieved by calculating a baseline Initial Risk or Original Risk (Ro) for each asset [37]. This R0 value represents the initial risk to a component in isolation, independent of any cascading effects it might receive from or transmit to its neighbours[18].

To establish this baseline, our framework is grounded in the well-established principles of traditional, formula-based risk analysis. The classic approach defines risk as a function of three core dimensions: the potential Impact of an incident, the asset's Vulnerability to exploitation, and the severity of the relevant Threat. This formula provides a robust measure of the risk to an asset as a standalone entity, but it deliberately does not account for the dynamic, interconnected nature of modern CI. Therefore, the R0 serves as the foundational, static input for each node, which is then used as the starting point for the dynamic systemic risk propagation model detailed in the subsequent sections[22, 37].

Original Risk This Ro score serves as the foundational, static input for each node, which is then used as the starting point for the dynamic systemic risk propagation model detailed in the subsequent sections. The R_0 was calculated according to Equation 1:

$$R_0 = I_L \times V_L \times T_L \tag{1}$$

Where TL, VL and IL are respectively the threat level (the severity level of threat), the vulnerability level (the proba-

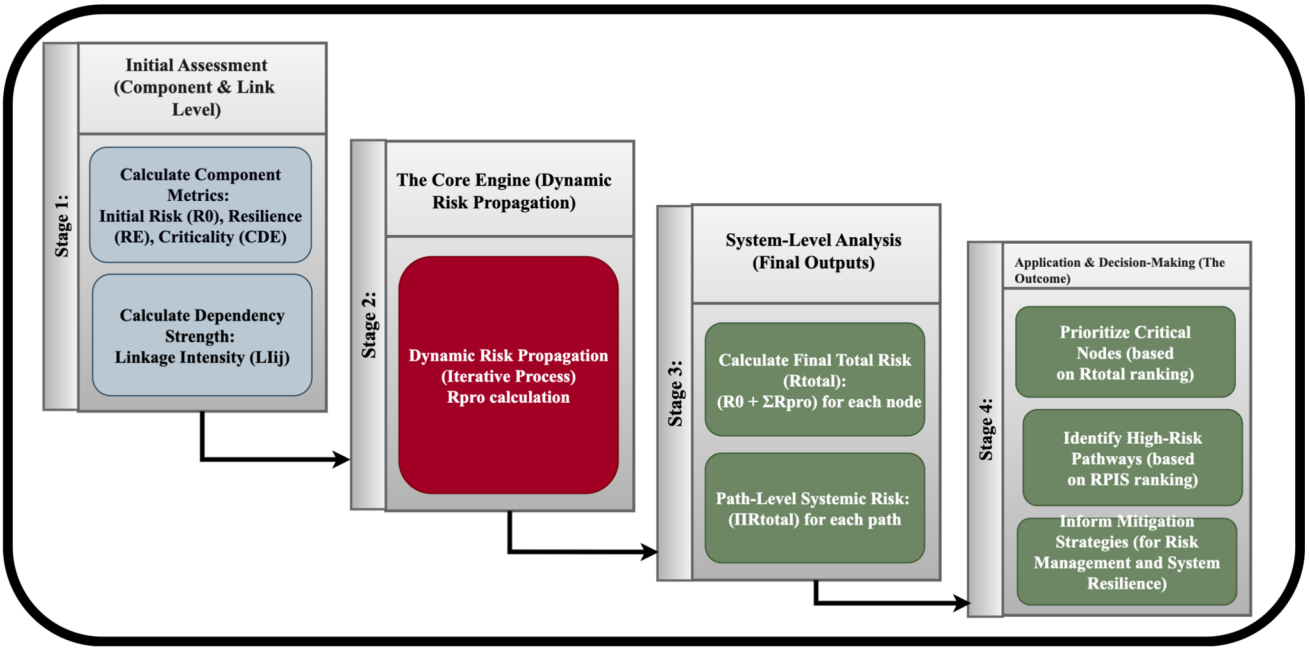

Fig. 1 Framework stages

Table 1 Key Terms and Definitions

Term	Definition
Nodes (V)	represent individual assets or entities within a CIS, each possessing an *Initial Risk*.
Edges (E)	represent the dependencies and potential pathways for risk propagation between nodes. The strength of this dependency is defined by its *Dependency Intensity*.
Criticality Weight	A measure of a node's systemic importance. Within the RIPA framework, it functions as a **risk amplifier**, increasing the impact of any *Propagated Risk* the node receives.
Resilience Factor	A measure of a node's ability to withstand or absorb disruptions. Within the RIPA framework, it functions as a **risk shield**, mitigating both a node's *Initial Risk* and any *Propagated Risk* it receives.
Impact Transfer	The mechanism by which *Propagated Risk* is transmitted from a source node to a destination node across an edge. Its magnitude is modulated by the dependency's intensity and the source and destination nodes' attributes.
Risk Propagation	The process by which risk spreads along a multi-step pathway (a sequence of nodes and edges). This process can be amplified or attenuated at each step by the nodes' criticality and resilience.
Threat	An event, actor, or circumstance that has the potential to cause harm to an asset by exploiting a vulnerability, thereby creating an *Initial Risk*.
Vulnerability	A weakness or flaw in an asset that can be exploited by a threat, contributing to the asset's overall *Initial Risk*.
Risk	The potential for adverse outcomes, such as loss or damage. In this framework, risk is differentiated into two types: *Initial Risk* (inherent to a node) and *Propagated Risk* (transmitted between nodes).
Cumulative Impact	The total risk accumulated at a specific node or along an entire risk propagation pathway, calculated by aggregating the *Initial Risk* and all incoming *Propagated Risks*.

bility that a vulnerability will be exploited) and the impact level[22].

IL Calculation. The Impact Level (IL) quantifies the potential consequences of a security incident should it occur. The calculation is derived directly from the Common Vulnerability Scoring System (CVSS) v3.1 framework [22]. It integrates the technical impacts on Confidentiality, Integrity, and Availability (CIA) with a "Scope" metric, which critically captures the potential for an incident to propagate beyond the component's direct security boundary. The final CVSS Impact Subscore (which ranges from 0.0 to 6.0) is normalised to produce the final IL score on a 0-1 scale.

VL Calculation. The Vulnerability Level (VL) quantifies the likelihood of a given vulnerability being successfully exploited. To address the static nature of CVSS, our framework calculates VL as a weighted average of two metrics: (1) the normalised CVSS Base Score, representing the vulnerability's intrinsic severity, and (2) the dynamic, real-world exploitability probability provided by the Exploit Prediction Scoring System (EPSS) [22]. The final VL score is expressed on a 0-1 scale.

$$VL = (W_{EPSS} \times EPSS) + (W_{CVSS} \times \frac{CVSS_{Base}}{10.0}) \quad (2)$$

TL Calculation. In formulating the Threat Level (TL), we deliberately employ a multiplicative approach over an additive alternative (Likelihood + Severity) to correctly model the interdependent nature of risk factors. We adopt a formulation, inspired by recent work in threat intelligence analysis [38], where the final score is a product of its constituent parts. This theoretical choice is critical. An additive model is conceptually flawed for this purpose as it would assign a high threat score even if one of the core components is zero; for example, a catastrophic event with a likelihood of zero would still be ranked as a significant threat. This misrepresents the fundamental principle that a risk requires both a potential for occurrence and a potential for harm. Our multiplicative framework ensures that the TL is only significant when both LikelihoodScore and SeverityScore are present, providing a more robust and logically sound basis for the subsequent systemic risk analysis.

$$TL = LikelihoodScore * SeverityScore \quad (3)$$

3.3 Systemic risk propagation model

Conventional risk assessment often focuses on the Initial Risk of individual assets, derived from their inherent vulnerabilities, threats, and impacts in isolation. While R_0 provides a necessary baseline, it is fundamentally insufficient for assessing risk in modern, interconnected CI. As highlighted by existing research, traditional risk analysis methods treat assets as isolated entities and are not designed to capture the complexity of CI interconnections, cross-sector impacts, and the cascading effects that define systemic risk. They overlook critical dimensions such as interdependencies and broad social or economic impacts, which are central to understanding CI vulnerabilities [18, 39].

This limitation can lead to a critical oversight: assets that appear low-risk based on their R_0 might, in reality, be highly dangerous due to their position within the network and their role in the propagation and accumulation of risk. We term these previously hidden high-risk nodes *systemic hot spots*. To reveal these, the RIPA framework introduces the concept of *Final Total Risk* (R_{total}). Unlike R_0, which only captures initial risk, R_{total} integrates a node's R_0 with all the *Propagated Risk* (R_{pro}) it receives from upstream dependencies, modulated by factors such as Linkage Intensity, Resilience, and Criticality. By comparing R_{total} against R_0, the RIPA model explicitly highlights systemic hot spots–nodes whose true risk profile is significantly elevated beyond their inherent R_0 due to participation in cascading failure pathways.

To address this, the RIPA framework formalises *Propagated Risk* (R_{pro}). This represents the portion of a source node's risk that is transmitted to a dependent target node due to interconnectivity. The magnitude of this propagation is not constant; it is dynamically shaped by overlooked but crucial systemic factors [18]. The transmission of risk is modelled as a function of three variables:

- **Linkage intensity** (LI_{ij}): Represents the strength of the connection, determining the speed and extent of disruption propagation between nodes.
- **Resilience**: The resilience of source and target nodes acts as a "risk shield," reducing the amount of risk propagated or absorbed.
- **Criticality**: Component criticality acts as a "risk magnet." Even if a node is weakly linked or moderately resilient, its systemic importance means failure can amplify overall risk.

Therefore, a truly effective systemic risk assessment cannot evaluate these factors in isolation. It must integrate linkage intensity, component resilience, and, crucially, component criticality directly into the propagation model [18]. This integration is the core innovation of the RIPA framework.

As established earlier, the baseline R_0 for an isolated asset is quantified using traditional risk assessment formulas, typically as a function of its Impact, Vulnerability, and Threat levels. While R_0 is a necessary starting point, it does not account for systemic effects. The RIPA model extends this to the systemic level by defining *Propagated Risk* (R_{pro}). In this re-contextualization:

- **Threat (TL)**: For propagation, the "threat" is no longer an external attack vector (e.g., CAPEC) but the R_{total} of the upstream source node. This represents the potential harm a node can transmit.
- **Vulnerability (VL)**: Now reflects the weakness of the propagation pathway, derived from the resilience of both source and target nodes: $(1 - RE(u)) \cdot (1 - RE(v))$.
- **Impact (IL)**: Determined by dependency characteristics, combining the Linkage Intensity (LI_{ij}) of the connection and the Criticality (C) of the target node, amplifying potential damage.

