International Journal of Technology

http://ijtech.eng.ui.ac.id

Research Article

Synergy-Based Multi-Domain Risk Integration for Critical E-Government Infrastructure: The MuSyRI Framework and Policy Implications

Yuri Chernenko[1,*], **Olena Borodina**[2]

[1] Department of Doctoral Studies, International University of Business and Law

[2] Faculty of Management, Public Administration and Marketing, Kyiv University of Market Relations

*Corresponding author: info@sridd.org; Tel.: +38(067)970–83–69

Abstract: This study aims to develop and validate the MuSyRI early-warning index for critical e-government infrastructure. This study introduces the Multi-Domain Synergistic Resilience Index (MuSyRI), a bounded [0–1] metric that identifies nonlinear, compound risks across operational, financial, regulatory, and cyber domains in critical e-government infrastructure. MuSyRI explicitly integrates domain-specific resilience factors to modulate synergy-driven escalation. A multiple-case study of four anonymised organizations – a housing-services agency, a specialized construction firm, a water-tech startup, and a partially state-owned energy – water utility – validates MuSyRI. ERP-BPMS logs are converted into fuzzy sub-indices and aggregated via a Cascading Amplification Function (CAF) to capture concurrent moderate hazards and offset by a resilience term. Parameters were calibrated using Delphi panels, genetic algorithms, and expert elicitation. MuSyRI detects overlapping medium-level risks 1–4 weeks earlier than standard additive approaches. Early synergy alerts enabled proactive interventions, reducing housing-service disruptions by 8%–12% and boosting pilot adoption in the water-tech case by 12%–15%. Resilience offset curtails overestimation and preserves policymakers' and managers' interpretability. Unlike linear or unbounded fuzzy methods, MuSyRI formally integrates a nonlinear synergy function with domain-specific resilience into one bounded index. Consequently, it offers an actionable early warning framework for multi-domain oversight, resource prioritization, and digital governance reforms in e-government ecosystems.

Keywords: Critical infrastructure; E-government; Multi-domain risk; MuSyRI; Synergy-based index

1. Introduction

Public services and critical infrastructure increasingly confront risks that span the operational, financial, regulatory, and cyber domains. These risks require a structured management approach across the entire project lifecycle (Beckers and Stegemann, 2013; National Institute of Standards and Technology, 2020; OECD, 2019). Moderate stress in one domain can align with latent vulnerabilities elsewhere, triggering compounding threats before any single indicator signals a danger (National Institute of Standards and Technology, 2020; OECD, 2019). Governance structures generally divide these domains into separate teams, each focusing on isolated metrics that overlook how moderate disruptions can escalate when they converge (Lin and Pan, 2022). Critical e-government platforms must sustain 24/7 citizen services under simultaneous operational, financial, regulatory, and cyber pressures; siloed governance often masks these compound threats. This siloed approach is particularly problematic for cyber risks, which can cascade across all operational domains in critical infrastructure systems (Kelic, 2019). Even sophisticated ERP-BPMS environments that centralize data flows typically lack dedicated analytics to flag synergy effects, leaving concurrent anomalies undetected until the situation becomes urgent (Gopalakrishnan and Sankaranarayanan, 2023). Recent incidents, including large-scale pan-

https://doi.org/10.14716/ijtech.v16i6.7815
Received May 2025; Revised June 2025; Accepted August 2025

demic disruptions and climate-related shocks, highlight the limitations of fragmented oversight in managing multi-factor risks (Boni et al., 2025; Hochrainer-Stigler et al., 2023).

1.1 Context and Rationale

Risk management often remains compartmentalized in separate operational, financial, regulatory or cyber units. Each unit tracks distinct indicators and intervenes within its domain without recognizing how moderate issues in one area can amplify hazards in others (Larsson and Große, 2023). Bentahar and Rifai, 2022 proposed a theoretical framework that distinguishes strategic, operational, and compliance-based risks in the public sector, arguing that these domains require distinct governance approaches while maintaining cross-domain visibility. Woods, 2022 further emphasized that public sector risk management must simultaneously balance service continuity, political accountability, and resource constraints. Their work emphasizes the unique accountability demands that public agencies face when monitoring overlapping threats. Moreover, oversight bodies rely on silo-based dashboards, which cannot capture nonlinear amplification across domains (OECD, 2019). Although digital innovations have enhanced data consolidation, most existing frameworks still additively sum domain hazards, missing the escalations that arise from concurrency (Menoni et al., 2024). Policy specialists increasingly emphasize the need for models that highlight cross-domain synergies before multiple thresholds are breached (Moussa et al., 2024; Schlosser et al., 2023). A unified index that detects compounding hazards early can improve how governments allocate contingency budgets, set regulatory triggers, and orchestrate coordinated responses.

1.2 Focused Literature Review

Prior multi-domain risk studies introduced multi-criteria or partial-fuzzy aggregation but relied on linear assumptions that obscured the non-linear nature of compound events (Akbari Ahmadabadi and Heravi, 2019). Although integrated risk management approaches have attempted to address these limitations, they often lack specific mechanisms for detecting nonlinear interactions (Dudauri, 2022). Bayesian or fuzzy-logic approaches recognize interdependence but often produce unbounded or opaque outputs that are unsuitable for public dashboards (Cai et al., 2017; Labaka et al., 2016). These approaches frequently overlook the critical governance and vulnerability factors that shape risk outcomes in practice. More recent work has used machine learning to predict cross-domain anomalies (Moussa et al., 2024); however, explicit resilience offsets that dampen synergy effects rarely appear (Lin and Pan, 2022). Scholars of digital transformation have noted that ERP-BPMS platforms can collect operational, financial, regulatory, and cyber logs in a single repository (National Institute for Strategic Studies (NISS), 2021). Despite this, synergy-based metrics remain scarce, preventing policymakers from seeing how moderate warnings in the two domains might multiply rather than simply add (Gopalakrishnan and Sankaranarayanan, 2023; Mahama et al., 2022). Few studies have modeled domain-specific resilience as a formal offset within a single bounded measure (Boni et al., 2025), and disaster risk research sometimes incorporates multi-hazard perspectives (Hochrainer-Stigler et al., 2023), including emerging frameworks for disaster risk management pathways (Ward, 2022). This absence leaves agencies lacking a straightforward approach to encode synergy in their licensing, auditing, or resource allocation processes (Božović et al., 2020).

1.3 Research gap and novelty

A persistent gap remains: a holistic, multi-factor risk integration tool that detects nonlinear interactions while offsetting them through domain-specific resilience factors, all within an interpretable [0,1] scale, is lacking (OECD, 2019). Existing models often treat hazards in isolation or combine them linearly, overlooking how small indicators can escalate into severe disruptions when they overlap (Lin and Pan, 2022). Petit et al., 2018 proposed an integrated framework for critical infrastructure protection that explicitly addressed cross-sector interde-

pendencies and cascading effects. Their work demonstrates how protection strategies focused on single infrastructure sectors often miss crucial vulnerabilities that emerge at intersectoral boundaries. Scholars argue that synergy-based metrics can capture moderate simultaneous signals early and show how robust mitigation curbs potential escalation (Menoni et al., 2024). To fill this gap, this study introduces the Multi-Domain Synergistic Resilience Index (MuSyRI). MuSyRI consolidates data from the operational, financial, regulatory, and cyber domains, applies a cascading amplification function to capture concurrency, and moderates the result with a resilience factor (Gopalakrishnan and Sankaranarayanan, 2023). The framework's emphasis on integrating multiple resilience dimensions—including robustness, resourcefulness, redundancy, and rapidity—aligns with contemporary approaches to resilience index development in critical infrastructure (Sambowo and Hidayatno, 2021). It differs from conventional additive or fuzzy models in that it formally models synergy and resilience in one metric.

