University of Kent

Kent Academic Repository

Fu, Xiuwen, Tian, Mengyao, Liu, Xiangwei, Wu, Shaomin and Peng, Rui (2025) ***Systematic review and future perspectives on cascading failures in supply chains: modeling and optimization.*** **Reliability Engineering and System Safety, 270 . ISSN 0951-8320.**

Downloaded from

https://kar.kent.ac.uk/112489/ The University of Kent's Academic Repository KAR

The version of record is available from

https://doi.org/10.1016/j.ress.2025.112150

This document version

Author's Accepted Manuscript

DOI for this version

Licence for this version

CC BY (Attribution)

Additional information

For the purpose of open access, the author(s) has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in ***Title of Journal*** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).

Systematic Review and Future Perspectives on Cascading Failures in Supply Chains: Modeling and Optimization

Xiuwen Fu[a], Mengyao Tian[a], Xiangwei Liu[a], Shaomin Wu[b], Rui Peng[c,*]

[a]*Logistics Engineering College, Shanghai Maritime University, Shanghai, 201306, China*
[b]*Kent Business School, University of Kent, Canterbury, Kent CT2 7FS, UK*
[c]*School of Economics and Management, Beijing University of Technology, Beijing, 100124, China*

Abstract

Under the impact of cascading failures, the failure of a small number of nodes in a supply chain network can trigger a chain reaction, leading to the impairment or even collapse of the entire supply chain system. Cascading failures have become a critical bottleneck affecting the stability and reliability of supply chains, attracting widespread attention from researchers. To better understand the complex mechanisms of cascading failures in supply chains, this paper systematically reviews the current research progress, covering network metrics, failure triggering factors, modeling methods, and optimization strategies. Finally, the paper highlights the challenges in network coupling, model realism, recovery optimization, and risk prediction in existing research, and proposes future research directions to provide theoretical support and decision-making guidance for mitigating cascading failures in supply chains.

Keywords: supply chain; cascading failure; modeling methods; system optimization

1. Introduction

The supply chain concept, linking raw material suppliers to end consumers, emerged in the 1960s. J.W. Forrester, the founder of system dynamics, introduced a systematic analytical framework for the supply chain in *Industrial Dynamics* (1961)[1]. He analyzed feedback mechanisms and dynamic behaviors across supply chain stages, arguing that the supply chain is a dynamic system of interconnected business segments, driven by the flow of information and materials. In 1982, R. K. Oliver and M. D. Webber coined the term "Supply Chain Management"[2], emphasizing that the supply chain is a cross-enterprise network covering raw material acquisition, production, distribution, and delivery to end consumers.

In complex systems, cascading failure denotes a chain reaction in which local disturbances, such as external shocks, internal malfunctions, or systemic risk factors, cause certain nodes or edges to fail and spread through the network, resulting in large-scale functional disruptions [3]. From a risk perspective, the Society for Risk Analysis (SRA) defines risk as the potential for adverse consequences of future activities under uncertainty [4]; thus, the propagation of risk factors can be regarded as a manifestation of cascading failure. At the system level, cascading failure reflects the dynamic process whereby local disturbances diffuse along functional paths under structural coupling. Such failures are widespread in transportation, power grids, and communication networks, and supply chain networks share comparable vulnerabilities, making cascading failure a critical topic in stability research.

With the development of global trade and the integration of emerging technologies into traditional supply chain models, business relationships within supply chains have become increasingly interconnected. Unlike traditional linear supply chains characterized by simple enterprise

*Corresponding author: Rui Peng, pengrui1988@bjut.edu.cn

relationships and clear information flows, modern supply chains have progressively evolved into complex systems involving multiple actors across national boundaries. The application of new technologies—such as the Internet of Things, artificial intelligence, and blockchain—has enhanced information exchange between nodes, shifting enterprise interactions beyond purely upstream–downstream relationships toward horizontally collaborative, more tightly coupled many-to-many network structures. As a result, the overall supply chain exhibits high connectivity and multi-path characteristics. In this process, the supply chain system has also evolved into a structurally diverse and operationally flexible networked system. The dynamic nature of these networks, combined with the strong interdependence among their members[5], suggests that any disruption in one part of the network can quickly spread to other businesses, potentially causing a collapse of the entire system[6]. This failure, referred to as the 'avalanche effect,' is known as cascading failures[7]. Cascading failures occur when certain nodes or links in a network fail. Due to the interdependence between nodes, a failure can propagate triggering a chain reaction that ultimately impacts the entire network and may lead to system collapse. Supply chain disruptions are a typical example. In this context, cascading failures often begin with problems in one part of the chain, causing other parts to malfunction. In extreme cases, it can paralyze the entire system. A notable example is the significant production loss experienced by semiconductor manufacturers after Typhoon Maria's impact on Taiwan in 2018[8], which caused chip shortages and production shutdowns at global automotive manufacturers.

Given the significant threat cascading failures posed to supply chains, substantial research has focused on modeling, analyzing, and optimizing resilience, achieving notable progress. However, there is a lack of comprehensive reviews on cascading failures, with limited summaries and comparisons available. This gap hinders the progress of future research. Therefore, this paper aims to summarize existing research on cascading failures, highlight the latest theories and methods, identify current challenges, and propose future research directions, providing valuable references for related fields. Specifically, this study develops a structured classification framework encompassing application scenarios, network topologies, failure causes, and optimization strategies, thereby enabling systematic comparisons across studies and providing a unified foundation for future research.

The structure of the remainder of the paper is as follows: Section 2 presents an overview of supply chain cascading failure research; Section 3 discusses failure causes; Section 4 focuses on network modeling; Section 5 explores cascading failure modeling; Section 6 discusses optimization strategies; Section 7 outlines challenges and future prospects; Section 8 concludes the paper.

2. Research Overview of in Supply Chains

This section presents network capacities related to supply chain cascading failures, followed by an introduction to tools and methods used for data collection. It subsequently provides an overview of research on supply chain cascading failures.

2.1. System capacities in supply chain cascading failures

This section introduces the system capacities of supply chains under cascading failure scenarios, including the capacities to withstand, recover, cope, and persist, as well as their manifestations within supply chain systems.

1) Capacity to withstand (currently called robustness): refers to the ability of a network to resist risks, maintain its core functions, and avoid immediate collapse when subjected to disruptions. In the context of supply chain cascading failures, robustness reflects the extent to which the system can effectively isolate local failures and prevent them from spreading across the network. A high level of robustness typically arises from redundancy,

connectivity, fault tolerance, balanced node distribution, and local shock resistance, manifested in multiple supply sources or backup routes, flexible production or alternative designs, and temporary inventory or emergency capacity. Accordingly, robustness can be quantitatively assessed using metrics such as network connectivity, node survival rate, and topological entropy.

2) Capacity to recover (currently called resilience): originates from the Latin word *resilio* (meaning "to bounce back" or "to recover"), and refers to the ability of a system to maintain or rapidly restore its normal functional level through adaptation, recovery, or adjustment after experiencing external shocks. More precisely, resilience represents a composite capacity encompassing both maintenance and recovery. Unlike robustness, which emphasizes functional stability during disruptions, resilience focuses on restoring and sustaining core functions through rapid responses and structural adjustments after the system has been affected. In the context of supply chain cascading failures, resilience reflects the system's capability to adapt, recover, and reconstruct following disturbances or interruptions. A high level of resilience typically arises from flexibility, responsiveness, and adaptability—manifested in resource reallocation, multi-path sourcing, production line switching, and rapid processing or scheduling adjustments. Accordingly, resilience can be quantitatively assessed using metrics such as recovery time, node recovery ratio, and post-disruption operational efficiency.

3) Capacity to cope (currently called vulnerability): refers to the degree to which a network is prone to collapse due to failures or errors. In the context of supply chain cascading failures, vulnerability emphasizes the network's sensitivity to risk-induced damage and its limited capacity to cope with shocks—when key nodes or links are disrupted, local disturbances may quickly evolve into a system-wide collapse [9]. Jüttner equates supply chain risk with vulnerability [10], while Peck defines it as "the destruction caused by internal and external risks within the supply chain" [11], and Svensson [12] defines it as "random disturbances that may cause deviations between supply and planned schedules." From a network structural perspective, vulnerability often arises from bottleneck dependence and limited substitutability. When resources or flows are overly concentrated on a few nodes or paths, a single-point failure can trigger system-wide cascading collapses. Therefore, low redundancy, high load concentration, and strong coupling among key nodes significantly increase system vulnerability. Vulnerability can be quantitatively assessed using metrics such as variations in the size of the largest connected component and the proportion of cut points.

4) Capacity to persist (currently called reliability): refers to the ability of a network to continuously perform its designated functions under specific conditions and within a defined period, emphasizing the system's stable operation over the long term. In the context of supply chain cascading failures, reliability reflects the system's capability to consistently meet predefined standards and demands while efficiently delivering products and services over time. A high level of reliability typically arises from well-designed redundancy, rapid fault-recovery mechanisms, and flexible adaptability. Therefore, reliability can be regarded as an integrative capacity that embodies the system's ability to withstand, recover, and cope, representing the comprehensive capability for long-term stability and persistence in supply chain systems.

2.2. Data collection tools and sources

This study primarily retrieved literature from the Web of Science (WoS) Core Collection and Scopus databases, supplemented by Google Scholar to capture potentially relevant studies not

indexed in the aforementioned databases. The search results indicate that the earliest research in this field dates back to 2013, when Geng et al. published an article titled *Research on Self-Organization in Resilient Recovery of Cluster Supply Chains* in journal *Discrete Dynamics in Nature and Society*, which examined the self-organizing characteristics and cascading failure recovery of cluster supply chains [13]. Accordingly, the literature retrieval period for this section spans from 2013 to 2026, aiming to provide a comprehensive overview of the evolution of supply chain cascading failure research over the past 13 years. Given that the term "cascading failures" appears in the literature in two forms—"cascading failures" and "cascade failures"—we conducted searches using both "cascading failures & supply chain" and "cascade failures & supply chain," and further expanded the search to related topics such as "failure propagation & supply chain," "ripple effect & supply chain," and "risk diffusion & supply chain." After removing obviously irrelevant and duplicate studies, a total of 113 articles were included.

2.3. Analysis of current research hotspots

Using keyword clustering methods, this study employs VoSviewer software to identify and visualize research directions in cascading failures in supply chains, as shown in Figure 1. Existing research in this field can be classified into three categories: empirical analysis, modeling and failure mechanisms, and prevention and restoration.

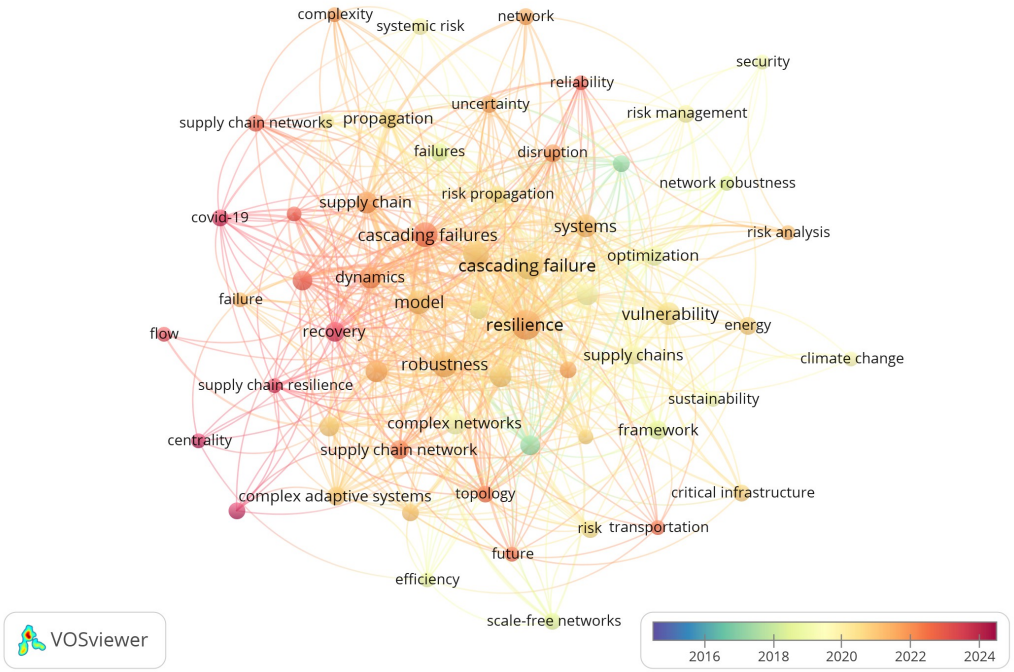


Figure 1: Keywords co-occurrence timeline spectrum

1) In empirical analysis, researchers explore basic concepts and principles of cascading failures, often using qualitative methods or economic perspectives to construct theoretical frameworks and identify key phenomena.

2) In modeling and failure mechanisms, researchers develop supply chain network models to analyze the influence of network features on failure propagation. Key focuses include the role of topological characteristics in triggering and spreading failures, and the use of dynamic network models to study failure evolution.

3) In prevention and restoration, researchers employ data analysis and simulation techniques to optimize failure models and propose targeted strategies. Common approaches include identifying and protecting critical nodes or enhancing redundancy to reduce system risks. Additionally, dynamic recovery strategies, such as resource reallocation, network adjustments, and real-time monitoring, aim to restore normal supply chain operations after failures.

3. Causes of Cascading Failures in Supply Chains

Supply chain failures often start from small disturbances in specific links, which can propagate and cause cascading failures, potentially collapsing the entire system. Given the multiple stages in supply chains, such as procurement, manufacturing, logistics, sales, and after-sales, risks at any stage can trigger cascading failures. Based on a comprehensive review of the existing literature on cascading failures in supply chains, this section synthesizes the main causes, including internal failures, sudden events, and external attacks (see Figure 2), covering the types most frequently discussed in the field.

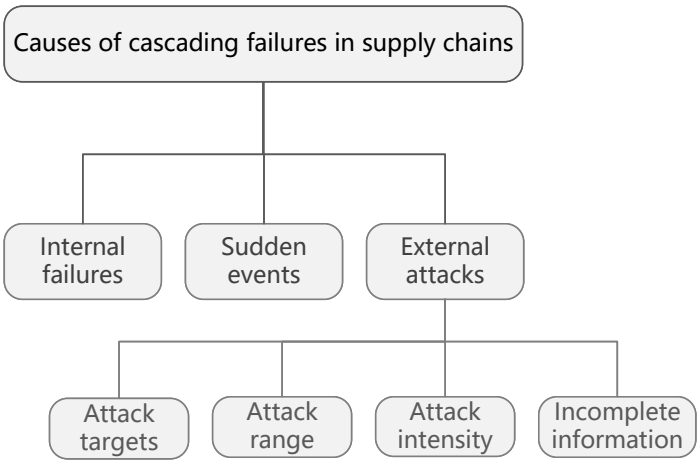


Figure 2: Causes of cascading failures in supply chains

3.1. Internal failures

Internal failures triggering cascading disruptions in the supply chain often stem from network design flaws or operational errors. When an initial disruption occurs and the network cannot absorb or recover from it, cascading failures may spread, causing widespread damage. In supply chains, the logistics and distribution segments are particularly vulnerable, as logistics service providers maintain complex relationships with multiple coordinators who consolidate upstream logistics to meet downstream demands, forming a multi-layered network that is difficult to coordinate. This network is susceptible to market pressure and transportation failures, leading to delays, rerouting, or service disruptions that may cause breakdowns. If the dispatch center fails or operational fault tolerance is insufficient, and the logistics network lacks redundancy and backup measures, the entire system may collapse, ultimately bringing down the supply chain.

3.2. Sudden events

As a complex social network, supply chains are exposed to potential threats from events like natural disasters, public health crises, economic downturns, political instability, regulatory

shifts, and human-made disruptions. These global events challenge societal resilience and increase in scope and severity. The 2011 Japan earthquake and tsunami damaged local factories and infrastructure, halting semiconductor production and triggering a global materials shortage for electronics[14]. In 2021, the grounding of the *EverGiven* container ship in the Suez Canal blocked the waterway, disrupting production schedules for energy and manufacturing companies[15]. Since 2019, COVID-19 has posed serious challenges to regional supply chains in China. These events expose the vulnerabilities of supply chains to unexpected disruptions.