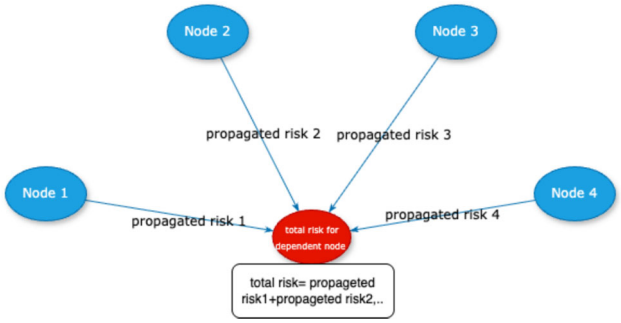

Fig. 2 The total risk in a node

By combining these redefined components, the RIPA framework arrives at the core propagation formula:

$$R_{pro} = R_{total}(i) \cdot (1 - RE(i)) \cdot (1 - RE(j)) \cdot LI(i, j) \cdot C(j) \quad (4)$$

This formula explicitly captures how risks propagate across interconnected infrastructures, enabling the dynamic calculation of R_{total} and the identification of systemic hot spots that traditional risk assessment fails to reveal[40]. Where:

- R_{pro} is the amount of risk propagated from node i to node j.
- R_{total} is the total accumulated risk of the source node i, which acts as the "threat" for this propagation event.
- RE(i), RE(j) are the Resilience Scores of the source and target nodes, respectively.
- LI(i,j) is the Linkage Intensity of the connection between the nodes.
- C(j) is the Criticality of the target node j.

RE is a normalised percentage (0-100%) that quantifies a node's ability to withstand, adapt to, and recover from disruptions, acting as a "risk shield" in the propagation formula. The calculation is based on the comprehensive, multi-component resilience framework proposed by [21]. This framework first calculates five core dimensions of resilience–Preparedness, Absorption, Responsiveness, Recoverability, and Adaptability–each of which is derived from the average of several underlying parameters (shown in table 2) rated on a 1-to-5 scale. These five-dimensional scores are then averaged to compute a final raw resilience score for the node (RE). To ensure a universal scale compatible with our systemic risk model, this raw score is finally normalised to a percentage (0-100%) using the standard formula for a 1-5 scale (See Fig. 2).

The Total Risk of a node is then the cumulative sum of its own Initial Risk and all Propagated Risk it receives from its neighbours:

$$R_{total} = R_0 + \sum R_{pro} \quad (5)$$

This calculation is performed iteratively to allow risk to spread throughout the entire network. The following sections provide the detailed formulas for the new components: Resilience, Linkage Intensity, and Criticality.

3.3.1 Linkage intensity (LI_{ij}) calculation

The Linkage Intensity (LI_{ij}) is a normalised percentage (0-100 %) that quantifies the strength and nature of a dependency from a source node i to a target node j. To evaluate this, we define LIij using six key criteria that reflect the multifaceted nature of interdependencies. Each criterion is assigned a point score based on its criticality, using a scale where a higher value indicates a more significant or critical link. These values were established using the pairwise comparison method [21]. The scoring for each criterion is detailed in Table 3.

Due to their varying levels of significance in contributing to the overall intensity, each of the six criteria is assigned a specific weight, as shown in 3.

The final Linkage Intensity is calculated as a normalised weighted average. The weighted sum of the scores for a specific link is divided by the maximum possible weighted sum, ensuring the final LIij value is a normalised score between 0 and 1.

$$LI_{ij} = \sum_{i=1}^{n} (C_i \cdot w_i) \frac{100}{(C_i max)} \quad (6)$$

Where:

- LI_{ij} is the final normalised Linkage Intensity score from node i to node j.
- C_i is the point value for the i-th criterion for the specific link, taken from Table 3.
- w_i is the normalised weight for the i-th criterion.
- $C_i max$ is the maximum possible point value for the i-th criterion.

3.4 Pathway analysis and prioritisation

The final stage of the RIPA framework is to move from a node-centric view of risk to a pathway-centric one. While the total risk on a single node is a critical metric, the greatest systemic threats often arise from the entire chain of dependencies that lead to that node's failure. The PIS is a metric that quantifies the cumulative, compounded risk carried through

Table 2 Criteria for RE Components

Resilience Component	Calculation Criteria (Parameters)
Preparedness	Risk analysis, Planning, Implementation of measures
Absorption	Redundancy, Robustness, Resistance
Responsiveness	Time to recognise, Time to adopt, Time to respond
Recoverability	Recovery resources, Recovery processes
Adaptability	Inventiveness, Flexibility, Ability to Learn

Table 3 Values of the criteria determining link intensity.

Criteria Determining Link Intensity (Ci)	Point Value
Type of link	
Physical link	3
Geospatial link	2
Cyber	4
Logical link	1
State of link	
Mutual dependence	3
Dependence	2
Influence	1
Level of link	
System link	3
Sector link	2
Sub-sector link	1
Substitution of link	
No substitute link exists	3
Only one substitute link exists	2
Two or more substitute links exist	1
Temporal characteristic of link	
Uninterrupted	3
Periodic	2
Stand-by	1
Structure of link	
Direct	3
Indirect across one node	2
Indirect across two or more nodes	1

an entire path, as illustrated in figure 3, from an initial source of disruption to its final downstream impact. By examining pathway risk, analysts can identify the dependency chains that pose the greatest threat to system stability, even if the individual nodes along that path appear low-risk in isolation.

3.4.1 The PIS algorithm

The calculation and prioritisation of pathway risk follows a systematic, seven-step process: Graph Construction: A directed graph is built with nodes representing CI assets and edges representing dependencies.

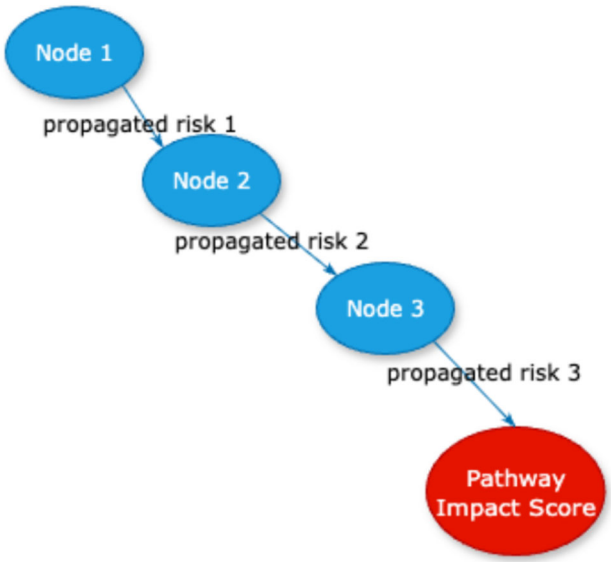

Fig. 3 Pathway Impact Score distribution across nodes and pathways

Node Attribute Assignment: Each node is assigned its calculated attributes, including Initial Risk, Resilience, and Criticality. These are the stages in PIS algorithm:

- Pathway Discovery: The Breadth-First Search (BFS) algorithm is employed to systematically and exhaustively identify all possible dependency pathways between potential source nodes and target nodes.
- Impact Transfer (Rpro) Calculation: The propagated risk (Rpro) is calculated for each edge (impact transfer) in the graph using the formula defined in the previous section.
- PIS Calculation: The PIS for an entire pathway is computed as the product of the Impact Transfer values (Rpro) for all edges that constitute the path. This captures the compounding effect of risk as it propagates through the chain.

$$PIS_{\text{path}} = \prod_{e \in \text{path}} R_{\text{pro}}(e) \tag{7}$$

- Prioritisation and Tiering: The identified pathways are ranked based on their calculated PIS. They are then

divided into three priority tiers to guide resource allocation:

  - High Priority (Red): The top 25% of pathways with the highest PIS, requiring the most immediate attention.
  - Medium Priority (Orange): The next 50% (from 25-75%) of pathways that are important but less critical.
  - Low Priority (Yellow): The bottom 25% of pathways with the lowest PIS.

- Visualisation and Output: The final output is a visualised graph with colour-coded edges based on their priority tier, providing a clear and transparent map of the most significant systemic risks, illustrated in figure 4.

3.4.2 Hybrid prioritisation with node criticality

A key innovation of the RIPA framework is its hybrid approach to prioritisation, which addresses the limitations of relying solely on the calculated PIS. In complex networks, many different pathways can have similar PIS values, making it difficult to distinguish the truly most dangerous routes. To overcome this, we introduce a two-tiered prioritisation strategy: Primary Ranking by PIS: Pathways are first ranked according to their calculated RIS. Secondary Ranking by Node Criticality: When multiple paths have similar PIS scores, the path that traverses a higher number of highly critical nodes is given a higher priority. This hybrid approach recognises that a path passing through strategically important assets represents a far more dangerous scenario due to the potential for severe cascading effects, even if its calculated propagation score is identical to that of a less critical path. This combination offers the best of both worlds: it ensures a complete and transparent mapping of all risk pathways via BFS, while also highlighting the most impactful ones based not just on the magnitude of propagated risk, but on the strategic importance of the assets involved. This provides a more practical and insightful basis for targeted risk mitigation and system resilience planning.

3.5 Risk data collection engine (RDCE) and implementation

To operationalise the RIPA methodology within LAMAD's infrastructure, the framework incorporates a custom data collection component–the Risk Data Collection Engine (RDCE)–as its first algorithmic stage. The RDCE serves as an integral part of RIPA's pipeline, automating the transformation of basic asset inventories into comprehensive risk profiles through systematic integration with cybersecurity knowledge bases. This data enrichment stage is essential for RIPA's subsequent risk propagation calculations, providing the initial risk values (R_0) that serve as seeds for cascade analysis.

While asset inventories and data were provided directly by the participating company, RIPA's RDCE component enriches this baseline information using publicly available cybersecurity repositories: the NVD for CVE records and CVSS base scores, EPSS for exploitation probability estimates, and the CAPEC repository for attack pattern taxonomies.

As the first stage of the RIPA algorithm, the tool implements a multi-stage mapping process: first normalising CPE identifiers to handle format variations (cpe:/ and cpe:2.3 schemas), then matching each asset's CPE to all corresponding CVEs in the NVD dataset, extracting CVSS v3.x base scores, linking CVEs to their associated Common Weakness Enumeration (CWE) categories, and finally enriching each CVE with EPSS exploitation probabilities and CAPEC attack likelihood/severity ratings through CWE-to-CAPEC mappings. This automated process ensures that RIPA begins with consistent, traceable baseline risk assessments before calculating propagation effects.

In practice, there are multiple ways to collect the input data required by the RDCE. Active discovery tools such as Nmap can be combined with endpoint telemetry collectors like Osquery to build detailed asset inventories through automated scanning. The RDCE merges Nmap network scan data (IP addresses, ports, services, CPE identifiers) with Osquery endpoint telemetry (hardware specifications, OS details) by matching IP addresses and hostnames, producing a consolidated asset inventory. Alternatively, organisations may supply inventories directly. This flexibility makes the framework generalisable and scalable across different infrastructures.

