Risk Assessment Models Identify Potential Supply Chain Disruptions Through Scenario Analysis Monte Carlo Simulation Predictive Analytics

Benjamin Yaw Kokroko[1]; Joseph Kobi[2]; Edmund Kofi Yeboah[3]

[1]Worcester Polytechnic Institute School of Business Master's Degree Operations Management and Supply Chain Analytics Department of Business Analytics and Operations Analytics
[2]Worcester Polytechnic Institute School of Business Master's Degree Business Analytics Department of Business Analytics and Operations Analytics
[3]Clark University School of Business Master’s Degree FinTech Concentration Department of Finance

Publication Date: 2025/11/08

Abstract: The modern global supply chains are more vulnerable to disruptions than ever due to their complex geographically distributed designs. This in-depth research evaluates three advanced analytical tools, scenario analysis, Monte Carlo simulation, and predictive analytics, and their application to the problem of supply chain disruption to prevent its development into an operational crisis. This study shows how organizations use these methods to quantify the disruption probabilities, vulnerability exposure and mitigation strategies by using systematic literature review, quantitative modeling, and empirical case analysis. Monte Carlo simulation can be used to give probabilistic quantification of risks in multi-tier supply networks and, through this approach, produce probability distributions of possible outcomes in the thousands of possible outcomes. Scenario analysis allows the strategic assessment of the possible disruption pathways based on systematic exploration of the possible what-if. Using machine learning algorithms and patterns of historical data, predictive analytics provides real-time functionality of risk detection. Findings have shown that hybrid methods which incorporate both these methods can have high predictive accuracy (76-86%), which is better than single-method methods. The analysis of the applications in the manufacturing, healthcare, and food supply chain shows that there are sector-related profiles of risks and mitigation needs. Results indicate the sensitivity of the lower-level visibility of suppliers since the disturbance of Tier 3 is transmitted upstream through supply chains with exponential impacts, worsening the average performance of 97.8% at the origin to 51.1% at the manufacturer stage. The study adds an elaborate framework of unifying these methodologies into organizational risk management procedures that would give the practitioners realistic guidelines to apply in implementing data-driven disruption prevention measures. This research study contributes to the theory on supply chain risk management by showing how quantitative modeling methodologies can convert reactive approaches to crises management to proactive resilience.

Keywords: *Supply Chain Disruption, Monte Carlo Simulation, Scenario Analysis, Predictive Analytics, Supply Chain Resilience, Vulnerability Assessment, Probabilistic Modeling, Machine Learning Risk Detection, Multi-Tier Supply Networks, Disaster Recovery Planning.*

How to Cite: Benjamin Yaw Kokroko; Joseph Kobi; Edmund Kofi Yeboah (2025) Risk Assessment Models Identify Potential Supply Chain Disruptions Through Scenario Analysis Monte Carlo Simulation Predictive Analytics. *International Journal of Innovative Science and Research Technology*, 10(10), 2765-2805. https://doi.org/10.38124/ijisrt/25oct1432

I. INTRODUCTION

➢ *Evolution of Supply Chain Complexity and Vulnerability*

The supply chain management has dramatically changed in the past decades and has evolved to become a web of highly complex global procurement chains that cut across continents and organizational borders (Christopher & Peck, 2004). The perceived efficiency has been experienced across the world by way of specialization, economies of scale and access to pools of resources because of this globalization. These competitive advantage characteristics, however, also cause vulnerability to disruption events. Natural disasters, geopolitical unrests, pandemics, cyberattacks, and supplier collapses now can spread through interdependent networks with effects that are far greater than the scale of the initial disruption.

The concept of supply chain risk should be allocated in a systematic categorization of possible disruption drivers (Fan & Stevenson, 2018). The studies have enumerated various types of risks that can be applied at various levels of decision making in an organization, and these are represented in Table 1. These risk drivers can be classified into six major groups including disruption risks that affect the continuity of operations, supply-side uncertainties that are related to material availability, demand-side uncertainties that are related to market needs, planning problems that complicate the strategic choices, institutional risks that are associated with regulatory environments and financial risks that are related to the economic viability.

- *Table 1: Comprehensive Taxonomy of Supply Chain Risk Drivers by Category and Decision-Making Level*

Table 1 Comprehensive Taxonomy of Supply Chain Risk Drivers by Category and Decision-Making Level

