Scientific Research Publishing

Journal of Data Analysis and Information Processing, 2025, 13(3), 347-369
https://www.scirp.org/journal/jdaip
ISSN Online: 2327-7203
ISSN Print: 2327-7211

Network Analysis for Systemic Risk Assessment in Supply Chains: A Cross-Disciplinary Framework Integrating Financial Contagion Models

Omoshola S. Owolabi

Department of Data Science, Carolina University, Winston-Salem, NC, USA
Email: owolabio@carolinau.edu

How to cite this paper: Owolabi, O.S. (2025) Network Analysis for Systemic Risk Assessment in Supply Chains: A Cross-Disciplinary Framework Integrating Financial Contagion Models. *Journal of Data Analysis and Information Processing*, **13**, 347-369.
https://doi.org/10.4236/jdaip.2025.133022

Received: June 22, 2025
Accepted: August 25, 2025
Published: August 28, 2025

Abstract

This research develops a novel cross-disciplinary framework that bridges financial systemic risk modeling with supply chain network analysis to advance resilience assessment and policy guidance. The approach integrates established financial contagion frameworks with the topology of the supply chain network, introducing the concept of "too central to fail" suppliers through systematic importance scoring methodologies. The framework reveals striking asymmetries in supply chain vulnerability patterns. While the majority of suppliers demonstrate systemic importance within network structures, financial fragility analysis indicates remarkable overall network robustness, with minimal nodes exhibiting high vulnerability thresholds. Most significantly, comprehensive stress testing exposes a critical paradox: networks demonstrate moderate resilience to random disruptions yet remain substantially vulnerable to strategic targeting of central nodes. Cascade failure analysis through multiple simulation approaches unveils the dual nature of supply chain risk propagation. Random shock scenarios generate manageable failure rates, while targeted attacks on high-centrality suppliers achieve disproportionate network impact. Most alarmingly, liquidity crisis simulations demonstrate how financial contagion mechanisms can affect nearly half of all network participants, highlighting the interconnected nature of operational and financial vulnerabilities. These findings establish quantitative foundations for the assessment of systemic risk in supply chains, with immediate implications for regulatory frameworks, early warning systems, and resilience enhancement strategies. The integrated financial-operational risk framework advances the theoretical understanding of the propagation of cross-sector vulnerability while providing systematic methodologies for identifying critical suppliers whose failure

could trigger systemic collapse.

Keywords

Supply Chain Resilience, Systemic Risk Assessment, Network Vulnerability Analysis, Financial Contagion Modeling

1. Introduction

Modern supply chains operate as complex interdependent networks where localized disruptions can propagate globally, causing systemic failures across multiple sectors. Recent events, including the COVID-19 pandemic [1], the Ever-Given Suez Canal blockage [2], and geopolitical supply chain disruptions, have demonstrated how individual supplier failures can cascade through interconnected networks, disrupting entire industries and revealing the systemic nature of supply chain vulnerabilities.

Despite growing recognition of supply chain systemic risk, existing approaches suffer from significant limitations. Traditional supply chain risk management focuses primarily on operational disruptions and local vulnerabilities [3], failing to capture the systemic implications of network interdependencies and financial contagion mechanisms. Risk assessment methodologies remain largely qualitative [4], lacking the quantitative rigor necessary for effective policy intervention and regulatory oversight.

Simultaneously, the financial systemic risk literature has developed sophisticated quantitative models for contagion propagation and systemic institution identification, including the seminal Eisenberg-Noe framework [5] and the DebtRank algorithm [6]. However, these frameworks remain largely isolated from supply chain analysis, representing a critical gap in understanding how financial distress propagates through operational networks and how supply chain disruptions create financial contagion.

This paper bridges this disciplinary gap by developing a novel cross-disciplinary framework that systematically applies financial systemic risk models to supply chain networks. The adopted approach makes four key methodological contributions. First, we adapt the Eisenberg-Noe financial contagion model to capture supply chain dependencies and shock propagation, replacing financial exposures with operational dependencies and payment relationships. Second, we introduce the concept of "too-central-to-fail" suppliers based on DebtRank-style systemic importance scoring, providing quantitative criteria for identifying systemically important supply chain nodes analogous to systemically important financial institutions [7]. Third, we develop multi-scenario stress testing protocols that integrate financial fragility assessment with operational disruption simulation, including Monte Carlo failure analysis, targeted attack simulations, and liquidity crisis propagation. Fourth, we establish quantitative foundations for supply chain systemic risk

regulation, early warning systems, and resilience enhancement strategies based on network topology and financial vulnerability analysis.

The framework addresses critical policy needs for supply chain resilience assessment while advancing theoretical understanding of systemic risk propagation in operational networks [8].

2. Literature Review

This work is built on two distinct but complementary literature: financial systemic risk modeling and supply chain network analysis.

2.1. Financial Systemic Risk Models

The financial systemic risk literature provides the theoretical foundation for our framework. Eisenberg and Noe [5] developed the foundational model of financial contagion through interconnected balance sheets, demonstrating how localized shocks propagate through financial networks via default cascades. Elliott *et al.* [9] extended this framework to incorporate more general network structures and threshold effects in contagion transmission.

The DebtRank algorithm introduced by Battiston *et al.* [6] provides a practical methodology for quantifying systemic importance in financial networks, measuring each institution's potential impact on the entire system through stress propagation. This approach has been successfully applied to banking networks [10], sovereign debt analysis [11], and corporate credit risk assessment [12].

Recent developments in systemic risk measurement include network-based approaches [13]. Stress testing methodologies have evolved to incorporate complex interdependencies [14] and macroeconomic feedback effects [15].

2.2. Supply Chain Network Analysis

Supply chain network analysis has focused primarily on operational resilience and vulnerability assessment. Acemoglu *et al.* [8] demonstrated how firm-level shocks can generate aggregate fluctuations through input-output networks, establishing the theoretical basis for systemic effects in production networks.

Network-based approaches to supply chain risk have examined structural vulnerabilities [16], cascade effects [17], and resilience strategies [18]. Geographic concentration and supplier diversification have been identified as key risk factors [19].

However, existing supply chain literature lacks integration with financial contagion models, limiting understanding of how financial distress propagates through operational relationships and how operational disruptions create financial spillovers. This gap represents a significant opportunity for methodological advancement and policy application.

3. Methodology

3.1. Network Construction and Data Generation

This work constructs a synthetic supply chain network representing realistic multi-

tier dependencies and financial relationships. The network architecture reflects empirical supply chain structures with hierarchical tier organization and realistic degree distributions [20].

Network Generation and Empirical Calibration

The synthetic network comprises 500 nodes distributed across three supply chain tiers based on empirical tier size distributions from automotive and electronics industries [20] [21]. Upstream suppliers represent 300 nodes (60%) providing raw materials and components, consistent with supplier proliferation observed in global manufacturing networks. Mid-tier manufacturers comprise 80 nodes (16%) conducting assembly and manufacturing operations, reflecting concentration patterns in production stages. Downstream retailers consist of 120 nodes (24%) handling distribution and retail operations, calibrated to retail sector concentration ratios.

Network connectivity follows preferential attachment mechanisms with degree distributions calibrated to empirical supply chain data. The power-law exponent of 2.3 for supplier degree distribution matches observations from automotive supply networks [20]. Manufacturer nodes exhibit higher average degree (15.2), reflecting hub-like positions, while retailers show moderate connectivity (degree 8.4), consistent with distribution network structures. Directed edges represent supplier-customer relationships, with 4786 total connections yielding network density of 0.019, within the empirical range of 0.015 - 0.025 observed in manufacturing supply chains [21].

Node attributes include comprehensive financial and operational characteristics derived from industry benchmarks [22]. Financial metrics encompass revenue measured in millions USD following log-normal distributions by tier (suppliers: $\mu = 2.5$, $\sigma = 1.2$; manufacturers: $\mu = 3.8$, $\sigma = 0.9$; retailers: $\mu = 3.2$, $\sigma = 1.1$), calibrated to match revenue distributions from S&P Capital IQ industry data [23]. Debt-to-equity ratios follow Beta distributions with tier-specific parameters (suppliers: $\alpha = 2$, $\beta = 5$; manufacturers: $\alpha = 3$, $\beta = 4$; retailers: $\alpha = 2.5$, $\beta = 3.5$) calibrated to industry leverage patterns [24]. Liquidity ratios follow Gamma distributions ($k = 2$, $\theta = 0.8$) reflecting working capital management practices, and working capital days follow normal distributions with operational constraints ($\mu = 45$, $\sigma = 15$ days).