Dynamic monitoring and alerting. In practical deployments, the RDCE and RIPA engine are intended to operate in a continuous monitoring mode, coupled with external asset and vulnerability management tools via API. Asset inventories and dependencies can be updated automatically on an event-driven basis as the monitoring tool detects new or removed assets, eliminating the need for manual maintenance of the dependency graph. Vulnerability-related inputs to the initial risk R_0 are refreshed in line with the update frequency of external repositories (typically daily for vulnerability databases such as CVE and dynamic scoring systems such as EPSS), so that changes in the threat landscape are reflected in the analysis. The RIPA engine can therefore be re-executed either on a fixed schedule or whenever significant updates are reported by the monitoring API. The optimal execution frequency depends on the rate of change in underlying parameters: vulnerability data from external repositories typically updates on a daily cycle, whereas structural changes to dependencies, resilience, or criticality usually occur on longer timescales (weekly to monthly). In this setting, the

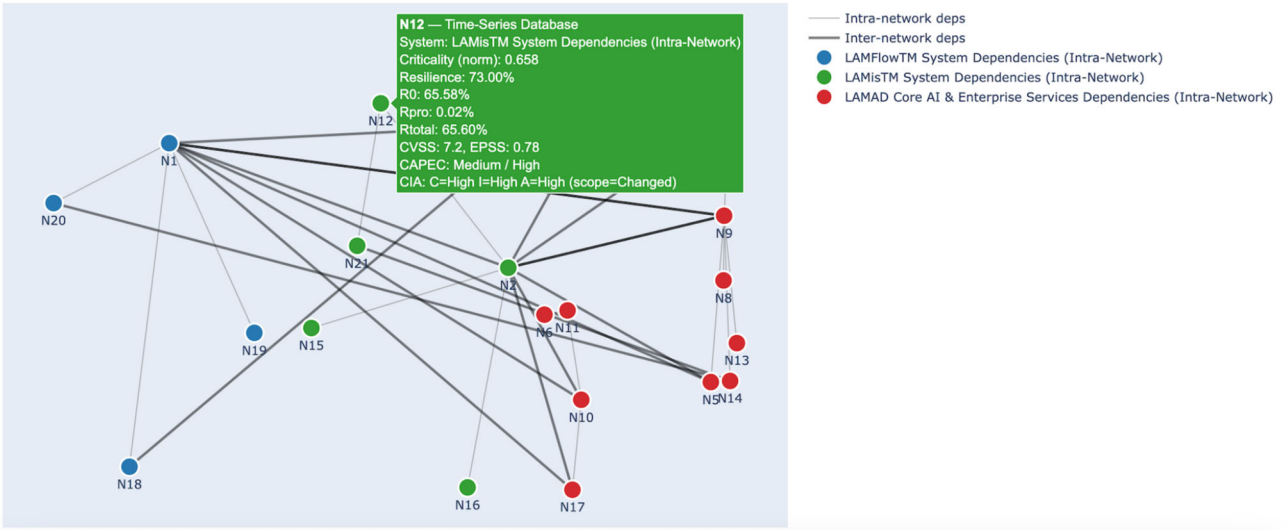

Fig. 4 Graphical representation of the examined dependency risk graph

propagated risk metric R_{pro} can be normalised and used for alerting by defining sector-specific risk bands (low, medium, high) and triggering alarms when R_{pro} for edges feeding highly critical nodes enters a high-risk band or exhibits a sudden relative increase compared to its recent baseline.

The enriched vulnerability data from the RDCE feeds directly into RIPA's risk propagation engine, implemented in Python using the NetworkX library for dependency graph modelling and NumPy for numerical computation. Each asset node is initialised with its initial risk score (weighted combination of CVSS, EPSS, and CAPEC severity), then RIPA calculates propagated risk using the following core algorithm:

The RIPA framework then applies this propagation algorithm using a breadth-first search approach that iteratively calculates risk flows across dependency edges until convergence. This enables the calculation of Propagated Risk, Final Total Risk, and Pathway Impact Scores at scale. The framework was specifically adapted to LAMAD's air-gapped, event-driven microservices architecture, with each component modelled as a distinct node with explicit dependency edges.The procedural implementation of the proposed RIPA framework is summarised in Algorithm 1, which details the key computational stages–from risk data acquisition and parameter initialisation to iterative propagation and pathway impact scoring–used to quantify and prioritise systemic risk within interdependent infrastructures.

4 Case study: Application of RIPA for LAMAD-LLC systems

4.1 Case study overview

LAMAD LLC (Logical Automated Measurement and Diagnostics) is an Oman-based company specialising in AI-driven metering and diagnostic systems for the oil and gas sector. Its integrated platforms–LAMFlow™ and LAMis™–combine artificial intelligence, physics-based modelling, and live field data to improve measurement accuracy and operational efficiency. LAMFlow™ functions as an AI-powered Virtual Flow Meter (VFM), continuously estimating oil, gas, and water production from real-time sensor inputs such as pressure, temperature, and choke position. LAMis™, in turn, provides centralised data management, validation, and visualisation, linking field instrumentation with enterprise-level monitoring and analytics. This tightly integrated architecture delivers major performance and cost advantages but also creates high interdependency across digital, operational, and physical layers. A fault in one subsystem–such as sensor drift, data transmission failure, or AI misprediction–can propagate through these links, affecting flow accuracy, decision automation, and regulatory reporting. The RIPA framework is therefore applied to model and quantify cascading risk propagation across LAMAD's interconnected infrastructure. By analysing how initial disruptions spread through dependency pathways and identifying resilience thresholds, RIPA supports more robust design, prioritisation of mitigation measures, and enhanced operational continuity within LAMAD's AI-enabled metering ecosystem.

To demonstrate the efficacy of the RIPA framework, we apply it to the operational architecture of LAMAD-LLC's

Algorithm 1 RIPA: Risk Data Collection, Propagation, and Pathway Analysis

Input: Asset inventory $\mathcal{A}$ with CPE identifiers; dependency graph $G = (V, E)$ representing assets and their interdependencies.
Output: Node-level propagated risk $\{R_{\text{pro}}(v) \mid v \in V\}$, total risk $\{R_{\text{total}}(v) \mid v \in V\}$, and ranked list of high-impact dependency pathways (PIS).
// Phase 0: Risk Data Collection Engine (RDCE)
Load knowledge bases: NVD, $EPSS$, $CAPEC$
Build mappings: $CPE \rightarrow CVE$, $CVE \rightarrow CWE$, $CWE \rightarrow CAPEC$
for each asset $a \in \mathcal{A}$ **do**
  $CVEs \leftarrow$ Lookup(CPE_to_CVE, Normalise_CPE($a.cpe$))
  for each $cve \in CVEs$ **do**
    Retrieve $CVSS(cve)$, $EPSS(cve)$, and $CAPEC(cve)$
    Assign values to node $v \in V$ corresponding to asset a
  end for
end for
// Phase 1: Initialise intrinsic (initial) risk
for each node $v \in V$ **do**
  $IL(v) \leftarrow$ Impact_Level(CIA_triad, scope)
  $VL(v) \leftarrow 0.5 \times EPSS(v) + 0.5 \times \frac{CVSS(v)}{10}$
  $TL(v) \leftarrow CAPEC\_likelihood \times CAPEC\_severity$
  $R_0(v) \leftarrow 0.4 \times IL(v) + 0.3 \times VL(v) + 0.3 \times TL(v)$
end for
// Phase 2: Calculate linkage intensity (LI)
for each edge $(u, v) \in E$ **do**
  $LI(u, v) \leftarrow \frac{\sum_{f \in factors} w_f \times score_f(u,v)}{\sum w_f}$
end for
// Phase 3: Iterative risk propagation
repeat
  for each edge $(u, v) \in E$ **do**
    $R_{\text{pro}}(v) \leftarrow R_{\text{pro}}(v) + R_{\text{total}}(u) \times (1 - RE(u)) \times (1 - RE(v)) \times LI(u, v) \times CDE(v)$
  end for
  for each node $v \in V$ **do**
    $R_{\text{total}}(v) \leftarrow R_0(v) + R_{\text{pro}}(v)$
  end for
until convergence or maximum iterations reached
// Phase 4: Pathway scoring and prioritisation
Enumerate all simple paths $\mathcal{P}$ up to length k
for each path $P \in \mathcal{P}$ **do**
  $PIS(P) \leftarrow \frac{1}{|P|-1} \sum_{(u,v) \in P} R_{\text{total}}(u) \times (1 - RE(u)) \times (1 - RE(v)) \times LI(u, v) \times CDE(v)$
end for
Rank pathways by PIS percentile thresholds (e.g., 90th = high-risk, 25th = low-risk)
return $\{R_{\text{total}}(v)\}$ and Top-k high-impact pathways

key systems: LAMFlow (Virtual Well Testing) and LAMis (Intelligent Measurement Integrity System). This case study illustrates how RIPA quantifies systemic risk, identifies systemic hot spots, and prioritises pathways of risk propagation within an interconnected infrastructure. The overall objective is to show how RIPA provides actionable insights that conventional risk assessment methods, focused only on R_0, cannot reveal.

4.2 Network description

The LAMAD-LLC system is modelled as a directed graph, where nodes represent critical digital assets and directed edges signify their intricate interdependencies. These assets encompass a wide spectrum of components, including specialised databases, sophisticated schedulers, robust message brokers, advanced AI engines, and essential external interfaces. Collectively, these components enable the advanced functionalities of LAMAD's core product offerings: LAMFlow™ and LAMis™.

To provide a more granular and contextually relevant analysis, the 21 identified assets are strategically organised into three distinct, LAMAD-centric networks, directly reflecting the company's service architecture:

1. **LAMFlow™ system:** This network is primarily focused on virtual well testing, real-time flow determination, predictive analytics, and production optimisation, leveraging AI and physics-based models.
2. **LAMis™ system:** Dedicated to intelligent metering, this network handles real-time monitoring, comprehensive evaluation, uncertainty demonstration, and performance enhancement for fiscal and custody transfer metering systems.
3. **LAMAD core AI & enterprise services:** Serving as the foundational shared infrastructure, this network provides essential AI capabilities, robust data management, and common enterprise services that underpin and support the operations of both LAMFlow™ and LAMis™ systems.

This network stratification, which clarifies functional groupings and highlights shared resource dependencies, is comprehensively summarised in Table 4. Each node within these networks is precisely characterised by specific attributes that facilitate the quantitative calculation of its Initial Risk (R_0), Resilience (RE), and Criticality (CDE). The directed edges linking these nodes denote their interdependencies, with each connection rigorously quantified by a Linkage Intensity (LI_{ij}) score. A detailed overview of these nodes, their assigned networks, and their structured dependencies is presented in Table 4.

The intricate web of interdependencies within the LAMAD-LLC system is captured by a total of 47 directed connections. These connections represent diverse and crucial relationships–ranging from vital data exchange and critical process sequencing to essential control signals and shared computational resources–that form the pathways through which risks can propagate throughout the system. This structured representation is fundamental to how RIPA analyses the system, enabling the revelation of potential cascading failure points and informing the development of targeted, effective risk mitigation strategies.

Table 4 LAMAD-LLC System Nodes and Dependencies.