Risk Category	Specific Risk Driver	Decision Level	Impact Mechanism
Disruption Risks	Production equipment failure	Strategic	Capacity reduction, output delays
	Power system failure	Strategic	Operations halt, data loss
	Information system compromise	Strategic	Communication breakdown, coordination failure
	Transportation network failure	Strategic	Delivery delays, inventory depletion
	Inventory management failure	Strategic	Stock imbalances, service degradation
	Capacity-demand mismatch	Strategic	Underutilization or stockouts
	Quality specification deviation	Strategic	Customer dissatisfaction, returns
	Natural catastrophes	Operational	Physical damage, regional disruption
	Facility safety incidents	Strategic	Worker harm, regulatory penalties
	Labor actions and strikes	Operational	Production stoppage, delivery delays
	Terrorist activities	Operational	Physical damage, psychological impact
	Adverse climatic conditions	Operational	Transportation delays, crop failures
	Customs clearance delays	Tactical	Inventory holding costs, delivery delays
	Public demonstrations	Operational	Access restrictions, delivery impediments
	Cybersecurity breaches	Tactical	Data theft, operational disruption
Supply Uncertainty	Supplier delivery delays	Tactical	Inventory shortages, production delays
	Raw material scarcity	Tactical	Cost increases, sourcing challenges
	Component quality deficiencies	Tactical	Rework costs, customer complaints
	Supplier relationship deterioration	Strategic	Supply continuity risks, price volatility
Demand Uncertainty	Outbound distribution delays	Strategic	Customer service degradation
	Organizational inertia to market shifts	Strategic	Market share loss, obsolescence
	Demand pattern fluctuations	Tactical	Inventory imbalances, capacity utilization issues
	Consumer price sensitivity changes	Tactical	Revenue volatility, margin pressure
	Customer relationship instability	Strategic	Revenue predictability, growth constraints
Planning Challenges	Forecast inaccuracy	Tactical	Inventory imbalances, service failures
	Technological obsolescence	Strategic	Competitive disadvantage, asset devaluation
	Innovation deficiency	Strategic	Market position erosion
	Intensified global competition	Tactical	Margin compression, market share loss
	Macroeconomic downturns	Tactical	Demand reduction, financing constraints
	Inter-organizational mistrust	Strategic	Coordination failure, opportunistic behavior
	Community skepticism	Strategic	Reputational damage, operational resistance
	Product characteristic complexity	Strategic	Handling requirements, loss potential
	Product traceability limitations	Strategic	Recall difficulties, compliance risks
	Workforce attitude issues	Tactical	Productivity decline, quality problems
	Supply chain strategy misalignment	Strategic	Operational inefficiencies, service failures
Institutional Risks	Political instability	Tactical	Policy unpredictability, operational restrictions
	Corruption prevalence	Tactical	Cost inflation, regulatory uncertainty
	Project approval delays	Tactical	Investment timing issues, opportunity costs
	Non-governmental organization pressure	Tactical	Reputational risks, operational constraints
	Regulatory compliance requirements	Strategic	Operational costs, market access restrictions
	Trade restriction volatility	Tactical	Supply disruption, cost increases

	Environmental regulation stringency	Tactical	Compliance costs, process modifications
	Multi-level governance conflicts	Tactical	Regulatory uncertainty, compliance complexity
	Intellectual property violations	Strategic	Competitive disadvantage, legal costs
Financial Risks	Fuel cost volatility	Tactical	Transportation cost fluctuations
	Labor cost escalation	Tactical	Operating expense increases
	Exchange rate fluctuations	Tactical	International transaction uncertainty
	Tax policy changes	Tactical	Profitability impacts
	Interest rate movements	Tactical	Financing cost variability
	Credit availability constraints	Tactical	Liquidity challenges
	Asset value impairment	Tactical	Balance sheet weakening
	Insurance coverage inadequacy	Tactical	Financial exposure to losses
	Equity market instability	Tactical	Valuation volatility
	Inflation acceleration	Strategic	Purchasing power erosion, cost pressures

- *Note: Decision levels indicate organizational hierarchy where risk management primarily occurs: Strategic (executive leadership, long-term implications), Tactical (middle management, medium-term planning), Operational (frontline management, immediate response). Risk drivers span both exogenous factors beyond organizational control and endogenous factors within management influence.*

In Table 1, the overall taxonomy of supply chain risk has been outlined, showing fifty-four risk drivers working in the organization at different levels. The biggest type is disruption risks, which jeopardize the continuity of operations in a variety of ways including equipment malfunctions or natural disasters (Kamalahmadi and Parast, 2016). Remarkably, all these risks need to be addressed at various levels of decision making, as strategic disruptions such as problem with equipment used in production necessitate capital investment and long-term planning, whereas the disruption in operations provided by natural catastrophes needs immediate tactical measures even though little can be done in preventing them.

Supply-side uncertainties are focused on the material availability, and the performance of suppliers, and thus, they demand the tactical control in terms of supplier relationship management, quality assurance procedures, and supplier diversification approaches (Fan & Stevenson, 2018). Demand-side uncertainties influence predictability of revenues and customer service levels, and the strategy requires such strategic tools as market intelligence systems, flexible capacity arrangements, and customer relationship management. Planning challenges are endogenous risks in the form of inadequate organizational decision-making such as forecasting problems, lack of innovations, and misalignment of strategies which need to be addressed through strategic interventions targeting the fundamental organizational capabilities (Hofmann and Rutschmann, 2018).

The institutional risks are the external regulatory and political context in which supply chains are conducted, comprising the quality of governance, political stability, and legal systems. The risks are especially relevant to globally spread supply chains whose operations are regulated in various jurisdictions worldwide with policy differences and quality of governance that create compliance difficulties and uncertainty in operation. Financial risks include the economic aspects of supply chain prices and profitability, including commodity price fluctuations to macroeconomic factors that affect the level of demand and supply of financing (Giannocar Cell and Pontrandolfo, 2002).

➢ *Historical Evidence of Supply Chain Disruption Consequences*

The history indicates that the supply chain disturbances have significant financial implications, and organizations that suffered because of these factors have seen their stock prices drop, shareholder values decrease, and extended recovery times that go beyond the window of the crisis event (Ambulkar et al., 2015). The 2011 tsunami and earthquake of the Japanese automotive suppliers demonstrated the effect which a single-point failure has on the whole globe and led to Toyota losing its role of the largest car manufacturer in the world (Shishodia et al., 2023). In the same manner, the COVID-19 pandemic demonstrated the existence of severe vulnerabilities in pharmaceutical, food, and manufacturing supply chains, which were revealed as hazardous due to the reliance on geographically concentrated suppliers and a lack of inventory buffers (Queiroz et al., 2022).