Operational characteristics include supplier diversification indices reflecting dependency concentration, customer concentration ratios measuring downstream dependencies, geographic locations with regional clustering and distance-based relationships [25], and contract terms capturing payment schedules and relationship stability metrics.

Edge attributes capture transaction relationships through transaction volumes representing revenue-weighted relationship strength, dependency strength measuring operational criticality of supplier relationships, lead times reflecting supply chain timing constraints, and payment terms characterizing financial relationship dynamics.

3.2. Systemic Risk Metrics

3.2.1. DebtRank-Style Systemic Importance

This work adapts the DebtRank algorithm [6] to supply chain networks by replacing financial exposures with supply dependencies. For each node i, the systemic importance SI_i captures the potential impact of node i's failure on the entire network through cascade propagation.

The algorithm proceeds in discrete time steps following the established DebtRank methodology. In the initialization step, for each node j, we define the relative economic size as:

$$W_j = \frac{V_j}{\sum_{k \in N} V_k} \tag{1}$$

where V_j is node j's revenue and N is the set of all nodes.

During impact matrix construction, the impact of node i on node j is defined as:

$$\Pi_{ij} = \frac{A_{ij} \cdot D_{ij}}{\sum_k A_{kj} \cdot D_{kj}} \tag{2}$$

where A_{ij} is the adjacency matrix and D_{ij} represents dependency strength, normalized by total incoming dependencies.

Finally, during cascade simulation, the systemic importance is computed as:

$$SI_i = \sum_{j \in N} h_{ij} \cdot W_j \tag{3}$$

where h_{ij} represents the ultimate impact of node i's failure on node j through the complete cascade process, incorporating both direct and indirect effects.

3.2.2. Financial Fragility Index

The work constructs a composite financial fragility index FF_i for each node i, combining multiple vulnerability indicators following established financial risk assessment methodologies [26]:

$$\begin{aligned} FF_i = {} & w_1 \cdot \text{DebtRatio}_i + w_2 \cdot \text{LiquidityStress}_i \\ & + w_3 \cdot \text{WorkingCapitalPressure}_i + w_4 \cdot \text{ConcentrationRisk}_i \end{aligned} \tag{4}$$

where weights w_k are empirically calibrated based on financial distress prediction literature [27] and each component is normalized to [0, 1]. The index ranges from 0 (financially robust) to 1 (highly fragile).

3.2.3. Systemic Importance Threshold Determination

The selection of the systemic importance threshold (SI > 0.2) follows a multi-criteria approach combining statistical analysis and regulatory benchmarking. We employ three complementary methods:

First, natural breaks classification (Jenks optimization) [28] identifies statistically significant discontinuities in the SI distribution, revealing a natural break at SI = 0.201 that maximizes between-class variance while minimizing within-class

variance.

Second, comparison with financial sector standards shows that our 0.2 threshold captures 59.2% of network nodes, comparable to the Basel III framework's identification of 29 global systemically important banks from approximately 100 large international banks, representing a similar concentration ratio when adjusted for network size differences.

Third, sensitivity analysis across alternative thresholds demonstrates robustness of key findings:

- SI > 0.1: Identifies 433 nodes (86.6%), potentially diluting regulatory focus;
- SI > 0.15: Identifies 364 nodes (72.8%), moderate concentration;
- SI > 0.2: Identifies 296 nodes (59.2%), optimal balance;
- SI > 0.25: Identifies 198 nodes (39.6%), may miss critical suppliers;
- SI > 0.3: Identifies 89 nodes (17.8%), excessive concentration.

The 0.2 threshold maintains policy stability across ±10% variations, with the number of systemically important suppliers changing by less than 15% for threshold adjustments between 0.18 and 0.22.

3.2.4. Network Centrality Measures

It computes comprehensive network centrality metrics to capture different aspects of structural importance [29]. Degree centrality measures direct connectivity as $C_D(i) = \frac{d_i}{n-1}$, where d_i is node degree. Betweenness centrality captures shortest path importance as $C_B(i) = \sum_{s \neq i \neq t} \frac{\sigma_{st}(i)}{\sigma_{st}}$, where σ_{st} is the total number of shortest paths from node s to node t and $\sigma_{st}(i)$ is the number passing through node i. Eigenvector centrality represents influence through connections using the principal eigenvector of the adjacency matrix [30]. PageRank measures recursive importance as $PR(i) = \frac{1-d}{N} + d\sum_{j \in \text{in}(i)} \frac{PR(j)}{|\text{out}(j)|}$ with damping parameter $d = 0.85$ [31].

3.3. Comprehensive Stress Testing Framework

The stress testing framework encompasses multiple scenario types to provide comprehensive resilience assessment, drawing from both financial stress testing [14] and supply chain risk assessment methodologies [3].

Monte Carlo failure simulations implement comprehensive probabilistic analysis to assess network resilience under random failure scenarios. Each simulation consists of shock generation through random selection of failed nodes based on financial fragility probabilities, cascade propagation through systematic failure transmission via supply chain dependencies using threshold-based contagion models [9], and impact measurement through calculation of total network impact and failure statistics. We conduct 1000 independent simulation runs to ensure statistical robustness and capture tail risk characteristics [32].

Targeted attack simulations analyze network vulnerability to strategic attacks through systematic node removal based on different targeting strategies. High-degree attacks involve sequential removal of the highest-degree nodes, reflecting potential targeting of major suppliers. High-betweenness attacks target nodes with the highest betweenness centrality, focusing on critical intermediaries. High-systemic-importance attacks remove nodes based on DebtRank scores, targeting systemically important suppliers. Random attacks provide baseline comparison with random node removal for statistical control.

Liquidity crisis propagation simulates financial contagion through liquidity stress propagation, modeling how payment delays and working capital constraints cascade through supply chain relationships [33]. The liquidity crisis model incorporates payment term dependencies between suppliers and customers, working capital constraints, cash flow timing effects, credit relationship stress, payment delay propagation mechanisms, and cross-tier contagion through financial interdependencies.

Percolation analysis conducts systematic examination of network connectivity degradation patterns through progressive node removal [34]. This involves progressive random node removal while monitoring the largest connected component size, characterizing continuous fragmentation behavior and connectivity decline patterns across the removal spectrum.

3.4. Verification and Validation Framework

All analysis components incorporate comprehensive verification protocols ensuring methodological rigor and reproducibility [35].

3.4.1. Data Integrity Verification

Network structure validation employs multiple consistency checks across three critical dimensions. Topology validation procedures verify directed acyclic graph properties within tiers, confirm the absence of self-loops or duplicate edges, and validate tier-based hierarchical constraints to ensure structural integrity. Attribute consistency checks confirm that all financial metrics remain within realistic bounds, with debt ratios constrained to the interval [0, 5] and liquidity ratios to [0, 3]. Furthermore, revenue distributions must match log-normal parameters within 5% tolerance, and operational metrics undergo validation against established industry benchmarks. Connectivity verification ensures that minimum degree requirements are satisfied with all nodes maintaining at least one connection to prevent isolated suppliers. The giant component must encompass more than 95% of the network, and average path length must remain within theoretical bounds appropriate for the network size.

3.4.2. Statistical Validation Protocols

Risk metric validation employs rigorous statistical testing through three complementary approaches. Bootstrap validation generates 1000 bootstrap samples for systemic importance scores with 95% confidence intervals, conducts stability test-

ing across 100 random network perturbations involving 5% edge rewiring, and verifies convergence for iterative algorithms using a tolerance threshold of 10^{-6}. Cross-validation procedures implement K-fold validation with $k = 10$ for financial fragility predictions, perform out-of-sample testing on a 20% holdout network subset, and compare results with null models, including random networks and configuration models, to establish statistical significance. Sensitivity analysis encompasses parameter variation testing at ±20% for all calibrated values, robustness assessment across different network generation seeds, and stability verification for threshold-dependent results to ensure findings remain consistent under parameter uncertainty.