1.4 Research questions and contributions

The four anonymised pilots, offering a rigorous cross-jurisdiction test, span a post-Soviet housing utility (Case A), an EU construction integrator (B), a US water-tech start-up (C) and a Middle East state-owned utility (D). This study develops and validates the Multi-Domain Synergistic Resilience Index (MuSyRI) and asks the following questions: RQ1 – How can multi-domain risks be fused into a single non-linear, resilience-aware metric?; RQ2 – What governance insights emerge when the metric is deployed in critical e-government settings? The theoretical contribution is a nonlinear framework, MuSyRI, which highlights cross-domain escalation and integrates resilience offsets. The practical contribution involves pilot applications demonstrating how synergy-based detection can strengthen oversight, licensing, and emergency planning in critical service sectors (Moussa et al., 2024).

1.5 Roadmap

Section 2 details the MuSyRI framework and explains the multiple-case study design. Section 3 compares synergy-based risk signals to simpler additive baselines to illustrate how early detection windows shift when concurrency is recognized. Section 4 links these findings to risk governance theory and digital transformation agendas and proposes policy applications that leverage synergy metrics to allocate resources and set compliance thresholds. Section 5 outlines the key contributions, acknowledges the calibration and data limitations, and proposes avenues for future research.

2. Methods

This study uses a multiple-case design to develop and validate the Multi-Domain Synergistic Resilience Index (MuSyRI) in four anonymised organizations, hereafter referred to as case companies A, B, C and D. Each company faces overlapping operational, financial, regulatory, and cyber risks, but varies in terms of scale, digital readiness, and public or semi-public oversight. This design enables analytical generalization by examining how a unified risk index captures multi-domain concurrency under contrasting conditions rather than pursuing large-sample representativeness (Yin, 2018). It also aligns with the calls for practice-oriented approaches that reveal the compounding nature of moderate vulnerabilities in real governance contexts (Chang et al., 2023; National Institute for Strategic Studies (NISS), 2021).

2.1 Material (Case Selection and Data Sources)

The investigation adopts theoretical replication logic, where each site tests whether the same synergy-driven risk pattern recurs despite sector, data richness, and policy interactions differences (Menoni et al., 2024; Schlosser et al., 2023). Case company A manages housing and communal services in an urban region using an ERP-BPMS to log daily operations, monthly financial audits, and municipal compliance reports. Case company B delivered specialized construction projects across diverse jurisdictions, tracking project costs, scheduling data, and weather fluctuations. Case company C, a water technology startup, monitors R&D milestones, pilot usage, and licensing processes. Case Company D is a partially state-owned utility that integrates SCADA streams, financial statements, cyber alerts, and state policy directives. Their diversity supports cross-case insights into the manner in which MuSyRI detects non-linear concurrency and offers policy-relevant risk information.

2.2 Methods (MuSyRI Framework)

In [0,1], MuSyRI consolidates four domain-specific sub-indices—operational, financial, regulatory, and cyber—into a single bounded metric in [0,1]. Raw logs, such as downtime records, budget variances, compliance flags, and cyber alerts, are transformed into fuzzy subindices, each denoted RSI_i. For cyber-domain indicators, adaptive approaches that respond to evolving threat landscapes have been considered (Samanis et al., 2022), recognizing that cyber risks in critical infrastructure require dynamic assessment methodologies (Kelic, 2019). Figure 1 illustrates the overall MuSyRI framework, showing the transformation from raw domain data to the integrated risk index through fuzzy membership functions, synergy amplification, and resilience offsetting.

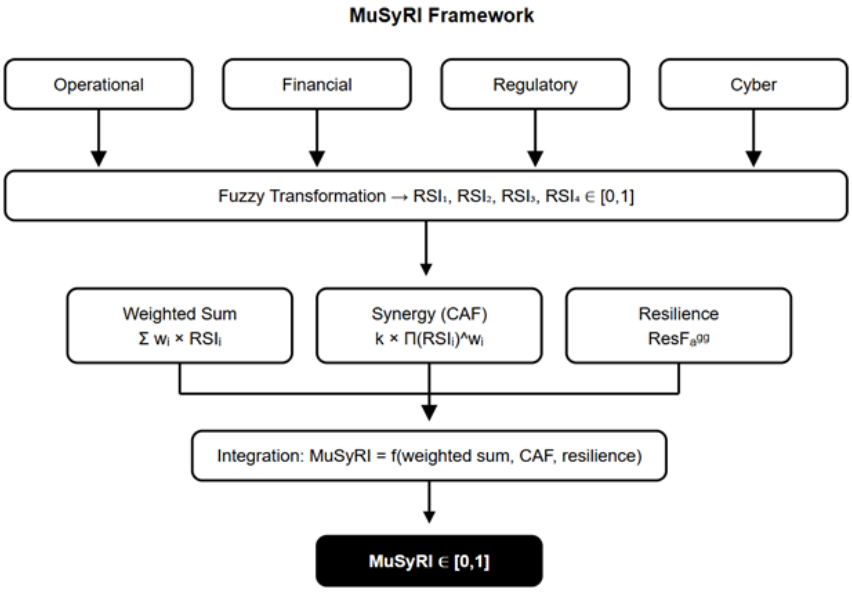

Figure 1 Conceptual framework of the multi-domain synergistic resilience index (MuSyRI)

Note: The diagram illustrates the transformation pathway from domain-specific operational, financial, regulatory, and cyber data sources to a unified risk index. Raw logs undergo fuzzy membership transformation into standardized sub-indices (RSI_i), which are then processed through three parallel components: (1) a linear weighted sum forming the base risk estimate, (2) a CAF capturing non-linear synergy effects when multiple domains experience concurrent stress, and (3) a resilience offset term ($ResF_{agg}$) that moderates the final index based on available mitigation resources. The bounded [0,1] MuSyRI output integrates these components to detect cross-domain risk concurrency while accounting for SR capacity.

These sub-indices reflect low to high risk states, typically defined through membership functions that accommodate uncertain thresholds (Cai et al., 2017; Labaka et al., 2016). A weighted sum (Eq. 1) $\Sigma_{i=1}^{4}\ w_i RSI_i$ forms a base multidomain risk estimate, with $\Sigma_{i=1}^{4}\ w_i$=1.

$$Aggregate\ risk = \sum_{i=1}^{4}\ w_i RSI_i \tag{1}$$

Our approach builds on Theoharidou et al., 2011, who developed one of the earliest methodologies specifically designed to assess interdependent risks across critical infrastructure systems, introducing a tiered approach to identify both direct and cascading effects. Their methodology emphasizes the importance of capturing second-order dependencies that are often undetected in conventional assessments.

The Cascading Amplification Function (Eq. 2) is a key innovation, which models nonlinear escalation when two or more domains simultaneously exceed moderate risk thresholds. To capture this interaction effect, the CAF is defined in the following general form:

$$CAF = k \times \prod_{i=1}^{4}\ (RSI_i)^{W_i} \tag{2}$$

where k is the scaling factor (usually set to one). The parameter $\alpha\epsilon$[0,1] activates synergy when domain concurrency arises, whereas $\eta \geq$1 sets how steeply the overall risk grows under concurrency (Akbari Ahmadabadi and Heravi, 2019; Moussa et al., 2024). The Cascading Amplification Function (Eq. 2) captures nonlinear escalation, whereas Eq. (4) guarantees boundedness [0–1].