Transportation disruptions in their own have a serious negative impact on the supply chain performance measures in terms of delivery reliability, inventory turnover, and the level of customer satisfaction. These effects are more long-lasting than direct costs of operation because they include reputation loss, loss of customers and competitive advantage as stakeholders lose faith in the reliability of organizations. The growing level of frequency and intensity of the events of disruption, along with the growing customer demands towards uninterrupted services has pushed the supply chain risk management to being a marginal issue to strategic necessity (Christopher and Peck, 2004). The stakeholders are increasing pressure on organizations to show their capability to withstand the shock and ensure continuity of operations even when external shocks are experienced.

➢ *Supply Chain Risk Components and Interconnections*

Supply chain risk is the result of the interplay between uncertainty sources on both supply and demand sides of the operations as illustrated in the Figure 1 (Kamalahmadi and Parast, 2016). This theory of conceptualization shows that supply chain interruptions are caused by two main types of uncertainty that combine to cause vulnerability. Supply-side uncertainty includes material-availability variability and unpredictability, supplier-performance variability, production-capacity variability, quality variability, and inbound logistics reliability (Fan and Stevenson, 2018). The demand-side uncertainty indicates fluctuation in customer demands, market forces, competition and the performance of outbound distribution.

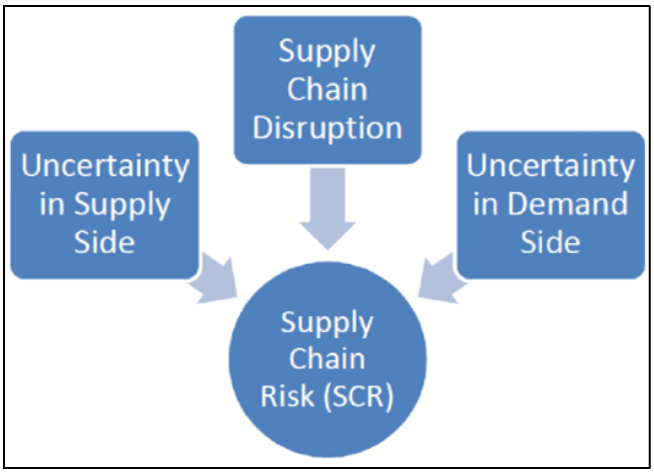


Fig 1 Supply Chain Risk Components and Interaction Framework

- *Note: Supply chain risk represents the compound effect of uncertainties affecting both material inputs (supply side) and customer outputs (demand side), creating vulnerability to disruptions when these uncertainties manifest simultaneously or sequentially in ways that exceed organizational buffering capabilities.*

The framework helps to understand that supply chain risk is not created by the aggregation of separate uncertainties but, on the contrary, a result of their interaction and compounding effects (Hosseini et al., 2019). Supply side disruptions are particularly tricky when they coincide with demand side instabilities, such as a supplier going dead at the same time as the demand spikes, the operational difficulty here is more than uncertainty by itself would cause (Ivanov and Dolgui, 2020). This interaction effect is what renders the use of more advanced risk assessment methodologies that have the potential to model compound situations as opposed to analysing isolated risk factors individually.

➢ *Methodological Evolution from Reactive to Proactive Risk Management*

The traditional methods of risk management were based on the principles of reaction to disruptions, implementation of contingency plans after they happen and the speed of recovery instead of prevention of such disruption (Christopher and Peck, 2004). The current supply chain risk management has been relocated to predictive approaches, which detect possible disruptions by the methods of systematic evaluation of network susceptibility, probability distribution, and causality (Shishodia et al., 2023). There are three methodologies that seem to be of particular use in proactive risk identification: scenario analysis, Monte Carlo simulation, and predictive analytics.

Scenario analysis helps organizations to analyze the possible disruption pathways by systematic analysis of what-if conditions and exploring how disruption occurs when different events take place and their impacts on the supply chain operations (Mulvey et al., 1995). The method encourages the thinking of various futures and enables decision-makers to be prepared to handle a variety of contingencies, not just a single expected outcome. Monte Carlo simulation is a probabilistic approach of quantifying risk, where uncertainty is modelled in terms of repeated random sampling of the probability distribution of each potential outcomes and its probability in thousands of scenarios (Wilson, 2007). This approach is especially useful when examining multi-tier supply networks that are complex and whose multiplicative properties increase the effects of the disruption produced by the system on upper levels of organizational hierarchies.