3.3. External attacks

Deliberate attacks that trigger cascading failures are common in corporate competition and military logistics. Due to the complexity of cascading failures and data limitations, most supply chain studies simulate external disruptions by attacking nodes or edges in a network model. In existing studies, the most commonly used method for triggering failures is to attack nodes in the network from different dimensions based on specific strategies. From a mechanistic perspective, the formulation of these attack strategies primarily involves four key factors: attack target, attack scope, attack intensity, and attack perspective.

3.3.1. Attack targets

The attack target refers to the entity selected by an attacker when launching an attack in the context of supply chain cascading failures. These targets typically include enterprises or logistic routes, corresponding to network nodes and edges. Since supply chain participants play different roles with varying importance, selecting attack targets requires considering their attributes. Common strategies include node-degree-based and edge-weight-based attacks. A node-degree-based attack selectively disrupts nodes based on their degree values. The degree represents the number of edges connecting a node to others. Higher-degree nodes are more crucial in network topology, so their failure disproportionately impacts connectivity and stability. In contrast, an edge-weight-based attack targets the weights of edges between nodes. Edge weight reflects traffic volume or interaction intensity. In supply chains, it is often linked to transaction volume, transportation costs, or information flow frequency. Higher weights indicate stronger interactions or more frequent resource flows. The failure of high-weight edges can severely disrupt resource flow, weakening network connectivity and operational efficiency.

3.3.2. Attack range

The attack range refers to the scope of targets selected by the attacker in a single network attack, typically categorized into single-point and multi-point attacks. In single-point attacks, researchers sequentially select nodes for attack and observe the network's changes, without needing to consider target selection, often to explore the impact of modeling parameters on cascading resilience. A multi-point attack removes multiple nodes at once, evaluating the overall impact of different attack strategies on network failure. Tang et al.[16] employed three node removal methods based on node degree (from largest to smallest, smallest to largest, and random) and analyzed cascading failures in supply chains under single-node and multi-node attack scenarios. While current research mainly focuses on single-stage attack models, recent studies have explored sequential attacks. A sequential attack involves staged attacks, with the attacker adjusting the strategy based on the network's state. Zhang et al.[17] proposed a reinforcement learning-based sequential attack strategy to study cascading failures in supply chains and compared it with traditional sequential attack methods.

3.3.3. Attack intensity

Attack intensity describes the extent of damage to target nodes or edges in external attack–induced failures, differing from attack scope, which concerns the number of targets. It can range from complete functional removal to partial capacity reduction or decreased edge

transmission. In supply chain cascading failures, it reflects constraints on attributes such as production capacity, inventory, or logistics path load-bearing capability. Higher intensity accelerates large-scale failures and collapse, while lower intensity leads to gradual performance degradation. Modeling approaches typically adopt binary processing (normal/failed), graded degradation (proportional loss of function), or dynamic attenuation (time-varying impact with possible recovery). Whether node states are reversible also shapes resilience. Thus, attack intensity influences both the initial damage and the subsequent failure propagation and recovery. Wu et al.[18] examined cascading failure risks in global supply networks from static and dynamic perspectives, modeling attack intensity through varying node capacity reductions. Luo et al.[19] developed a hierarchical supply chain network to study how disturbance intensity shapes failure diffusion paths and inter-layer transmission. Habibi et al.[20] investigated the effects of disturbance intensity and diffusion patterns on propagation paths and resilience, focusing on cross- and intra-layer connections.

3.3.4. Incomplete information

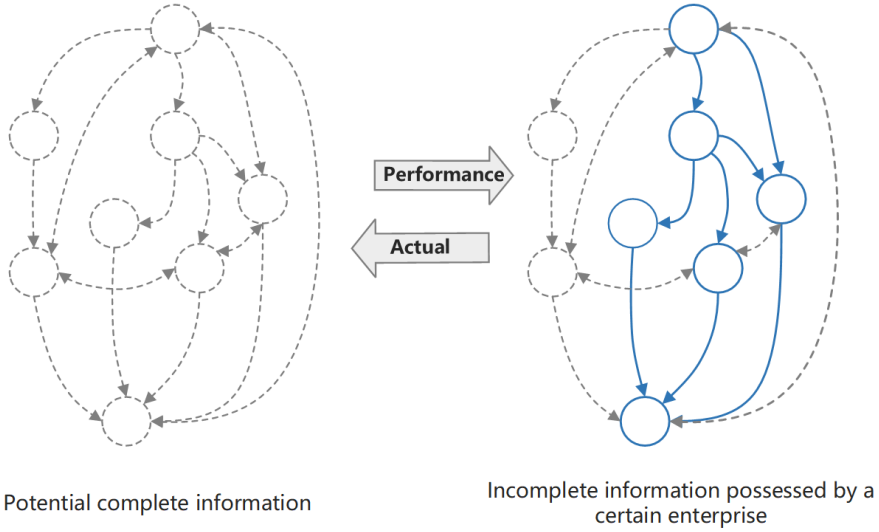


Figure 3: Incomplete information in supply chain

The information condition reflects an attacker's understanding of network operations when planning attack strategies. In supply chain cascading failure research, two common assumptions are: 1) the attacker has full global network information (complete information condition); 2) network failures propagate and recover with delay, preventing real-time status access. However, in actual supply chain operations, competitive dynamics lead enterprises to withhold or distort failure information, affecting node interactions and load transfers (Figure 3). Currently, supply chain cascading failure research has yet to widely consider incomplete information conditions. Some scholars have addressed time-delay-related cases: Zhang et al. [21] proposed a delay-time hybrid cascading failure model with boundary-node-based recovery to improve network resilience. Although not widely applied in supply chains, incomplete information has been explored in military logistics and infrastructure networks. Shi et al. [22] examined network robustness under attacks with incomplete information, while Chi et al. [23] modeled infrastructure protection as a two-stage game under such conditions. These studies highlight incomplete information's potential for supply chain cascading failure research.

In summary, cascading failures in supply chains arise mainly from three sources: internal system failures, disruptive events, and external attacks. Internal failures stem from structural defects or coordination errors, often evident in logistics and distribution systems. Disruptive events—such as natural disasters, public health crises, and geopolitical conflicts—can trigger

large-scale supply interruptions. External attacks, a common simulation approach, deliberately disrupt network nodes or edges under specific strategies to test resilience, with effects shaped by attack targets, scope, intensity, and information conditions. Together, these causes define the mechanisms and characteristics of cascading failures in supply chains.

4. Network modeling

To reflect cascading failures in supply chains, it is essential to construct a network model that accurately represents real-world conditions. This section summarizes representative supply chain models based on application scenarios and network topologies, as shown in Figure 4.

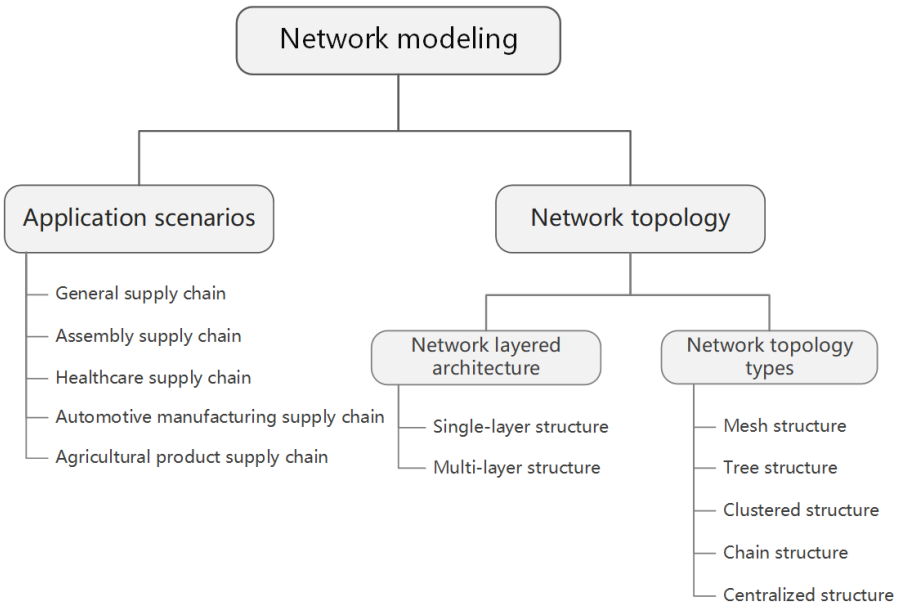


Figure 4: Network modeling of supply chain

4.1. Application scenarios

This section classifies research on cascading failures in supply chains from the perspective of application scenarios. Different scenarios exhibit distinct characteristics and operating mechanisms, which affects the occurrence and propagation of failures. Representative scenarios include general supply chains, assembly supply chains, vaccine supply chains, maritime supply chains, automotive manufacturing supply chains, and agricultural product supply chains, as shown in Table 1.

4.1.1. General supply chain

A general supply chain is a system composed of producers, manufacturers, distributors, and consumers, encompassing various stages, including raw material procurement, manufacturing, inventory management, business decision-making, and logistics transportation to distribution and retail. Due to its broad representativeness, the general supply chain is a fundamental basis for studying cascading failures in supply chains. Papachristou et al.[24] focused on structural factors, studying the impact of cascading failures on the resilience of supply chain networks and deriving various boundaries for network resilience. Gomez et al.[25] employed a multi-region input-output model to build a multi-layer network for the supply chain, investigating the propagation of cascading failures caused by economic shocks. Shi et al.[26] constructed supply chain network models with different types and interconnection patterns, considering both functional and structural cascading failures, and investigated the factors influencing the

Table 1: Comparison of application scenarios in supply chain cascading failure research

Application Scenario	**Characteristics**	**Main Risk Factors**	**Representative Studies**
General supply chain	Covers production, manufacturing, distribution, retail	Structural shocks; economic disruptions	[24–27]
Assembly supply chain	Assembly-centered; strong component dependence	Shortage/delay of key components	[28–31]
Healthcare supply chain	Medicines/vaccines; cold-chain & traceability	Temperature sensitivity; public health events	[32–34]
Maritime supply chain	Sea transport-based; cross-regional/international	Port congestion; extreme weather; route blockages	[35–41]
Automotive manufacturing supply chain	Multi-tier components; global complexity	Natural disasters; energy supply issues	[42–50]
Agricultural product supply chain	Planting/breeding/processing; strong seasonality	Perishability; climate events; epidemics	[51–59]

robustness of interdependent supply chain networks. Hao et al.[27] modeled a multi-layer network to investigate the propagation effects of global steel product supply shocks under the dual impacts of trade and price, and quantitatively analyzed the roles of different countries in this process.

4.1.2. Assembly supply chain

The assembly supply chain is a system centered on product assembly, covering all manufacturing stages from component procurement to final assembly. Its core function is to process and assemble components and raw materials provided by various suppliers to produce the finished product. Due to the high interdependence between stages, the assembly supply chain emphasizes the timeliness and quality of component delivery. A shortage or delay of critical components can disrupt the assembly process, trigger cascading failures, and even halt production. Researchers have studied cascading failures in assembly supply chains from various perspectives. Tang et al.[28] studied the resilience of assembly supply chain networks from the perspective of risk propagation. Nguyen et al.[29] developed a multi-level framework based on elasticity indices to explore network reliability under cascading failures. Du et al.[30] investigated the functional reliability of a prefabricated component assembly supply chain model under underloaded cascading failures. Skeete et al.[31] proposed an assembly supply chain model considering node adaptability and redundancy, aiming to suppress cascading failure propagation by addressing the impact of upstream fault nodes on downstream production.

4.1.3. Healthcare supply chain

Since the outbreak of COVID-19 in 2019, the importance of the healthcare supply chain has become increasingly evident, establishing it as a key research area. The healthcare supply chain (Figure 5) encompasses the entire process from the production of medicines and medical supplies to their final use, including raw material procurement, manufacturing, cold chain transportation, storage management, and distribution. Due to the high sensitivity of medicines and vaccines to temperature, this supply chain places significant demands on cold chain coordination and information tracking. Additionally, to respond to public health emergencies, the

healthcare supply chain must have strong emergency response capabilities to ensure the timely supply and distribution of critical materials. In recent years, research on cascading failures within healthcare supply chains has increased. Lavassani et al.[32, 33] simulated disruptions through random failures and targeted attacks, assessing the cascading resilience of the healthcare supply chain network. Trumpeng et al.[34] addressed disruptions in the vaccine supply chain using design and intervention approaches, emphasizing the role of risk management and coordinated cooperation in minimizing disruption impacts and optimizing resource allocation.

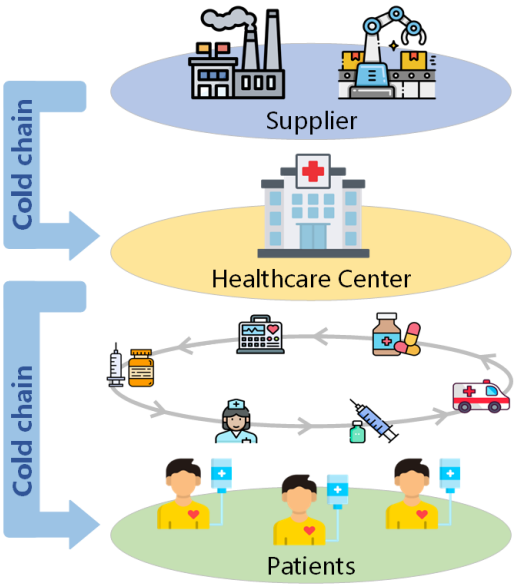


Figure 5: Healthcare supply chain

4.1.4. Maritime supply chain

The maritime supply chain is a cross-regional supply chain system centered on maritime transportation, encompassing the entire process from cargo departure at the port, transportation via sea routes, arrival at the destination port, and subsequent distribution to the final destination through land or other modes. It relies on large vessels to achieve bulk and long-distance transportation of goods, serving extensively in international trade sectors such as energy, minerals, agricultural products, and manufacturing components. Due to long shipping cycles, complex capacity scheduling, and high susceptibility to external environmental influences, the maritime supply chain places high demands on port operation efficiency, route stability, and the connectivity of multimodal transportation. Events such as port congestion, extreme weather, route blockages, or capacity shortages can cause transportation delays and interrupt material supply in upstream and downstream links, thereby triggering cascading failures within the supply chain network. In recent years, research on cascading failures in maritime supply chains has been increasing, focusing primarily on the assessment of port network structural resilience, analysis of disruption propagation paths in shipping, and the design of emergency scheduling strategies. Xu et al.[35] considered distance constraints and transportation time factors to construct a shipping network resilience evaluation model, analyzing the structural vulnerability and recovery capability of the shipping supply chain under cascading failures. Jiang et al. [36] modeled cascading failures in the container shipping network of the 21st Century Maritime Silk Road, analyzing vulnerability and propagation characteristics under disruptions. Verschuur et al. [37] proposed a systemic risk diffusion framework integrating ports and supply chain networks under natural disaster scenarios to evaluate cascading failures and resilience. Ding et al. [38] constructed a cascading failure model of land–sea transportation networks to examine network robustness and failure propagation under disruptive events. Xu et al. [39, 40]

developed a cascading failure model of the global container shipping network based on vessel data to simulate port failure propagation and network resilience under disturbances. Lu et al. [41] developed a port–inland dry port container transportation model with a multi-stage load redistribution mechanism to assess robustness and recovery dynamics under node failures.

4.1.5. Automotive manufacturing supply chain

The automotive manufacturing supply chain includes stages such as raw material procurement, component production, assembly, logistics, quality testing, distribution, and after-sales services (Figure 6). Compared to general manufacturing supply chains, it is more complex globally, requiring coordination of multi-tiered component production, assembly, quality control, and multi-point logistics management. Its complexity and global nature make it vulnerable to external events. For example, in February 2021, an extreme cold weather event in Texas caused power outages, disrupting automotive production schedules both in North America and globally[42]. Carvalho et al.[43] simulated the Portuguese automotive supply chain, assessing the impact of disruption scenarios and mitigation strategies on its resilience. Brintrup et al.[44] developed a manufacturing supply chain framework based on network theory using a global automotive industry case, focusing on supplier and product network robustness analysis. Xiao et al.[45] constructed a supply chain network model based on Poisson distribution and preference mechanisms, analyzing node interactions and cascading failure processes. Feng et al.[46] developed a cascading disruption model for automotive system-on-chip enterprises and proposed a supply information acquisition method.