MuSyRI embeds resilience by including an aggregated resilience term Resilience offset – $ResF_{agg}$ (Eq. 3). This term is computed as follows to account for the mitigating effect of the available resilience resources on potential risk escalation:

$$ResF_{egg} = \sum_{j=1}^{m}\ \beta_j ResF_j \tag{3}$$

where β_j scales each ResF$_j$ (e.g., contingency funds and backup systems) (Božović et al., 2020). The coefficient $y\epsilon$[0,1] moderates synergy by pulling the index downward when resilience is high. The complete MuSyRI expression is:

$$MuSyRI = \frac{(\sum_{i=1}^{4} w_i RSI_i) \times [1 + \alpha CAF]^{\eta}}{1 + \alpha + \gamma ResF_{agg}} \tag{4}$$

Boundedness follows because each $RSI_i\epsilon$[0,1], CAFϵ[0,1], Σw_i=1, α, $\gamma\epsilon$[0,1], and $\eta \geq$1. Empirical Monte Carlo checks by sampling random RSI vectors confirm that MuSyRI never exceeds 1 (Chang et al., 2023). This structure highlights how overlapping MLD stresses can amplify total risk, yet resilience resources can offset this escalation (Lin and Pan, 2022). Figure 1 shows the schematic data flow.

2.3 Data collection and analysis

Data were collected over 12–24 months, capturing operational logs, financial or cost records, relevant regulatory data, where available SCADA metrics, or R&D reports (Hochrainer-Stigler et al., 2023). In the case of company A, daily ERP-BPMS logs and monthly audit statements were matched to detect points where equipment downtimes coincided with unexpected budget gaps. The project cost records, scheduling updates, and weather archives of case company B

illustrate the concurrency between moderate schedule slips and cost overruns during adverse conditions. Case company C contributed R&D logs, pilot usage metrics, and local approvals, revealing synergy when regulatory or market constraints aligned moderate development issues. Case Company D integrated SCADA streams, quarterly financial data, cyber alerts, and policy mandates, demonstrating the emergence of risk overlaps at larger scales.

Fuzzy sub-indices were derived from domain fields using expert-defined or data-informed membership thresholds. This approach to fuzzy logic implementation aligns with proven methodologies for resource allocation optimization in emergency response contexts, where multiple criteria must be balanced under uncertainty (Berawi et al., 2019). The parameter calibration followed different procedures for each case. Case companies A and D held Delphi panels (two or three rounds), converging once the interquartile ranges for α, γ, η dropped below an agreed threshold. Case company B deployed a genetic algorithm (population $\sim$50, stopping when fitness improvement fell below 1% over multiple generations) to optimize synergy parameters against known historical cost-weather disruptions (Moussa et al., 2024). Case Company C, with fewer recorded events, relied on structured expert elicitation supplemented by $\pm$10% sensitivity checks. Missing or partial logs were imputed via last-observation-carried-forward, a common approach in weekly level risk assessment (Menoni et al., 2024). Scenario testing introduced synthetic concurrency in two or more domains, confirming that MuSyRI spiked above linear sums and dropped when resilience increased incrementally raised (Božović et al., 2020).

2.4 Methodological rigor and ethical

Researchers minimized bias by triangulating operational, financial, regulatory, and cyber data and then cross-checking synergy results with local experts, who attested that synergy peaks aligned with known multi-domain incidents (Yin, 2018). All logs were anonymized, removing personal details or proprietary tags, and managed through a secure repository that complied with recognized data protection guidelines (Carpignano et al., 2021). Because these records were organizational, aggregated, and lacked human subjects, formal review board approval was not required (Farrington, 2016). Each organization consented to writing to share anonymised data for research. Version-controlled scripts document membership definitions, parameter calibrations and scenario tests, ensuring reproducibility if new evidence arises (Chang et al., 2023).

This method-centric approach establishes an empirical foundation for testing whether synergy-based risk detection fosters earlier interventions in critical service contexts. The systematic approach to risk assessment employed here draws from established methodologies in critical infrastructure sectors, where standardized guidelines have proven essential for comprehensive hazard identification (Hendra et al., 2024). MuSyRI responds to the need for integrated, policy-relevant metrics that illuminate how moderate signals interact across the financial, operational, regulatory, and cyber domains by modeling nonlinear escalation and resilience in a single bounded measure (Lin and Pan, 2022; Schlosser et al., 2023). The next section compares synergy-driven alerts to simpler baselines, revealing how concurrency and resilience factors shape multidomain outcomes in each case.

3. Results

Section 3 answers RQ1 and RQ2 using four anonymised cases.

3.1 Case-Company A (Housing and Communal Services)

Case Company A manages an urban housing and communal services network, recording equipment downtime, budget variances, and regulatory notices in an ERP-BPMS. A two-round Delphi panel (ten experts) established domain weights of 0.40 (operational), 0.35 (financial), and 0.25 (regulatory), with synergy parameters α=0.80 and η=1.25. The baseline additive method rarely exceeded 0.50 for moderate incidents over 24 months.

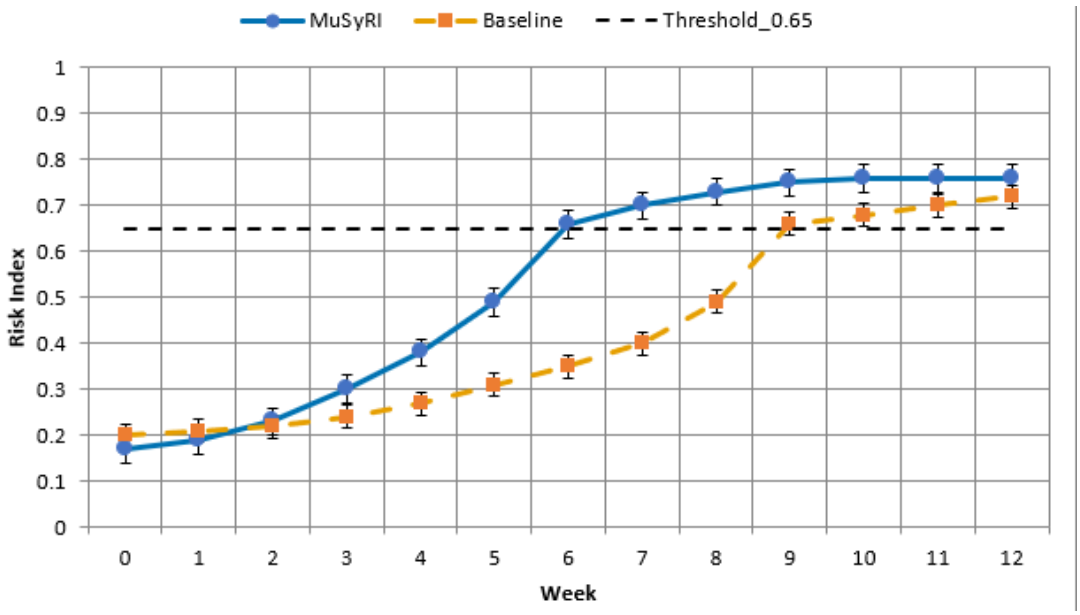

Figure 2 Evolution of risk index for Case-Company A: MuSyRI versus baseline approach

Concurrent operational downtime and a modest budget gap overlapped with a delayed municipal inspection in one event, producing sub-indices of (0.40, 0.35, and 0.30). A simple average remained below 0.50, but the Cascading Amplification Function (CAF) pushed the composite synergy near 0.68. An aggregated resilience term ($ResF_{agg}$≈0.10, including emergency crews and repair funds) then reduced the final MuSyRI to approximately 0.58 when multiplied by γ≈0.80. Management, by comparing ERP-BPMS logs before and after MuSyRI deployment, reported roughly 8%–12% fewer service disruptions and observed synergy alerts arriving around 2–3 weeks earlier than domain-specific dashboards. Figure 2 illustrates this early detection capability, showing how MuSyRI crossed the critical risk threshold of 0.65 at week 6, while the baseline approach reached the same threshold only at week 9, demonstrating the three-week early warning advantage.