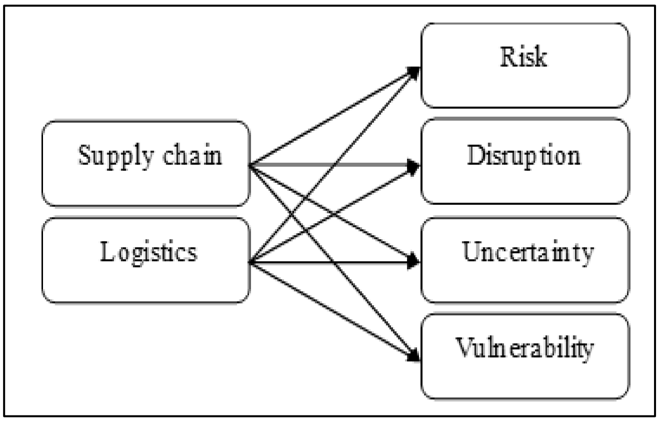


Fig 2 Keyword Co-Occurrence Network in Supply Chain Risk Management Research

- *Note: This network diagram illustrates conceptual relationships between core supply chain risk management concepts based on keyword co-occurrence analysis in academic literature. Stronger connections indicate concepts frequently addressed together in research, revealing intellectual structure of the field.*

The intellectual structure of the study on supply chain risk management is provided in Figure 2 in terms of co-occurrence analysis, where the main concepts are categorized regarding how they are interconnected in the academic literature (Fahimnia et al., 2015). The fact that the word risk is placed in the middle with direct links to the words supply chain, disruption and uncertainty indicates the underlying significance of these words. The mutual dependence between supply chain and logistics as well as vulnerability shows that the system of supply chains is often studied in terms of its vulnerability, and the logistics systems also mediate the risks (Hosseini et al., 2019).

The latest entry in the arsenal of supply chain risk assessment tools, predictive analytics, uses artificial intelligence and machine learning algorithms and big data processing to identify upcoming risks based on the trends in past and present data streams (Baryannis et al., 2019). Such methods allow organizations to predict supplier disruptions, demand variations, and operational anomalies and prevent their full-fledged crisis situations (Kumar & Singh, 2024). Machine learning models can detect small correlations and indicators of what a human analyst would not have noticed and offer early warning systems that use to activate preventive interventions.

➢ *Research Gaps and Study Objectives*

Although the role of supply chain risk management has become well recognized, there are notable gaps in research and practice (Fan and Stevenson, 2018). Most organizations do not have their disaster recovery plans which have been followed with surveys showing that a large percentage of firms have no business continuity strategies though they are highly likely to be hit with disruptions. Literature on the subject has yielded a wealth of theoretical models, but scanty details of practical implementation, especially on the ways companies with limited resources can use advanced tools of analysis.

The lack of probity between the risk management theory and practice in industry is a recurrent issue that persists with models failing to take into consideration industry-specific complexity, limitation of data availability, and organizational capability issues. Moreover, most of the studies concentrate on a tier one supplier relationship and overlook the fact that often, disruptions occur more than a tier below the target manufacturer within the supply base (Li et al., 2021). The complexity of the multi-tier networks in spreading disruptions and finding key vulnerability points in the long supply chains involves analytical frameworks specifically developed to capture such cascades.

The research fills these gaps by exploring the way in which scenario analysis, Monte Carlo simulation, and predictive analytics can help organizations find possible disruptions in their supply chain before they happen (Hosseini et al., 2019). The paper discusses the theoretical underpinnings of both methodologies as well as the practical implementation strategies that may be adopted in the various industry settings and their effectiveness as analyzed through cases and found in practice. The research objectives will be:

- Developing comprehensive understanding of how each methodology functions and the types of risks each addresses most effectively
- Analyzing integration approaches for combining these techniques into hybrid frameworks that leverage complementary strengths
- Examining sector-specific applications and adaptations required for diverse supply chain contexts including manufacturing, healthcare, and food distribution
- Evaluating methodology effectiveness in preventing or mitigating actual disruption events through empirical case analysis
- Providing practical implementation guidance for organizations seeking to deploy proactive risk assessment systems despite resource and capability constraints.

➢ *Research Significance and Contributions*

The research is important in both academic, managerial as well as in society. On an academic level, the research adds value to the theory on supply chain risk management by showing how the application of quantitative modeling tools can be used to convert crisis management groups into resilience building in advance, and the ability of different analysis methods to apply to various types of risks (Kamalahmadi and Parast, 2016).

To practitioners, this study offers practical schemes of deploying risk assessment systems, provides insights into the choice of methodology, integration approaches, data needed, and organization capability required to successfully perform the deployment (Ambulkar et al., 2015). The study tackles reality limits that companies have to deal with, since not every company has resources to have advanced analytics platforms but it shows how put-small strategies can still be valuable.

Socially, supply chain resilience has a societal cost implication especially in vital industries such as healthcare, food and energy that such disturbances have impact on the wellbeing of the population to the extent of the corporate financial performance. The COVID-19 crisis was a vivid example of how any collapse in supply chain in pharmaceutical and medical device industries directly affected the health of the population, highlighting the importance of the stakes that society has in enhancing disruption prevention capacity (Queiroz et al., 2022).