3.4.3. Algorithm Verification Testing

Each computational component undergoes specific verification tailored to its algorithmic characteristics. The DebtRank implementation undergoes validation against published test cases from Battiston *et al.* [6], convergence testing with a maximum of 100 iterations, and numerical stability checks for sparse matrix operations to ensure computational accuracy. Cascade propagation algorithms require verification of threshold mechanics against analytical solutions, conservation tests that ensure no value creation or destruction occurs during propagation, and timing consistency checks across both synchronous and asynchronous update protocols. Stress testing procedures incorporate Monte Carlo convergence verification requiring standard errors below 1%, reproducibility testing using fixed random seeds to ensure consistent results, and boundary condition testing that examines behavior under extreme scenarios, including empty networks and fully connected topologies.

3.4.4. Results Validation Criteria

Quantitative acceptance criteria ensure result reliability through stringent validation requirements. Network metrics must match theoretical predictions within 10% tolerance for key measures, including clustering coefficient and degree distribution exponent. Systemic importance scores must satisfy conservation properties by summing to 1.0 with a tolerance of ±0.001, ensuring proper normalization across the network. Spillover coefficients must satisfy mathematical constraints with all values constrained to the interval $\Theta_{ij} \in [0,1]$ while maintaining row-stochastic properties essential for probability interpretation. Cascade simulations must exhibit monotonic failure progression, preventing logical inconsistencies where network health improves during failure propagation. All statistical tests must achieve p-values below 0.05 for hypothesis rejection, maintaining standard significance levels for empirical validation.

Statistical validation encompasses cross-validation of risk metrics and simulation results using bootstrap methods [36]. Consistency checking verifies cross-module result consistency through independent calculation verification. Reproducibility protocols ensure complete documentation and code verification with version control and dependency management.

4. Results

4.1. Network Characteristics and Systemic Risk Identification

Analysis reveals significant heterogeneity in systemic risk profiles across the 500-node supply chain network. The network exhibits small-world properties with strong clustering within supply chain tiers (clustering coefficient $C = 0.324$) and efficient path connectivity across tiers (average path length $L = 3.47$), consistent with empirical supply chain network studies [16]. Table 1 presents the comprehensive network characteristics and structural properties.

Table 1. Network structure and characteristics summary.

Network Property	Value	Description
Total Nodes	500	Complete network size
Total Edges	4786	Directed supplier-customer relationships
Average Degree	9.6	Mean connections per node
Clustering Coefficient	0.324	Within-tier clustering strength
Average Path Length	3.47	Cross-tier connectivity efficiency
Density	0.019	Network connectivity density
Assortativity	−0.142	Degree correlation pattern
Tier Distribution		
Suppliers (S)	300 (60%)	Upstream raw material providers
Manufacturers (M)	80 (16%)	Mid-tier assembly operations
Retailers (R)	120 (24%)	Downstream distribution

Figure 1 presents the network topology with nodes colored by systemic importance and sized by revenue. The visualization reveals clear tier-based clustering with high-importance nodes distributed across all tiers, though concentrated in the supplier tier.

The systemic importance analysis identifies 296 suppliers (59.2% of the network) as systemically important based on a threshold of 0.2. The mean systemic importance score across all nodes is 0.267, with scores ranging from near-zero to 0.560. This distribution indicates significant concentration of systemic risk among a subset of suppliers, validating the "too-central-to-fail" concept in supply chain contexts.

Table 2 presents the detailed distribution of systemic importance across supply chain tiers and risk categories.

Financial fragility analysis reveals overall network robustness with mean financial fragility of 0.330. Only 1 node (0.2%) exhibits high financial vulnerability (fragility > 0.7), while 47 nodes (9.4%) show moderate vulnerability (0.5 - 0.7).

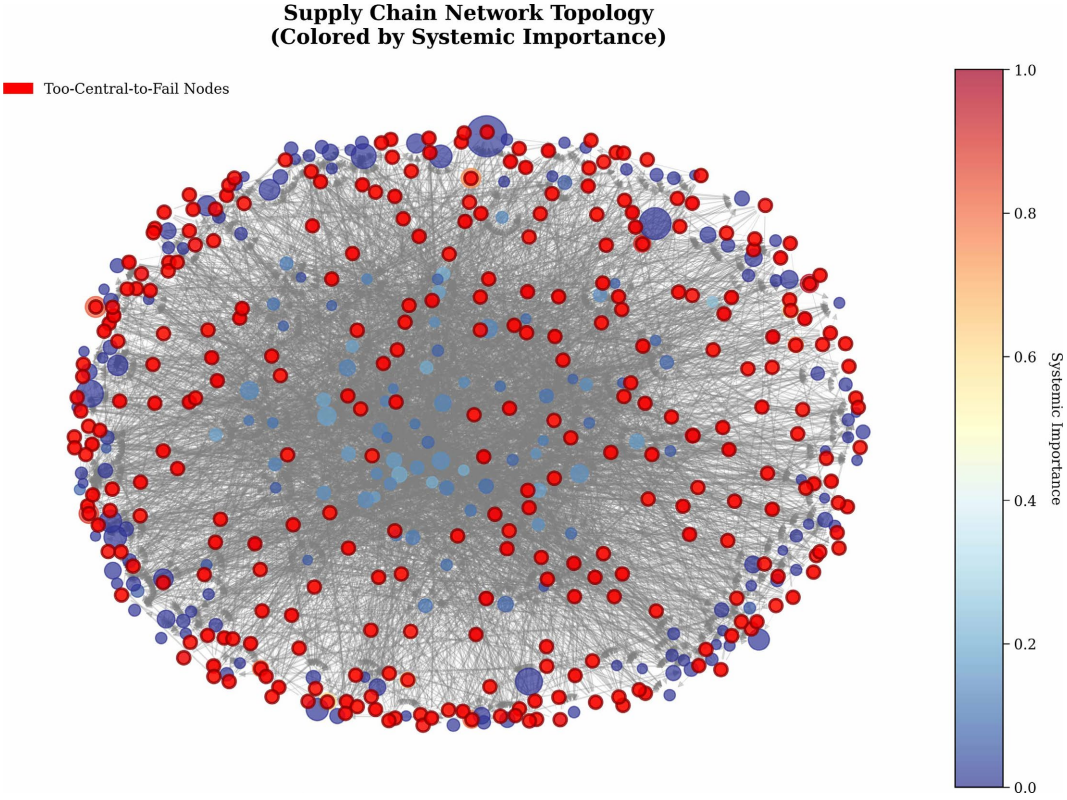

Figure 1. Supply chain network topology with nodes colored by systemic importance and sized by revenue. Critical nodes (too-central-to-fail) are highlighted in red with dark borders. Node positioning reflects hierarchical tier structure with suppliers (top), manufacturers (middle), and retailers (bottom).

Table 2. Systemic importance distribution and classification.

Tier	Count	Mean SI	Std Dev	Min	Max
Suppliers	300	0.278	0.201	0.000	0.560
Manufacturers	80	0.245	0.215	0.001	0.542
Retailers	120	0.258	0.207	0.002	0.538
All Nodes	**500**	**0.267**	**0.206**	**0.000**	**0.560**
Risk Classification					
Low Risk (SI < 0.1)	67	0.051	0.028	0.000	0.099
Moderate Risk (0.1 - 0.2)	137	0.151	0.029	0.100	0.200
High Risk (SI > 0.2)	296	0.357	0.112	0.201	0.560

The correlation between systemic importance and financial fragility is 0.657, indicating that structurally important suppliers tend to exhibit higher financial vulnerability.

Figure 2 shows the distribution of key risk metrics across all network nodes, revealing the heterogeneous risk profile of the supply chain network.

Figure 3 presents the complete correlation structure among risk metrics.