3.2 Case-Company B (Specialized Construction)

Case company B undertakes specialized construction projects in multiple regions, tracking scheduling, cost overruns, and external triggers (weather and permits) through distinct modules. A genetic algorithm (population ∼50, converging after ∼40 generations) was used to calibrate the domain weights at 0.45 (schedule), 0.35 (financial), and 0.20 (external), with synergy parameters α≈0.70 and η=1.30.

In a representative case, a project that lagged by approximately 12% in scheduling also faced moderate cost overruns during heavy rainfall, triggering additional permit checks. The baseline additive index remained near 0.48 and the compounding effect was missed. MuSyRI rose to approximately 0.73, and then resilience measures – chiefly contingency funds for reassigning crews – lowered the final index to approximately 0.63, once $ResF_{agg}$≈0.10 was applied with γ≈0.85. This signal appeared two to three weeks earlier than the firm's legacy alert system. Site managers noted fewer scheduling setbacks after the use of synergy-based prompts.

3.3 Case-Company C (Water-Tech Startup)

Case Company C is a small venture focused on hardware for water optimization, facing R&D bottlenecks, market adoption hurdles and municipal policy constraints. Expert-elicited calibration assigned domain weights of 0.40 (R&D), 0.35 (market), and 0.25 (regulatory), with synergy parameters α=0.75 and η=1.35. For moderate issues in each domain, a baseline sum often scored around 0.50 for moderate issues in each domain, yet their combined effect was overlooked.

Over 12 months, a three-week prototype delay merged with slower pilot uptake and pending municipal certification, raising MuSyRI to approximately 0.75 from a baseline of 0.50. A small resilience offset ($ResF_{agg}$≈0.05) reflected limited bridging funds and flexible engineering schedules, resulting in a final MuSyRI of approximately 0.70 once γ≈0.80 was applied. Alerts arrived 1–2 weeks before the quarterly reviews. Managers reassigned engineers to address regulatory gaps and noted a modest upturn in pilot ERP-BPMS tracking metrics.

3.4 Case-Company D (Energy–Water Utility)

Case Company D is a partially state-owned utility that operates water and energy services through integrated SCADA logs, quarterly financial audits, and separate policy or cyber channels. Conventional dashboards typically evaluate these domains separately, leaving moderate overlaps undetected. A three-round Delphi (ten participants) determined domain weights of approximately 0.30 (operations), 0.25 (finance), 0.25 (policy), and 0.20 (cyber), with α≈0.85 and η=1.40.

During an 18-month pilot, minor budget strain (0.30) and compliance lapses (0.35) converged with recurrent cyber alerts (0.40), lifting MuSyRI to approximately 0.74 compared to a baseline below 0.50. This convergence of cyber and operational risks exemplifies Kelic, 2019 critical infrastructure vulnerabilities. A substantial resilience reserve ($ResF_{agg}$≈0.20, comprising cybersecurity, compliance, and operational resources) then curbed the final index to the mid-0.50s once γ≈0.90 was applied. The synergy signals arrived approximately three to four weeks earlier than the monthly or quarterly combined metrics of the utility.

3.5 Cross-Case Synthesis

Table 1 summarizes the key metrics and findings across the four case organizations, providing a comparative overview of the results of the implementation of MuSyRI.

Table 1 Comparative Analysis of MuSyRI Implementation Across Case Organizations

Case	Peak MuSyRI[1]	Baseline	Resilience Offset[1]	Early-warning lead (weeks)	Calibration technique	Observable service gain
A	≈ 0.68	≈ 0.50	≈ 0.10	2 – 3	Delphi (two rounds)	8 – 12 % fewer service disruptions
B	≈ 0.73	≈ 0.48	≈ 0.08 – 0.12	2 – 3	Genetic-algorithm tuning	Noticeably fewer scheduling delays
C	≈ 0.75	≈ 0.50	≈ 0.05	1 – 2	Expert elicitation	12 – 15 % increase in pilot-project uptake
D	≈ 0.74	≈ 0.50	≈ 0.20	3 – 4	Delphi (three rounds)	Averted projected service outages

[1]Note: Data derive from organizational ERP–BPMS logs and expert calibration sessions (2023–2025)

All four pilots showed that MuSyRI detected concurrent, moderate-level risks 1–4 weeks earlier than domain-isolated baselines, with the timing correlated with each site's log update frequency. Table I (summarizes the final version) summarizes peak synergy indices, baseline averages, resilience offsets, and estimated detection leads across all four organizations. The peak MuSyRI values varied from approximately 0.68 to 0.75, confirming that moderate signals can nonlinearly escalate when they overlap (Lin and Pan, 2022; Schlosser et al., 2023). Resilience offsets also diverged, approximating 0.05 for startup (C) and approximately 0.20 for large utility

(D), while companies A and B ranged approximately 0.08–0.12. These differences are consistent with distinct resource buffers ($ResF_{agg}$) and calibrated γ factors (Murasov et al., 2024).

The data's completeness varied between studies. Case company C lacked an extensive history but updated R&D metrics weekly, whereas case company D had detailed SCADA logs but slower policy and finance cycles. Cross-correlation methods that can handle incomplete datasets have been shown to benefit the performance evaluation of resilience indices across different data availability conditions (Jandhana and Agustini, 2024). Fuzzy sub-indices maintained stable risk signals under partial data, consistent with multi-factor resilience research (Menoni et al., 2024; Zogheib and Mahetaji, 2024).

3.6 Unexpected Observations

Two anomalies emerged. Case company A first resolved a budget gap within days, but MuSyRI remained elevated until the next monthly finance input. Second, company C experienced a transient synergy spike caused by a short-lived R&D slip and a minor regulatory hold; managers accepted such potential overestimates. Section 4 discusses the theoretical and practical implications of the study.