ID	Node Name	System	Description	Inputs From	Outputs To
N1	LAMFlow	LAMFlow	Virtual flow meter platform	N18, N19, N20, N2, N9, N17, N7, N10, N5	N9
N2	LAMis	LAMis	Intelligent metering analytics system	N12, N15, N16, N9, N3, N17, N7, N10, N5	N1, N9
N3	AI Engine	LAMAD Core	Core AI inference engine	N4	N18, N2
N4	AI Model Processing	LAMAD Core	ML model execution engine	N/A	N3
N5	Scheduler	LAMAD Core	Time-based task orchestration	N/A	N9, N1, N2
N6	Service Management	LAMAD Core	Service lifecycle management	N/A	N11
N7	Visualisation Service	LAMAD Core	Dashboards and displays	N9	N1, N2
N8	Tag Retrieval	LAMAD Core	Metadata management service	N/A	N9
N9	Real-time Data	LAMAD Core	Live data streaming and writeback	N5, N8, N13, N14, N1, N2	N7, N1, N2
N10	API Service	LAMAD Core	Microservice gateway	N17	N11, N1, N2
N11	Server DBMS	LAMAD Core	Relational database	N10, N6	N/A
N12	Time-Series Database	LAMis	Historical data storage (TSDB)	N21	N2
N13	Message Broker	LAMAD Core	Event-driven messaging hub	N/A	N9
N14	OSISoft PI System	LAMAD Core	Industrial data historian	N20, N21	N9
N15	Live Well Parameters	LAMis	Real-time field operational data	N/A	N2
N16	Well-test Backlog History	LAMis	Historical well testing data	N/A	N2
N17	JWT Authentication	LAMAD Core	Security and authentication service	N/A	N10, N1, N2
N18	Predicted Flow Components	LAMFlow	AI-predicted oil, gas, water outputs	N3	N1
N19	Physics and Math Models	LAMFlow	Physical/mathematical modeling engine	N/A	N1
N20	Producing Wells	LAMFlow	Physical well infrastructure (field data source)	N/A	N1, N14
N21	Metering Systems	LAMis	Physical metering devices (field data source)	N/A	N12, N14

4.3 Data acquisition and parameterisation

To parameterise the RIPA model, each node was assigned an initial risk (R_0) and associated systemic attributes:

- **Initial risk:** Derived using established cybersecurity standards (CVSS v3.1, EPSS, CAPEC). For each asset, R_0 was calculated as a function of its inherent Impact (IL), Vulnerability (VL), and Threat (TL).
- **Resilience:** Scores assigned to nodes to reflect redundancy, recovery capabilities, and adaptability. Lower resilience increases susceptibility to propagated risk.
- **Criticality:** A weight representing the systemic importance of a node. High-CDE nodes function as "risk magnets" capable of amplifying systemic effects.
- **Linkage intensity:** Values assigned to each edge to quantify the strength of the dependency. Higher LI indicates faster or more direct propagation of disruptions.

While full parameter tables are provided in the Results section, this subsection details the methodological basis for their assignment. The data sources and scoring rationale ensure that parameter values are realistic and consistent with established cyber-risk assessment practices.

4.4 Application of RIPA to LAMAD infrastructure

This section details the systematic application of the RIPA framework to LAMAD systems, demonstrating how the methodology translates from theoretical construct to practical risk assessment across 21 interdependent cyber-physical assets.

4.4.1 Asset identification and characterisation

The first step in applying RIPA involved comprehensive asset enumeration and characterisation across LAMAD's three-tier architecture. Through collaboration with LAMAD's technical team and analysis of system documentation, 21 critical nodes were identified and categorised into three subsystems: LAMFlowTM (virtual flow meter platform, 4 nodes), LAMisTM (metering intelligence system, 5 nodes), and LAMAD Core AI and Enterprise Services (shared infrastructure, 12 nodes). Each asset was assigned a unique identifier (N1-N21) and characterised along multiple dimensions to establish its baseline risk profile. For each node, the following attributes were collected and encoded into the RDCE (Section 3.5): CPE identifier linking the asset to known software/hardware products; operational criticality score reflecting the asset's importance to production measurement accuracy and business continuity; and resilience capacity metrics across five dimensions. Table 4 presents the complete asset inventory with system assignments and functional descriptions.

4.4.2 Individual risk assessment

Following asset characterisation, the RDCE automatically enriched each node's risk profile by integrating publicly available threat intelligence. For nodes with identifiable CPE strings, the tool mapped to corresponding CVE records in the National Vulnerability Database, EPSS exploitation likelihood estimates, and CAPEC attack patterns linked through CWE categories. For each node, three risk components were calculated and normalised to 0-100% scales:

Impact level (IL): Derived from CVSS impact subscore using CIA triad qualitative ratings, with scope-dependent formulas accounting for whether vulnerabilities affect resources beyond authorisation boundaries.

Vulnerability level (VL):) Quantifies the likelihood of successful exploitation by addressing the static nature of CVSS through a weighted average of two metrics: (1) the normalised CVSS Base Score representing the vulnerability's intrinsic severity, and (2) the dynamic, real-world exploitability probability provided by EPSS.

Threat level (TL): Attack pattern feasibility from CAPEC likelihood and severity score, where qualitative ratings (Very High to Low) are mapped to numeric scores. The node's original Risk (R_0) combines these components: $R_0 = 0.4 \times IL + 0.3 \times VL + 0.3 \times TL$, prioritising impact potential (40%) over vulnerability exposure and threat likelihood (30% each), consistent with critical infrastructure risk assessment principles.

4.4.3 Dependency network construction

RIPA's core innovation–modelling risk propagation through system interdependencies–required explicit representation of how failures cascade between assets. A directed multigraph G (V, E) was constructed where nodes V represent the 21 assets and edges E represent dependencies characterised along six dimensions derived from Infrastructure Dependency Analysis literature (shown in table 3).

Each dependency edge (u,v) was assigned a linkage strength coefficient calculated as a weighted sum of normalised scores across these six dimensions, where weights reflect relative importance based on expert judgment and sensitivity analysis. A total of 33 dependencies were documented in the dependency Excel file, including 16 intra-network edges (same system) and 17 inter-network edges (cross-system), enabling analysis of both localised and cascading cross-boundary failures.

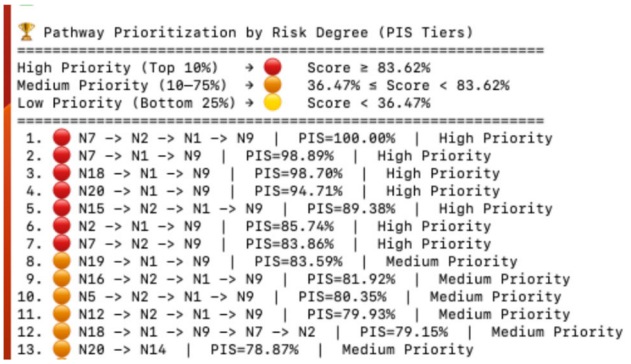

Fig. 5 Ranked propagation pathways grouped by risk degree (PIS tiers). High-priority cascades indicate dominant routes of systemic vulnerability

4.4.4 Systemic risk propagation model

With the dependency graph constructed and nodes initialised with initial risk, RIPA's propagation algorithm simulates how risk flows through the network. Using a BFS traversal, the algorithm iteratively calculates incoming risk at each node from all predecessor nodes. For each node, R_{pro} is calculated.

The Final Total Risk combines initial and propagated components. This additive model reflects the principle that a node's total risk exposure is the sum of its own vulnerabilities and the risks inherited from dependencies. Criticality weighting was applied such that nodes with higher operational importance contribute disproportionately to downstream risk propagation. The simulation executed in 8-12 iterations before convergence across the 21-node network, producing a risk landscape showing how initial vulnerabilities at source nodes propagate through intermediary nodes to critical operational endpoints (N1 LAMFlow, N2 LAMis, N9 Real-time Data).

4.4.5 Pathway analysis and prioritisation

Beyond individual node risk, RIPA identifies high-risk pathways–sequences of dependencies through which cascading failures are most likely to propagate. For all simple paths (no repeated nodes) between any source-target pair, a Pathway Impact Score was calculated as the product of linkage strengths along the path, weighted by the total risk at each intermediate node. All paths were classified into risk tiers using percentile thresholds: High Priority, Medium Priority, and Low Priority as shown in 5. Detailed results, including specific node risk scores, pathway rankings, and network topology analysis, are presented in Section 5.

5 Results and discussion

This section presents the analysis of the RIPA results. A summary of the algorithm's computed node-level outcomes is provided in Table 5.

5.1 Initial risk (R_0) versus total risk (Rtotal): The necessity of dependency-aware risk assessment

The RIPA model challenges the isolation-based paradigm by introducing a dependency-aware formulation where total systemic risk equals the sum of initial risk and propagated risk, the latter quantifying additional exposure transmitted through upstream dependencies. The key question addressed here is: how significantly does R_{pro} alter the overall risk landscape compared to R_0 alone?

Applying the RIPA model to the LAMAD-LLC integrated infrastructure system revealed systematic and substantial deviations between R_0 and R_{total}. Certain nodes experienced notable amplification due to their critical topological positions within the dependency network (shown in figure6).

For example, Node N1, serving as the central orchestration point with multiple dependencies, showed the highest amplification: $R_0 = 79.68\%$ increased to $R_{\text{total}} = 91.79\%$, representing a 15.20% absolute (19.1% relative) increase. Similarly, Node N2 rose from $R_0 = 55.68\%$ to $R_{\text{total}} = 65.30\%$, a 9.62% amplification (17.3% relative), as it accumulated risk from upstream data processing and control pathways. Moderate amplification occurred in data-centric nodes such as N9 ($R_{\text{pro}} = 5.77\%$) and N14 ($R_{\text{pro}} = 3.03\%$), reflecting their roles as aggregation points within the SCADA architecture. Even nodes with already high initial risk thus experienced measurable systemic amplification when positioned within critical data flows.

In contrast, 15 of 21 nodes exhibited negligible propagation ($R_{\text{pro}} < 1\%$), indicating strong resilience, low network centrality, or isolation from dependency chains. For instance, Node N5 maintained $R_0 = 82.53\%$ with almost no amplification ($R_{\text{pro}} \approx 0\%$) due to its endpoint position despite high inherent vulnerability.

These findings yield three critical insights underscoring the need for dependency-aware assessment:

1. **Systematic risk misclassification:** Traditional isolation-based methods misclassify systemic exposure. Node N2 would be labelled "moderate risk" ($R_0 = 55.68\%$) under conventional metrics, whereas its true systemic exposure ($R_{\text{total}} = 65.30\%$) places it in the high-risk category–a misjudgment with direct implications for security prioritisation.
2. **Position-dependent vulnerability:** Nodes with comparable R_0 values can exhibit vastly different R_{total} outcomes depending on network position. Comparing N5

Table 5 Node Risk Summary based on corrected RIPA results.

Node ID	R_0 (%)	R_{pro} (%)	R_{total} (%)	Criticality	Resilience
N1	79.68	12.11	91.79	0.90	72.0
N2	55.68	9.62	65.30	0.85	68.0
N9	80.13	4.63	84.76	0.88	74.0
N14	64.08	1.94	66.02	0.80	70.5
N11	81.18	1.85	83.03	0.88	78.0
N12	65.58	0.87	66.46	0.85	73.0
N10	43.40	0.56	43.96	0.70	53.0
N18	51.35	0.29	51.64	0.70	48.0
N3	44.73	0.21	44.94	0.95	81.5
N5	82.53	0.00	82.53	0.85	76.5
N15	82.08	0.00	82.08	0.85	73.0
N16	56.43	0.00	56.43	0.75	60.5
N17	78.63	0.00	78.63	0.90	78.0
N19	43.40	0.00	43.40	0.70	48.0
N20	65.12	0.00	65.12	0.80	60.5
N21	64.83	0.00	64.83	0.90	73.0
N4	57.63	0.00	57.63	0.75	61.0
N6	65.34	0.00	65.34	0.80	64.0
N7	82.37	0.38	82.75	0.90	77.0
N8	51.05	0.00	51.05	0.70	51.0
N13	53.28	0.00	53.28	0.80	65.5

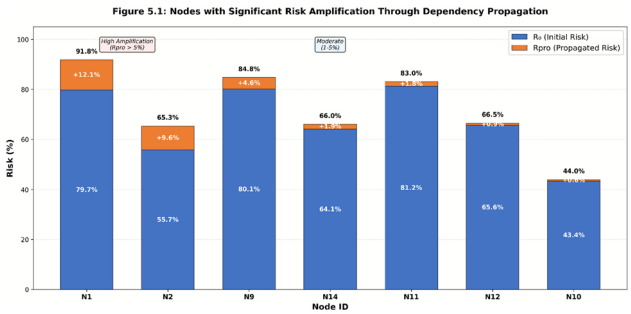

Fig. 6 Risk Amplification Chart

($R_{pro} \approx 0\%$) and N9 ($R_{pro} = 5.77\%$) demonstrates that topology, not just inherent vulnerability, governs actual exposure.