In recent years, with the rapid development of electric vehicles (EVs), researchers have focused on the EV supply chain and its relationship with the lithium battery supply chain. Unlike traditional automotive supply chains, the upstream of the EV supply chain centers on batteries, motors, and electric controls, while the downstream extends to charging services and used battery recycling. This unique structure creates high dependence on the lithium battery supply chain, introducing new risks. Ou et al.[47] developed a cascading failure model for the automotive supply chain using Tesla's EV supply chain as a case study, identifying key nodes through an improved K-shell algorithm. Zhang et al.[48] proposed a probabilistic graph model and constructed Bayesian networks and an alternating current cascading failure model to predict cascading failures in electric vehicle charging networks caused by hurricanes. Hao et al.[49] built a global lithium trade network model, simulating cascading failures under both random and malicious attacks, and analyzing its weaknesses and influencing factors. Ouyang et al.[50] integrated material flow analysis with complex network theory to develop a dynamic cascading risk model, exploring systemic risks within the global lithium supply chain.

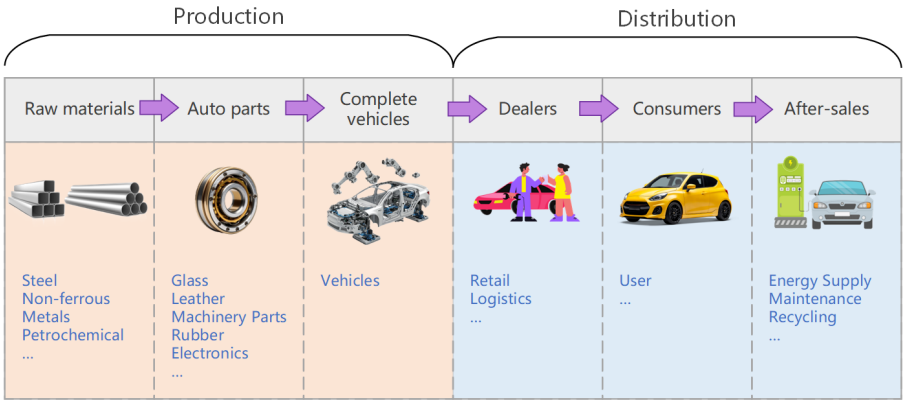


Figure 6: Automotive manufacturing supply chain

4.1.6. Agricultural product supply chain

The agricultural product supply chain encompasses the flow of products from producers (e.g., farmers) to consumers, including stages like planting, breeding, and processing, as shown in Figure 7. Due to their seasonal and perishable nature, these products require strict logistics, transportation, and storage management[60]. External factors such as weather, pests, diseases, and market interventions can cause fluctuations, challenging the stability of the agricultural supply chain. Recent research on cascading failures has focused on fresh vegetable, dairy, and livestock and poultry meat supply chains. These supply chains have distinct characteristics: the fresh vegetable supply chain emphasizes harvesting, packaging, and rapid transportation due to short shelf life and sensitivity to weather; the dairy supply chain depends on cold-chain logistics to maintain freshness, with stability influenced by breeding and processing; and the livestock and poultry meat supply chain involves slaughtering, processing, and cold-chain logistics, heavily impacted by temperature control, food safety, and animal diseases.

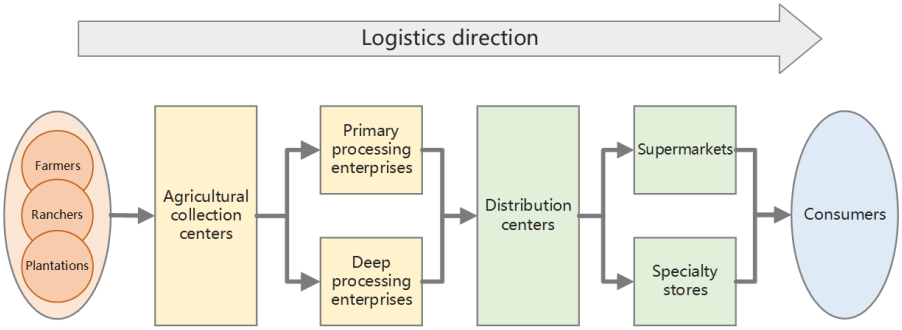


Figure 7: Agricultural product supply chain

Many scholars have studied cascading failures in agricultural supply chains from different perspectives. Li et al.[51] developed a cascading failure model for agricultural food supply chains, analyzing the impact of disruptions like extreme weather and market closures. Zhao et al.[52] proposed a disruption model, studying the effect of disruption propagation on network resilience. Vaid et al.[53] introduced a price/cost-based connection rule, creating a cascading failure model for agricultural supply chains and analyzing resilience indicators. Govindan et al.[54] developed a computational framework based on reinforcement learning and Markov decision processes to explore risk transmission in the food-energy-water system. Gholami-Zanjani et al.[55] built an agricultural food supply chain network considering pandemic disruptions, using scenario generation and decomposition methods to analyze network performance and resilience. Aboah et al.[56] used system dynamics modeling for Ghana's cocoa value chain to study cascading vulnerability and the impact of parameter changes on agricultural supply chains. Berardy et al.[57] developed a dynamic model for Arizona's agricultural production system, studying crop supply interdependence and cascading failure vulnerability under climate change. Chen et al.[58] integrated fitness-first connections and transport distance relationships to develop an evolution model for China's fresh cold-chain network, studying failure propagation. Geng et al.[59] developed a disruption model for fresh agricultural product supply chains and proposed resilience optimization strategies using an improved NSGA-II algorithm.

4.2. Network topology

This section classifies supply chain cascading failure research from a network topology perspective. Supply chain topology focuses on node and edge organization, with different topologies leading to varying cascading failure behaviors even in the same scenario. We classify topologies with two criteria: layered architecture (single-layer vs. multi-layer) and node connections (mesh, tree, cluster, chain, and centralized structures). A summary comparing network structures in supply chains is provided in Table 2.

Table 2: Comparison of network structures in supply chains

Network topology	Applicable scenarios	Cascading failures characteristics
Single-layer structure	Small-scale logistics network	Failures propagate rapidly due to lack of buffering mechanisms
Multi-layer structure	Supply chain with hierarchical relationships	Layered buffering effect, but cross-layer failure spreads rapidly
Mesh structure	Many-to-many supply chain	High redundancy, slow failure propagation
Tree Structure	Resource transmission from core enterprises	Root node failure leads to overall collapse
Cluster structure	Clustered supply chain	Failures within clusters are minor; failures between clusters are major
Chain structure	Serial supply chain	Failures propagate along the chain, no redundancy
Centralized structure	Core-centric supply chain	Risk concentration, failures spread rapidly from center outward

4.2.1. Network layered architecture

In supply chain systems, enterprises are typically classified into multiple tiers according to their functional roles, such as supply, manufacturing, and sales. This function-based division endows the supply chain with a distinct "hierarchical" characteristic and provides the foundation for defining "hierarchical structure" in network modeling. In this section, we discuss the hierarchical structure of supply chain networks based on the classification of functional roles.

1) Single-layer structure

A single-layer structure consists of nodes at the same hierarchical level, interconnected through simple links[61–64]. It is common in small-scale supply chains with few product types, simple relationships, and no hierarchical dependencies. Suppliers, manufacturers, distributors, and retailers operate independently in a planar network. For example, when a logistics provider collaborates with multiple companies, the companies remain relatively independent with weak interdependencies. The structure's simplicity facilitates management, but the lack of buffering increases risks. When a node fails, disruptions can quickly spread, causing cascading failures.

2) Multi-layer structure

A multi-layer structure consists of multiple interconnected levels, each with nodes and links[65–71]. It integrates multiple single-layer networks and is common in large-scale, complex, interdependent supply chains. Participants are assigned to levels based on function and connected through upstream-downstream relationships. There are both cross-layer connections between nodes linking different functional tiers (e.g., edges between suppliers and manufacturers) and intra-layer connections between nodes within the same functional tier (e.g., cooperative relationships among multiple manufacturers). In manufacturing, for example, raw material suppliers, manufacturers, distributors, and customers form a hierarchy: suppliers provide raw materials, manufacturers process them, and distributors deliver products to customers. This structure defines distinct functions at each level, facilitating collaboration while mitigating risk propagation. When disruptions occur, tasks are redistributed within the affected level to contain failures. However, inter-layer dependencies introduce vulnerabilities—critical node failures can cause congestion or task delays, spreading across layers as cascading failures, potentially paralyzing the system.

4.2.2. Network topology types

1) Mesh structure

The mesh structure is a widely used network topologies in supply chain cascading failure research[72, 73]. The mesh structure is a type of network topology where nodes can be directly connected to each other, endering it suitable for systems characterized by many-to-many relationships, as shown in Figure 8(a). In a mesh structure supply chain, each participant (node) can establish direct connections with multiple other participants, resulting in high redundancy and fault tolerance in the network. Even if a node or path fails, traffic can still be routed through other paths, effectively distributing the risk of network disruptions and significantly reducing supply chain instability. However, mesh structure supply chains may also face poten-

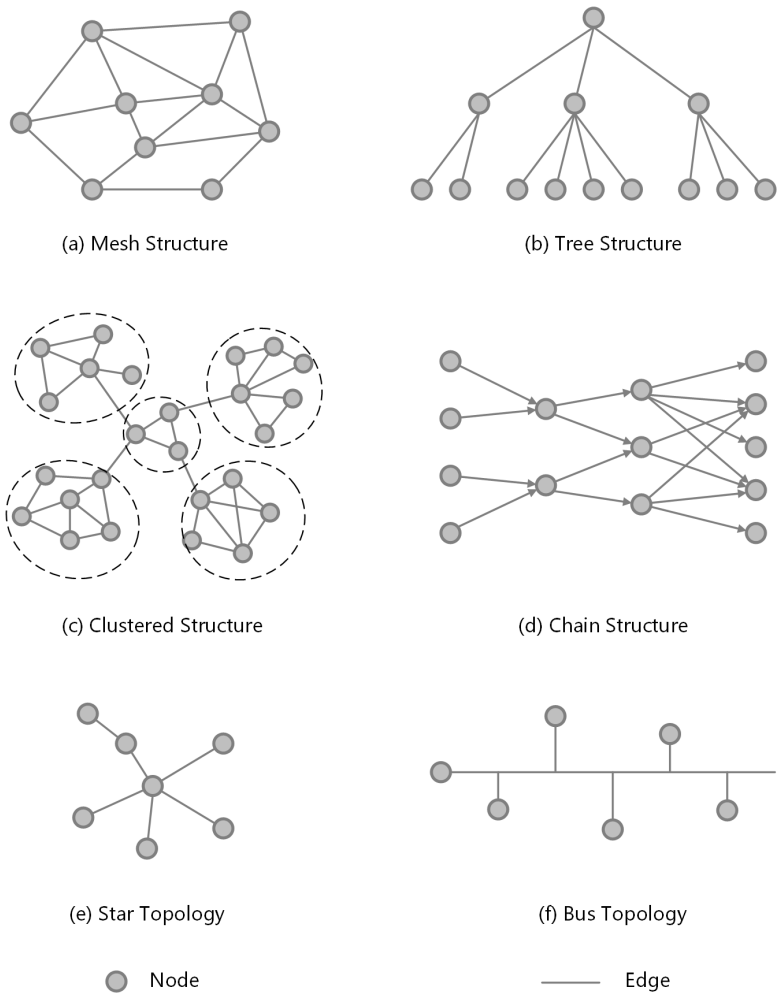


Figure 8: Topology structure of supply chain

tial failure risks due to complex dependencies between nodes or paths. Once a path fails, other associated paths may be affected and unable to function properly, leading to cascading failures.

2) Tree structure

The tree structure is a hierarchical network with a root node and multiple child nodes[74–76]. Each node connects to a single parent node, forming a clear hierarchy, as shown in Figure 8(b). In supply chain cascading failures, product resources, logistics, or disruption risks typically propagate downward through this structure. This supports effective labor division, centralized decision-making, and process visualization. The core manufacturer, as the root node, controls traffic to downstream vendors, ensuring the consistency of the supply chain. However, the tree structure's centralization introduces risks. As most nodes rely on the root or key nodes, any failure in these can lead to cascading failures and system paralysis. Hence, the tree structure is often used to study failure propagation and assess structural and performance changes under external shocks.

3) Clustered structure

A clustered structure is a network topology where nodes are grouped into clusters, with tight connections within each cluster and links between clusters through key nodes, as shown in Figure 8(c). This structure supports decentralized decision-making in autonomous supply chains, where each cluster represents a specific region, product, or business unit. Nodes within a cluster share resource information, forming regional advantages. Cooperation between clusters occurs through intermediary nodes (e.g., wholesale markets, logistics hubs). Unlike hierarchical tree structures, clustered networks offer "tight local connections and loose global connections,"

providing flexibility and adaptability. Each cluster can independently make decisions, enabling rapid responses to policy shifts. However, weak inter-cluster connections mean that failure of a key intermediary node can disrupt links, dissolve cooperation, and trigger cascading failures. In supply chain cascading failure research, clustered supply chains exhibit strong intra-cluster and weak inter-cluster links[13, 77, 78].

4) Chain structure

A chain structure is a linear topology where nodes are connected unidirectionally, and resources flow sequentially from upstream to downstream, as shown in Figure 8(d). It is common in production, distribution supply chains, or logistics systems, where each node represents a supply chain link, sequentially connected and dependent on the previous link's output[79, 80]. While the structure offers clear processes and simple management, its linear nature introduces risks. As specialization increases and the chain extends, resource transmission delays become more pronounced, and any node failure affects the entire supply chain. To mitigate risks, complex supply chains often adopt multi-path connections for redundancy, evolving into a multi-chain structure, which resembles a directed mesh structure.

5) Centralized structure

The centralized network topology relies on a single core node for resource management, mainly including star and bus structures, as shown in Figure 8(e) and Figure 8(f). The star structure features a core enterprise coordinating multiple peripheral enterprises, commonly used in complex supply chains. The bus structure uses a linear topology with shared communication channels for resource broadcasting. While rare in traditional supply chains, bus structures have gained traction with IoT platforms, especially in shared services, joint finance, and logistics. In this structure, nodes communicate via the bus, which centrally manages resource transmission, optimizing the star structure[81–84].

In summary, this section reviews network models of cascading failures in supply chains from two dimensions: application scenarios and network topologies. The former covers general, assembly-based, healthcare, maritime, automotive manufacturing, and agricultural product supply chains, analyzing their structures, operations, and vulnerable links. The latter distinguishes between single-layer and multi-layer structures, and examines mesh, tree, cluster, chain, and centralized topologies along with their failure propagation patterns and resilience performance. Application scenarios determine the functional scope of the model, while topology affects the paths and scale of failures; aligning topology with real-world contexts is key to accurate analysis.

5. Cascading Failure Model

This section provides an overview of common modeling approaches for cascading failures in supply chains, including Agent-based models, load-capacity models, Input-output (I-O) models, Petri nets-based models, Bayesian networks, epidemic models, coupled map lattice models, and cellular automata.