4. Discussion

4.1 Link to the prior literature

Risk integration studies have shown that moderate stressors often amplify each other once they occur together, rather than simply adding up linearly (Labaka et al., 2016; OECD, 2019). Jiwei et al., 2019 developed network-based models to capture the propagation of failures across interconnected infrastructure systems, revealing that moderate disruptions in two networks often produce nonlinear cascades at their intersection points. Their approach highlights how cyber-physical connections amplify risk beyond what siloed assessments would predict. Although e-government platforms collect diverse logs, they rarely incorporate explicit synergy metrics that reveal multi-domain concurrency (Arvidsson et al., 2021; National Institute for Strategic Studies (NISS), 2021). Although Bayesian models handle interdependencies, they can generate complex probability distributions that field managers find difficult to interpret (Cai et al., 2017; P. Zhang et al., 2025). Fuzzy AHP scores reflect expert weighting but usually sum domain hazards additively, thus missing how moderate levels can be combined into heightened vulnerability (Akbari Ahmadabadi and Heravi, 2019; Murasov et al., 2024). Recent accounts of water, construction, and energy infrastructures confirm that moderate disruptions in two or more domains escalate the total threat if they coincide (Menoni et al., 2024; Mohebbi et al., 2020; Wells et al., 2022). The importance of standardized risk management approaches became particularly evident during global disruptions, where organizations with robust frameworks demonstrated superior adaptability (Prasetya et al., 2023). Unifying risk detection and resilience in a single bounded index remains an unsolved challenge (Božović et al., 2020; Šarūnienė et al., 2024). MuSyRI addresses this gap by explicitly modeling synergy and resilience by building on prior theoretical calls for nonlinear concurrency functions (Gopalakrishnan and Sankaranarayanan, 2023; Lin and Pan, 2022).

4.2 Theoretical Contributions

MuSyRI advances the multi-factor risk integration theory through three main innovations. First, it codifies non-linear synergy by amplifying the composite score when two or more domain sub-indices simultaneously exceed moderate thresholds. This exponent-based design captures concurrency-driven escalation rather than treating risks as merely additive (Chang et al., 2023; Moussa et al., 2024). Rød et al., 2020 traced the evolution from traditional risk management to resilience management in critical infrastructure, highlighting the shift from avoiding specific threats to building adaptive capacities across multiple domains. Their work emphasized

that resilience-based approaches better accommodate the concurrent stressors that characterize modern infrastructure challenges. For instance, if two fuzzy sub-indices register around 0.40 and 0.35, their overlapping effect can substantially increase the total measure above 0.75, depending on the chosen parameters, rather than resting near a simple sum or product. This approach addresses the documented shortcomings of silo-based or linear risk approaches, where moderate levels of risk can appear benign when viewed in isolation (Akbari Ahmadabadi and Heravi, 2019; Zogheib and Mahetaji, 2024).

Table 2 compares MuSyRI with established multi risk frameworks (Labaka et al., 2016, Cai et al., 2017, Akbari Ahmadabadi and Heravi, 2019 along five methodological dimensions.

Table 2 Comparative analysis of multi-risk assessment frameworks

Framework / Study	Synergy Detection	Resilience Integration	Bounded - ness	Early-Warning Capability	Implementation Context
MuSyRI (this study)	Explicit nonlinear CAF (Eq. 2) captures concurrent domain interactions	Direct integration via resilience offset in the denominator (Eq. 4)	Guaranteed [0, 1] scale by design	1–4 weeks lead time demonstrated across cases	Real-time compatible; tested in four critical-infrastructure settings
Labaka et al., 2016	Qualitative framework recognises interdependencies	Resilience treated as a separate maturity model	No numerical bound	Not quantified	Conceptual framework; case studies in critical infrastructure
Cai et al., 2017	Dynamic Bayesian Networks model probabilistic dependencies	Resilience nodes embedded in network structure	Unbounded probabilities	Scenario-based forecasting	Theoretical demonstrations; computational complexity limits real-time use
Akbari Ahmadabadi and Heravi, 2019	Fuzzy-AHP recognises interactions via expert weighting	Not explicitly integrated	Normalised scores without formal guarantee	Not addressed	PPP megaprojects; requires extensive expert elicitation

As shown in Table 2, MuSyRI advances the field through three distinctive features. First, while Labaka et al., 2016 provided valuable qualitative insights into resilience building, MuSyRI operationalized these concepts through quantitative metrics suitable for automated monitoring systems. Second, compared with the computational complexity of dynamic Bayesian networks (Cai et al., 2017), the algebraic formulation of MuSyRI enables real-time calculation, which is essential for operational dashboards. Third, unlike the expert-dependent weights in Fuzzy-AHP approaches (Akbari Ahmadabadi and Heravi, 2019), MuSyRI combines expert calibration with data-driven validation, reducing subjectivity while maintaining domain expertise integration.

The mathematical foundation of MuSyRI's resilience integration draws parallels to production function approaches in resilience assessment, where similar mathematical structures have been used to model nonlinear relationships between inputs and outputs (Jandhana et al., 2018). This connection reinforces the theoretical validity of incorporating multiplicative factors to capture synergistic effects in multi-domain systems.

Beyond modeling nonlinear synergy, MuSyRI makes a second significant advancement to multi-factor risk integration theory: it integrates resilience directly into the main formula rather than treating preparedness as a separate monitoring domain. The offset $\gamma \times ResF_{agg}$ in the denominator scales how robust resources curb synergy-based escalation (Božović et al., 2020).

This aligns with the foundational elements of critical infrastructure resilience that emphasize both preparedness and adaptive capacity (Trifunović, 2020). Each organization's resilience level ($ResF_{agg}$=j ResF$_j$) adjusts the final scores downward if backup funds or equipment exist in that domain, reflecting how well-resourced companies mitigate concurrent hazards (Labaka et al., 2016; Nweke and Wolthusen, 2021). In case-company A, a modest $ResF_{agg}$ of about 0.10 lowered the synergy spike from 0.68 to 0.58, while case-company D, with ∼0.20, reduced the peaks from the mid-0.70 to mid-0.50 ranges. By combining concurrency detection and in-house capacity into one metric, MuSyRI operationalizes how synergy interacts with resilience rather than forcing managers to refer to separate dashboards.

In addition to integrating synergy and resilience, MuSyRI addresses another critical limitation of existing risk models: the model is bounded in [0,1]. This design choice addresses the practical criticisms of unbounded fuzzy or Bayesian outputs, where risk scores can exceed unity without clear cutoffs (Cai et al., 2017). A single composite in [0,1] allows managers to define numeric thresholds for moderate or high risk, such as 0.65 or 0.70 (OECD, 2019). All four case companies adopted similar synergy lines despite operating in different sectors (housing, specialized construction, water-tech and partial state-owned utility), demonstrating sector-agnostic adaptability (Gopalakrishnan and Sankaranarayanan, 2023; National Infrastructure Advisory Council (NIAC), 2010). This bounded nature supports straightforward color-coded risk scales in line with transparency and consistency demands of digital governance.

4.3 Practical Implications

Managers reported that MuSyRI revealed critical overlaps earlier than standard thresholds focused on single domains. In the case of company A, moderate budget strains combined with operational incidents spiked the index near 0.68 two to three weeks before domain-specific dashboards raised alarms, prompting a timely maintenance budget shift that reduced service slowdowns by approximately 8%–12%. In case company B, overlapping cost overruns and scheduling lags pushed the synergy score to ∼0.73, triggering crew realignments before the cost or schedule alone became severe. In the case of company C, a water-tech startup, MuSyRI jumped to ∼0.75 when moderate R&D setbacks coincided with regulatory licensing shortfalls, highlighting this concurrency around one to two weeks ahead of normal reviews. In the case of company D, synergy near 0.70–0.75 alerted managers to concurrent cyber, policy, and financial anomalies that averted broader service disruptions. These preventative actions align with the findings of Hallegatte et al., 2019, who documented how resilient infrastructure can generate a $4 return for each $1 invested when accounting for the avoided costs of multidomain disruptions and cascading failures. Their work emphasized that the early detection of overlapping vulnerabilities produces the highest economic returns for public systems.