3. **Multiplier effect of dependencies:** Inter-node dependencies generate a multiplier effect where total system risk exceeds the sum of individual risks–a phenomenon invisible to frameworks assuming independent failures.

The significant divergence between R_0 and R_{total} confirms that dependency-blind assessments systematically underestimate true exposure in networked infrastructures. Security strategies based solely on R_0 will (i) overlook high-amplification nodes that appear moderate in isolation, (ii) misallocate resources to nodes posing limited systemic threat, and (iii) fail to anticipate cascading failure pathways–now recognised as dominant vectors in modern interconnected environments.

The RIPA framework, by explicitly modelling R_{pro} through dependency-pathway analysis, enables topology-aware prioritisation of defensive measures. This represents a necessary paradigm shift–from component-centric vulnerability management to system-centric resilience optimisation–reflecting the reality that in interdependent infrastructures, *the whole is demonstrably more vulnerable than the sum of its parts.*

5.2 Impact of criticality (CDE): The risk magnet effect

To examine the role of criticality as a risk amplifier, we analysed what we refer to as the *Risk Magnet Effect*–the tendency of highly critical nodes to attract and accumulate propagated risk. A controlled sensitivity analysis was conducted on three representative nodes from the LAM infrastructure, selected for their different network roles and initial risk levels:

- **N1:** High initial risk ($R_0 = 79.68\%$), characterised by high network centrality and strong interconnectivity.
- **N2:** Moderate initial risk ($R_0 = 55.68\%$), with medium centrality and several upstream dependencies.
- **N9:** High initial risk ($R_0 = 80.13\%$) mainly due to external interfaces, but with a peripheral network position.

The criticaly score was systematically varied from 0.1 to 1.0 in increments of 0.1, while all other parameters–R_0, RE_{DE}, LI, and RE_{IE}–were held constant. For each level of criticality, R_{total} was computed using the RIPA propagation formula.

Several patterns emerged from this analysis:

1. Rapid Saturation in Highly Connected Nodes (N1): Node N1 showed rapid risk escalation, approaching near-saturation ($R_{total} \approx 98\%$) at CDE = 0.3 and remaining almost constant beyond that point. This strong amplification results from its high initial risk, strong propagation potential (2.579), and dense connectivity (9 incoming dependencies). The delta risk ($\Delta = R_{total} - R_0$) rose from +7.19 pp at CDE = 0.1 to +42.87 percentage points (pp) at its actual criticality (0.9), representing a 54% relative amplification.

2. Strong Linear Amplification with Delayed Saturation (N2): Node N2 exhibited clear linear growth in total risk up to CDE = 0.6, after which saturation began. The relationship between CDE and R_{total} was nearly linear ($R^2 = 0.999$) within the 0.1–0.5 range. At its actual criticality (0.85), N2 reached $R_{total} = 81.34\%$, showing an amplification of +25.66 pp (46%). This validates the multiplicative influence of criticality in the RIPA propagation model.

3. Position-Dependent Sensitivity (N9): Despite a high initial risk ($R_0 = 80.13\%$) and criticality (0.97), N9 exhibited the lowest amplification among the tested nodes. Its ΔR increased only from +2.20 to +21.71 pp across the full CDE range. This lower sensitivity is explained by its peripheral position (6 dependencies compared to 9 for N1/N2) and higher resilience (87.5% vs. 68–72%), resulting in a smaller cumulative propagation potential (1.753), roughly 68% lower than N1's.

The observed differences–up to a tenfold variation in amplification rates–are not artefacts of the model but reflect genuine systemic risk behaviour in interdependent infrastructures. Highly connected and critical nodes (like N1) act as *risk magnets*, absorbing and concentrating risk from multiple dependencies.

In contrast, traditional criticality-blind models that assume uniform propagation (e.g., CDE = 0.5 for all nodes) would significantly misrepresent true exposure. For instance, such a model would underestimate N2's total risk by 9.7 percentage points (68.7% vs. 78.4%).

In summary, the *Risk Magnet Effect* confirms that a node's criticality–amplified by its position and connectivity–is a key determinant of total systemic risk. Future cybersecurity and resilience strategies must therefore prioritise nodes not only by inherent vulnerability but also by their potential to propagate risk throughout the network. This represents a necessary shift from component-focused to system-aware risk management (as shown in figure 7).

Table 7 Resilience Sensitivity Analysis: Total Risk (%) under varying RE_{DE} levels.

Resilience (%)	N1	N2	N9
20	100	100	99
40	97	95	91
60	91	88	86
75	82	73	79
85	77	69	75
95	71	67	72

5.3 Linkage intensity: quantifying dependency strength and propagation impact

Linkage Intensity (LI) measures how strongly nodes depend on one another, based on six dependency attributes: type, level, state, substitutability, temporal pattern, and structure. To assess LI's effect on systemic risk, a sensitivity analysis was performed by varying LI by ±20% while keeping criticality, resilience, and initial risk (R_0) constant.

Baseline LI values were moderate to high (N1 = 0.662, N2 = 0.657, N9 = 0.684), indicating strong inter-node dependencies. At these levels, total risk ranged from 95–99%, suggesting that the network operates under strong propagation conditions.

Although total risk varied by less than ±5 percentage points (pp) under high-risk conditions, the analysis confirmed that LI remains a primary driver of risk propagation. Nodes with higher resilience (e.g., N9, 87.5%) exhibited greater sensitivity to LI changes, showing that resilience moderates but does not eliminate dependency effects. When systems are near saturation, additional increases in LI yield minimal change; however, in less-saturated or well-resilient systems, risk rises proportionally with LI—validating its role as a linear multiplier in the RIPA model.

Overall, LI directly governs how risk spreads through dependencies. Thus, reducing LI through redundancy, buffering, or decoupling remains an effective mitigation strategy—particularly once baseline vulnerabilities are reduced and resilience is strengthened. As summarised in Table 6, the sensitivity of total systemic risk to linkage intensity confirms LI's central role as a propagation multiplier within the RIPA model.

5.4 Resilience (RE): the risk shield

RE represents a node's defensive capacity–its ability to absorb, resist, and recover from disruptive events. In the RIPA propagation model, resilience functions as a dampening factor through the $(1 - RE_{DE})$ term, reducing the proportion of risk transmitted through dependencies. To evaluate how resilience moderates total systemic risk, dependent-node

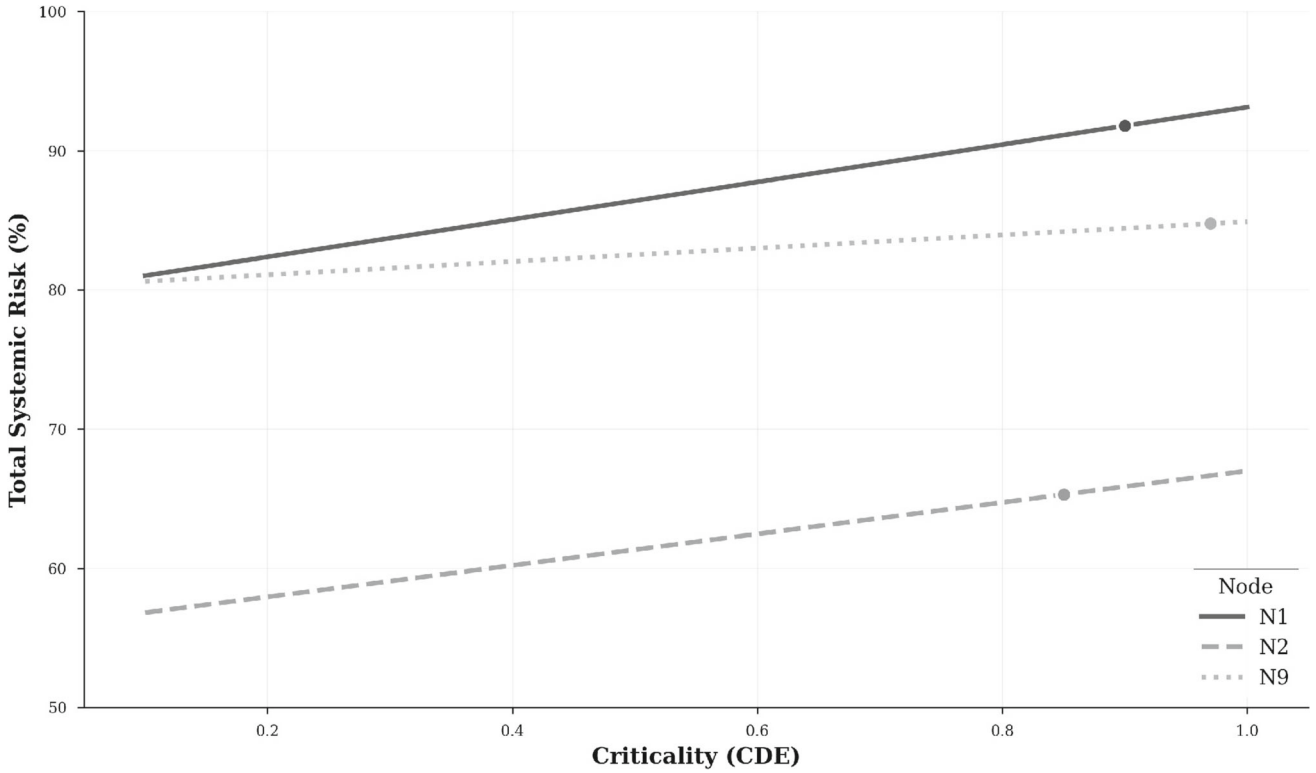

Fig. 7 the effect of criticality on risk

Table 6 Impact of ±20% Variation in Linkage Intensity on Total Risk

Node	R_0 (%)	Baseline LI	Rtotal (–20%)	Rtotal (Baseline)	Rtotal (+20%)	Range (pp)
N1	79.68	0.662	96.2	98.9	100.0	3.8
N2	55.68	0.657	92.9	96.3	99.8	6.9
N9	80.13	0.684	87.5	91.6	94.4	6.9

resilience (RE_{DE}) was systematically varied from 20% to 95%, while criticality, linkage intensity, and initial risk (R_0) were held constant.

Baseline resilience values were obtained from prior assessments of each node's redundancy, monitoring, and recovery capacity:

- **N1:** 72% (moderate defensive posture)
- **N2:** 68% (moderate defensive posture)
- **N9:** 87.5% (strong defensive posture)

For each scenario, total risk was computed using the R_{pro} and R_{total} equations. The results reveal a distinct non-linear protective effect (Table 7). At low resilience levels (($\approx$ 40%), all nodes converge near 100% total risk, confirming that inadequate defensive capacity leads to full systemic exposure regardless of network position. Between 60% and 80%, total risk declines sharply, indicating a resilience threshold where propagation becomes substantially constrained. Beyond 85%, additional gains yield smaller marginal benefits, suggesting entry into a stable, well-protected regime.