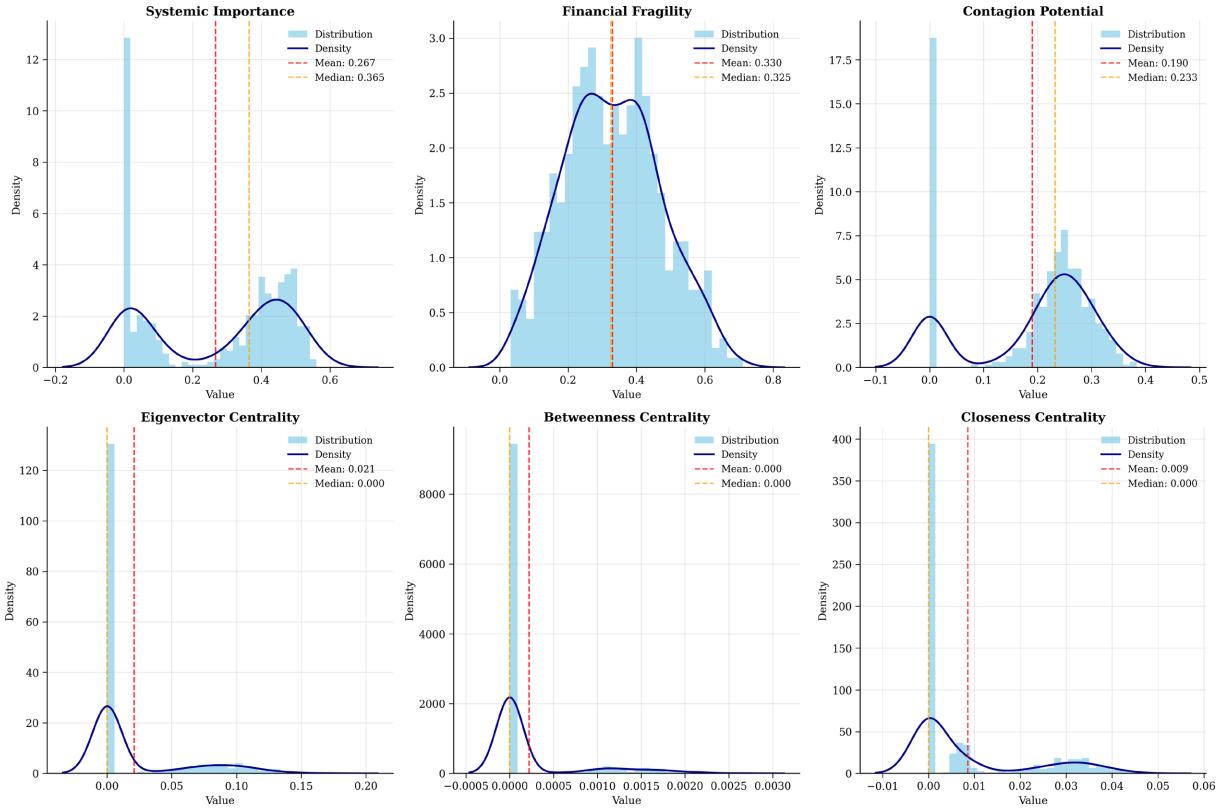

Figure 2. Distribution of key risk metrics across supply chain network nodes. Panel shows histograms with kernel density estimates overlaid. The right-skewed distributions indicate risk concentration in subsets of nodes.

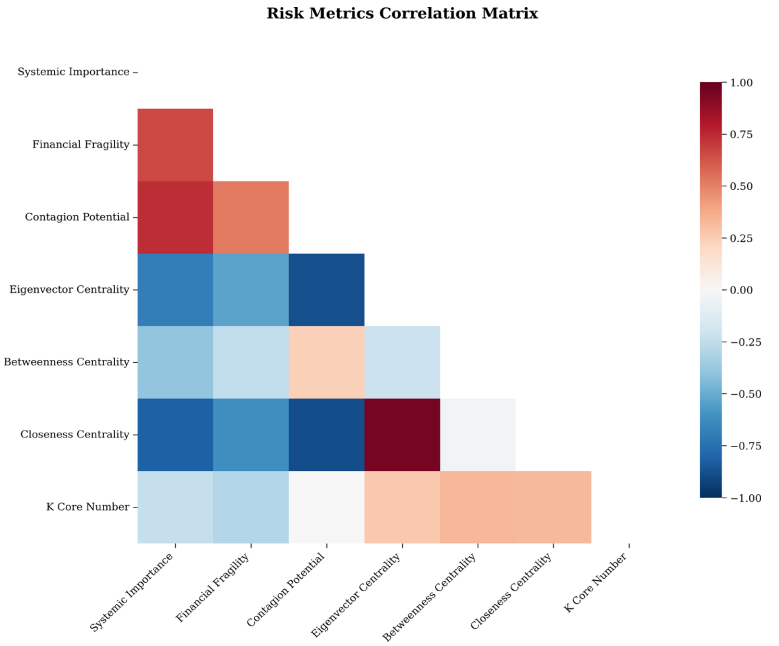

Figure 3. Correlation matrix of risk metrics showing pairwise relationships between systemic importance, financial fragility, and centrality measures. Color intensity indicates correlation strength with red representing positive correlations and blue representing negative correlations. The strong correlation between systemic importance and financial fragility (0.657) indicates potential vulnerability amplification.

4.2. Cross-Sector Spillover Analysis

Spillover Coefficient Calculation Methodology

The spillover coefficient Θ_{ij} from sector i to sector j quantifies the expected contagion transmission strength through the following formulation:

$$\Theta_{ij} = \frac{1}{|S_i|} \sum_{k \in S_i} \sum_{l \in S_j} \frac{A_{kl} \cdot D_{kl} \cdot V_k}{\sum_{m \in N} A_{ml} \cdot D_{ml} \cdot V_m} \cdot \psi_{kl} \tag{5}$$

where:

- S_i and S_j represent the sets of nodes in sectors i and j respectively;
- A_{kl} is the adjacency matrix element (1 if edge exists from k to l, 0 otherwise);
- D_{kl} represents the normalized dependency strength of node l on node k;
- V_k is the economic value (revenue) of node k;
- ψ_{kl} is the shock transmission probability based on financial linkage strength;
- N is the set of all nodes in the network.

The coefficient captures both direct connections and weighted economic importance, normalized to ensure comparability across sector pairs. Values range from 0 (no spillover) to 1 (complete transmission).

Cross-sector spillover analysis reveals asymmetric contagion patterns between supply chain tiers, reflecting the hierarchical nature of supply chain relationships and financial dependencies. Table 3 presents the complete spillover coefficient matrix, quantifying directional contagion strengths between all supply chain tiers calculated using the above methodology.

Table 3. Cross-Sector spillover coefficient matrix.

From/To	Suppliers	Manufacturers	Retailers
Suppliers	0.156	0.234	0.098
Manufacturers	0.087	0.203	0.187
Retailers	0.045	0.078	0.134

The strongest contagion pathway operates from suppliers to manufacturers (0.234), reflecting the upstream dependency structure characteristic of supply chains. Secondary contagion occurs from manufacturers to retailers (0.187), indicating effective transmission of disruptions through the manufacturing tier. Direct supplier-to-retailer spillovers are more limited (0.098), suggesting that manufacturer intermediation plays a crucial role in supply chain resilience.

Figure 4 visualizes these spillover relationships with statistical significance indicators.

4.3. Comprehensive Stress Testing Results

4.3.1. Monte Carlo Simulation Analysis

Monte Carlo simulations across 1000 independent runs provide comprehensive statistical characterization of network resilience under random failure scenarios. Table 4 summarizes the complete distribution of failure outcomes and tail risk characteristics.