Implementation requires only the calibration of fuzzy membership definitions and synergy parameters (α, η, γ) because an ERP-BPMS already consolidated domain logs (Falco et al., 2019). Two to three expert workshops and a short genetic algorithm were sufficient for the four pilots (Cai et al., 2017). Synergy patterns highlight which domain pairs or triads consistently overlap over time, guiding targeted resource allocations that enhance local resilience (Gopalakrishnan and Sankaranarayanan, 2023). This approach aligns with recent advances in the optimization of risk-response strategies when resources are limited (Zuo et al., 2022). Managers preferred the bounded [0,1] scale over unbounded or purely probabilistic methods because synergy triggers above 0.65 or 0.70 fostered faster and more coordinated responses across departments.

4.4 Policy and Government Implications

A synergy-based measure can help public agencies more effectively license, fund, and oversee critical and near-critical services, addressing the unique challenges of public sector risk management where multiple objectives must be balanced (Woods, 2022). Municipal authorities could

embed MuSyRI thresholds in operating permits, compelling organizations, such as case company A, to maintain synergy below a numeric cutoff or face mandatory mitigation (National Infrastructure Advisory Council (NIAC), 2010). Instead of siloed compliance checklists, regulators track whether concurrent moderate signals push the final index above 0.70, mandating earlier inspections or resource audits (OECD, 2019). Governments might also tie synergy scores to funding streams, awarding grants to providers that show sustained low synergy or directing extra support to those with recurring overlaps between particular domains (Mahama et al., 2022; Šarūnienė et al., 2024). Such approaches require disaggregated policy governance mechanisms that can coordinate across multiple agencies while maintaining accountability (X. Zhang, 2022). For state-influenced providers, such as case-company D, synergy alerts integrated into board-level governance can ensure that moderate domain hazards are not compound unrecognized (National Institute for Strategic Studies (NISS), 2021). Scolobig et al., 2017 analyzed policy barriers that prevent the effective implementation of multi-risk approaches, identifying fragmented governance, siloed expertise and lack of standardized metrics as key obstacles. Their work proposed policy mechanisms that can institutionalize cross-domain risk detection within existing regulatory frameworks.

Bayesian models often yield posterior probabilities that field inspectors may struggle to quickly interpret, whereas fuzzy AHP requires repeated pairwise comparisons that produce only linear composites (Akbari Ahmadabadi and Heravi, 2019; Cai et al., 2017). In contrast, MuSyRI's single bounded metric can be easily mapped onto color-coded dashboards in city council e-portals or national agency platforms, satisfying digital governance agendas that call for integrated, transparent data (Lin and Pan, 2022; Zogheib and Mahetaji, 2024). Municipalities may publish synergy indices for key utilities to foster public accountability and encourage early cross-domain interventions (Arvidsson et al., 2021; Uwe and Gerber, 2019). This shared concurrency scale helps agencies coordinate oversight because the environment, finance, and cyber regulators each see the same synergy range, aligning with the broader move toward adaptive and data-driven governance.

4.5 Limitations

These findings draw on four pilot cases, so the sample size remains too small for broad generalization (Yin, 2018). Each organization had a distinct data cadence (weekly in A and C, monthly in B and D), indicating that very rapid synergy spikes might remain undetected. Domain weights and fuzzy membership functions were defined through local experts or partial computational methods, introducing potential subjectivity, although minor parameter shifts (±10–20%) did not alter which weeks breached the synergy thresholds. Region-specific availability and completeness of financial, operational, regulatory, and cyber logs can affect model performance (OECD, 2019). Overestimating organizational resilience might artificially depress synergy scores and delay alerts (Božović et al., 2020). Additionally, the current framework includes four core domains but omits environmental or social factors that could intersect with existing vulnerabilities, especially in large-scale infrastructure (Hochrainer-Stigler et al., 2023; Wells et al., 2022). Sakic Trogrlic et al., 2024 surveyed European stakeholders to identify persistent challenges in multi-hazard risk assessment and found that organizations struggle most with methodologies that capture the interaction effects between moderate hazards. Their findings reveal a gap between the theoretical multi-risk frameworks and practical implementation tools accessible to infrastructure managers.

4.6 Future Research

Future studies could extend MuSyRI to other critical sectors, such as healthcare, transportation, and telecommunications, where moderate concurrency may escalate rapidly (Menoni et al., 2024; Mohebbi et al., 2020). Cross-national comparisons would clarify how legal or cultural differences in data-sharing and compliance norms shape synergy calibration (Lin and

Pan, 2022). Ward et al., 2021 outlined a comprehensive research agenda for advancing disaster risk management through MRA, highlighting key knowledge gaps in capturing the dynamic interactions between hazards. Their work proposed that next-generation frameworks must integrate synergistic HA and adaptive capacity within unified metrics. Advanced sensor feeds from Internet-of-Things or SCADA systems may enable real-time synergy detection, capturing short-lived overlaps missed by weekly or monthly logs (Falco et al., 2019). Machine learning or artificial intelligence (AI)-based calibration can reduce reliance on expert panels, making synergy detection more automated as risk landscapes evolve (Gopalakrishnan and Sankaranarayanan, 2023; Moussa et al., 2024). Comparative experiments that benchmark MuSyRI against Bayesian copula networks or enhanced fuzzy-AHP may quantify lead time gains, false positives, or cost-effectiveness (Chang et al., 2023). Researchers may also track how synergy-based prevention offsets implementation costs through longitudinal cost-benefit analyses, bolstering the adoption of synergy methods in public governance. Expanding MuSyRI to incorporate environmental or social indicators would capture how climate events or demographic shifts can magnify operational or financial strains (Boni et al., 2025; Nweke and Wolthusen, 2021).

These pilot results indicate that moderate anomalies across multiple domains often trigger an outsized risk earlier than that suggested by single-domain metrics. MuSyRI formalizes this process by embedding concurrency detection in one bounded index, integrating domain-level resilience as an offset, and providing a clearer measure for managers and policymakers. The synergy signals arrived early enough to prompt maintenance reallocation in case company A, crew shifts in case company B, bridging funds for case company C, and cross-department coordination in case company D. By bridging detection and mitigation under a single measure, MuSyRI addresses the limitations of silo-based monitoring and enables organizations to respond more proactively in multidomain risk settings. If scaled further, this synergy approach could reshape how digital governance frameworks define licensing, compliance, and resource allocation for critical infrastructures, shifting from reactive thresholds to adaptive concurrency-aware oversight.

5. Conclusions

This study introduced MuSyRI, a bounded [0–1] index that fuses operational, financial, regulatory, and cyber signals into a single nonlinear measure of compound risk. Validation across four anonymised organizations (Cases A–D) delivered 1–4-week early-warning leads over additive baselines and cut service disruptions by 8%–12%. MuSyRI avoids false positives yet captures cascading effects by embedding a resilience offset, enabling regulators to move from reactive silo-based monitoring to proactive, cross-domain governance. Future work should enlarge the dataset to a national scale and embed environmental or social indicators to further reinforce e-government resilience.

Author Contributions

Conceptualization, Yuri Chernenko; Methodology, Yuri Chernenko and Olena Borodina; Formal analysis, Yuri Chernenko; Investigation, Yuri Chernenko; Data curation, Yuri Chernenko; Visualization, Yuri Chernenko; Writing – original draft, Yuri Chernenko; Writing – review & editing, Olena Borodina and Yuri Chernenko; Project administration, Yuri Chernenko. Overall contribution: Yuri Chernenko 80%, Olena Borodina 20%.

Conflict of Interest

The authors declare no conflicts of interest.