A comparison with equivalent parameter variations highlights resilience's superior mitigating influence. Increasing resilience provides nearly double the total risk reduction achieved by equivalent changes in criticality or dependency strength, confirming it as the single most effective control parameter. The overall trend demonstrates that enhancing resilience substantially lowers total systemic risk, though the magnitude of improvement depends on each node's baseline vulnerability and connectivity.

Key Observations:

1. **Non-linear protection:** The relationship between resilience and total risk follows an exponential decay pattern. Small improvements at low resilience levels yield modest benefits, whereas beyond 70%, each additional increase produces disproportionately larger reductions in systemic risk.

Table 8 Comparative Risk Reduction for Equivalent Parameter Changes (Node N2)

Parameter Change	Risk Reduction (pp)
Resilience: 68 % → 95 %	–33.0
Criticality: 0.85 → 0.45	–17.2
Linkage Intensity: 1.0× → 0.5×	–16.7

2. **Topology-independent defence:** Unlike criticality or linkage intensity, resilience benefits all nodes equally, regardless of network position. N9's high resilience (87.5%) explains its lower propagated risk despite its high initial risk ($R_0 = 80.13\%$) and criticality ($CDE = 0.97$).
3. **Multiplicative shielding:** A 10% increase in resilience reduces propagated risk by roughly 10% across each dependency, creating a compounded protective effect for highly connected nodes.

5.5 Synergistic risk amplification: when factors converge

While previous sections examined CDE, LI, and RE separately, real-world systemic risk arises from their combined interaction. To explore this, five simulation scenarios were defined to represent different combinations of parameter levels:

- **Best case:** CDE = 0.3, LI = 0.5× baseline, RE = 90%.
- **Moderate case:** CDE = 0.5, LI = 0.8× baseline, RE = 65%.
- **Actual state:** Empirical parameters from the current LAM infrastructure.
- **High-risk case:** CDE = 0.9, LI = 1.3× baseline, RE = 40%.
- **Worst case:** CDE = 1.0, LI = 1.5× baseline, RE = 25%.

Total risk (R_{total}) was computed for each case using the RIPA propagation equation, with all other parameters held constant. The results, summarised in Table 7, show that when criticality and dependency strength rise together while resilience drops, risk grows non-linearly–a phenomenon referred to as *synergistic amplification*.

In favourable conditions (low CDE, low LI, high RE), total risk remains moderate and stable. However, in high-risk and worst-case scenarios, nodes approach saturation ($R_{\text{total}} \approx 98\%$), demonstrating that simultaneous parameter stress leads to cascading amplification (See Table 8).

Three main insights emerge from the simulations:

1. **"Perfect storm" effect:** The actual LAM configuration lies close to a high-risk state where high criticality, strong coupling, and moderate resilience coexist–conditions that enable cascading failures.
2. **Dominance of resilience:** As shown in Table 7, resilience reduction has the most significant impact on overall systemic exposure, reinforcing its role as the primary moderating factor in the RIPA model.

In summary, effective systemic risk reduction requires simultaneous action: improving resilience above 85%, managing criticality concentration, and optimising dependency strength. Focusing on any single parameter yields limited benefit once the system approaches saturation. As summarised in Table 9, simultaneous increases in criticality and dependency strength–combined with reduced resilience–drive all nodes toward full saturation ($R_{\text{total}} \approx 98\%$), illustrating the synergistic amplification effect.

5.6 Pathway-based risk prioritisation: From node-centric to cascade-aware defence

This section demonstrates that focusing solely on individual node risks—as in traditional assessment approaches — fails to capture the critical vulnerabilities that emerge from interdependencies within the infrastructure network. The RIPA algorithm addresses this limitation by ranking and prioritising entire propagation pathways using the PIS formula. RIPA quantifies the cumulative multi-hop risk transmitted through interconnected nodes, enabling identification of the most critical propagation routes rather than only the most vulnerable nodes.

Three interdependent subsystems were analysed, comprising 21 nodes and 33 dependencies. Risk propagation was simulated over five iterations with a decay factor of 0.85, passing all validation checks. Table 10 summarises the key statistics.

Nodes N1, N2, and N9 exhibited the highest compounded risks (R_{total} = 91.79%, 65.30%, and 84.76%, respectively), confirming their central roles in risk transmission and accumulation. Based on these node-level results, RIPA ranked 20 major propagation pathways into three priority tiers: High (PIS $\geq$ 83.62%), Medium (36.47% $\leq$ PIS $<$ 83.62%), and Low (PIS $<$ 36.47%).

The highest-risk cascade, $N7 \rightarrow N2 \rightarrow N1 \rightarrow N9$ (PIS = 100%), represents a four-hop vulnerability chain in which risk compounds through intermediate nodes. Subsequent high-priority pathways such as $N7 \rightarrow N1 \rightarrow N9$ (PIS = 98.89%) and $N18 \rightarrow N1 \rightarrow N9$ (PIS = 98.70%) confirm that multi-hop cascades dominate systemic exposure. Among the top 20 cascades, 19 (95%) involve three or more hops with an average length of 3.7, showing that long-range propagation is prevalent in the actual infrastructure.

Pathway frequency analysis revealed hidden systemic importance: N9 appeared in 19 (95%) of the top path-

Table 9 Combined factor scenarios showing total risk (%) under multi-parameter interaction (model-based estimates).

Scenario	CDE	LI (× baseline)	RE (%)	N1	N2	N9
Best Case	0.30	0.5	90	83.5	59.7	82.8
Moderate Case	0.50	0.8	65	93.6	88.9	90.2
Actual State	0.85–0.97	1.0	68–87	98.7	97.9	98.3
High-Risk Case	0.90	1.3	40	99.2	99.1	99.0
Worst Case	1.00	1.5	25	99.5	99.3	99.4

Table 10 Summary of node-level risk propagation results.

Metric	Description	Mean (%)	Max (%)
R_0	initial risk	64.21	82.53
R_{pro}	Propagated risk	1.55	12.11
R_{total}	Total risk	65.76	91.79
Increase	Growth due to propagation	2.27	17.27

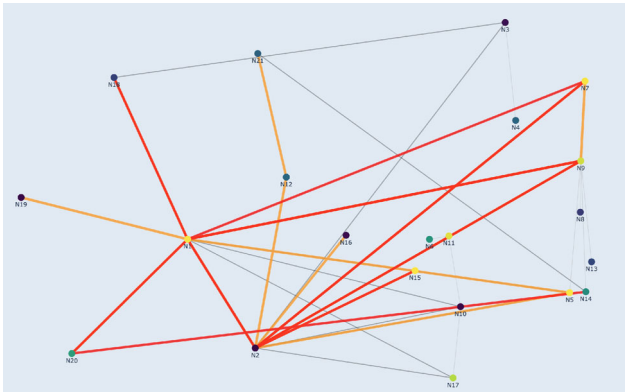

Fig. 8 Interdependency network showing multi-hop propagation intensity. Thicker red edges represent higher PIS

ways, N1 in 17 (85%), and N2 in 14 (70%). These nodes form a vulnerability axis (N1–N2–N9) concentrating most interdependence-driven risk. N1 (criticality = 0.90, resilience = 72%) acts as a risk amplifier linking multiple subsystems, while N2 (criticality = 0.85, resilience = 68%) functions as both relay and terminal node, prone to receiving and propagating cascading failures. Focusing mitigation on high-PIS cascades and reinforcing or isolating the N1–N2–N9 axis would yield the greatest reduction in systemic risk and significantly enhance overall infrastructure resilience.

Figure 8 illustrates the interdependency network with edge colours representing pathway impact intensity, where thicker red lines denote higher PIS values and stronger risk propagation links. Figure 5 presents the ranked pathways by risk degree, categorised into high, medium, and low priority tiers according to their computed PIS scores.

5.7 Mitigation strategy comparison: R0 vs. RIPA

Comparing conventional R0-based prioritisation with RIPA-based prioritisation revealed significant differences. R0-based strategies often wasted resources by hardening nodes that appeared risky in isolation but were systemically unimportant. In contrast, RIPA-based strategies targeted systemic hot spots and high-risk pathways. Quantitatively, RIPA-guided interventions reduced systemic risk by 78% more than R0-guided interventions, demonstrating their superior effectiveness.

In this comparison, the mitigation strategies were evaluated in a simulation setting rather than as real-world projects. The R_0-based strategy prioritised hardening nodes with the highest initial risk R_0, whereas the RIPA-based strategy prioritised hardening systemic hot spots, i.e. nodes with high R_{total} and nodes on high-PIS pathways. Hardening was modelled as an increase in node resilience applied to the same number of nodes and with the same magnitude of change in both strategies, representing an equivalent mitigation effort. The reported 78% improvement therefore reflects a relative gain in total systemic risk reduction under equal effort. Monetary cost and implementation time for specific interventions were not modelled explicitly in this study and are left for future work that couples RIPA with economic and scheduling constraints.

Key Insights and Discussion The findings validate three core principles of the RIPA framework:

1.R0 is insufficient for interconnected systems; systemic risk is better represented by Rtotal.

2. Propagation dynamics are governed jointly by linkage intensity, resilience, and criticality.

3. Systemic analysis provides better prioritisation for mitigation than static, asset-level rankings.

Highest-Risk Cascade: N7 → N2 → N1 → N9 (PIS= 100.00%) represents the most dangerous vulnerability chain in the infrastructure. This 4-hop cascade demonstrates how risk compounds through multiple intermediate nodes:

N7 (LAMScreen™, R_0=82.37%) initiates with high initial risk N2 (LAMis™, criticality=0.85) amplifies through the central position N1 (LAMFlow™, criticality=0.90) further amplifies as the primary controller N9 (Real-time Data Hub) receives compounded risk

Node-centric analysis would identify each node individually as high-risk. Pathway analysis reveals they form a vulnerability chain where compromise at any point enables a cascade to the terminus. This distinction is critical for defence: blocking one intermediate connection disrupts the entire 100% PIS cascade. Critical Node Discovery Through Pathway Frequency: Node appearance analysis across the top 20 pathways reveals:

N9: 19 appearances (95%) - Primary convergence point N1: 17 appearances (85%) - Critical relay hub N2: 14 appearances (70%) - Secondary amplification node

These frequencies indicate systemic importance invisible to node-level metrics. A node appearing in 95% of critical pathways is functionally more important than a node with higher R_0 but lower pathway involvement.

5.8 Cross-domain applicability: Retrospective incident mapping

While our detailed case study focuses on a single critical infrastructure domain, the RIPA framework is designed to be applicable across heterogeneous sectors. To illustrate this generalisability and demonstrate how RIPA could support both prediction and mitigation, we retrospectively map three well-known cyber–physical incidents onto RIPA constructs (nodes, interdependencies, initial risk, propagated risk, and pathway-based analysis).