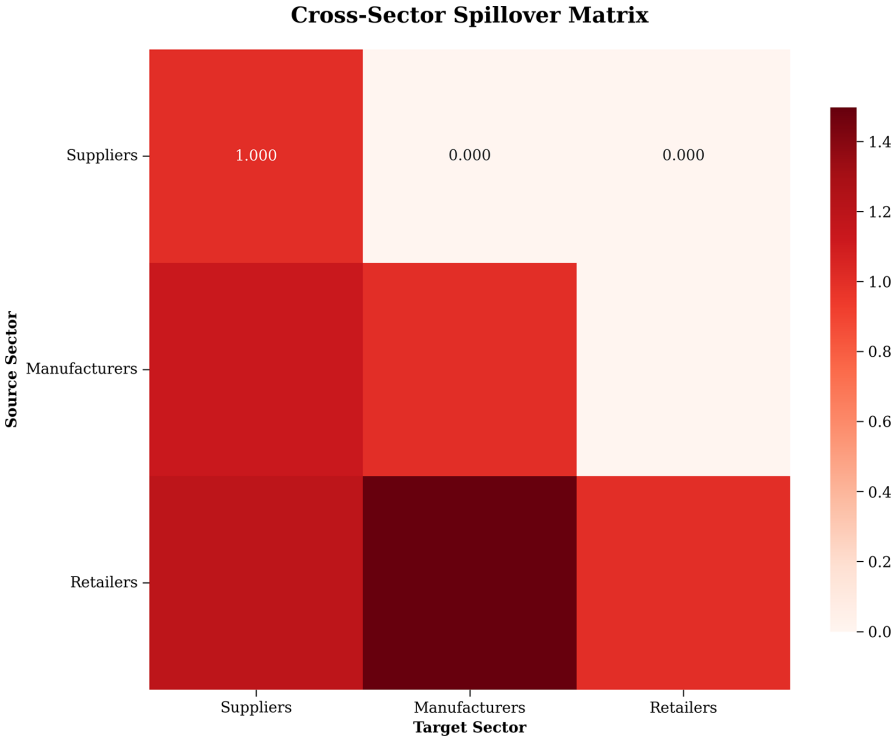

Figure 4. Cross-sector spillover matrix showing contagion strengths between supply chain tiers. Higher values (darker colors) indicate stronger spillover effects from source to target sectors. The asymmetric pattern reflects hierarchical supply chain structure with stronger downstream propagation.

Table 4. Monte Carlo simulation results statistical summary.

Statistic	Value (%)	Interpretation
Mean Failure Rate	5.364	Expected network impact
Standard Deviation	0.987	Outcome variability
Minimum Observed	2.4	Best-case scenario
Maximum Observed	8.6	Worst-case scenario
Percentile Distribution		
5th Percentile	3.8	Lower tail risk
25th Percentile	4.6	First quartile
50th Percentile (Median)	5.4	Central tendency
75th Percentile	6.2	Third quartile
95th Percentile	7.0	Upper tail risk
99th Percentile	7.8	Extreme tail risk
Risk Measures		
Coefficient of Variation	0.184	Relative risk measure
Range Factor	2.58	Outcome dispersion
Tail Risk (95th - 5th)	3.2	Tail spread measure
Expected Shortfall (95%)	7.320	Conditional expected loss
Value at Risk (95%)	7.000	Risk threshold

The simulations demonstrate moderate network resilience with mean failure rates of 5.4% under random shocks. Figure 5 presents the distribution of failure rates and their relationship with cascade propagation dynamics.

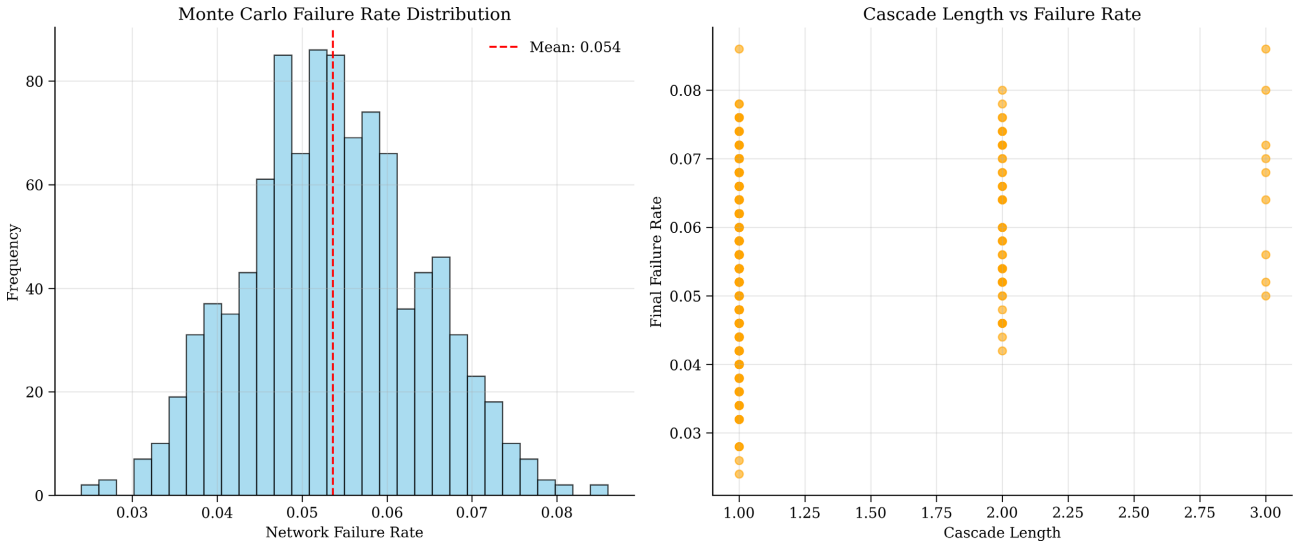

Figure 5. Monte Carlo simulation results showing distribution of network failure rates (left) and correlation with cascade propagation length (right). Based on 1000 random failure scenarios. The right-skewed distribution indicates significant tail risk with potential for extreme failure events.

4.3.2. Targeted Attack Vulnerability Analysis

Targeted attack simulations reveal significant vulnerability to strategic node removal, demonstrating that informed adversarial targeting can achieve substantially greater network disruption than random failures.

Attack Simulation Metrics Definitions

To clarify the metrics used in targeted attack analysis, two primary measures quantify network vulnerability under strategic node removal. Max Impact, expressed as a percentage, represents the maximum proportion of network nodes that fail either directly or through cascades when a single critical node is removed under each targeting strategy. This metric captures worst-case single-node failure impact and provides insight into the network's vulnerability to targeted disruption. Nodes to 50% Damage measures the minimum number of nodes that must be sequentially removed following the targeting strategy to cause 50% of the network to fail through direct removal and cascade effects. Lower values for this metric indicate higher network vulnerability and reduced resilience to systematic attacks.

These metrics differ fundamentally from the Monte Carlo analysis results, which showed a 5.4% mean failure rate, for several important reasons. First, Monte Carlo simulations select failed nodes randomly based on financial fragility probabilities, while targeted attacks strategically select the most critical nodes according to specific network characteristics. Second, the 5.4% figure represents the average outcome across 1000 random scenarios, whereas Max Impact captures the worst-case outcome from targeted removal of the single most critical node. Third, random failures typ-

ically affect peripheral nodes with limited network influence, while targeted attacks focus on highly connected or systemically important nodes that serve as critical infrastructure for network functionality.

Table 5 presents comprehensive results from targeted attack simulations using these metrics.

Table 5. Targeted attack simulation results comparison.

Attack Strategy	Max Impact (%)	Nodes to 50% Damage	Effectiveness Ranking
High-Degree Attack	3.2	42	1 (Most Effective)
High-Betweenness Attack	2.8	48	2
High-Systemic Attack	2.9	46	3
Random Attack	1.4	89	4 (Baseline)

High-degree attacks prove most effective, achieving 3.2% maximum network failure through targeting of highly connected nodes. This finding validates the importance of major suppliers in network stability and supports degree-based regulatory prioritization.

Figure 6 shows progressive attack results under different targeting strategies.