References

Akbari Ahmadabadi, A., & Heravi, G. (2019). Risk assessment framework of ppp-megaprojects focusing on risk interaction and project success. *Transportation Research Part A: Policy and Practice*, *124*, 169–188. https://doi.org/10.1016/j.tra.2019.03.011

Arvidsson, B., Johansson, J., & Guldåker, N. (2021). Critical infrastructure, geographical information science and risk governance: A systematic cross-field review. *Reliability Engineering and System Safety*, *213*, 107741. https://doi.org/10.1016/j.ress.2021.107741

Beckers, F., & Stegemann, U. (2013). A risk-management approach to a successful infrastructure project [Viewed 14 May 2025]. https://www.mckinsey.com/business-functions/operations/our-insights/a-risk-management-approach-to-a-successful-infrastructure-project

Bentahar, A., & Rifai, A. (2022). Risk and risk management in the public sector: A theoretical contribution. *Journal of Economics, Finance and Management Studies*, *5*(9), 2492–2506. https://doi.org/10.47191/jefms/v5-i9-03

Berawi, M., Leviakangas, P., Muhammad, F., Sari, M., Gunawan, Yatmo, Y., & Suryanegara, M. (2019). Optimizing search and rescue personnel allocation in disaster emergency response using fuzzy logic. *International Journal of Technology*, *10*(7), 1416. https://doi.org/10.14716/ijtech.v10i7.3709

Boni, M., Faiella, A., Gazzola, V., & Pergalani, F. (2025). A multi-hazard and multi-risk assessment methodological approach to support civil protection planning in wide areas. *International Journal of Disaster Risk Reduction*, *119*, 105343. https://doi.org/10.1016/j.ijdrr.2025.105343

Božović, M., Mihajlović, E., & Živković, S. (2020). Risk management in the context of multi-risk assessment. *Facta Universitatis, Series: Working and Living Environmental Protection*, *161*(3), 161–169. https://doi.org/10.22190/FUWLEP1903161B

Cai, B., Xie, M., Liu, Y., Liu, Y., Ji, R., & Feng, Q. (2017). A novel critical infrastructure resilience assessment approach using dynamic bayesian networks. *AIP Conference Proceedings*, *1890*(1), 040043. https://doi.org/10.1063/1.5005245

Carpignano, A., Grosso, D., Gerboni, R., & Bologna, A. (2021). Resilience of critical infrastructures: a risk assessment methodology for energy corridors. In V. Rosato & A. Di Pietro (Eds.), *Issues on Risk Analysis for Critical Infrastructure Protection*. IntechOpen. https://doi.org/10.5772/intechopen.94755

Chang, J., Yin, Z., Zhang, Z., Xu, X., & Zhao, M. (2023). Multi-disaster integrated risk assessment in city range-a case study of jinan, china. *International Journal of Environmental Research and Public Health*, *20*(4), 3483. https://doi.org/10.3390/ijerph20043483

Dudauri, T. (2022). Peculiarities of integrated risk management. *Economics*, *105*(6-8), 112–123. https://doi.org/10.36962/ecs/105/6-8/2022-112

Falco, G., Noriega, A., & Susskind, L. (2019). Cyber negotiation: A cyber risk management approach to defend urban critical infrastructure from cyberattacks. *Journal of Cyber Policy*, *4*(1), 90–116. https://doi.org/10.1080/23738871.2019.1586969

Farrington, S. (2016). Enterprise risk management powers up at utilities [Viewed 14 May 2025]. https://www.risk.net/commodities/energy/2473744/enterprise-risk-management-powers-utilities

Gopalakrishnan, S., & Sankaranarayanan, S. (2023). Cooperative security against interdependent risks. *Production and Operations Management*, *32*(11), 3504–3520. https://doi.org/10.1111/poms.14047

Hallegatte, S., Rentschler, J., & Rozenberg, J. (2019). *Lifelines: The resilient infrastructure opportunity*. World Bank Group. https://doi.org/10.1596/978-1-4648-1430-3

Hendra, F., Mohammad, R., Amrin, A., Maarop, N., & Zagloel, T. (2024). Systematic literature review of risk assessment techniques, standard and guidelines for railway. *International Journal of Technology*, *15*(4), 1148. https://doi.org/10.14716/ijtech.v15i4.6384

Hochrainer-Stigler, S., Trogrlić Šakić, R., Reiter, K., Ward, P., De Ruiter, M., Duncan, M. J., Torresan, S., Ciurean, R., Mysiak, J., Stuparu, D., & Gottardo, S. (2023). Toward a framework for systemic multi-hazard and multi-risk assessment and management. *iScience*, *26*(5), 106736. https://doi.org/10.1016/j.isci.2023.106736

Jandhana, I., & Agustini, H. (2024). Performance evaluation of the industrial resilience index by using cross-correlation method. *International Journal of Technology*, *15*(5), 1462. https://doi.org/10.14716/ijtech.v15i5.5599

Jandhana, I., Nurcahyo, R., & Zagloel, T. (2018). Resilient structure assessment using cobb-douglas production function: The case of the indonesian metal industry. *International Journal of Technology*, *9*(5), 1061. https://doi.org/10.14716/ijtech.v9i5.1862

Jiwei, L., Kang, T., Kong, R., & Soon, S. (2019). Modelling critical infrastructure network interdependencies and failure. *International Journal of Critical Infrastructures*, *15*(1), 1–23. https://doi.org/10.1504/IJCIS.2019.096557

Kelic, A. (2019). Cyber risk in critical infrastructure. *ACM SIGMETRICS Performance Evaluation Review*, *46*(2), 72–75. https://doi.org/10.1145/3305218.3305243

Labaka, L., Hernantes, J., & Sarriegi, J. (2016). A holistic framework for building critical infrastructure resilience. *Technological Forecasting and Social Change*, *103*, 21–33. https://doi.org/10.1016/j.techfore.2015.11.005

Larsson, A., & Große, C. (2023). Data use and data needs in critical infrastructure risk analysis. *Journal of Risk Research*, *26*(5), 524–546. https://doi.org/10.1080/13669877.2023.2181858

Lin, J., & Pan, T.-C. (2022). Modelling of multi-sectoral critical infrastructure interdependencies for vulnerability analysis. *Disaster Prevention and Resilience*, *1*, 2. https://doi.org/10.20517/dpr.2021.05

Mahama, H., Elbashir, M., Sutton, S., & Arnold, V. (2022). Enabling enterprise risk management maturity in public sector organisations. *Public Money and Management*, *42*(6), 403–407. https://doi.org/10.1080/09540962.2020.1769314

Menoni, S., Galderisi, A., Carrion, D., & Gerosa, C. (2024). Cross-sectoral and multilevel dimensions of risk and resilience management in urban areas enabled by geospatial data processing. *Sustainability*, *16*(19), 8712. https://doi.org/10.3390/su16198712

Mohebbi, S., Zhang, Q., Christian Wells, E., Zhao, T., Nguyen, H., Li, M., Abdel-Mottaleb, N., Uddin, S., Lu, Q., Wakhungu, M., Wu, Z., Zhang, Y., Tuladhar, A., & Ou, X. (2020). Cyber-physical-social interdependencies and organisational resilience: A review of water, transportation, and cyber infrastructure systems and processes. *Sustainable Cities and Society*, *62*, 102327. https://doi.org/10.1016/j.scs.2020.102327