5.1. Load-capacity model

The load-capacity model is a dynamic model based on complex network theory, describing the relationship between nodes, load, and capacity in network systems. It defines the load and capacity for each node and edge in the supply chain network and has been widely used in supply chain cascading failure research. The load represents the flow or load a node or edge bears, typically referring to order volumes or logistics, while capacity is the maximum load a node or edge can handle. When the load exceeds capacity, the node or edge fails, and the failure propagates, triggering a cascading effect. The cascading failure modeling process using the L-C model involves: 1) setting initial node/edge loads and capacities; 2) defining load

redistribution strategies based on network topology and practical features; and 3) applying external attacks or disturbances and observing failure propagation. In a supply chain, when an enterprise node is unable to perform its original functions due to operational disruption, its load will be redistributed to other upstream and downstream enterprises. These additional demands or resource pressures may cause the receiving nodes to fail from overload. At the same time, when the demand for cooperation between upstream and downstream partners decreases, an enterprise's resources and capacity may remain idle for an extended period, leading to reduced operational efficiency and consequently underload failure. A single disturbance may simultaneously trigger both underload and overload at different nodes, with the two occurring alternately and interacting with each other, thereby accelerating the spread of failures. Existing models focus on overload failures. However, unlike most other networks where overload failures are more likely to occur, underload failures are equally prevalent in supply chain systems. To address underload failures, Wang et al.[85] proposed a cascading failure model based on demand and supply changes, studying the impact of node capacity constraints on cascading failure propagation. Liu et al.[86] built a COVID-19 supply chain cascading failure model using ER and BA frameworks, focusing on node capacity thresholds and underload failure performance under random and targeted attacks. Mu et al.[87] developed a multi-level supply chain load-capacity model and proposed a cascading risk propagation model based on node disturbances to study risk propagation and robustness. Wang et al.[88] constructed a cascading failure model for construction supply chains and proposed a method for identifying key risk nodes. The advantage of a load-capacity is its ability to intuitively describe resource flow in a supply chain network, helping identify underload or overload failures. However, this theoretical model may over-rely on key parameters, leading to incomplete or inaccurate analysis of cascading failure behaviors. Therefore, this model is suitable for networks with clearly defined capacity limits and measurable logistics or orders, such as product manufacturing or regional logistics networks.

5.2. Agent-based model

In agent-based modeling (ABM) for supply chain cascading failures, each enterprise is modeled as an autonomous agent that makes decisions based on predefined rules like production capacity, inventory, and resource allocation. ABM captures the complex interactions between nodes and non-linear agent behavior, making it suitable for dynamic supply chain systems. Figure 9 illustrates agent-based supply chain modeling. The ABM process involves: 1) Defining supply chain participants (enterprises, facilities, etc.) as agents, with attributes like production capacity and inventory; 2) Defining agent decision-making processes and interaction rules (e.g., priority-based resource scheduling, inventory allocation protocols, and production switching strategies); 3) Constructing the supply chain network, initializing agent states, and setting environment variables. Using simulation tools, agent behaviors and failure propagation are observed to analyze cascading failure impacts on the supply chain network. Kang et al.[89] modeled global trade supply chains using agents to analyze cascading failures and fault propagation in international trade networks. Zhao et al.[90] modeled supply chains as complex adaptive systems, simulating enterprise adaptation to disruptions and studying proactive and reactive strategies. Chatfield et al.[91] integrated ABM with discrete event theory to construct an inventory system model, focusing on cascading stockouts. Geng et al.[92] developed a multi-agent-based resilience model to explore cascading failure evolution. The advantage of ABM lies in its ability to realistically depict agent behaviors, making it particularly suitable for scenarios with complex interaction rules and multiple decision factors for nodes, such as multi-stage supply chains and decentralized manufacturing networks. However, building such models requires large amounts of high-quality data, and the simulation process is complex and time-consuming. In practice, it is often difficult to obtain comprehensive data on agent capacities, inventories,

response strategies, and interaction records, making effective validation against real-world situations challenging. Compared with the load–capacity model, ABM has significant advantages in capturing complex behaviors such as enterprise decision-making and strategic interactions, but it comes with higher computational and data requirements.

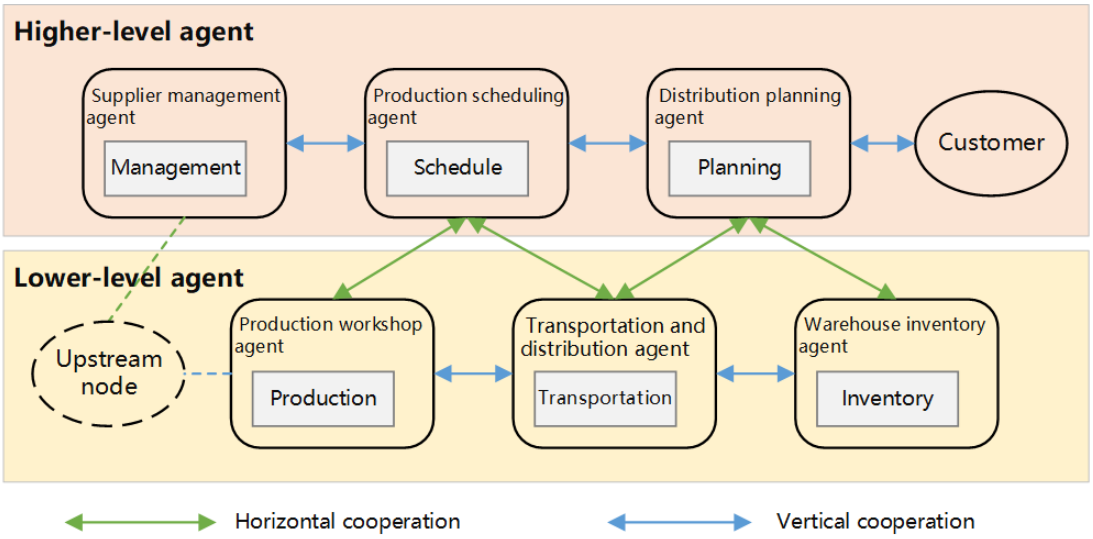


Figure 9: Agent-based model of supply chain

5.3. Input-output model

The input-output (I-O) model quantifies inter-industry relationships to enable dependency analysis, trend prediction, and policy evaluation. In supply chain cascading failure research, it is primarily used to assess disruption risks on supply chain systems by quantifying input-output dependencies between nodes, as shown in Figure 10. As a core economic model for studying cascading failures, the I-O model is often paired with general equilibrium models, each offering unique insights into disruption propagation:

- General Equilibrium Model: This model examines market and sector interactions, analyzing interconnections through market mechanisms. It is particularly useful for exploring how external shocks affect overall supply chain operations.

- Inoperability I-O Model(IIM): This approach quantifies inter-industry dependencies to analyze the flow of information, resources, and capital. As an extension of the I-O model, the IIM strengthens the analysis of failure propagation and deepens the study of industrial linkages and node failure impacts.

Several studies on supply chain cascading failures have advanced the development of these models. Tan et al.[93] proposed a cascading failure propagation method based on the I-O model to quantify the impact of cascading failures in supply chains. Wei et al.[94] applied the IIM to the Chinese liquor production supply chain to assess cascading failure risks and economic losses. Baqaee et al.[95] developed a general equilibrium model with input-output linkages, focusing on how firm behavior influences shock propagation in supply chains. Ocampo et al.[96] introduced a supply-side IIM based on the Ghosh model, analyzing the propagation of supply disturbance risks. Omega et al.[97] proposed a supply-driven IIM, studying the cascading impacts of supply disturbances. Taschereau-Dumouchel[98] proposed a production network theory and constructed an I-O model to analyze how production decisions affect network structures. Sarkar et al.[99] combined interval programming with the IIM to model port supply chains, studying the COVID-19 impact on port logistics. Xing et al.[100] proposed a novel algorithm

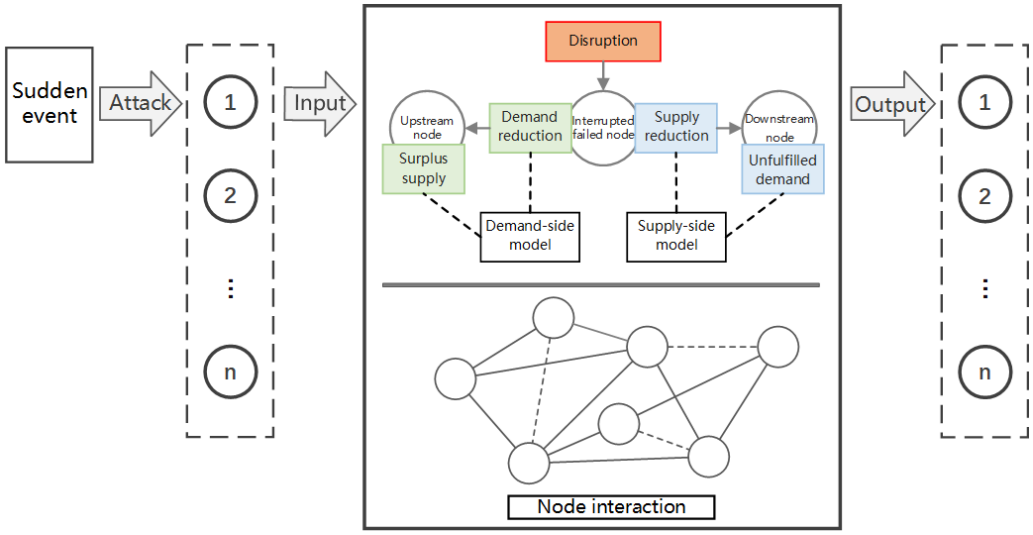


Figure 10: I-O model of supply chain

and metrics based on the I-O model to conduct cascading analysis. Yu et al.[101] proposed an IIM-based approach for biomass supply chain risk propagation analysis. The I–O model can quantify the interdependencies within a supply chain, making it suitable for macro-level assessments of multi-industry and multi-regional supply chains. However, due to its reliance on an assumption matrix and a static equilibrium framework, it tends to overlook dynamic and nonlinear processes as well as non-economic factors. Therefore, compared with other models, the I–O model is better suited for macro-level supply chains with stable structures, readily available data, and scenarios involving systemic failure propagation, while it is less effective in simulating complex interactive networks with strong node heterogeneity. In particular, in studies that require detailed characterization at the enterprise level, the standalone application of the I–O model has relatively weak adaptability.

5.4. Petri net-based model

Petri net, developed by Carl A. Petri in the 1960s, are a network model used to describe asynchronous and concurrent systems. They provide a graphical method for modeling resource flow and failure propagation, making them suitable for modeling cascade failure processes in supply chains involving resource allocation, logistics, and dynamic processes. Figure 11 illustrates Petri net-based supply chain modeling. The general process for Petri net-based model is as follows: 1) Define nodes (places), transition rules, directed arcs (connections), and tokens, representing system states, resource allocation, and flow relationships; 2) Simulate supply chain cascade failures with resource flow through token passing. Fridgen et al.[102, 103] developed a supply network model based on an improved modular Petri net and showed that cascading failures from external shocks impact the network's safety inventory levels. Skorupski et al.[104] used a Petri net model to create a supply chain material flow diagram and proposed a risk analysis method for cascading failures. Wang et al.[105] integrated economic IIM with Petri net to build a corporate economic health cascading failure model and proposed a resilience management theory for supply chain networks, designed for disruption detection and resource recovery. The main advantage of Petri nets is their intuitive graphical representation and strong theoretical foundation, which effectively describe the dynamic behavior of resource allocation. However, resource allocation modeling typically requires large amounts of detailed data, which increases the complexity of model construction and validation, and also limits the ability to accurately characterize dynamic networks. Compared with the I–O model, which focuses on macro-level failure propagation, the Petri net is more suitable for supply chain scenarios

that require precise tracking of resource flow paths and process control, such as integrated manufacturing–assembly–distribution processes.

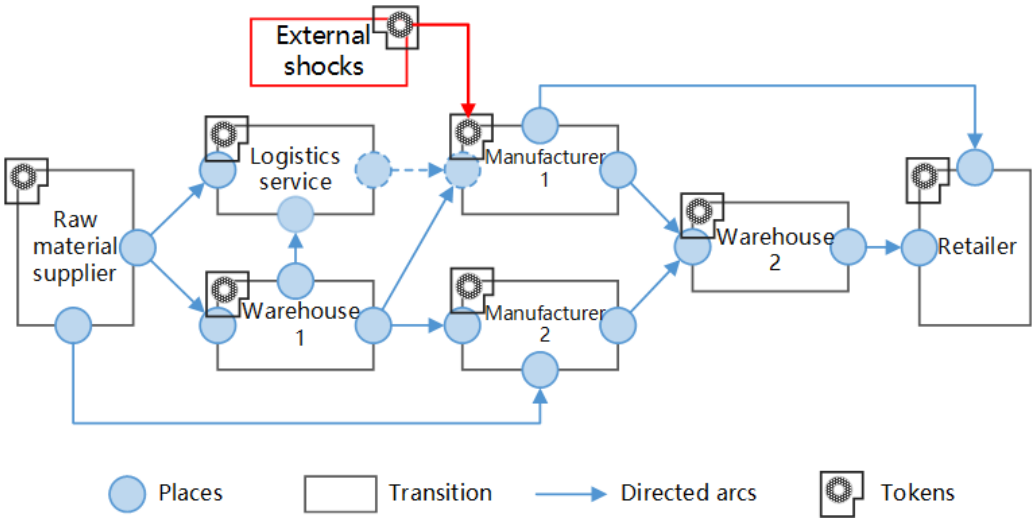


Figure 11: Petri net-based modeling of supply chain

5.5. Bayesian networks

Bayesian networks, as probabilistic graphical models, quantify causal relationships and uncertainties between node failures and are widely used in modeling supply chain cascading failures to analyze dependencies between variables. Figure 12 shows a Bayesian model of a supply chain with different time relationships. The process for modeling supply chain cascading failures with Bayesian networks is as follows: 1) Identify key nodes in the supply chain (such as enterprises, logistics channels) and their interdependencies, define the nodes and directed edges, and construct a directed acyclic graph; 2) Assign probability distributions to each node, including conditional probability tables (CPT) or probability density functions (PDF), to describe the probability of a node's state based on upstream nodes; 3) Use data related to the nodes and apply Bayes' theorem to compute posterior probabilities of unknown nodes, analyzing the propagation paths and extent of cascading failures. Hosseini et al.[106] proposed a supply chain model combining discrete-time Markov chains (DTMC) and dynamic Bayesian networks (DBN), quantifying ripple effects from supplier disruptions, and proposing metrics based on expected utility and service levels. Hossain et al.[107] used Bayesian networks to model inland ports and surrounding supply chains, analyzing the interdependence between inland ports and their networks, using Vicksburg port as an example to explore the impact of port disruptions on the supply chain. Zhang et al.[108] proposed a framework based on Bayesian networks to analyze ripple effects in cross-tier shipbuilding supply chains. Nocera et al.[109] employed a Bayesian network to analyze the impacts of different structural characteristics on supply chain risk propagation and system vulnerability. Kang et al.[110] examined the propagation process of supply risk shocks in the global copper industry chain and quantitatively analyzed the roles and criticality of different countries in risk transmission based on the principles of Bayesian networks. The advantage of the Bayesian network model is its ability to capture dependencies among supply chain components and, through probabilistic inference, identify critical elements and risk sources, predicting the likelihood of cascading failures. However, for complex systems with many nodes and dynamic dependencies, computing conditional probability distributions can become difficult and less accurate. Bayesian networks, along with ABM and I–O models, are all modeling approaches based on dependencies between nodes, but they differ significantly in modeling concepts and analytical perspectives. ABM characterizes enterprise decision-making behaviors and interactions at the micro level, whereas the I–O model describes the macro-level

input–output transmission mechanism of global failures. Bayesian networks lie between these two, using probabilistic inference to quantify causal dependencies and uncertainties between nodes of different tiers and scales. Therefore, this approach is particularly suitable for supply chain scenarios with abundant historical data, relatively stable dependency relationships, and the need for risk inference under conditions of incomplete information, such as port logistics networks.