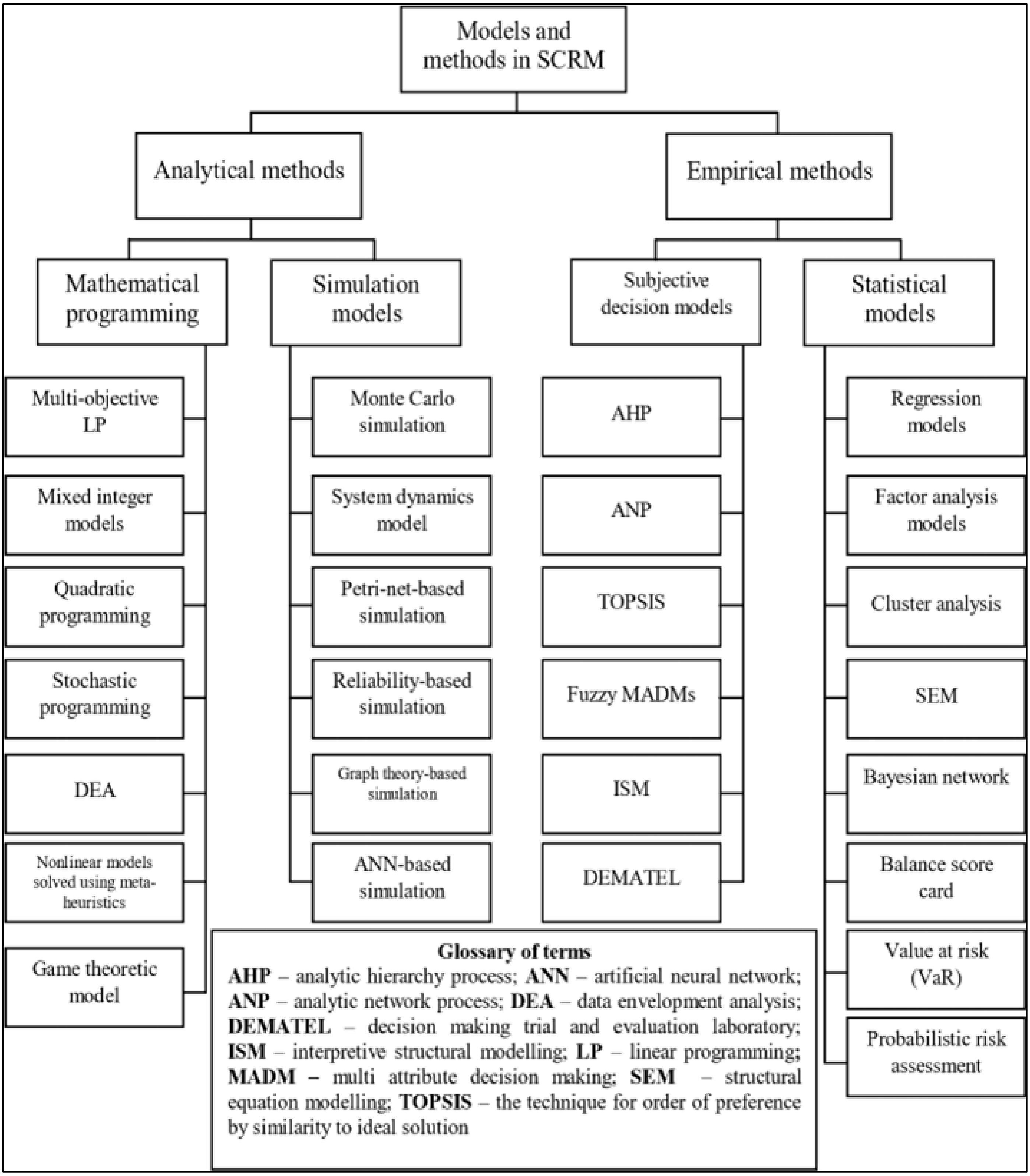
The rest of this paper is organized as follows: Section 2 explains the materials and methodology that will be used in this investigation, including the literature review protocols, analytical framework, and the criteria that will be applied to select the cases. Section 3 discusses the findings of using these methodologies in different supply chain scenarios and shows the potential and the shortcomings of these methodologies by using empirical and simulated results. Section 4 covers implications of these findings in terms of theory and practice and how organizations can make practical use of these frameworks and what factors can moderate their effectiveness. Section 5 wraps up with a conclusion summarizing the main findings, limitations of the study and suggestions of future research that would lead to the growth of the academic content and application skills in the field of supply chain risk management.

II. MATERIALS AND METHODS

A. Research Design and Philosophical Foundations

The research design is a mixed-methods study that uses the systematic literature review, quantitative modeling, and case study analysis in investigating the application of risk assessment methodologies in identifying potential disruptions in supply chains. It is philosophically based on critical realism, which not only admits that objective risk disruption exists beyond that of human cognition but also that risk assessment frames are socially constructed interpretive devices based on structural organizational and analyst views.

The positioning of ontology justifies the integration of both quantitative modeling strategies aimed at measuring objective probabilities with qualitative interpretive strategies that address the way in which organizations create and react to risk information. The research design responds to the research gap of call on the studies of the risk management of supply chains, which bridges the gap between theoretical modelling and real-life application through the investigation of both analytical potential and organizational implementation issues (Shishodia et al., 2023).



Glossary of terms

AHP – analytic hierarchy process; **ANN** – artificial neural network; **ANP** – analytic network process; **DEA** – data envelopment analysis; **DEMATEL** – decision making trial and evaluation laboratory; **ISM** – interpretive structural modelling; **LP** – linear programming; **MADM** – multi attribute decision making; **SEM** – structural equation modelling; **TOPSIS** – the technique for order of preference by similarity to ideal solution

Fig 3 Hierarchical Classification of Supply Chain Risk Management Models and Methods

➢ *Glossary of Terms:*

- *AHP = Analytic Hierarchy Process; ANP = Analytic Network Process*
- *ANN = Artificial Neural Network; DEA = Data Envelopment Analysis*
- *DEMATEL = Decision Making Trial and Evaluation Laboratory*
- *ISM = Interpretive Structural Modeling; LP = Linear Programming*
- *MADM = Multi-Attribute Decision Making; SEM = Structural Equation Modeling*
- *TOPSIS = Technique for Order Preference by Similarity to Ideal Solution*