Moussa, A., Ezzeldin, M., & El-Dakhakhni, W. (2024). Predicting and managing risk interactions and systemic risks in infrastructure projects using machine learning. *Automation in Construction*, *168*, 105836. https://doi.org/10.1016/j.autcon.2024.105836

Murasov, R., Nikitin, A., & Meshcheriakov, I. (2024). Mathematical model of risk assessment of the operation of critical infrastructure objects based on the theory of fuzzy logic. *Journal of Scientific Papers "Social Development and Security"*, *14*(5), 166–174. https://doi.org/10.33445/sds.2024.14.5.17

National Infrastructure Advisory Council (NIAC). (2010). *A framework for establishing critical infrastructure resilience goals: Final report and recommendations* (tech. rep.) (Viewed 14 May 2025). United States Department of Homeland Security. Washington, DC. https://www.cisa.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf

National Institute for Strategic Studies (NISS). (2021). *The state critical infrastructure protection system in the national security and defense sector: Analytical report* (tech. rep.) (English ed. Viewed 14 May 2025). NISS. Kyiv. https://niss.gov.ua/sites/default/files/2021-02/english-version-cip-dopovid-1.pdf

National Institute of Standards and Technology. (2020). *Nist privacy framework: A tool for improving privacy through enterprise risk management, version 1.0* (tech. rep.). National Institute of Standards and Technology. Gaithersburg, MD. https://doi.org/10.6028/NIST.CSWP.01162020

Nweke, L., & Wolthusen, S. (2021). A holistic approach for enhancing critical infrastructure protection: Research agenda. In J. Abawajy, K. K. R. Choo, & H. Chiroma (Eds.), *International conference on emerging applications and technologies for industry 4.0 (eati'2020)* (pp. 220–228). Springer International Publishing. https://doi.org/10.1007/978-3-030-80216-5_16

OECD. *Good governance for critical infrastructure resilience*. 2019. https://doi.org/10.1787/02f0e5a0-en

Petit, F., Verner, D., Phillips, J., & Lewis, L. (2018). Critical infrastructure protection and resilience – integrating interdependencies. In A. Masys (Ed.), *Security by design: Innovative perspectives on complex problems* (pp. 193–219). Springer International Publishing. https://doi.org/10.1007/978-3-319-78021-4_10

Prasetya, B., Tampubolon, B., & Yopi, Y. (2023). Role of risk management and standardization for supporting innovation in new normal based on lessons learned during pandemic covid-19. *International Journal of Technology*, *14*(5), 954. https://doi.org/10.14716/ijtech.v14i5.5299

Rød, B., Lange, D., Theocharidou, M., & Pursiainen, C. (2020). From risk management to resilience management in critical infrastructure. *Journal of Management in Engineering*, *36*(4). https://doi.org/10.1061/(ASCE)ME.1943-5479.0000795

Sakic Trogrlic, R., Team, M.-E., Ma, L., Torresan, S., Ciurean, R., Reiter, K., Ward, P., Gottardo, S., Tatman, S., Daloz, A., & Padron-Fumero, N. (2024). Challenges in assessing and managing multi-hazard risks: A european stakeholders' perspective [Conference Presentation]. *EGU General Assembly 2024, Abstract EGU24-3843*. https://doi.org/10.5194/egusphere-egu24-3843

Samanis, E., Gardiner, J., & Rashid, A. (2022). Adaptive cyber security for critical infrastructure. *2022 ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS)*, 304–305. https://doi.org/10.1109/ICCPS54341.2022.00043

Sambowo, A., & Hidayatno, A. (2021). Resilience index development for the manufacturing industry based on robustness, resourcefulness, redundancy, and rapidity. *International Journal of Technology*, *12*(6), 1177. https://doi.org/10.14716/ijtech.v12i6.5229

Šarūnienė, I., Martišauskas, L., Krikštolaitis, R., Augutis, J., & Setola, R. (2024). Risk assessment of critical infrastructures: A methodology based on criticality of infrastructure elements. *Reliability Engineering and System Safety*, *243*, 109797. https://doi.org/10.1016/j.ress.2023.109797

Schlosser, C., Frankenfeld, C., Eastham, S., Gao, X., Gurgel, A., McCluskey, A., Morris, J., Orzach, S., Rouge, K., Paltsev, S., & Reilly, J. (2023). Assessing compounding risks across multiple systems and sectors: A socio-environmental systems risk-triage approach. *Frontiers in Climate*, *5*, 1–19. https://doi.org/10.3389/fclim.2023.1100600

Scolobig, A., Komendantova, N., & Mignan, A. (2017). Mainstreaming multi-risk approaches into policy. *Geosciences*, *7*(4), 129. https://doi.org/10.3390/geosciences7040129

Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2011). Risk assessment methodology for interdependent critical infrastructures. *International Journal of Risk Assessment and Management*, *15*(2-3), 128–148. https://doi.org/10.1504/IJRAM.2011.042113

Trifunović, D. (2020). Elements of critical infrastructure resilience. *National Security and the Future*, *20*(1-2), 51–61. https://doi.org/10.37458/nstf.20.1-2.6

Uwe, B.-R., & Gerber, B. (2019). Smart cities and the challenges of cross domain risk management: Considering interdependencies between ict-security and natural hazards disruptions. *Economics and Culture*, *16*(2), 106–116. https://doi.org/10.2478/jec-2019-0026

Ward, P. (2022). Myriad-eu: Towards disaster risk management pathways in multi-risk assessment [Conference Abstract, Presentation ID: EGU22-9323]. *EGU General Assembly 2022*, EGU22–9323. https://doi.org/10.5194/egusphere-egu22-9323

Ward, P., Daniell, J., Duncan, M., Dunne, A., Hananel, C., Hochrainer-Stigler, S., Tijssen, A., Torresan, S., Ciurean, R., Gill, J., Sillmann, J., Couasnon, A., Koks, E., Padrón-Fumero, N., Tatman, S., Tronstad Lund, M., Adesiyun, A., Aerts, J. C. J. H., Alabaster, A., ... de Ruiter, M. (2021). Invited perspectives: A research agenda towards disaster risk management pathways in multi-(hazard-)risk assessment. *Natural Hazards and Earth System Sciences*, *22*(4), 1487–1497. https://doi.org/10.5194/nhess-2021-326

Wells, E., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*, *15*, 100244. https://doi.org/10.1016/j.pdisas.2022.100244

Woods, M. (2022). *Risk management in the public sector*. Routledge. https://doi.org/10.4324/9781315208336-8

Yin, R. (2018). *Case study research and applications: Design and methods* (6th). Sage Publications.

Zhang, P., Zhang, Z.-J., & Gong, D.-Q. (2025). A full domain decision model for robust risk control based on minimum linkage space and copula bayesian networks. *Reliability Engineering and System Safety*, *260*, 111046. https://doi.org/10.1016/j.ress.2025.111046

Zhang, X. (2022). Understanding innovation policy governance: A disaggregated approach. *Review of Policy Research*, *39*(3), 303–329. https://doi.org/10.1111/ropr.12456

Zogheib, C., & Mahetaji, K. (2024). Cross-domain information integration in government: Hierarchies and responsibilities. *Proceedings of the Association for Information Science and Technology*, *61*(1), 469–480. https://doi.org/10.1002/pra2.1043

Zuo, F., Zio, E., & Yuan, Y. (2022). Risk-response strategy optimisation considering limited risk-related resource allocation and scheduling. *Journal of Construction Engineering and Management*, *148*(11). https://doi.org/10.1061/(ASCE)CO.1943-7862.0002392