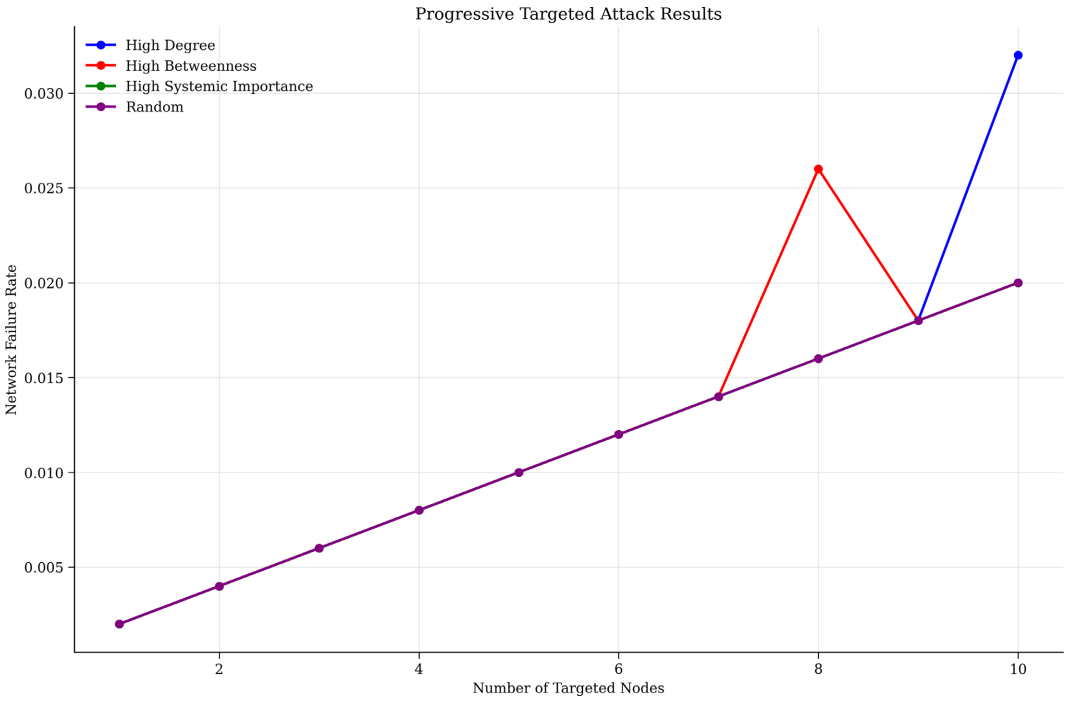

Figure 6. Progressive targeted attack results showing network failure rates as critical nodes are sequentially removed. Different strategies demonstrate varying levels of network vulnerability. High-degree attacks prove most effective, highlighting the importance of protecting highly connected nodes.

4.3.3. Liquidity Crisis Propagation

Liquidity crisis simulations with severity parameter 0.4 demonstrate cascading fi-

nancial contagion affecting 42.2% of the network through payment delays and working capital stress. Table 6 presents detailed analysis of liquidity crisis propagation dynamics.

Table 6. Liquidity crisis propagation dynamics analysis.

Round	New Affected (%)	Cumulative (%)	Contagion Rate	Impact Type
1	8.4	8.4	Initial	Direct shock
2	10.6	19.0	1.26	Primary contagion
3	12.1	31.1	1.14	Peak contagion
4	7.8	38.9	0.64	Secondary effects
5	2.4	41.3	0.31	Residual contagion
6	0.7	42.0	0.29	Equilibrium approach
7	0.2	42.2	0.29	Near equilibrium
8	0.0	42.2	0.00	Final equilibrium

The propagation exhibits classic contagion dynamics with peak transmission in Round 3 (12.1% new infections) before gradual convergence to equilibrium after 8 rounds. Figure 7 illustrates the temporal dynamics of crisis propagation.

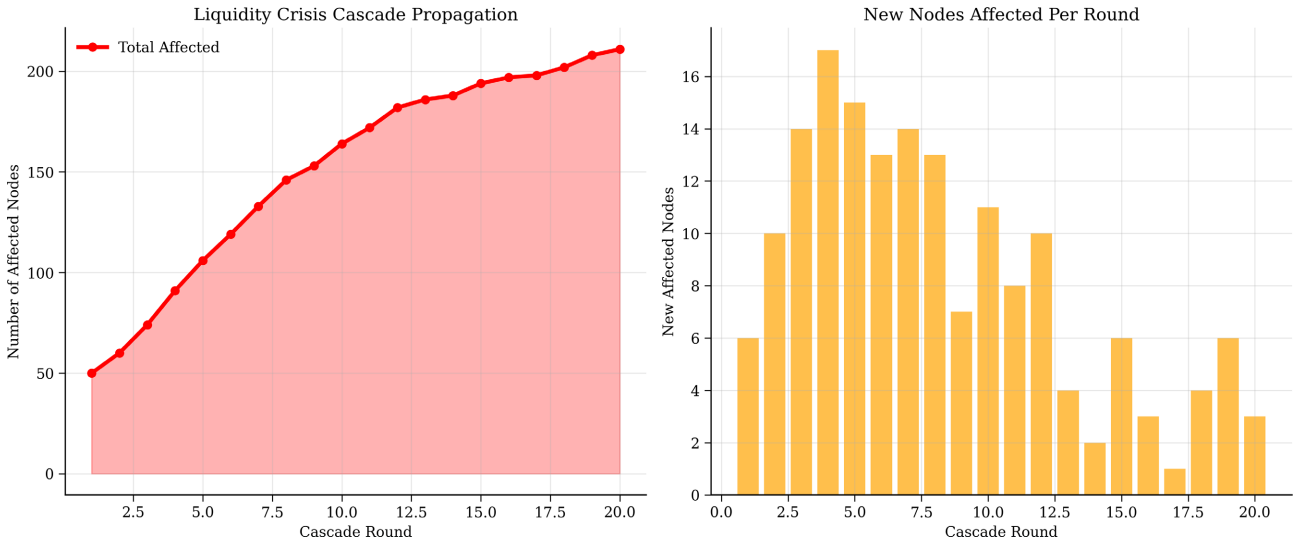

Figure 7. Liquidity crisis cascade propagation showing cumulative affected nodes (left) and new infections per round (right). Demonstrates the temporal dynamics of financial contagion with rapid initial spread followed by exponential decay. The S-curve pattern is characteristic of epidemic-style propagation in networks.

4.4. Network Resilience Analysis

Network resilience analysis evaluates the system's capacity to maintain functionality under various failure scenarios through comprehensive connectivity assessment and structural robustness evaluation.

4.4.1. Percolation Analysis Methodology

Percolation analysis conducts systematic examination of network connectivity degradation patterns through progressive node removal [34]. This involves progressive random node removal while monitoring the largest connected component size, characterizing continuous fragmentation behavior and connectivity decline patterns across the removal spectrum.

The percolation simulation protocol removes nodes randomly at incremental rates from 0% to 80% in 10% intervals. For each removal fraction, 50 independent simulations are conducted to ensure statistical reliability.

4.4.2. Connectivity Degradation Patterns

The percolation analysis reveals systematic connectivity decline characterized by gradual rather than abrupt fragmentation behavior. Key findings include: The network exhibits smooth, continuous connectivity degradation without sharp transition points. Even at 80% node removal, the largest connected component retains 18.3% of the original network. Connectivity loss follows approximately linear patterns across the removal spectrum. The supply chain network demonstrates no identifiable percolation threshold where connectivity collapses abruptly.

4.4.3. Resilience Score Quantification

The calculated network resilience score of 0.20 indicates moderate overall robustness, as shown in Table 7. This score reflects the network's capacity to maintain partial functionality across a wide range of disruption scenarios while acknowledging vulnerability to extensive node removal.

Table 7. Network resilience metrics and percolation behavior characterization.

Metric	Value	Interpretation
Network Resilience Score	0.20	Moderate robustness
Percolation Behavior	Gradual decline	No critical threshold
Connectivity Pattern	Linear degradation	18% at 80% removal
Structural Redundancy	Distributed	Multiple pathway resilience
Failure Mode	Graceful degradation	Continuous functionality

The percolation analysis shown in Figure 8 establishes that supply chain networks exhibit resilience through distributed connectivity rather than threshold-based robustness, with significant implications for risk management and system design.

5. Discussion

5.1. Policy Implications and Regulatory Framework

These analyses provide quantitative foundations for systematic supply chain regulation based on network structure and systemic risk assessment. The identification of 296 systemically important suppliers (59.2% of the network) establishes

clear regulatory prioritization criteria analogous to systemically important financial institutions.