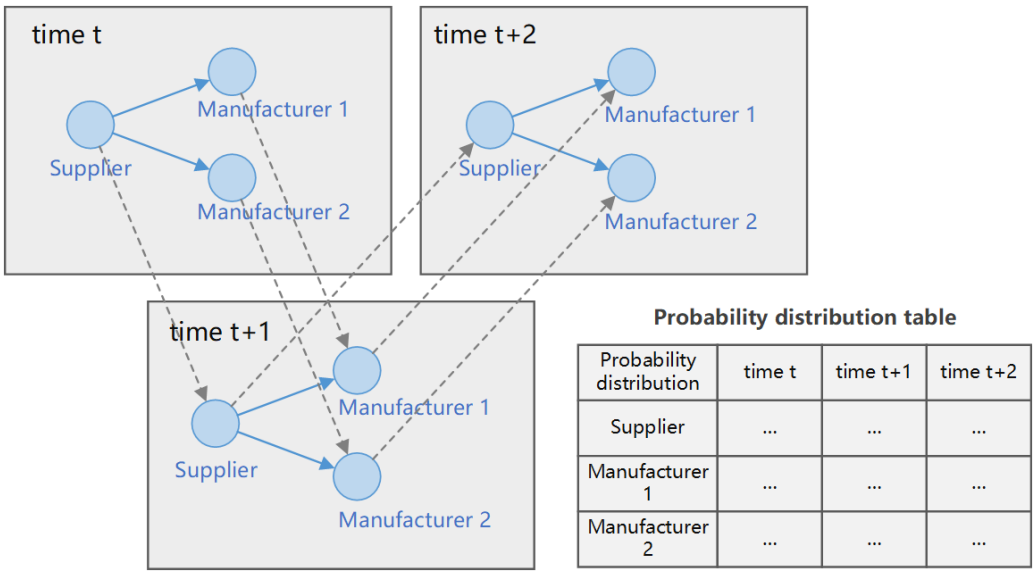


Figure 12: Bayesian network-based supply chain modeling

5.6. Epidemic model

The epidemic model is a dynamic modeling approach derived from epidemiological theory, commonly used to describe the temporal processes of disturbance or failure propagation and recovery in networked systems. In this framework, supply chain enterprise nodes are abstracted into several discrete states, and disturbances propagate along the connections between nodes. The probabilities of propagation and recovery are determined based on the specific characteristics of the actual supply chain. Common epidemic models include the SIS (Susceptible–Infected–Susceptible) model, the SIR (Susceptible–Infected–Recovered) model, and several other extended forms such as SEIR and SIRS. In the context of cascading failures in real-world supply chains, susceptible nodes represent enterprises that are currently operating normally but may be affected by disturbances; infected nodes denote enterprises that have already failed and may transmit shocks to neighboring nodes; recovered nodes refer to enterprises that have been repaired and have regained operational capability. The modeling process based on epidemic models typically involves the following steps: 1) constructing the supply chain topology and assigning an initial state (S, I, or R) to each node; 2) setting the failure propagation and recovery parameters according to the network structure and actual characteristics; 3) iteratively updating node states under predefined initial disturbance conditions, and recording the temporal evolution of failure scale and distribution. Song et al.[111] modeled a guarantee network from a supply chain perspective using the SIR model to capture risk propagation under credit guarantee relationships. Yu et al.[112] used real online freight data to build a supply chain logistics network and applied the SIR model to examine risk propagation and key influencing factors. Zheng et al.[113] applied the SEIR model to analyze supply risk diffusion and paths in the international tungsten trade network. Liu et al.[114] treated supply disruptions as “infections” and used SEIR to model the global iron ore trade network, assessing the roles of different countries in risk diffusion. Yao et al.[115] examined

how partial mapping relationships affect risk transmission in double-layer networks using an epidemic model. Xie et al.[116] modeled trade credit risk contagion in supply chains and evaluated firm-level roles with network structure analysis. Yu et al.[117] studied risk propagation and diffusion patterns in partially mapping double-layer hypernetworks under varying conditions. Epidemic model–based approaches are simple in structure, intuitive in parameters, and effective for characterizing the dynamic process of failure propagation. However, their idealized assumptions about propagation and recovery make it difficult to capture the complex resource dependencies and competitive–cooperative relationships in real supply chains. They are thus more suitable for scenarios with relatively homogeneous failure and recovery processes and stable propagation paths, such as trade or regional logistics networks. For complex supply chains with strong node heterogeneity, epidemic models are often combined with other methods (e.g., load–capacity models) to improve simulation realism.

5.7. Coupled mapping lattice model

The Coupled Mapping Lattice (CML) model is a nonlinear dynamic model for analyzing the spatiotemporal evolution of complex systems. In supply chains, it divides the system into nodes, forming coupled points representing subsystems. These points are coupled through a mapping formula, with the coupling strength determining the degree of interaction, thereby simulating the failure propagation process. The CML modeling process for supply chain cascading failures is as follows: 1) Construct a dynamic system for each node with state variables and update rules; 2) Define coupling relationships and update formulas, where the next state depends on the current state and neighboring nodes; 3) Initialize node states, apply external attacks, and observe the spatiotemporal evolution of cascade failures. Liu et al.[118] proposed a new definition of supply chain resilience and developed a multi-layer network model to study nonlinear characteristics of disrupted supply chain networks in chaotic environments. Hong et al.[119] developed a blockchain-IoT grain supply chain system, applying CML for encryption to optimize architecture and mitigate risks. The CML model features a discrete-time interaction mechanism, flexible lattice structure, and concise mathematical expressions, enabling analysis of the spatiotemporal dynamics of failure propagation. In cascading failures, it simplifies node interactions: while capturing the influence of interaction patterns on the network, it overlooks node heterogeneity, limiting realism. Like epidemic models, it is best suited for scenarios with relatively homogeneous nodes when analyzing spatiotemporal propagation, such as regional supply networks or systems with regular link topologies.

5.8. Cellular automaton model

The cellular automaton model (CA model) is a discrete grid-based system that models node state evolution through local rules. The system is divided into cells (nodes), each with discrete states (e.g., load, inventory), updating according to predefined rules based on neighboring cells. When modeling a supply chain, the CA model typically follows three steps: 1) Define the system structure (e.g., spatial architecture and cell neighborhood); 2) Set cell states and update rules, then initialize states; 3) Adjust cell states based on attack strategies and update them over time. As shown in Figure 13, this simulates supply chain failure propagation. The CA model simulates supply chains through simple rules, allowing flexible adjustments to dynamic characteristics. Suryawanshi and Doere[120] constructed a CA model to analyze supply-demand impacts and neighbor decisions for optimization. Shan et al.[121] developed a CA model for emergency logistics risk propagation, analyzing risk patterns and proposing protection strategies. Ma et al.[122] combined a stochastic SEIR model with a cellular automaton to model and analyze the dynamic risk propagation process in supply chain networks. The CA model offers transparent rules, high computational efficiency, and easy rule adjustment, enabling rapid simulation of how local interactions affect system evolution. However, its rule-driven local updates and grid

layout limit representation of multi-level networks with diverse node types and asymmetric dependencies. Market fluctuations may also trigger resource redistribution and global diffusion, exceeding the scope of CA's local rules. Compared with the continuous-mapping CML model, CA focuses on rule-based discrete evolution, making it suitable for supply chains with discrete node distributions and clear, localized interaction rules, such as regional warehouse networks or industrial park logistics systems.

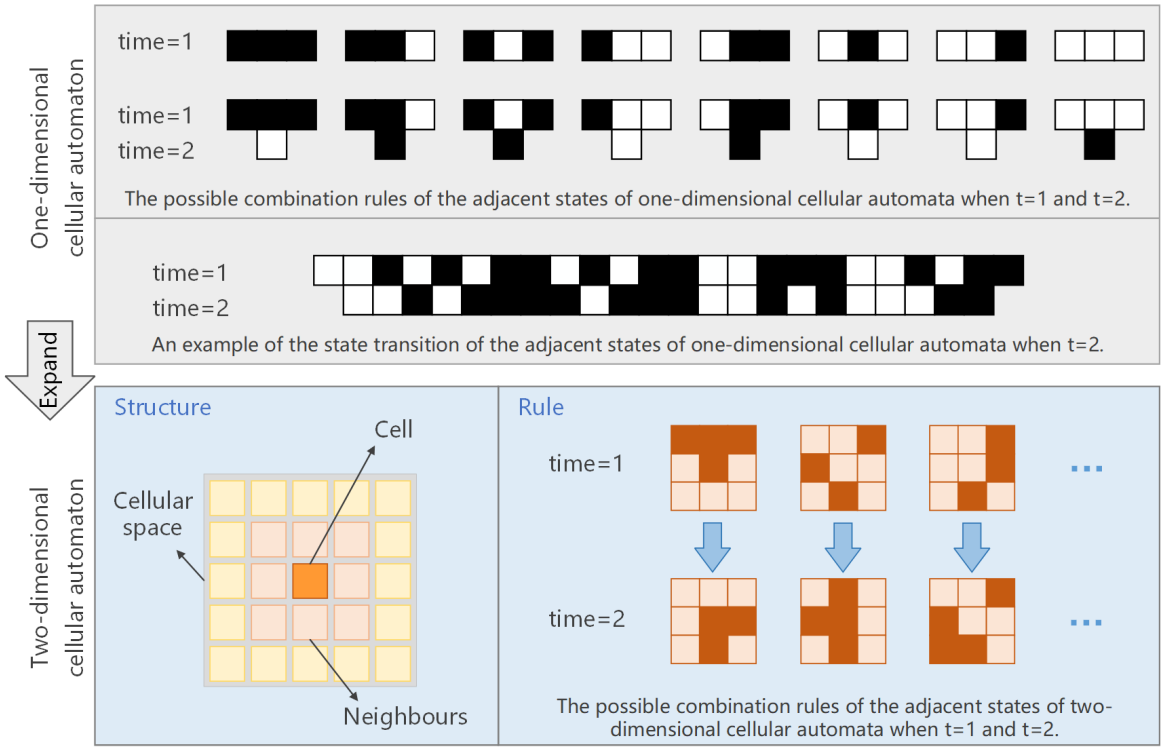


Figure 13: Cellular automaton model

In summary, this section reviews key modeling approaches for cascading failures in supply chains, including load–capacity, agent-based, input–output, Petri net, epidemic, Bayesian network, coupled map lattice, and cellular automata models. Their applicability varies with research objectives, network structure, and data availability. The load–capacity model intuitively captures resource flows and overload/underload failures but relies heavily on parameters. Agent-based model details enterprise decisions and interactions but demands extensive data and is hard to validate. Input–output models quantify dependencies and economic shocks yet miss nonlinear and dynamic features. Petri nets support intuitive resource allocation and process modeling but are complex to build. Epidemic models suit homogeneous propagation but require integration with other methods. Bayesian networks handle uncertainty and risk tracing but are computationally intensive at scale. Coupled map lattices simulate spatiotemporal dynamics but simplify heterogeneity. Cellular automata model rule-based local propagation but cannot fully represent multi-level, highly heterogeneous networks.

6. Cascading Failure Optimization in Supply Chains

The goal of cascading failures research in supply chains is to enhance the resilience of the supply chain network, reduce potential disruption risks, and establish a robust and reliable supply chain system. Existing optimization approaches commonly aim to maximize network robustness and resilience, as well as to reduce vulnerability. The definitions and calculation methods of these performance metrics have been systematically discussed in Section 2.1. Those

optimization strategies can be broadly classified into three categories: prevention, real-time mitigation and recovery.

6.1. Prevention strategy

The prevention strategy focuses on the pre-disruption phase, using protective measures, optimizing resource allocation, or adjusting the network structure to reduce the potential risk of cascading failures. Common prevention strategies in existing optimization studies include identifying and protecting critical components.

1) Identify and strengthen critical components

Supply chain networks are multi-level collaborative systems where nodes and links at different positions differentially impact system performance. Critical positions can be particularly vulnerable–their failures often trigger chain reactions that significantly affect the entire system. Identifying and protecting these critical components (core suppliers, key logistics nodes, and special supply links) is crucial for reducing cascading failure risks. Yan et al.[123] proposed a dynamic evaluation method to identify critical nodes and quantify failure damages. Pavlov et al.[124] developed a hybrid fuzzy-probability approach combining fuzzy logic and graph theory to assess supplier resilience. Kosasih et al.[125] transformed supply chain visibility into a link prediction problem using Graph Neural Networks (GNN) to predict cascading failure risks. Hua et al.[126] integrated topological attributes, business attributes, and structural–business coupling attributes based on multi-dimensional fusion metrics to comprehensively evaluate node importance in supply chain networks. Liu et al.[127] constructed a firm-level network of a copper value chain, analyzed the cascading risk propagation mechanism within it, and identified the key nodes that may amplify systemic risk. Meng et al.[128] constructed a global lithium supply chain network, evaluated the risk propagation process in the trade network under different technological risk scenarios, and identified the key nodes with significant impacts on system stability.

2) Optimizing network topology

Optimizing network topology is essential for enhancing supply chain resilience. This involves improving operational efficiency while considering logistics, cost control, and risk management. Common strategies include node layout optimization, redundant connections, and path optimization. Node layout optimization adjusts node positions and connections to balance load distribution, reducing underload or overload risk and improving resistance to cascading failures. Redundant connections provide backup paths, ensuring resource flow during failures and reducing single points of failure. These connections also offer extra pathways during high traffic, improving flexibility and efficiency. Path optimization selects optimal routes to avoid congestion, increasing resource flow efficiency. Liu et al. [129] assessed survivability using an underload cascading failure model and found that collaboration between hub and non-hub manufacturers enhances resilience. Fan et al.[130] explored transportation failures of perishable goods, introducing a Dijkstra-GA in path optimization models.

3) Risk early warning

Early risk warnings help networks withstand shocks and prevent cascading failures. Unlike other networks, supply chains are dynamic systems consisting of multiple enterprises and stages, with risks closely linked to indicators like inventory, logistics efficiency, transportation, production progress, and profit margins, which are often dynamic. Therefore, early risk warning in supply chains depends not only on traditional network topologies but also on the analysis of real-time changes in information and material flows, as shown in Figure 14. Researchers mainly use machine learning and data mining to identify potential risks in supply chains, including stockouts, transportation disruptions, and order delays, helping to pinpoint weak links that could cause cascading failures. Khan et al.[131] proposed a framework focused on real-time monitoring and early risk warning to enhance supply chain resilience during national

emergencies and prevent cascading failures. Ivanov[132] developed a universal decision-making framework for supply chain stress testing and resilience analysis using digital twins. Miao et al.[133] constructed a cascading failure model for the photovoltaic supply chain, analyzing the risk propagation of raw material disruptions and quantifying the risk transmission capabilities of various countries.

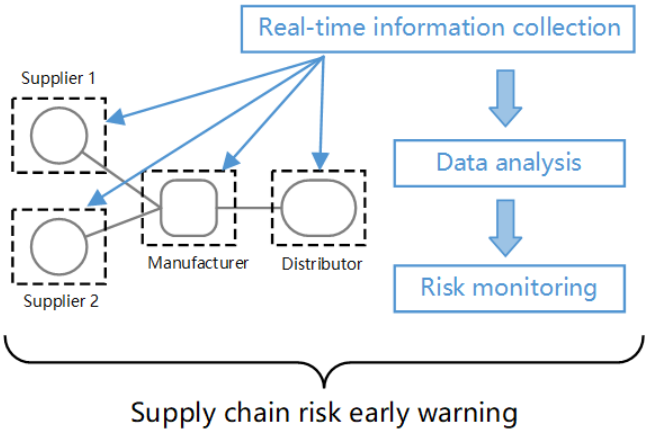


Figure 14: Risk early warning for cascading failures in supply chains

4) Management improvement

Supply chain optimization depends on technical advancements (e.g., topology and algorithms) and effective organizational management. It is a dynamic system where business and individual interactions impact the entire network. Key steps include optimizing management models, improving information sharing, and enhancing coordination to strengthen resilience and prevent cascading failures. This involves refining processes, fostering collaboration, optimizing information flow, and establishing emergency mechanisms. Additionally, optimization must balance technical upgrades with cross-enterprise management and resource sharing. Ding et al.[134] analyzed factors affecting cascading failure resilience in supply chains and proposed strategies like enhancing information symmetry and management systems. Wang et al.[135] improved a cascading failure model for the iron ore supply chain by securing supply from key exporters, setting up an early warning system, and optimizing import/export management. Yang et al.[136] found that node load constraints (e.g., inventory and costs) affect cascading failures and proposed adjusting inventory and backup supplier strategies. Sengupta et al.[137] proposed strategies to reduce losses in India's agricultural food supply chain by transitioning to a sustainable, networked business model.