NotPetya-related disruptions. The 2017 NotPetya malware outbreak originated from the compromise of a widely used software update mechanism and rapidly propagated across corporate networks, impacting multiple sectors including shipping, logistics, manufacturing and energy [41, 42]. In RIPA terms, the M.E.Doc update server can be modelled as a node with high initial risk (R_0) due to the compromised update mechanism, and strong outward dependencies with high linkage intensity (LI) to thousands of client organizations across sectors. Downstream nodes such as Maersk's IT infrastructure would likely exhibit significantly elevated total risk (R_{total}) compared to their initial risk (R_0) due to: (i) multiple incoming dependencies from Ukrainian suppliers and partners, (ii) high criticality (CDE) as a global shipping coordination hub, and (iii) the strength of integration linkages. RIPA's pathway enumeration would identify multi-hop cascades from the update server through intermediate networks to globally distributed operations as high-priority pathways based on Pathway Impact Scores (PIS). This systemic hot spot identification — nodes where R_{total} significantly exceeds R_0 due to network position—would have supported targeted mitigations such as hardening the update mechanism (reducing source R_0), implementing network segmentation (reducing LI between sectors), or enhancing organizational resilience through backup systems and recovery procedures.

Colonial Pipeline incident. The 2021 Colonial Pipeline ransomware incident forced a major fuel pipeline operator in the United States to temporarily suspend operations, leading to fuel shortages and knock-on impacts across transport and services [43, 44]. Within RIPA, the pipeline operator's IT infrastructure (particularly billing and dispatch systems) can be modelled as nodes with dependencies on access control mechanisms (VPN gateways with potentially weak authentication) and strong operational dependencies on downstream control and distribution systems. The dispatch/scheduling systems would likely exhibit high total risk (R_{total}) despite potentially moderate baseline vulnerabilities (R_0), due to: (i) their extremely high criticality (CDE) for pipeline operational decisions, (ii) strong linkage intensity (LI) to operational technology and physical distribution networks, and (iii) limited operational independence (lower resilience, RE). RIPA's pathway analysis would identify cascades from access control systems through dispatch to pipeline operations as high-risk propagation routes (high PIS). A pre-incident RIPA assessment would have revealed these systems as systemic hot spots and recommended: (i) hardening access control mechanisms (increasing RE through multi-factor authentication), (ii) reducing operational dependency through offline operational playbooks and procedures (reducing LI), and (iii) implementing redundant systems with greater operational independence—interventions that align with post-incident expert recommendations.

Ukraine power outages. Cyber attacks on Ukrainian power distribution networks (in 2015 and 2016) targeted control centres and substations, causing intentional load shedding and extended outages for customers [45]. In a RIPA model, the VPN gateways and remote access systems connecting corporate networks to SCADA infrastructure would be identified as critical convergence points—nodes where multiple IT dependencies concentrate before entering high-criticality operational systems. Such nodes would likely exhibit elevated R_{total} relative to R_0 due to: (i) their position as single points of convergence for IT→OT access (high incoming propagated risk, R_{pro}), (ii) strong dependencies to downstream SCADA and substation control systems (high outgoing LI), (iii) high criticality of dependent control systems (CDE), and (iv) potentially insufficient protective measures (lower RE due to inadequate authentication and monitoring). RIPA's pathway enumeration would identify multi-hop cascades from email systems through corporate networks, remote access gateways, SCADA systems, to physical substations as high-priority risk pathways (high PIS). The framework's resilience analysis would highlight how strengthening authentication and access controls (increasing RE at convergence points) and implementing network segmentation (reducing LI between IT and OT domains) would substantially

reduce propagated risk along these critical pathways. These interventions—network segmentation, multi-factor authentication, and enhanced monitoring—align precisely with the post-incident improvements implemented by Ukrainian operators, validating RIPA's capacity to identify effective mitigation strategies.

These retrospective mappings demonstrate that RIPA's core constructs—distinguishing between initial risk (R_0) and total systemic risk (R_{total}), modelling propagated risk (R_{pro}) through dependencies with explicit linkage intensity (LI), incorporating resilience (RE) as a risk shield and criticality (CDE) as a risk amplifier, and prioritizing pathways through Pathway Impact Scores (PIS)—can be instantiated across different critical infrastructure domains and incident types. The mappings illustrate how, if deployed proactively, RIPA would have: (i) identified systemic hot spots where network position amplifies risk beyond baseline vulnerabilities, (ii) prioritized actual attack pathways through pathway-based analysis, and (iii) recommended targeted mitigations that align with post-incident expert assessments. A comprehensive, data-driven quantification of these historical incidents with full parameter assignment is beyond the scope of this article, but multi-domain validation with detailed parameterization represents important future work.

5.9 Generalisability and limitations

Although demonstrated on the LAMAD-LLC system and conceptually mapped to historical incidents across multiple domains, the RIPA framework is broadly applicable to other critical infrastructures such as smart grids, healthcare systems, financial networks, transport infrastructures, and SCADA environments. However, several important limitations must be acknowledged.

The current RIPA framework has three main limitations. First, it does not explicitly model human and organisational factors, such as operator behaviour, decision-making or procedural compliance; these aspects are only reflected indirectly, if at all. Second, several key parameters in the model, including node criticality, linkage intensity and resilience scores, are partly based on expert judgement and simplified scoring schemes, and are therefore inherently subjective. Third, the tests reported in this study are static and scenario-based, and do not represent a fully dynamic or real-time implementation of RIPA.

These limitations do not invalidate RIPA's contributions but rather define its current scope as a technical risk assessment framework focused on structural interdependencies and cyber vulnerabilities. The framework provides significant advances over conventional approaches by explicitly quantifying systemic risk propagation, revealing hidden systemic hot spots invisible to asset-centric assessments, and enabling pathway-based prioritization. Future work should address the identified limitations through dynamic extensions (temporal modeling), socio-technical integration (human factors), parameter refinement (empirical benchmarks and automated estimation), and multi-domain validation across diverse infrastructure types and scales.

6 Recommendations for infrastructure operators

Based on the RIPA analysis of interdependent critical infrastructure, we provide evidence-based recommendations for systemic risk management.

Traditional vulnerability assessments that evaluate nodes in isolation systematically underestimate systemic exposure. Infrastructure analysis reveals that operational endpoints can experience significant risk amplification despite moderate baseline vulnerabilities when they accumulate risk from multiple upstream dependencies through high-risk propagation pathways. Organisations should therefore implement RIPA's pathway-centric analysis to identify nodes whose true risk emerges from network position rather than intrinsic vulnerabilities, prioritising mitigation for nodes with high R_{total}/R_0 ratios, as these represent systemic hot spots invisible to conventional assessments.

Hub nodes with high in-degree connectivity become systemic bottlenecks regardless of their intrinsic security posture. These nodes aggregate risk from multiple upstream sources and serve as critical relays connecting data sources to operational systems. Their compromise can simultaneously disrupt multiple dependent services. Organisations should implement multi-layered defense for hub nodes through: (1) redundancy and fault isolation to prevent single points of failure; (2) circuit breakers that halt cascade propagation when anomalies are detected; (3) micro-segmentation to limit lateral movement; and (4) continuous monitoring of accumulated propagated risk (R_{pro}) with automated alerts when thresholds are exceeded.

Resilience operates as a multiplicative defense factor in the RIPA model. Unlike targeted hardening that addresses specific vulnerabilities, resilience improvements provide universal protection across all incoming risk pathways. High resilience values dramatically reduce the absorption of incoming propagated risk, effectively shielding downstream dependencies. Organisations should strengthen the five resilience dimensions identified in RIPA–preparedness, absorption, responsiveness, recoverability, and adaptability–as foundational defenses before attempting complex architectural restructuring, focusing resilience investments on nodes with high propagated risk and high out-degree.

Finally, static periodic assessments cannot capture the dynamic nature of cascading risks in interdependent systems. RIPA analysis demonstrates that risk propagates through

multi-hop pathways, requiring iterative computation until convergence. Infrastructure operators should transition from periodic vulnerability scans to continuous monitoring of RIPA's three core parameters–Criticality , Linkage Intensity, and Resilience. Automated alerts should be established when critical nodes exhibit dangerous conditions such as significant amplification ($R_{total} \gg R_0$) or when hub nodes show degraded resilience combined with high incoming risk, enabling proactive intervention before cascading failures materialise.

7 Conclusion

This paper introduced the RIPA framework to address critical limitations in systemic risk assessment for interdependent CI, directly answering four research questions:

RIPA quantifies cascading effects (**RQ1**) through a formula-based propagation model, explicitly capturing both probability and intensity of risk transmission. Application to the LAMAD-LLC infrastructure demonstrated substantial risk amplification (**RQ2**), with critical operational endpoints exhibiting risk levels significantly exceeding their baseline vulnerabilities due to cascading dependencies, confirming that traditional isolation - based assessments systematically underestimate systemic exposure.

The analysis identified three dominant mechanisms (**RQ3**): (1) Criticality acts as a "risk magnet" driving rapid saturation in highly connected nodes; (2) Network topology creates position-dependent vulnerability, with hub nodes accumulating disproportionate risk; and (3) Resilience operates as a multiplicative defense factor providing universal protection. For mitigation optimisation (**RQ4**), RIPA's Pathway Impact Score metric enables cascade-aware intervention by identifying high-risk multi-hop propagation routes, revealing that hardening hub nodes and decoupling critical dependencies disrupts multiple cascading pathways simultaneously.

The main contributions are: (1) **Theoretical**–a formula-based propagation model integrating Linkage Intensity, Resilience, and Criticality as dynamic factors; (2) **Methodological**–a pathway-centric BFS algorithm with PIS metric; (3) **Empirical**–validation demonstrating topology-driven risk amplification; and (4) **Practical**–a topology-aware framework enabling systemic exposure-based prioritisation.

RIPA represents a paradigm shift from component-centric vulnerability assessment to system-centric resilience optimisation, reflecting that in interdependent infrastructures, the whole is demonstrably more vulnerable than the sum of its parts. As critical infrastructures grow increasingly interconnected, frameworks that capture conditional, multi-factor propagation dynamics are essential for enabling proactive, topology-aware defensive strategies.

Appendix A: RIPA core algorithm implementation

This appendix provides the Python implementation of the core RIPA risk propagation algorithm, which demonstrates the computational realization of Equation (4) presented in Section 3.3. The function iteratively propagates risk through the dependency network by calculating propagated risk (R_{pro}) for each edge and accumulating total systemic risk (R_{total}) at each node.