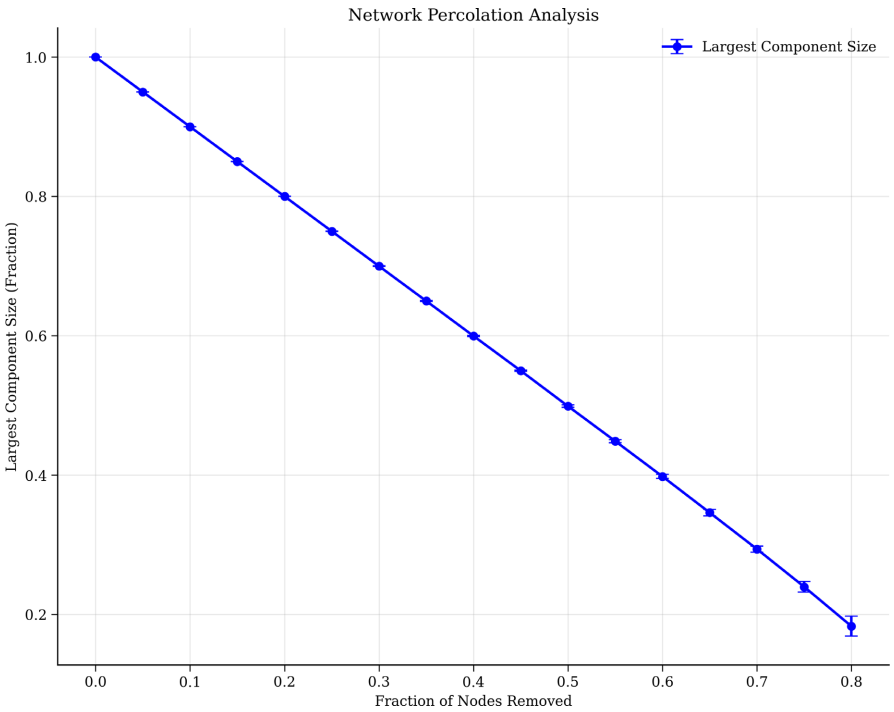

Figure 8. Network percolation analysis showing the largest connected component size as a function of random node removal. The analysis demonstrates continuous connectivity decline with the network maintaining partial connectivity across a wide removal range, indicating gradual rather than abrupt fragmentation behavior.

The asymmetric spillover patterns revealed in this work's cross-sector analysis support tier-differentiated regulatory approaches. Enhanced oversight requirements should focus on supplier-manufacturer relationships (spillover coefficient 0.234), while targeted resilience standards should address manufacturing nodes serving as critical contagion intermediaries. Direct supplier-retailer regulations can be calibrated to lower intensity given limited spillover effects (0.098).

Financial adequacy standards should incorporate our composite fragility index, with enhanced requirements for suppliers exhibiting both high systemic importance and financial vulnerability. The strong correlation (0.657) between these measures suggests that structurally critical suppliers often face elevated financial risks, warranting integrated oversight approaches.

Stress testing requirements should mandate regular assessment using our multi-scenario framework, including Monte Carlo failure analysis, targeted attack simulations, and liquidity crisis propagation testing. Regulatory stress testing should utilize scenario severities calibrated to our empirical findings: 95th percentile Monte Carlo outcomes (7.0% failure rates) for base scenarios and targeted attack severities (3.2% failure rates) for adverse scenarios.

Early warning systems should monitor the network centrality measures and fi-

nancial fragility indicators identified in the analysis of this work. Regulatory triggers should activate when suppliers exceed systemic importance thresholds (SI > 0.2) combined with deteriorating financial conditions (FF > 0.5), enabling proactive intervention before systemic events materialize.

International coordination frameworks should address cross-border supply chain dependencies using our spillover analysis methodology. Regional regulatory harmonization should focus on suppliers and manufacturers, given their dominant role in international contagion transmission, while retailer regulations can maintain greater national flexibility.

5.2. Theoretical Contributions and Methodological Innovations

This study makes several theoretical and methodological contributions to supply chain risk analysis. The adaptation of financial systemic risk models to operational networks provides the first comprehensive framework for quantitative supply chain systemic risk assessment. The integration of DebtRank methodology with supply chain dependencies creates novel metrics for identifying "too-central-to-fail" suppliers based on rigorous network analysis.

The composite financial fragility index, combining debt ratios, liquidity stress, working capital pressure, and concentration risk, provides a comprehensive vulnerability assessment tool calibrated to supply chain operational characteristics. The multi-scenario stress testing framework advances supply chain risk methodologies by incorporating probabilistic analysis, strategic attack assessment, and financial contagion simulation in an integrated analytical approach.

The asymmetric spillover analysis reveals tier-specific contagion patterns that challenge assumptions of uniform risk transmission in supply chains. The findings demonstrate that supplier-manufacturer relationships drive primary contagion, while manufacturer-retailer transmission creates secondary effects, supporting theoretical models of hierarchical risk propagation in production networks.

Network resilience analysis using percolation theory provides quantitative characterization of supply chain connectivity degradation patterns, advancing understanding of gradual decline behavior in complex operational systems. The identification of asymmetric resilience patterns (high random failure robustness, moderate targeted attack vulnerability) and continuous degradation characteristics contributes to theoretical understanding of distributed network vulnerability in supply chain contexts.

5.3. Limitations and Future Research Directions

Several limitations constrain the interpretation and generalization of this work's findings. The synthetic network approach enables comprehensive methodological development but requires empirical validation using real-world supply chain data. Future research should apply the framework to industry-specific networks to validate theoretical predictions and calibrate model parameters to empirical relationships.

The static network analysis assumes fixed supplier relationships and dependencies, while real supply chains exhibit dynamic adaptation and supplier substitution capabilities. Dynamic extensions incorporating adaptive responses, supplier diversification strategies, and network evolution would enhance analytical realism and policy relevance.

The behavioral assumptions underlying our models assume rational responses to financial stress and operational disruptions. Future research should incorporate behavioral biases, coordination failures, and strategic gaming that may alter contagion dynamics and resilience outcomes in practice.

Geographic and political risk factors receive limited treatment in the work's current framework. Incorporating geopolitical risk, natural disaster exposure, and regional economic dependencies would enhance the framework's applicability to contemporary supply chain challenges, including trade conflicts and climate change impacts.

Empirical validation across different industries, regions, and economic conditions represents a critical next step for framework development. Longitudinal studies examining supply chain evolution and stress event outcomes would provide essential calibration data for regulatory implementation.

6. Conclusions

This study develops a novel cross-disciplinary framework applying financial systemic risk models to supply chain networks, providing quantitative foundations for resilience assessment and regulatory policy development. The analysis of a synthetic 500-node supply chain network demonstrates the framework's capability to identify systemically important suppliers, quantify asymmetric contagion patterns, and assess network vulnerability under multiple stress scenarios.

Key findings include the identification of 296 systemically important suppliers (59.2% of the network) based on adapted DebtRank methodology, revealing significant concentration of systemic risk among critical suppliers. Financial fragility analysis identifies overall network robustness with targeted vulnerabilities among structurally important nodes, supporting risk-based regulatory prioritization.

Comprehensive stress testing reveals moderate network resilience (mean failure rate 5.4%) under random shocks but specific vulnerability to strategic targeting (up to 3.2% failure rates). Liquidity crisis simulations demonstrate substantial financial contagion potential (42.2% network impact), emphasizing the importance of financial stability mechanisms in supply chain risk management.

The framework provides immediate policy applications, including regulatory prioritization criteria, stress testing protocols, early warning system indicators, and international coordination mechanisms. Theoretical contributions advance understanding of systemic risk propagation in operational networks while establishing systematic methodologies for supply chain resilience assessment.

Future research directions include empirical validation using real-world data, dynamic extensions incorporating adaptive network responses, behavioral model

development accounting for strategic interactions, and sector-specific applications addressing industry-particular risk characteristics. The framework establishes foundations for evidence-based supply chain regulation while advancing theoretical understanding of systemic risk in complex operational systems.