6.2. real-time mitigation strategy

Real-time mitigation strategies refer to intervention measures taken during the disturbance and failure propagation stage of a supply chain network to suppress failure spread and thereby mitigate its impact on the overall system functionality. Unlike preventive strategies implemented beforehand or recovery strategies applied afterward, real-time risk mitigation is planned based on analysis of real-time monitoring data and the current operational state of the network, emphasizing rapid response and dynamic adjustments before the failures cause systemic damage. Once a disturbance occurs and enters the failure propagation stage, the supply chain system often still retains a certain degree of regulatory flexibility. At this point, dynamic interventions based on real-time operating conditions can effectively suppress further spread of failures and help maintain the system's overall stable operation. On one hand, resource scheduling and allocation can be adjusted in real time—by modifying inventory levels, transportation capacity, and production pace—to prioritize limited resources for critical links and ensure the

continuous operation of core nodes. On the other hand, when certain nodes or links experience failure, strategies such as introducing backup suppliers, reconfiguring logistics routes, or adjusting distribution methods can locally restructure the network and maintain continuity of resource flows. At the same time, it is necessary to implement isolation and protection measures for high-risk nodes in the network to block cross-tier or cross-regional failure propagation. In practical applications, the implementation of real-time mitigation strategies is often constrained by time, information availability, and resources. For instance, reconfiguring logistics routes or introducing backup suppliers can restore production supply but may incur additional costs. The trade-off between real-time network optimization and cost is also an important issue worthy of discussion in the study of cascading failures in supply chains. Ivanov et al.[138] investigated the propagation of the ripple effect in intertwined supply networks under sudden disruptions and proposed a collaborative emergency adaptation mechanism to reduce risk diffusion. Liu et al.[139] used the SEIR model to examine supply chain financial risk contagion from a commercial bank perspective, assessing how intervention timing and intensity affect risk diffusion, and proposed a strategy to dynamically adjust credit limits and structures.

6.3. Recovery strategy

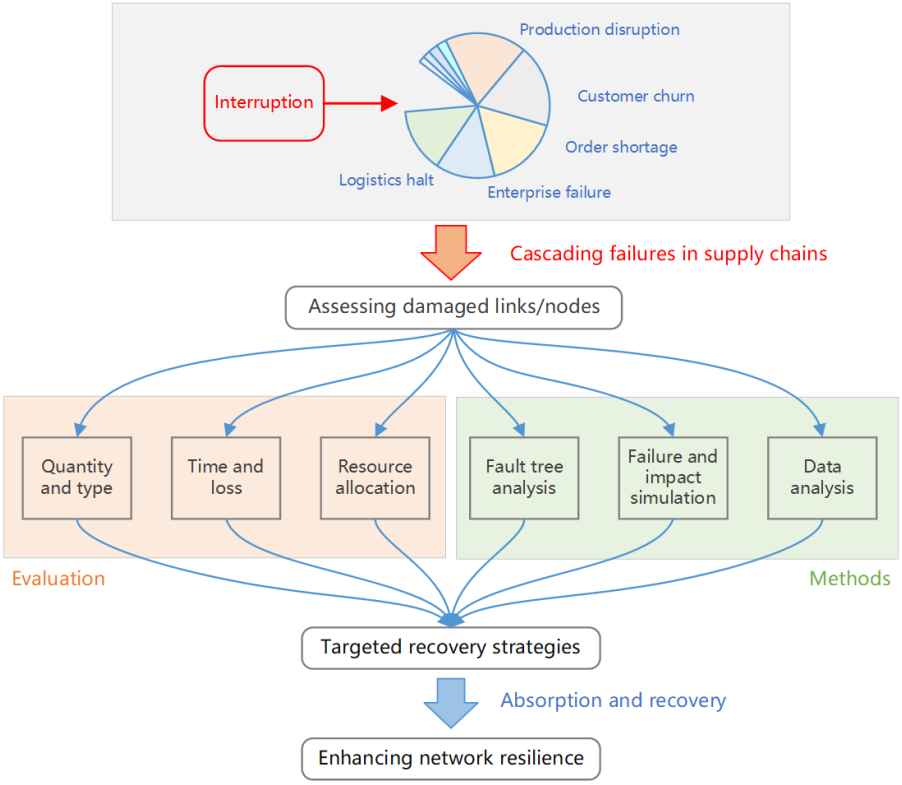


Figure 15: Supply chain recovery strategy for cascading failures

When a supply chain network faces significant disruptions causing operational interruptions or paralysis, recovery strategies help restore normal operations, mainly focusing on the post-disruption phase of cascading failures. These strategies aim to enhance the network's capacity to absorb and recover from disasters, thus improving resilience (Figure 15). Since the supply chain system is a complex network, the extent and nature of overall damage can vary significantly depending on the location and type of damage, and thus the choice of repair sequence and strategy will directly affect the final recovery outcome. In addition, in practical applications, the formulation of recovery strategies often faces a trade-off between cost and timeliness. For example, rapidly concentrating efforts on repairing key nodes can significantly shorten downtime but may result in high economic costs, whereas phased recovery may be less costly but could

prolong the duration of disruption. This balance between resource allocation and efficiency during the long-term recovery phase is also a factor that must be considered when developing post-disruption optimization strategies. Therefore, recovery strategies are often formulated based on an assessment of the impact of network failures and recovery performance. Recovery of damaged links or nodes typically requires different types and amounts of resources, including repair time, economic costs, and resource allocation, necessitating comprehensive planning for the specific network. Recovery strategies are often based on assessments of network failure impacts. Many scholars use fault tree analysis, failure simulation, and data analysis to study cascading failure mechanisms and impacts. By evaluating the scope, severity, and duration of failures' effects on various links and the entire network, targeted recovery strategies can be developed. Geng et al.[140] developed a self-organizing cascading failure model for cluster supply chains, proposing local self-reconstruction strategies. Fu et al.[141] developed a two-stage recovery strategy for automotive supply chains: recovering degraded nodes first, then isolated nodes. Li et al.[142] constructed a supply chain disruption propagation model considering recovery strategies and proposed using a memetic algorithm to determine the recovery node set under resource constraints. Zhang et al.[143] created a mixed-failure model for cyber-physical supply chains and proposed a two-stage recovery strategy, combining in-event and post-event recovery with time constraints. Vimal[144] analyzed the ripple effects of copper supply chain disruptions, suggesting strategies such as expanding safety stock, multi-source procurement, optimizing transportation, and using project management tools to restore the supply chain.

This section summarizes optimization strategies for cascading failures in supply chains across three stages: prevention, propagation, and recovery. Prevention focuses on reducing the chance of chain reactions through actions such as protecting critical nodes, optimizing layouts and redundancy, and establishing early-warning systems. Propagation control involves real-time, dynamic interventions—e.g., resource scheduling, network reconfiguration, and risk isolation—to curb failure spread. Recovery centers on repair and reconstruction based on damage severity and available resources, balancing cost and efficiency to restore functionality. Together, these strategies form a full life-cycle optimization framework, each stage differing in objectives, methods, and applicable conditions.

7. Challenges and Pespectives for Future Development

Although research on supply chain cascading failures has made significant progress, challenges remain due to the complex and changing market environment and the evolution of supply chain systems. Table 3 summarizes the literature from the three years, which studies have investigated specific aspects of the research area in the last three years. Existing research focuses mainly on failure propagation mechanisms and modeling methods, but there is still room for improvement in network coupling, model authenticity, recovery optimization, and risk prediction. The following key challenges require further investigation:

1) Developing multi-layer coupled networks

With the development of the Internet of Things and geopolitical factors, supply chains are increasingly intertwined with other social networks. Faced with a constantly changing market, the forms and demands of supply chains are becoming more complex. However, existing research on supply chain cascade failures mainly focuses on single-type supply chain networks, analyzing participants and flow demands while neglecting interactions at various levels. Future research should focus on assessing and optimizing the resilience of multi-layer coupled supply chain networks, particularly in accurately depicting dependencies across different networks to enhance supply chain reliability. For example, in outsourced manufacturing supply chains, complex interactions occur between enterprises, manufacturers, and logistics providers, involving multiple sub-networks. Therefore, building comprehensive, multi-dimensional coupled network

Table 3: Analysis of literature on cascading failures in supply chains (past three years)

Literatures	Scenarios						Network structures							Cascading failure models								Optimization					
	General supply chain	Assembly supply chain	Healthcare supply chain	Maritime supply chain	Automotive manufacturing supply chain	Agricultural product supply chain	Single-layer	Multi-layer	Mesh structure	Tree structure	Clustered structure	Chain structure	Centralized structure	Load-capacity model	Agent-based modeling	I-O model	Petri net-based modeling	Bayesian networks	Epidemic model	Coupled mapping lattice model	Cellular automaton model	Identify and strengthen key components	Optimizing network topology	Risk early warning	Management improvement	Real-time mitigation strategy838	Recovery strategy
[144]	•	–	–	–	–	–	–	•	•	–	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	•
[137]	–	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	•	–	–
[141]	–	–	–	–	•	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	•
[142]	•	–	–	–	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	•
[143]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	•
[120]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	•
[34]	–	–	•	–	–	–	–	•	•	–	–	–	–	○	–	–	–	–	–	–	–	•	–	–	–	–	–
[129]	•	–	–	–	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[74]	•	–	–	–	–	–	–	•	–	•	–	–	–	•	–	–	–	–	–	–	–	•	–	–	–	–	–
[64]	•	–	–	–	•	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[71]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	•	•	–	–	–	–
[133]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[87]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
[88]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[99]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–
[65]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[72]	•	–	–	–	–	–	•	–	•	–	•	–	–	•	–	–	–	–	–	–	–	–	•	–	•	–	–
[145]	•	–	–	–	–	–	–	•	•	–	–	–	–	–	–	–	–	•	–	–	–	•	–	–	•	–	–
[80]	•	–	–	–	–	–	•	–	–	–	–	•	–	–	–	–	–	–	–	•	–	–	–	–	–	–	–
[58]	–	–	–	–	–	•	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	•	–	–
[59]	–	–	–	–	–	•	–	•	•	–	–	–	–	–	–	–	–	–	–	–	–	–	•	–	–	–	–
[62]	•	–	–	–	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	•	•	–	–	–	–
[35]	•	–	–	–	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	•	–	–
[51]	–	–	–	–	–	•	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	•	–	–	•	–	•
[49]	–	–	–	–	•	–	–	–	•	–	–	–	–	•	–	–	–	–	–	–	–	•	–	–	–	–	–
[53]	–	–	–	–	–	•	•	–	•	–	–	–	–	–	–	–	–	–	–	–	–	•	–	–	–	–	–
[33]	–	–	•	–	–	–	•	–	•	–	–	–	–	–	–	–	–	–	–	–	–	•	–	–	–	–	–
[46]	–	–	–	–	•	–	–	–	•	–	–	–	–	•	–	–	–	–	–	–	–	•	–	–	–	–	–
[17]	•	–	–	–	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	•	–	–	–	–	–
[21]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	•
[26]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[30]	•	–	–	–	–	–	–	•	–	–	–	–	–	•	–	–	–	–	–	–	–	•	–	–	•	–	–
[24]	•	–	–	–	–	–	•	–	•	•	–	–	–	–	–	–	–	–	–	–	–	•	–	–	–	–	–
[134]	•	–	–	–	–	–	–	–	–	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	•	–	–
[104]	–	–	–	–	•	–	•	–	•	–	–	–	–	–	–	–	•	–	–	–	–	–	–	–	–	–	•
[86]	•	–	–	–	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	•
[89]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	•	–	–	–	–	–	–	•	–	–	–	–	–
[32]	–	–	•	–	–	–	–	•	•	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
[50]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	•	–	–	–	–
[66]	•	–	–	–	–	–	–	•	•	•	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[131]	•	–	–	–	–	–	–	•	•	–	–	–	–	–	•	–	–	–	–	–	–	–	–	•	–	–	–
[47]	–	–	–	–	•	–	–	•	•	–	–	–	–	–	•	–	–	–	–	–	–	–	–	•	–	–	–
[48]	–	–	–	–	•	–	○	–	•	–	–	–	–	–	–	–	–	•	–	–	–	–	–	•	–	–	–
[121]	–	–	•	–	–	–	•	–	•	–	–	–	–	–	–	–	–	–	–	–	•	•	–	–	–	–	–
[51]	–	–	–	–	–	•	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	•	–	–	–	–	•
[79]	–	–	–	–	–	•	•	–	–	–	–	•	–	–	•	–	–	–	–	–	–	•	–	–	–	–	–
[132]	•	–	–	–	–	–	–	•	–	•	–	–	–	–	○	–	–	–	–	–	–	•	–	•	–	–	•
[135]	•	–	–	–	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	•	–	•	•	–	–
[127]	•	–	–	–	–	–	–	•	•	–	–	–	–	–	–	–	–	–	•	–	–	–	–	–	–	–	–
[111]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	–	–	•	–	–	–	–	–	–	–	–	–
[128]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	–	–	–	•	–	–	–	–	•	•	–	–
[122]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	–	–	–	•	–	•	–	–	•	–	–	–
[139]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	–	–	–	•	–	–	–	–	•	•	–	–
[114]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	–	–	–	•	–	–	–	–	•	•	–	–
[113]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	•	–	–	–	–	–	•	–	–	•	–	–
[126]	•	–	–	–	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	•	–	–	–	–	–
[146]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–
[138]	•	–	–	–	–	–	–	•	•	–	–	–	–	–	•	–	–	–	–	–	–	–	–	–	•	–	•
[110]	–	–	–	•	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	•	–	–	–	–	–
[117]	–	–	–	•	–	–	–	•	•	–	–	–	–	–	–	–	–	–	•	–	–	–	–	–	–	–	–
[116]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	–	–	–	•	–	–	–	–	–	–	–	–
[115]	•	–	–	–	–	–	•	–	•	–	–	–	–	–	–	–	–	–	•	–	–	–	–	–	–	–	–
[18]	•	–	–	–	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[19]	–	•	–	–	–	–	–	•	–	•	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[20]	•	–	–	–	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[41]	–	–	–	•	–	–	–	•	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	•
[38]	–	–	–	•	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[36]	–	–	–	•	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–
[39]	–	–	–	•	–	–	•	–	•	–	–	–	–	•	–	–	–	–	–	–	–	–	–	–	–	–	–

• represents YES, – represents NO, and ○ represents not explicitly stated but inferred as YES.

models and integrating them with technologies such as data science is a key direction for future research on supply chain cascading failures.

2) Enhancing the authenticity of modeling by incorporating real-world scenarios

Although existing models have made progress, a significant gap remains between them and the cascading failure behavior in real-world supply chains. Most research focuses on overload failures, while in practice, supply chains are more prone to fail due to underloading, often overlooked in current models. Additionally, disruptions are typically modeled as complete node or edge failures, neglecting localized disruption effects. As dynamic networks with asymmetric nodes, supply chains inherently operate with incomplete information. Future research should account for varying disruption intensities, impact scopes, information conditions, and target heterogeneity to refine partial failure rules. Furthermore, existing models primarily focus on the impact of key node failures on downstream links but neglect how failures can propagate horizontally through shared links, affecting both upstream and downstream enterprises. To improve practical relevance, future studies should integrate real-world supply chain scenarios, develop realistic failure mechanisms, and introduce comprehensive rule systems to enhance the credibility and predictive power of cascading failure models.

3) Exploring effective recovery optimization strategies

Current research mainly focuses on modeling supply chain cascade failures, while post-failure recovery optimization remains unexplored. As environmental changes increase, relying solely on disruption prevention is insufficient to address supply chain failure risks, and the likelihood and scope of disruptions have become more unpredictable. Enhancing supply chain recovery capabilities has thus become a critical research direction. Future studies should prioritize developing optimal recovery strategies under resource constraints, exploring system recovery mechanisms (automated or semi-automated), and establishing post-disaster recovery optimization plans. Moreover, more realistic models should integrate recovery strategies to analyze network failure processes, improving supply chain adaptability and recovery efficiency after unexpected events.

4) Leveraging AI technologies for enhanced risk prediction

Existing risk assessment methods mainly rely on simulation models, but in complex supply chain systems, their authenticity and accuracy are limited, making it hard to evaluate the risks of supply chain cascade failures. With the rapid development of artificial intelligence (AI), machine learning, and big data technologies, future research can use these advancements to create data-driven risk assessment methods, enhancing predictive capabilities for cascade failures. For example, integrating dynamic behavior models to identify supply chain vulnerabilities, using machine learning to optimize recovery decisions, and leveraging big data to analyze external impacts on supply chain resilience are promising directions. Exploring these areas will improve supply chain risk perception and response capabilities in complex environments.