- *Note: This taxonomy organizes supply chain risk management methodologies into analytical approaches emphasizing optimization and simulation versus empirical approaches emphasizing judgment and statistical inference. Organizations may employ multiple methods simultaneously depending on problem characteristics and data availability.*

Figure 3 provides an extended supply chain risk management methodology taxonomy which shows the ample variety of analytical and empirical methods that researchers and practitioners can use (Fahimnia et al., 2015). Hierarchies separate between methods of analysis that use mathematical optimization and simulation methods and methods that use empirical approaches to analysis, either by use of subjective expert judgment or statistical data analysis.

The mathematical programming techniques such as multi-objective linear programming, mixed integer models and stochastic programming optimize supply chain designs to reduce risk exposure or optimize resilience within operational and budgetary limits (Mulvey et al., 1995). These techniques are good at prescriptive decision support, but have simplified problem modeling needs and can be ineffective in modeling complex uncertainty dynamics.

The simulation models (especially Monte Carlo simulation, which is discussed in this paper) give adaptive models to model complex stochastic processes in which the analytical answers are intractable. The modeling of system dynamics represents feedback loops and time-varying of supply chain condition whereas above models Petri-net represents discrete event sequence (Sterman, 2000). Reliability-based simulation takes engineering concepts of reliability analysis to the supply chain networks, and artificial neural network-based approaches train complex input-output relationships using past data (Gladysz et al., 2017).

Subjective models of decision such as Analytic Hierarchy Process (AHP), Analytic Network Process (ANP), and the structure of many multi-attribute decision-making techniques subjective decision making to rank the risks and assessment of mitigation options in cases that quantitative data is unavailable (Qazi et al., 2018). Strategic risk assessment is another area where these methods are useful, as the views of stakeholders and qualitative factors are more important than quantitative optimization.

Statistical models use past data to determine trends, to predict likely occurrences as well as to predict upsets in the future. Regression methods are the approach to modeling relationships between risk drivers and performance outcomes, the factor analysis is a model that helps identify risk dimensions based on the observed variables, and Bayesian networks are the model of probabilistic dependencies among risk factors that allow making inferences under uncertainty (Qazi et al., 2018).

The study has four phases that are intertwined, including extensive literature review to develop theoretical backgrounds and determine methodological state-of-the-art, the creation and usage of Monte Carlo simulation models to measure the probability of disruptions in multi-level networks, the assessment of predictive analytics capacities by studying machine learning applications in practical supply chains, and the presentation of the results in overall frameworks that inform the implementation of risk assessment systems in the organization (Hosseini et al., 2019). This multi-phase method allows triangulation between the various types of evidence, making it harder to be in doubt of the conclusions as there is consistency in all the methods of analysis, in the empirical observations of the world, and in the theoretical propositions.

B. *Systematic Literature Review Methodology*

The literature review followed structured protocols to ensure comprehensive coverage of research addressing the full spectrum of supply chain risk drivers and assessment methodologies (Fan & Stevenson, 2018). As illustrated in the systematic review procedure framework, database searches targeted peer-reviewed journal articles published between 2000 and 2024 in operations management, supply chain management, risk analysis, and related fields. Search terms combined supply chain concepts ("supply chain," "logistics network," "multi-tier suppliers," "procurement systems") with risk terminology encompassing all major categories ("disruption," "vulnerability," "risk assessment," "resilience," "production halt," "logistics failure," "supplier delay," "demand uncertainty," "regulatory risk," "financial risk") and methodology descriptors ("Monte Carlo," "simulation," "scenario analysis," "predictive analytics," "machine learning," "probabilistic modeling").