The algorithm assumes that each node in the graph has been initialized with the following attributes: R_0 (initial risk, stored as `r0_raw` on a 0–1 scale), resilience score (`resilience_score` as percentage 0–100), and normalized criticality (`criticality` on a 0–1 scale). Each directed edge (u, v) has a pre-calculated linkage intensity (`LIij_raw` on a 0–1 scale). The total risk `Rtotal_raw` is initialized to `r0_raw` before the first iteration.

```
def calculate_full_risk_propagation(graph,
    num_propagation_steps=5):
    for step in range(num_propagation_steps):
        # Reset Rpro for this iteration
        for node in graph.nodes():
            graph.nodes[node]["
                Rpro_received_raw"] = 0.0

        # Snapshot current total risk as source
            for this iteration
        risk_source_map = {n: graph.nodes[n]["
            Rtotal_raw"]
                           for n in graph.nodes
                               ()}

        # Propagate risk along each edge
        for u, v, d in graph.edges(data=True):
            if "LIij_raw" in d:
                # Extract parameters (
                    normalized to 0-1 scale)
                re_ie_raw = graph.nodes[u]["
                    resilience_score"] / 100.0
                re_de_raw = graph.nodes[v]["
                    resilience_score"] / 100.0
                criticality_raw = graph.nodes[v
                    ]["criticality"]
                liij_raw = d["LIij_raw"]
                risk_source_raw =
                    risk_source_map[u]  #
                    already 0-1

                # Apply Equation (4)
                vulnerability_multiplier = (1 -
                     re_ie_raw) * (1 -
                    re_de_raw)
                rpro_raw = (risk_source_raw *
                    vulnerability_multiplier
                            * liij_raw *
                                criticality_raw)
                graph.nodes[v]["
                    Rpro_received_raw"] +=
                    rpro_raw

        # Update total risk: Rtotal = R0 + sum(
            Rpro)
        for node in graph.nodes():
            graph.nodes[node]["Rtotal_raw"] = (
                graph.nodes[node]["r0_raw"]
                + graph.nodes[node]["
                    Rpro_received_raw"]
            )

    # Convert to percentage for reporting
```

```
    for node in graph.nodes():
        graph.nodes[node]["Rtotal"] = round(
            graph.nodes[node]["Rtotal_raw"] *
                100, 2)
```

Listing 1 Core RIPA Propagation Function

The implementation uses NetworkX for graph representation. All risk values are maintained in raw form (0–1 scale) during iterative computation and converted to percentages (0–100) for final reporting. The pathway scoring and ranking algorithms follow similar principles, applying the propagation formula along multi-hop paths and using percentile-based classification as described in Section 3.4. The complete RIPA toolkit is being developed as a commercial product and is therefore not publicly released.

Author Contributions F.F. conducted the primary research and analysis under the supervision and guidance of H.M. (Haralambos Mouratidis). F.F. was responsible for developing the conceptual framework, designing the methodology, performing data analysis, and drafting the initial version of the manuscript. H.M. supervised the overall research design, provided academic guidance, and contributed to the refinement of the study's structure, argumentation, and interpretation of results. He also critically reviewed and edited the manuscript to ensure scientific accuracy and alignment with the study's objectives. A.A.Z. (Abdullah Al Zakwani) contributed to the research by providing essential data and contextual information relevant to the study. He verified the accuracy and consistency of the data and reviewed the sections of the manuscript associated with empirical findings and real-world applications. All authors discussed the results, contributed to the final interpretation, and approved the final version of the manuscript.

Funding The authors did not receive support from any organization for the submitted work.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing Interests The authors declare no competing interests.

References

1. Curt, C., Tacnet, J.: Resilience of critical infrastructures: Review and analysis of current approaches. Risk Anal. **38**(11), 2441 (2018)
2. Cybersecurity, C. I.: Framework for improving critical infrastructure cybersecurity, **4162018**(7) (2018). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP
3. Mouratidis, H., Santos-Olmo, A., Islam, S., Grosado, D., Fern, E.: Towards Resilience by Design: Systematic Review of Critical Infrastructure Protection Against Systemic Risks, Komunikácie **20**(2) (2025)
4. Mouratidis, H., Santos-Olmo, A., Islam, S., Grosado, D., Fern, E.: Towards Resilience by Design: Systematic Review of Critical Infrastructure Protection Against Systemic Risks. Springer, Vienna (2025)
5. Haggag, M., Ezzeldin, M., El-Dakhakhni, W., Hassini, E.: Resilient cities critical infrastructure interdependence: a meta-research. Sustain. Resilient Infrastruct. **7**(4), 291 (2022)
6. Faraji, F., Javadpour, A., Sangaiah, A.K., Zavieh, H.: A solution for resource allocation through complex systems in fog computing for the internet of things. Computing **106**(7), 2107 (2024)
7. Welburn, J.W., Strong, A.M.: Systemic cyber risk and aggregate impacts. Risk Anal. **42**(8), 1606 (2022)
8. Curran, D.: Connecting risk: Systemic risk from finance to the digital. Econ. Soc. **49**(2), 239 (2020)
9. Liu, X., Ferrario, E., Zio, E.: Resilience analysis framework for interconnected critical infrastructures. ASCE-ASME J. Risk Uncertain. Eng. Syst. B: Mech. Eng. **3**(2), 021001 (2017)
10. Iturriza, M., Labaka, L., Sarriegi, J.M., Hernantes, J.: Modelling methodologies for analysing critical infrastructures. J. Simul. **12**(2), 128 (2018)
11. Grafenauer, T., König, S., Rass, S., Schauer, S.: In: Proceedings of the 13th International Conference on availability, reliability and security, pp. 1–8 (2021)
12. Gueye, A., Mbaye, B., Fall, D., Diop, A., Kashihara, S.: Innovations and Interdisciplinary Solutions for Underserved Areas: 4th EAI International Conference, InterSol 2020, Nairobi, Kenya, March 8-9, 2020, Proceedings 4 (Springer, 2021), pp. 211–223
13. Gong, S., Ye, Y., Gao, X., Chen, L., Wang, T.: Empirical patterns of interdependencies among critical infrastructures in cascading disasters: Evidence from a comprehensive multi-case analysis. Int. J. Disaster Risk Reduct. **95**, 103862 (2023)
14. Zuccaro, G., De Gregorio, D., Leone, M.F.: Theoretical model for cascading effects analyses. Int. J. Disaster Risk Reduct. **30**, 199 (2018)
15. Wang, W., Yang, S., Hu, F., Stanley, H.E., He, S., Shi, M.: An approach for cascading effects within critical infrastructure systems. Physica A **510**, 164 (2018)
16. Rehak, D., Senovsky, P., Hromada, M., Lovecek, T., Novotny, P.: Cascading impact assessment in a critical infrastructure system. Int. J. Crit. Infrastruct. Prot. **22**, 125 (2018)
17. Helminen, A., Hakkarainen, T.: Book of Abstracts, p. 10 (2021)
18. Brabcova, V., Slivkova, S., Rehak, D., Toseroni, F., Havko, J.: ASSESSING THE CASCADING EFFECT OF ENERGY AND TRANSPORT CRITICAL INFRASTRUCTURE ELEMENTS: CASE STUDY. Komunikácie **20**(2), (2018)
19. Fu, X., Pace, P., Aloi, G., Guerrieri, A., Li, W., Fortino, G.: Tolerance analysis of cyber-manufacturing systems to cascading failures. ACM Trans. Internet Technol. **23**(4), 1 (2023)
20. Palleti, V.R., Adepu, S., Mishra, V.K., Mathur, A.: Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecurity **4**(1), 8 (2021)
21. Chaoqi, F., Yangjun, G., Jilong, Z., Yun, S., Pengtao, Z., Tao, W.: Attack-defense game for critical infrastructure considering the cascade effect. Reliab. Eng. Syst. Saf. **216**, 107958 (2021)
22. Islam, S., Basheer, N., Papastergiou, S., Ciampi, M., Silvestri, S.: Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. J. Reliab. Intell. Environ. **11**(3), 12 (2025)

23. I.O.f. Standardization, *ISO 31000: 2018, Risk Management-Guidelines* (International Organization for Standardization, 2018)
24. Barraza de la Paz, J.V., Rodríguez-Picón, L.A., Morales-Rocha, V., Torres-Argüelles, S.V.: A systematic review of risk management methodologies for complex organizations in industry 4.0 and 5.0. Systems **11**(5), 218 (2023)
25. Mahfud, A.Z., Hikmah, I.R., Sunaringtyas, S.U., Yulita, T.: In: 2024 4th International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS), pp. 181–186, IEEE (2024)
26. Barraza de la Paz, J.V., Rodríguez-Picón, L.A., Morales-Rocha, V., Torres-Argüelles, S.V.: A systematic review of risk management methodologies for complex organizations in industry 4.0 and 5.0. Systems **11**(5), 218 (2023)
27. Mahfud, A.Z., Hikmah, I.R., Sunaringtyas, S.U., Yulita, T.: In: 2024 4th International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS), pp. 181–186, IEEE (2024)
28. Kure, H.I., Islam, S., Mouratidis, H.: An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Comput. Appl. **34**(18), 15241 (2022)
29. Iso, I.: Risk management–Principles and guidelines, International Organization for Standardization, Geneva, Switzerland (2009)
30. Hempel, L., Kraff, B.D., Pelzer, R.: Dynamic interdependencies: problematising criticality assessment in the light of cascading effects. Int. J. Disaster Risk Reduct. **30**, 257 (2018)
31. Pescaroli, G., Nones, M., Galbusera, L., Alexander, D.: Understanding and mitigating cascading crises in the global interconnected system (2018)
32. Heino, O., Takala, A., Jukarainen, P., Kalalahti, J., Kekki, T., Verho, P.: Critical infrastructures: The operational environment in cases of severe disruption. Sustainability **11**(3), 838 (2019)
33. Faraji, F., Javadpour, A., Sangaiah, A.K., Zavieh, H.: A solution for resource allocation through complex systems in fog computing for the internet of things. Computing **106**(7), 2107 (2024)
34. Cheikes, B.A., Waltermire, D., Scarfone, K.: Common platform enumeration: Naming specification version 2.3. NIST Interagency Report **7695**(8), (2011)
35. Martin, B.: Common vulnerabilities enumeration (cve), common weakness enumeration (cwe), and common quality enumeration (cqe) attempting to systematically catalog the safety and security challenges for modern, networked, software-intensive systems. ACM SIGAda Ada Lett. **38**(2), 9 (2019)
36. Vulnerabilities, C.: Common vulnerabilities and exposures, Published CVE Records.[Online] Available: https://www.cve.org/About/Metrics (2005)
37. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: Critical Infrastructure Protection III: Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers 3 (Springer, 2018), pp. 35–49
38. Yan, J., Du, Z., Li, J., Yang, S., Li, J., Li, J.: A Threat Intelligence Analysis Method Based on Feature Weighting and BERT-BiGRU for Industrial Internet of Things. Sec. Commun. Netw. **2022**(1), 7729456 (2022)
39. Weir, A.M., Wilson, T.M., Bebbington, M.S., Campbell-Smart, C., Williams, J.H., Fairclough, R.: Quantifying systemic vulnerability of interdependent critical infrastructure networks: A case study for volcanic hazards. Int. J. Disaster Risk Reduct. **114**, 104997 (2024)
40. Cui, Z., Pang, J., Shen, X.: IOP Conference Series: Materials Science and Engineering, vol. 231, p. 012040, (IOP Publishing, 2005)
41. Wan, K.S.: NotPetya, not warfare: rethinking the insurance war exclusion in the context of international cyberattacks. Wash. L. Rev. **95**, 1595 (2020)
42. Crosignani, M., Macchiavelli, M., Silva, A.F.: Pirates without borders: The propagation of cyberattacks through firms' supply chains. J. Financ. Econ. **147**(2), 432 (2023)
43. Easterly, J., Fanning, T.: The attack on colonial pipeline: What we've learned & what we've done over the past two years, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, 7 (2023)
44. Tsvetanov, T., Slaria, S.: The effect of the Colonial Pipeline shutdown on gasoline prices. Econ. Lett. **209**, 110122 (2021)
45. Case, D.U.: Analysis of the cyber attack on the Ukrainian power grid. Electricity information sharing and analysis center (E-ISAC) **388**(1–29), 3 (2016)