5) Strengthening system-level risk governance mechanisms

Cascading failures in supply chains are not merely issues of quantitative modeling and prediction but also require the integration of practical governance measures. As cross-industry and cross-sector complex systems, supply chains should adopt long-term governance strategies that integrate economic, social, and environmental dimensions [147]. Governance can be advanced through both bottom-up and top-down approaches: at the operational level (bottom-up), enterprises and local governments should establish joint mechanisms and shared platforms, such as regional emergency supply agreements and shared inventory centers, to enable rapid resource reallocation in the event of critical node failures; at the strategic level (top-down), national or industry bodies should develop emergency response frameworks, mandatory information disclosure standards[148], cross-sector coordination mechanisms, and digital supply chain platforms. Future research could integrate such governance measures into cascading failure models so that simulation results can directly inform the design of actionable risk management policies.

8. Conclusion

As supply chain systems grow in scale and complexity, cascading failures have become a critical threat to their reliability. While extensive research has made significant progress in modeling, analysis, and optimization, challenges remain in network coupling, model realism, recovery optimization, and risk prediction. Furthermore, as modern supply chain models evolve and supply chain networks increasingly couple with other complex networks, cascading failure characteristics have been evolving, exacerbating systemic failure risks.

Future research should develop more realistic, precise, and efficient cascading failure models, supported by advanced analytical methods and recovery strategies, to uncover the mechanisms and reduce impacts. This paper provided a systematic review of the core issues in cascading failures, covering network metrics, failure triggers, modeling methods, and optimization strategies. It also identified limitations in existing research and proposed future directions. It provided a foundation for further studies and stimulated interest in cascading failure research to enhance the reliability and resilience of supply chains.

Acknowledgement

This work is supported in part by the National Natural Science Foundation of China (NSFC) under Grant no. 72431008.

References

[1] J. W. Forrester, Industrial dynamics, Journal of the Operational Research Society 48 (10) (1997) 1037–1041.

[2] R. K. Oliver, M. D. Webber, Supply-chain management: logistics catches up with strategy, in: The Roots of Logistics, 2012, pp. 183–194.

[3] Buldyrev, Sergey V and Parshani, Roni and Paul, Gerald and Stanley, H Eugene and Havlin, Shlomo, Catastrophic cascade of failures in interdependent networks, Nature 464 (7291) (2010) 1025–1028.

[4] Society for Risk Analysis, Risk Analysis Glossary (2018).

[5] X. Yue, D. Mu, C. Wang, H. Ren, R. Peng, J. Du, Critical risks in global supply networks: A static structure and dynamic propagation perspective, Reliability Engineering & System Safety 242 (2024) 109728.

[6] C. Qian, D. Zhao, M. Zhong, H. Peng, W. Wang, Modeling and analysis of cascading failures in multilayer higher-order networks, Reliability Engineering & System Safety 253 (2025) 110497.

[7] J. Zhong, H. Sanhedrai, F. Zhang, Y. Yang, S. Guo, S. Yang, D. Li, Network endurance against cascading overload failure, Reliability Engineering & System Safety 201 (2020) 106916.

[8] C.-Y. Huang, T.-C. Juan, H.-C. Kuo, J.-H. Chen, Track deflection of typhoon maria (2018) during a westbound passage offshore of northern taiwan: Topographic influence, Monthly Weather Review 148 (11) (2020) 4519–4544.

[9] P. Chapman, M. Christopher, U. Jüttner, H. Peck, R. Wilding, Identifying and managing supply chain vulnerability, Logistics and Transport Focus 4 (4) (2002).

[10] U. Jüttner, Supply chain risk management: Understanding the business requirements from a practitioner perspective, The International Journal of Logistics Management 16 (1) (2005) 120–141.

[11] H. Peck, Drivers of supply chain vulnerability: an integrated framework, International Journal of Physical Distribution & Logistics Management 35 (4) (2005) 210–232.

[12] G. Svensson, A conceptual framework for the analysis of vulnerability in supply chains, International Journal of Physical Distribution & Logistics Management 30 (9) (2000) 731–750.

[13] L. Geng, R. Xiao, S. Xie, Research on self-organization in resilient recovery of cluster supply chains, Discrete Dynamics in Nature and Society 2013 (2013) 1–11.

[14] A. Ishigaki, H. Higashi, T. Sakamoto, S. Shibahara, The great east-japan earthquake and devastating tsunami: an update and lessons from the past great earthquakes in japan since 1923, The Tohoku journal of experimental medicine 229 (4) (2013) 287–299.

[15] J. M.-y. Lee, E. Y.-c. Wong, Suez canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain, in: MATEC web of conferences, Vol. 339, EDP Sciences, 2021, p. 01019.

[16] L. Tang, K. Jing, J. He, H. E. Stanley, Complex interdependent supply chain networks: Cascading failure and robustness, Physica A: Statistical Mechanics and its Applications 443 (2016) 58–69.

[17] L. Zhang, J. Zhou, Y. Ma, L. Shen, Sequential topology attack of supply chain networks based on reinforcement learning, in: 2022 International Conference on Cyber-Physical Social Intelligence (ICCSI), 2022, pp. 744–749.

[18] Wu, Tongyu and Li, Minjie and Lin, Shuangjiao, Vulnerability Analysis of a Multilayer Logistics Network against Cascading Failure, Algorithms 17 (9) (2024) 414.

[19] Luo, Li and Nian, Fuzhong, Cascading propagation of events in hierarchical supply chain networks, Nonlinear Dynamics 113 (13) (2025) 17057–17080.

[20] Habibi, Farhad and Chakrabortty, Ripon K and Abbasi, Alireza and Ho, William, Investigating disruption propagation and resilience of supply chain networks: interplay of tiers and connections, International Journal of Production Research (2025) 1–23.

[21] L. Zhang, J. Zhou, F. Zhang, P. Qiao, Y. Ma, Enhancing resilience of interdependent supply chain networks against delay-time cascading failures with recovery resource allocation, IEEE Transactions on Reliability (2024) 1–15.

[22] S. Xiao, G. Xiao, Nisp1-06: On intentional attacks and protections in complex communication networks, in: IEEE Globecom 2006, IEEE, 2006, pp. 1–5.

[23] C. Zhang, J. E. Ramirez-Marquez, Protecting critical infrastructures against intentional attacks: A two-stage game with incomplete information, IIE Transactions 45 (3) (2013) 244–258.

[24] M. Papachristou, M. A. Rahimian, Structural measures of resilience for supply chains, arXiv preprint arXiv:2303.12660 (2023).

[25] M. Gomez, S. Garcia, S. Rajtmajer, C. Grady, A. Mejia, Fragility of a multilayer network of intranational supply chains, Applied Network Science 5 (2020).

[26] X. Shi, W. Long, Y. Li, D. Deng, Robustness of interdependent supply chain networks against both functional and structural cascading failures, Physica A: Statistical Mechanics and its Applications 586 (2022) 126518.

[27] Hao, Xiaoqing and An, Haizhong and Jiang, Meihui and Sun, Xiaoqi, Supply shock propagation in the multi-layer network of global steel product chain: Additive effect of trade and production, Resources Policy 89 (2024) 104655.

[28] L. Tang, K. Jing, J. He, H. E. Stanley, Robustness of assembly supply chain networks by considering risk propagation and cascading failure, Physica A: Statistical Mechanics and its Applications 459 (2016) 129–139.

[29] H. Nguyen, T. C. Sharkey, S. Wheeler, J. E. Mitchell, W. A. Wallace, Towards the development of quantitative resilience indices for multi-echelon assembly supply chains, Omega 99 (2021) 102199.

[30] Q. Du, S. Li, Y. Zhang, Y. Zhang, Robustness of prefabricated construction supply chain network against underload cascading failure, RAIRO - Operations Research 58 (2024) 4905–4925.

[31] A. Skeete, T. Keyser, et al., Modelling cascading failure in assembly supply chain networks, in: IIE Annual Conference. Proceedings, Institute of Industrial and Systems Engineers (IISE), 2017, pp. 1424–1429.

[32] K. M. Lavassani, B. Movahedi, R. J. Iyengar, Multi-layer, multi-tier analysis of global supply chain in medical equipment sector: network science application, Transnational Corporations Review 14 (2) (2022) 193–209.

[33] K. M. Lavassani, Z. M. Boyd, B. Movahedi, J. Vasquez, Ten-tier and multi-scale supply chain network analysis of medical equipment: random failure & intelligent attack analysis, International Journal of Production Research 61 (24) (2023) 8468–8492.

[34] B. D. Trump, M. S. Golan, J. M. Keisler, J. C. Cegan, I. Linkov, Vaccine supply chain: Resilience-by-design and resilience-by-intervention, Vaccine 40 (2022) 1695–1698.

[35] K. Xu, Y. Cui, J. Liu, Modeling the resilience of liner shipping network under cascading effects: Considering distance constraints and transportation time, Computers & Industrial Engineering 197 (2024) 110559.

[36] Liupeng, Jiang and Guangsheng, Wang and Xuejun, Feng and Tong, Yu and Zhiyi, Lei, Study on cascading failure vulnerability of the 21st-century Maritime Silk Road container shipping network, Journal of Transport Geography 117 (2024) 103891.

[37] Verschuur, Jasper and Pant, Raghav and Koks, Elco and Hall, Jim, A systemic risk framework to improve the resilience of port and supply-chain networks to natural hazards, Maritime Economics & Logistics 24 (3) (2022) 489–506.

[38] Ding, Chaojun and Wang, Zhilin and Xu, Susu, Study on the Cascading Failure Robustness of the Belt and Road Land–Sea Transport Network under Emergencies, Symmetry 16 (6) (2024) 736.

[39] Xu, Yang and Peng, Peng and Claramunt, Christophe and Lu, Feng and Yan, Ran, Cascading failure modelling in global container shipping network using mass vessel trajectory data, Reliability Engineering & System Safety 249 (2024) 110231.

[40] Xu, Yang and Peng, Peng and Claramunt, Christophe and Xie, Wenxin and Lu, Feng, Modeling cascading risk diffusion in global container shipping network under dynamic flow reassignment, Reliability Engineering & System Safety 265 (2026) 111530.

[41] Lu, Zhigang and Qiu, Wenhao, Resilience Analysis of Seaport–Dry-Port Network in Container Transport: Multi-Stage Load Redistribution Dynamics Following Cascade Failure, Systems 13 (4) (2025) 299.

[42] T. Levin, A. Botterud, W. N. Mann, J. Kwon, Z. Zhou, Extreme weather and electricity markets: Key lessons from the february 2021 texas crisis, Joule 6 (1) (2022) 1–7.

[43] H. Carvalho, A. P. Barroso, V. H. Machado, S. Azevedo, V. Cruz-Machado, Supply chain redesign for resilience using simulation, Computers & Industrial Engineering 62 (2012) 329–341.

[44] A. Brintrup, A. Ledwoch, J. Barros, Topological robustness of the global automotive industry, Logistics Research 9 (2015).

[45] R. Xiao, S. Xie, T. Chen, Vulnerability of interaction-based supply chain network and its self-organised criticality, International Journal of Computing Science and Mathematics 8 (4) (2017) 324–341.

[46] J. Feng, M. Cai, F. Dai, T. Bu, X. Zhang, H. Zheng, X. Lu, Modeling supply chain interaction and disruption: Insights from real-world data and complex adaptive system, arXiv preprint arXiv:2405.10818 (2024).

[47] C. Ou, F. Pan, S. Lin, Cascade failure-based identification and resilience of critical nodes in automotive supply chain networks, Sustainability 16 (2024) 5514.

[48] T. Zhang, D. Tang, P. Fan, Q. Wang, P. Wang, A probabilistic graphical model for predicting cascade failures of electric vehicle charging networks caused by hurricanes, IEEE Transactions on Smart Grid (2024) 1–1.

[49] H. Hao, Z. Ma, A. Wang, W. Xing, H. Song, P. Zhao, J. Wei, S. Zheng, Modeling and assessing the robustness of the lithium global trade system against cascading failures, Resources Policy 85 (2023) 103822.

[50] X. Ouyang, L. Liu, W. Chen, C. Wang, X. Sun, C. He, G. Liu, Systematic risks of the global lithium supply chain network: From static topological structures to cascading failure dynamics, Environmental Science & Technology 58 (2024) 22135–22147.

[51] Z. Li, P. Zhao, X. Han, Agri-food supply chain network disruption propagation and recovery based on cascading failure, Physica A: Statistical Mechanics and its Applications 589 (2022) 126611.

[52] P. Zhao, Z. Li, X. Han, X. Duan, Supply chain network resilience by considering disruption propagation: Topological and operational perspectives, IEEE Systems Journal 16 (2022) 5305–5316.

[53] R. Vaid, K. Jain, G. K. Sahi, P. Modi, Designing a resilient agriculture supply network for mitigating the disruptions, Annals of Operations Research (2024).

[54] R. Govindan, T. Al-Ansari, Computational decision framework for enhancing resilience of the energy, water and food nexus in risky environments, Renewable and Sustainable Energy Reviews 112 (2019) 653–668.

[55] S. M. Gholami-Zanjani, W. Klibi, M. S. Jabalameli, M. S. Pishvaee, The design of resilient food supply chain networks prone to epidemic disruptions, International Journal of Production Economics 233 (2021) 108001.

[56] J. Aboah, M. M. Wilson, K. Bicknell, K. M. Rich, Identifying the precursors of vulnerability in agricultural value chains: A system dynamics approach, International Journal of Production Research 59 (2019) 683–701.

[57] A. Berardy, M. V. Chester, Climate change vulnerability in the food, energy, and water nexus: concerns for agricultural production in arizona and its urban export supply, Environmental Research Letters 12 (3) (2017) 035004.

[58] H. Chen, G. Chen, Q. Zhang, X. Zhang, Analysis of network disruption evolution of chinese fresh cold chain under covid-19, PLOS ONE 18 (2023) e0278697.

[59] N. Geng, Y. Lu, Optimizing the resilience of the fresh agricultural product supply chain considering supply chain disruptions, Research SquarePreprint (2024).

[60] M. Karanam, L. Krishnanand, V. K. Manupati, Quantifying performance indicators in perishable food supply chain networks: Assessing dynamic performance under ripple effects, Computers & Industrial Engineering (2025) 110873.

[61] Y. Li, Networked analysis approach of supply chain network, Journal of Networks 9 (2014).

[62] Y. Cao, X. Xin, P. Jarumaneeroj, H. Li, Y. Feng, J. Wang, X. Wang, R. Pyne, Z. Yang, Data-driven resilience analysis of the global container shipping network against two cascading failures, Transportation Research Part E: Logistics and Transportation Review 193 (2025) 103857.

[63] S. Zihao, S. Yurong, Risk cascading effect model in the supply chain networks, in: 2018 5th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), IEEE, 2018, pp. 138–141.

[64] Q. Xiao, G. Song, Z. Gao, The effect of strategic alliances on supply chain resilience under external shocks, Journal of Industrial and Production Engineering 41 (6) (2024) 556–575.

[65] B. Lu, R. Li, Overload cascading failure detection algorithm for multi-layer supply chain network considering delay probability factor, RAIRO - Operations Research 58 (2024) 5403–5419.

[66] B. Li, D. Saad, Infection-induced cascading failures – impact and mitigation, Communications Physics 7 (2024).

[67] C. Colon, Åke Brännström, E. Rovenskaya, U. Dieckmann, Fragmentation of production amplifies systemic risks from extreme events in supply-chain networks, PLOS ONE 15 (2020) e0244196.

[68] L. Zhang, J. Zhou, Y. Ma, Robustness of interdependent supply chain networks considering disruption propagation, in: Advances in Reliability, Safety and Security: Collection of Extended Abstracts, ESREL 2024, European Safety and Reliability Association (ESRA), Nanjing, Jiangsu, China, 2024.

[69] H. Guo, Y. Cheng, X. Xie, et al., A new model for supply chain risk propagation considering herd mentality and risk preference under warning information on multiplex networks, Physica A: Statistical Mechanics and Its Applications 545 (2020) 123506.

[70] J. Sun, J. Tang, W. Fu, Z. Chen, Y. Niu, Construction of a multi-echelon supply chain complex network evolution model and robustness analysis of cascading failure, Computers & Industrial Engineering 144 (2020) 106457.

[71] X. Yue, D. Mu, C. Wang, H. Ren, P. Ghadimi, Topological structure and covid-19 related risk propagation in tft-lcd supply networks, International Journal of Production Research 61 (8) (2023) 2758–2778.

[72] Y. Liu, C. Du, L. Shi, Establishing the robustness of chip trade networks by dynamically considering topology and risk cascading propagation, Scientific Reports 14 (2024).