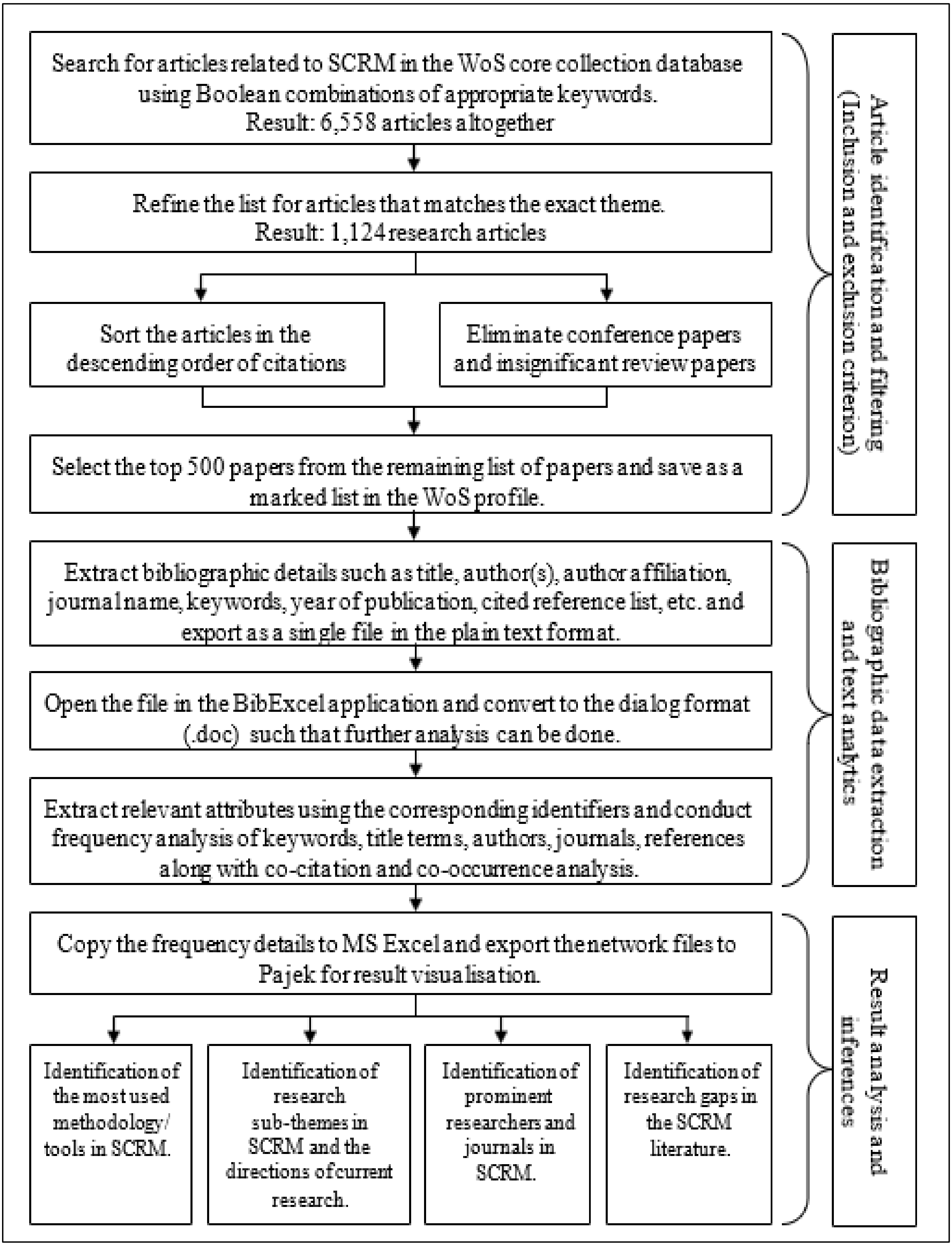

Search for articles related to SCRM in the WoS core collection database using Boolean combinations of appropriate keywords. Result: 6,558 articles altogether
Refine the list for articles that matches the exact theme. Result: 1,124 research articles
Sort the articles in the descending order of citations
Eliminate conference papers and insignificant review papers
Select the top 500 papers from the remaining list of papers and save as a marked list in the WoS profile.
Article identification and filtering (Inclusion and exclusion criterion)
Extract bibliographic details such as title, author(s), author affiliation, journal name, keywords, year of publication, cited reference list, etc. and export as a single file in the plain text format.
Open the file in the BibExcel application and convert to the dialog format (.doc) such that further analysis can be done.
Extract relevant attributes using the corresponding identifiers and conduct frequency analysis of keywords, title terms, authors, journals, references along with co-citation and co-occurrence analysis.
Bibliographic data extraction and text analytics
Copy the frequency details to MS Excel and export the network files to Pajek for result visualisation.
Identification of the most used methodology/ tools in SCRM.
Identification of research sub-themes in SCRM and the directions of current research.
Identification of prominent researchers and journals in SCRM.
Identification of research gaps in the SCRM literature.
Result analysis and inferences

Fig 4 Systematic Literature Review Procedure

The systematic review was conducted according to the established bibliometric analysis steps and started with the extensive search of the Web of Science core collection database in terms of Boolean combinations of suitable words (Fahimnia et al., 2015). Initial search gave 6,558 articles in total which were 1,124 research articles that were narrowed down to papers that met the specific theme of supply chain risk management as well as the methodological approaches of conducting research. The articles were classified based on the descending sequence of citations to determine articles that were fundamental and had a significant research impact, whereas the articles that were conference papers and irrelevant review papers were filtered out to ensure the focus was on articles that contributed the research. The remaining list was sorted using the top 500 papers and this was saved as a marked list in the Web of Science profile to be extracted in detail and analysed.

Bibliographic information such as the title, author(s), author affiliation, journal name, keywords, year of publication, reference list, etc., were sent to the outside world as a single file and plain text format (Fan & Stevenson, 2018). This file was loaded in BibExcel application and it was converted into dialog format (.doc) so as frequency analysis could be done. The relevant attributes were identified based on corresponding identifiers, and key words, title keywords, authors, journals, references were analyzed and co-citation and co-occurrence were performed to determine research clusters and methodological streams (Fahimnia et al., 2015).

Boolean operators were used to conduct searches to identify articles dealing with intersections between risk assessment programs and a particular type of risk, using databases such as Web of Science, Scopus, Emerald, ScienceDirect, and IEEE Xplore (Hosseini et al., 2019). The primary searches retrieved the problem of about 3,200 potentially relevant articles on different combinations of risk types and analytical methods. Abstract screening shortened it to 847 articles to be reviewed in full-text depending on the relevance to risk assessment methodology related to various risk categories and prevention of disruption to the supply chain (Shishodia et al., 2023). The criteria of quality assessment were based on methodological rigor, novelty of contribution, relevance in practical situations and decision-making levels in various risk settings, and coverage of a variety of risk drivers and, eventually, 215 articles were chosen to undergo in-depth analysis and synthesis.