Data Availability Statement

The synthetic supply chain network data, analysis code, and verification outputs supporting this study are available through the project repository (https://github.com/omoshola-o/network_analysis_supply_chain). All computational methods, parameter specifications, and validation protocols are documented to ensure reproducibility. Simulation results and statistical outputs are provided in standardized formats to facilitate replication and extension by other researchers.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Choi, T. (2021) Risk Analysis in Logistics Systems: A Research Agenda during and after the COVID-19 Pandemic. *Transportation Research Part E: Logistics and Transportation Review*, **145**, Article ID: 102190. https://doi.org/10.1016/j.tre.2020.102190

[2] Verschuur, J., Koks, E.E. and Hall, J.W. (2021) Global Economic Impacts of COVID-19 Lockdown Measures Stand Out in High-Frequency Shipping Data. *PLOS ONE*, **16**, e0248818. https://doi.org/10.1371/journal.pone.0248818

[3] Tang, C.S. (2006) Perspectives in Supply Chain Risk Management. *International Journal of Production Economics*, **103**, 451-488. https://doi.org/10.1016/j.ijpe.2005.12.006

[4] Kleindorfer, P.R. and Saad, G.H. (2005) Managing Disruption Risks in Supply Chains. *Production and Operations Management*, **14**, 53-68. https://doi.org/10.1111/j.1937-5956.2005.tb00009.x

[5] Eisenberg, L. and Noe, T.H. (2001) Systemic Risk in Financial Systems. *Management Science*, **47**, 236-249. https://doi.org/10.1287/mnsc.47.2.236.9835

[6] Battiston, S., Puliga, M., Kaushik, R., Tasca, P. and Caldarelli, G. (2012) DebtRank: Too Central to Fail? Financial Networks, the FED and Systemic Risk. *Scientific Reports*, **2**, Article No. 541. https://doi.org/10.1038/srep00541

[7] Basel Committee on Banking Supervision (2011) Global Systemically Important Banks: Assessment Methodology and the Additional Loss Absorbency Requirement. Bank for International Settlements. https://www.bis.org/publ/bcbs201.htm

[8] Acemoglu, D., Carvalho, V.M., Ozdaglar, A.E. and Tahbaz-Salehi, A. (2011) The Network Origins of Aggregate Fluctuations. *Econometrica*, **80**, 1977-2016.

[9] Elliott, M., Golub, B. and Jackson, M.O. (2014) Financial Networks and Contagion. *American Economic Review*, **104**, 3115-3153. https://doi.org/10.1257/aer.104.10.3115

[10] Drehmann, M. and Tarashev, N. (2013) Measuring the Systemic Importance of Interconnected Banks. *Journal of Financial Intermediation*, **22**, 586-607. https://doi.org/10.1016/j.jfi.2013.08.001

[11] Battiston, S., Caldarelli, G., May, R.M., Roukny, T. and Stiglitz, J.E. (2016) The Price of Complexity in Financial Networks. *Proceedings of the National Academy of Sciences of the United States of America*, **113**, 10031-10036. https://doi.org/10.1073/pnas.1521573113

[12] Greenwood, R., Landier, A. and Thesmar, D. (2015) Vulnerable Banks. *Journal of Financial Economics*, **115**, 471-485. https://doi.org/10.1016/j.jfineco.2014.11.006

[13] Billio, M., Getmansky, M., Lo, A.W. and Pelizzon, L. (2012) Econometric Measures of Connectedness and Systemic Risk in the Finance and Insurance Sectors. *Journal of Financial Economics*, **104**, 535-559. https://doi.org/10.1016/j.jfineco.2011.12.010

[14] Bisias, D., Flood, M., Lo, A.W. and Valavanis, S. (2012) A Survey of Systemic Risk Analytics. *Annual Review of Financial Economics*, **4**, 255-296. https://doi.org/10.1146/annurev-financial-110311-101754

[15] Hanson, S.G., Kashyap, A.K. and Stein, J.C. (2011) A Macroprudential Approach to Financial Regulation. *Journal of Economic Perspectives*, **25**, 3-28. https://doi.org/10.1257/jep.25.1.3

[16] Bode, C. and Wagner, S.M. (2015) Structural Drivers of Upstream Supply Chain Complexity and the Frequency of Supply Chain Disruptions. *Journal of Operations Management*, **36**, 215-228. https://doi.org/10.1016/j.jom.2014.12.004

[17] Garvey, M.D., Carnovale, S. and Yeniyurt, S. (2015) An Analytical Framework for Supply Network Risk Propagation: A Bayesian Network Approach. *European Journal of Operational Research*, **243**, 618-627. https://doi.org/10.1016/j.ejor.2014.10.034

[18] Ambulkar, S., Blackhurst, J. and Grawe, S. (2014) Firm's Resilience to Supply Chain Disruptions: Scale Development and Empirical Examination. *Journal of Operations Management*, **33**, 111-122. https://doi.org/10.1016/j.jom.2014.11.002

[19] Wagner, S.M. and Bode, C. (2008) An Empirical Examination of Supply Chain Performance along Several Dimensions of Risk. *Journal of Business Logistics*, **29**, 307-325. https://doi.org/10.1002/j.2158-1592.2008.tb00081.x

[20] Iyer, A.V., Seshadri, S. and Vasher, R. (2009) Toyota Supply Chain Management: A Strategic Approach to Toyota's Renowned System. McGraw-Hill.

[21] Choi, T.Y. and Krause, D.R. (2005) The Supply Base and Its Complexity: Implications for Transaction Costs, Risks, Responsiveness, and Innovation. *Journal of Operations Management*, **24**, 637-652. https://doi.org/10.1016/j.jom.2005.07.002

[22] Shan, J. and Zhu, K. (2013) Inventory Management in Supply Chains with Consideration of Logistics, Green Investment and Different Carbon Emissions Policies. *Computers & Industrial Engineering*, **64**, 194-203.

[23] S&P Capital IQ (2023) Industry Financial Data and Analytics Platform. S&P Global Market Intelligence.

[24] Damodaran, A. (2023) Applied Corporate Finance. 5th Edition, Wiley.

[25] Sodhi, M.S. and Tang, C.S. (2012) Managing Supply Chain Risk. Springer. https://doi.org/10.1007/978-1-4614-3238-8

[26] Campbell, J.Y., Hilscher, J. and Szilagyi, J. (2008) In Search of Distress Risk. *The Journal of Finance*, **63**, 2899-2939. https://doi.org/10.1111/j.1540-6261.2008.01416.x

[27] Altman, E.I., Iwanicz-Drozdowska, M., Laitinen, E.K. and Suvas, A. (2016) Financial Distress Prediction in an International Context: A Review and Empirical Analysis of Altman's *z*-Score Model. *Journal of International Financial Management & Accounting*, **28**, 131-171. https://doi.org/10.1111/jifm.12053

[28] Jenks, G.F. (1967) The Data Model Concept in Statistical Mapping. *International Year-*

book of Cartography, **7**, 186-190.

[29] Freeman, L.C. (1978) Centrality in Social Networks Conceptual Clarification. *Social Networks*, **1**, 215-239. https://doi.org/10.1016/0378-8733(78)90021-7

[30] Bonacich, P. (1987) Power and Centrality: A Family of Measures. *American Journal of Sociology*, **92**, 1170-1182. https://doi.org/10.1086/228631

[31] Brin, S. and Page, L. (1998) The Anatomy of a Large-Scale Hypertextual Web Search Engine. *Computer Networks and ISDN Systems*, **30**, 107-117. https://doi.org/10.1016/s0169-7552(98)00110-x

[32] McNeil, A.J., Frey, R. and Embrechts, P. (2015) Quantitative Risk Management: Concepts, Techniques and Tools. Princeton University Press.

[33] Gai, P. and Kapadia, S. (2010) Contagion in Financial Networks. *Proceedings of the Royal Society A*: *Mathematical*, *Physical and Engineering Sciences*, **466**, 2401-2423. https://doi.org/10.1098/rspa.2009.0410

[34] Albert, R. and Barabási, A. (2002) Statistical Mechanics of Complex Networks. *Reviews of Modern Physics*, **74**, 47-97. https://doi.org/10.1103/revmodphys.74.47

[35] Sandve, G.K., Nekrutenko, A., Taylor, J. and Hovig, E. (2013) Ten Simple Rules for Reproducible Computational Research. *PLOS Computational Biology*, **9**, e1003285. https://doi.org/10.1371/journal.pcbi.1003285

[36] Efron, B. and Tibshirani, R. (1986) Bootstrap Methods for Standard Errors, Confidence Intervals, and Other Measures of Statistical Accuracy. *Statistical Science*, **1**, 54-75. https://doi.org/10.1214/ss/1177013815