[73] X. Wang, H. Li, H. Yao, D. Zhu, N. Liu, Simulation analysis of the spread of a supply crisis based on the global natural graphite trade network, Resources Policy 59 (2018) 200–209.

[74] L. Wang, F. Yao, Z. Wu, R. Gao, Simulation system design for critical-node detection and robustness analysis of supply chains, Enterprise Information Systems 18 (5) (2024) 2326673.

[75] G. M. Chodur, X. Zhao, E. Biehl, J. Mitrani-Reiser, R. Neff, Assessing food system vulnerabilities: a fault tree modeling approach, BMC Public Health 18 (2018).

[76] N. Goldbeck, P. Angeloudis, W. Ochieng, Optimal supply chain resilience with consideration of failure propagation and repair logistics, Transportation Research Part E: Logistics and Transportation Review 133 (2020) 101830.

[77] Y. Wang, R. Xiao, An ant colony based resilience approach to cascading failures in cluster supply network, Physica A: Statistical Mechanics and its Applications 462 (2016) 150–166.

[78] Y. Zeng, R. Xiao, Modelling of cluster supply network with cascading failure spread and its vulnerability analysis, International Journal of Production Research 52 (2014) 6938–6953.

[79] C. Diem, W. Schueller, M. Gerschberger, J. Stangl, B. Conrady, M. Gerschberger, S. Thurner, Supply network stress-testing of food security on the establishment-level, International Journal of Production Research (2024) 1–25.

[80] J. Gudmundsson, J. L. Hougaard, J. Sethuraman, Managing cascading disruptions through optimal liability assignment, arXiv preprint arXiv:2408.07361 (2024).

[81] R. Bierkandt, L. Wenz, S. N. Willner, A. Levermann, Acclimate—a model for economic damage propagation. part 1: basic formulation of damage transfer within a global supply network and damage conserving dynamics, Environment Systems and Decisions 34 (2014) 507–524.

[82] S. Allesina, A. Azzi, D. Battini, A. Regattieri, Performance measurement in supply chains: new network analysis and entropic indexes, International Journal of Production Research 48 (2009) 2297–2321.

[83] C. Huixia, Q. Jianlong, G. Ming, Z. Runfa, Resilience of cascading failures in directed weighted supply chain networks, Control Theory & Applications 38 (11) (2021).

[84] Z. Kan, Research on supply chain coordination technology with a hybrid topology structure, Metallurgical Automation 39 (02) (2015) 17–21.

[85] Y. Wang, F. Zhang, Modeling and analysis of under-load-based cascading failures in supply chain networks, Nonlinear Dynamics 92 (2018) 1403–1417.

[86] H. Liu, Y. Han, J. Ni, A. Zhu, Modelling underload cascading failure and mitigation strategy of supply chain complex network in covid-19, Mathematical Problems in Engineering 2022 (2022) 1–12.

[87] N. Mu, S. Han, J. Liu, Y. Wang, Z. Wang, A. Mardani, Z.-S. Chen, Exploring risk propagation in a multi-level supply chain network: a perspective of node perturbation, Annals of Operations Research (2024).

[88] H. Wang, Z. Zhou, Identification of key risk nodes and invulnerability analysis of construction supply chain networks, Buildings 14 (2024) 1997.

[89] H. Kang, K.-M. Lee, J.-S. Yang, The potential for cascading failures in the international trade network, PLOS ONE 19 (2024) e0299833.

[90] K. Zhao, Z. Zuo, J. V. Blackhurst, Modelling supply chain adaptation for disruptions: An empirically grounded complex adaptive systems approach, Journal of Operations Management 65 (2019) 190–212.

[91] D. C. Chatfield, J. C. Hayya, D. P. Cook, Stockout propagation and amplification in supply chain inventory systems, International Journal of Production Research 51 (2013) 1491–1507.

[92] L. Geng, R. Xiao, X. Xu, Research on mas-based supply chain resilience and its self-organized criticality, Discrete Dynamics in Nature and Society 2014 (2014) 1–14.

[93] C. Tan, P. Tan, S. Lee, M. Pham, An inoperability input-output model (iim) for disruption propagation analysis, in: 2013 IEEE International Conference on Industrial Engineering and Engineering Management, IEEE, 2013, pp. 186–190.

[94] H. Wei, M. Dong, S. Sun, Inoperability input-output modeling (iim) of disruptions to supply chain networks, Systems Engineering 13 (4) (2010) 324–339.

[95] D. R. Baqaee, Cascading failures in production networks, Econometrica 86 (5) (2018) 1819–1838.

[96] L. Ocampo, J. G. Masbad, V. M. Noel, R. S. Omega, Supply-side inoperability input–output model (siim) for risk analysis in manufacturing systems, Journal of Manufacturing Systems 41 (2016) 76–85.

[97] R. Omega, V. Noel, J. Masbad, L. Ocampo, Modelling supply risks in interdependent manufacturing systems: A case study, Advances in Production Engineering & Management 11 (2016) 115–125.

[98] M. Taschereau-Dumouchel, Cascades and fluctuations in an economy with an endogenous production network, Available at SSRN 3115854 (2020).

[99] B. D. Sarkar, R. Shankar, A. K. Kar, A scenario-based interval-input output model to analyze the risk of covid-19 pandemic in port logistics, Journal of Modelling in Management 17 (4) (2022) 1456–1480.

[100] L. Xing, X. Dong, J. Guan, X. Qiao, Betweenness centrality for similarity-weight network and its application to measuring industrial sectors' pivotability on the global value chain, Physica A: Statistical Mechanics and its Applications 516 (2019) 19–36.

[101] K. D. S. Yu, K. B. Aviso, M. K. A. Aziz, N. A. Morad, M. A. B. Promentilla, J. R. Santos, R. R. Tan, Inoperability input–output modeling approach to risk analysis in biomass supply chains, Process Design Strategies for Biomass Conversion Systems (2015) 183–213.

[102] G. Fridgen, C. Stepanek, T. Wolf, Investigation of exogenous shocks in complex supply networks – a modular petri net approach, International Journal of Production Research 53 (2014) 1387–1408.

[103] G. Frigen, C. Stepanek, T. Wolf, Simulating exogenous shocks in complex supply networks using modular stochastic petri nets, in: ECIS 2012 Proceedings, Association for Information Systems AIS Electronic Library (AISeL), 2012, p. 195.

[104] J. Skorupski, A. A. Tubis, S. Werbińska-Wojciechowska, A. Wróblewski, Petri nets-based method for operational risk analysis in supply chains based on timeliness and recovery time, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 238 (3) (2024) 523–539.

[105] J. Wang, R. Dou, R. Muddada, W. Zhang, Management of a holistic supply chain network for proactive resilience: Theory and case study, Computers & Industrial Engineering 125 (2018) 668–677.

[106] S. Hosseini, D. Ivanov, A. Dolgui, Ripple effect modelling of supplier disruption: integrated markov chain and dynamic bayesian network approach, International Journal of Production Research 58 (2019) 3284–3303.

[107] N. U. I. HOSSAIN, S. E. Amrani, R. Jaradat, M. Marufuzzaman, R. Buchanan, C. Rinaudo, M. Hamilton, Modeling and assessing interdependencies between critical infrastructures using bayesian network: A case study of inland waterway port and surrounding supply chain network, Reliability Engineering & System Safety 198 (2020) 106898.

[108] Zhang, Yiqi and Ma, Yanhui and Wang, Le and Wang, Zhiqiong and Zhang, Lixia, A Bayesian network based framework for ripple effect analysis in cross-tier shipbuilding supply chains, Expert Systems with Applications 296 (2026) 129184.

[109] Nocera, Fabrizio and Contento, Alessandro and Gardoni, Paolo, Risk analysis of supply chains: The role of supporting structures and infrastructure, Reliability Engineering & System Safety 241 (2024) 109623.

[110] Kang, Xinyu and Wang, Minxi and Chen, Lu and Li, Xin, Supply risk propagation of global copper industry chain based on multi-layer complex network, Resources Policy 85 (2023) 103797.

[111] Song, Lei and Qian, Shuoge and Chen, Yu, Credit guarantee, and risk contagion in guarantee networks: A supply chain perspective, Mathematics and Financial Economics (2025) 1–34.

[112] Yu, Yu and Li, Zhaoyue and Wei, Yuqi and Zhu, Weiwei, Risk Propagation Evaluation of Logistics Network Based on Freight Information: Taking the Yumman Platform as an Example, Available at SSRN 4572053.

[113] Zheng, Xinxin and Li, Huajiao and Liu, Xiaojie and Wang, Xingxing and Zhang, Yuqi and Tang, Qianyong and Ren, Bo, Supply risk propagation in international trade networks of the tungsten industry chain, Humanities and Social Sciences Communications 12 (1) (2025) 1–16.

[114] Liu, Chao and Zhao, Ting and Wang, Gaoshang and Liu, Shengqian, Research on the supply risk propagation in the global iron ore trade network, Frontiers in Earth Science 13 (2025) 1520813.

[115] Yao, Qianyi and Fan, Ruguo and Chen, Rongkai and Qian, Rourou, A model of the enterprise supply chain risk propagation based on partially mapping two-layer complex networks, Physica A: Statistical Mechanics and its Applications 613 (2023) 128506.

[116] Xie, Xiaofeng and Zhang, Fengying and Liu, Li and Yang, Yang and Hu, Xiuying, Assessment of associated credit risk in the supply chain based on trade credit risk contagion, PloS One 18 (2) (2023) e0281616.

[117] Yu, Ping and Wang, Zhiping and Sun, Ya'nan and Wang, Peiwen, Supply Chain Risk Diffusion in Partially Mapping Double-Layer Hypernetworks, Entropy 25 (5) (2023) 747.

[118] X. Liu, K. Wen, Y. Xu, G. Yu, Non-linear behavior of supply chains under chaos environment with disruptions: Based on coupled map lattices, Intelligent Decision Technologies 11 (2017) 399–414.

[119] Y. Hong, New model of food supply chain finance based on the internet of things and blockchain, Mobile Information Systems 2021 (2021) 1–8.

[120] R. Suryawanshi, R. P. Deore, Simulation of supply chain performance in the period of implicit uncertainty using cellular automata, International Journal of Mathematical, Engineering and Management Sciences 8 (2023) 163–175.

[121] H. Shan, J. Fei, J. Shi, Q. Zhang, F. Yan, J. Qiu, Investigation of risk propagation and control in emergency response logistics networks: A cellular automata based approach, Computers & Industrial Engineering 193 (2024) 110267.

[122] Ma, Jinrong and Hou, Qiaoming, Nonlinear dynamics of risk propagation in supply chains: a stochastic SEIR-cellular automaton approach, Nonlinear Dynamics (2025) 1–33.

[123] Y. Yan, L. Xiao, Z. Xintian, Analyzing and identifying of cascading failure in supply chain networks, in: 2010 International Conference on Logistics Systems and Intelligent Management (ICLSIM), Vol. 3, IEEE, 2010, pp. 1292–1295.

[124] A. Pavlov, D. Ivanov, A. Dolgui, B. Sokolov, Hybrid fuzzy-probabilistic approach to supply chain resilience assessment, IEEE Transactions on Engineering Management 65 (2018) 303–315.

[125] E. E. Kosasih, A. Brintrup, A machine learning approach for predicting hidden links in supply chain with graph neural networks, International Journal of Production Research 60 (2021) 5380–5393.

[126] Hua, Zhen and Xia, Yongxiang and Chen, Yucheng and Sun, Weigang, Identification of critical nodes in supply chain networks, AIP Advances 15 (1) (2025).

[127] Liu, Qiyan and Adriaens, Peter, Unraveling risk propagation in the copper value chain: A firm-level network analysis, Resources, Conservation and Recycling 222 (2025) 108435.

[128] Meng, Zhenghao and Sun, Han and Daigo, Ichiro and Guan, Yuru and Shan, Yuli, Technological Risks Disrupting Trade Stability in the Global Lithium Supply Chain Network, iScience (2025).

[129] H. Liu, Y. Han, A. Zhu, Modeling supply chain viability and adaptation against underload cascading failure during the covid-19 pandemic, Nonlinear dynamics 110 (3) (2022) 2931–2947.

[130] Z. Fan, H. Ding, W. Zhang, Research on cold chain logistics path optimization considering cascading failure, IOP Conference Series: Materials Science and Engineering 787 (2020) 012031.

[131] R. S. Khan, M. R. M. Sirazy, R. Das, S. Rahman, An ai and ml-enabled framework for proactive risk mitigation and resilience optimization in global supply chains during national emergencies, Sage Science Review of Applied Machine Learning 5 (2) (2022) 127–144.

[132] D. Ivanov, Blackout and supply chains: Cross-structural ripple effect, performance, resilience and viability impact analysis, Annals of Operations Research (2022).

[133] C. miao, Y. wan, M. kang, F. Xiang, Topological analysis, endogenous mechanisms, and supply risk propagation in the polycrystalline silicon trade dependency network, Journal of Cleaner Production 439 (2024) 140657.

[134] T. Ding, Q. Liu, X. Li, M. Liu, Influencing factors of inflammability of supply chain quality risk cascade failure, Financial Engineering and Risk Management 6 (3) (2023) –.

[135] C. Wang, H. Yang, X. Hu, X. He, J. Liu, C. Liang, M. K. Lim, Deciphering iron ore trade dynamics: Supply disruption risk propagation in global networks through an improved cascading failure model, Resources Policy 95 (2024) 105157.

[136] Q. Yang, C. M. Scoglio, D. M. Gruenbacher, Robustness of supply chain networks against underload cascading failures, Physica A: Statistical Mechanics and its Applications 563 (2021) 125466.

[137] S. Sengupta, S. Choudhary, R. Obayi, R. Nayak, Reducing food loss through sustainable business models and agricultural innovation systems, Supply Chain Management: An International Journal 29 (2024) 540–572.

[138] Ivanov, Dmitry, Collaborative emergency adaptation for ripple effect mitigation in intertwined supply networks, Annals of Operations Research (2023) 1–17.

[139] Liu, Xiaojing and Gao, Jie and He, Mingfeng, Risk Contagion Mechanism and Control Strategies in Supply Chain Finance Using SEIR Epidemic Model from the Perspective of Commercial Banks, Mathematics 13 (13) (2025) 2051.

[140] L. Geng, R. Xiao, J. Chen, Resilience design of healthcare resources supply network based on self-organized criticality, Healthcare 8 (2020) 245.

[141] X. Fu, X. Xu, W. Li, Cascading failure resilience analysis and recovery of automotive manufacturing supply chain networks considering enterprise roles, Physica A: Statistical Mechanics and its Applications 634 (2024) 129478.

[142] Z. Li, P. Zhao, C. Wang, Y. Mi, Research on recovery strategies of supply chain network under disruption propagation using memetic algorithm, Advances in Production Engineering & Management 19 (2024) 21–30.

[143] L. Zhang, J. Zhou, Y. Ma, X. Wang, F. Zhang, Resilience improvement of cyber-physical supply chain networks considering cascading failures with mixed failure modes, Computers & Industrial Engineering 187 (2024) 109812.

[144] V. K.E.K, S. P. Nadeem, M. Ravichandran, M. Ethirajan, J. Kandasamy, Resilience strategies to recover from the cascading ripple effect in a copper supply chain through project management, Operations Management Research 15 (2022) 440–460.

[145] N. U. I. Hossain, I. Ahmed, S. Chowdhury, K. Govindan, R. Jaradat, Assessing the cascading impact of industry 4.0 disruption on supply chain analytics through the lens of dependency concepts, Computers & Industrial Engineering 192 (2024) 110225.

[146] Tabachová, Zlata and Diem, Christian and Borsos, András and Burger, Csaba and Thurner, Stefan, Estimating the impact of supply chain network contagion on financial stability, Journal of Financial Stability 75 (2024) 101336.

[147] Colon, Celian and Hochrainer-Stigler, Stefan, Systemic risks in supply chains: a need for system-level governance, Supply Chain Management: An International Journal 28 (4) (2023) 682–694.

[148] Guidotti, Roberto and Gardoni, Paolo and Chen, Yuguo, Network reliability analysis with link and nodal weights and auxiliary nodes, Structural Safety 65 (2017) 12–26.