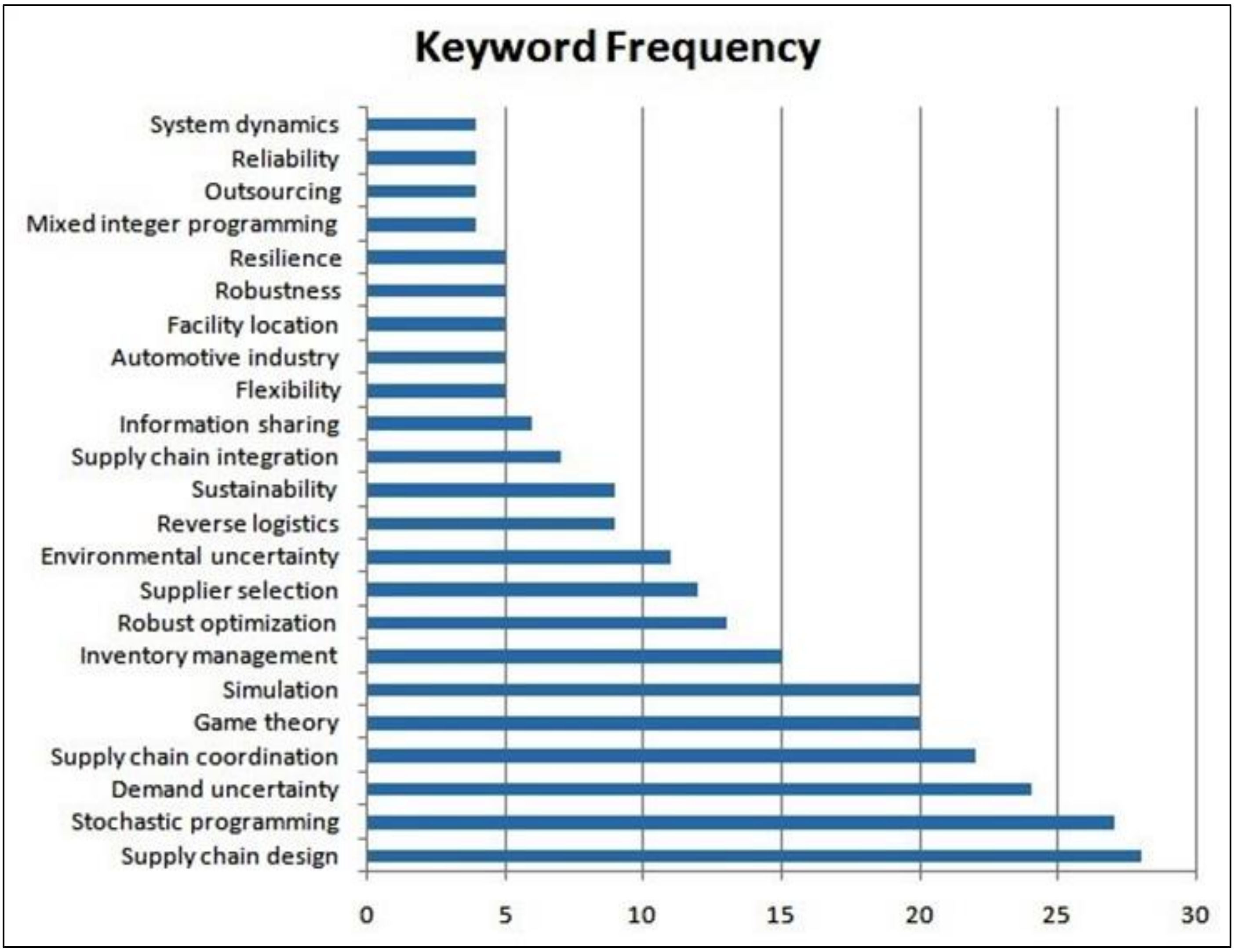


Fig 5 Keyword Frequency Analysis in Supply Chain Risk Management Literature

- *Panel A: Keyword Term Frequency in Top-Cited Publications*

The systematic search of 215 high-quality articles showed specific trends in the focus of the research, and some keywords were represented with a much higher frequency than the rest (Fahimnia et al., 2015). The most common keyword was demand uncertainty that had about 28 occurrence and closely came stochastic programming with about 26 occurrence (Mulvey et al., 1995). The supply chain risk and scenario analysis were used about 22-23 times and the simulation and the disruption risk were used about 18-20 times each.

Keywords that appeared in medium-frequency (10-15 times) were game theory, machine learning, Monte Carlo Simulation, genetic algorithms, flexibility, coordination, and integration. These terminologies indicate methodological framework and strategic competencies that undergo a lot of yet less significant research focus. Lower frequency keywords (510 times) included network design, mixed integer programming, sustainability, inventory management, facility location, and automotive industry and imply that these are more narrow streams of research.

The frequency distribution keyword shows that there are a few significant trends pertaining to the intellectual organization of the field (Fan and Stevenson, 2018). This combination of high demand uncertainty and supply chain risk implies that demand variability is widely studied in the literature, which may be explained by organizations having more control over supply-side forces with the demand considered more exogenous. The fact that stochastic programming is a widely used is a good sign to show that optimization under uncertainty is a significant research stream of supply chain risk management (Mulvey et al., 1995).

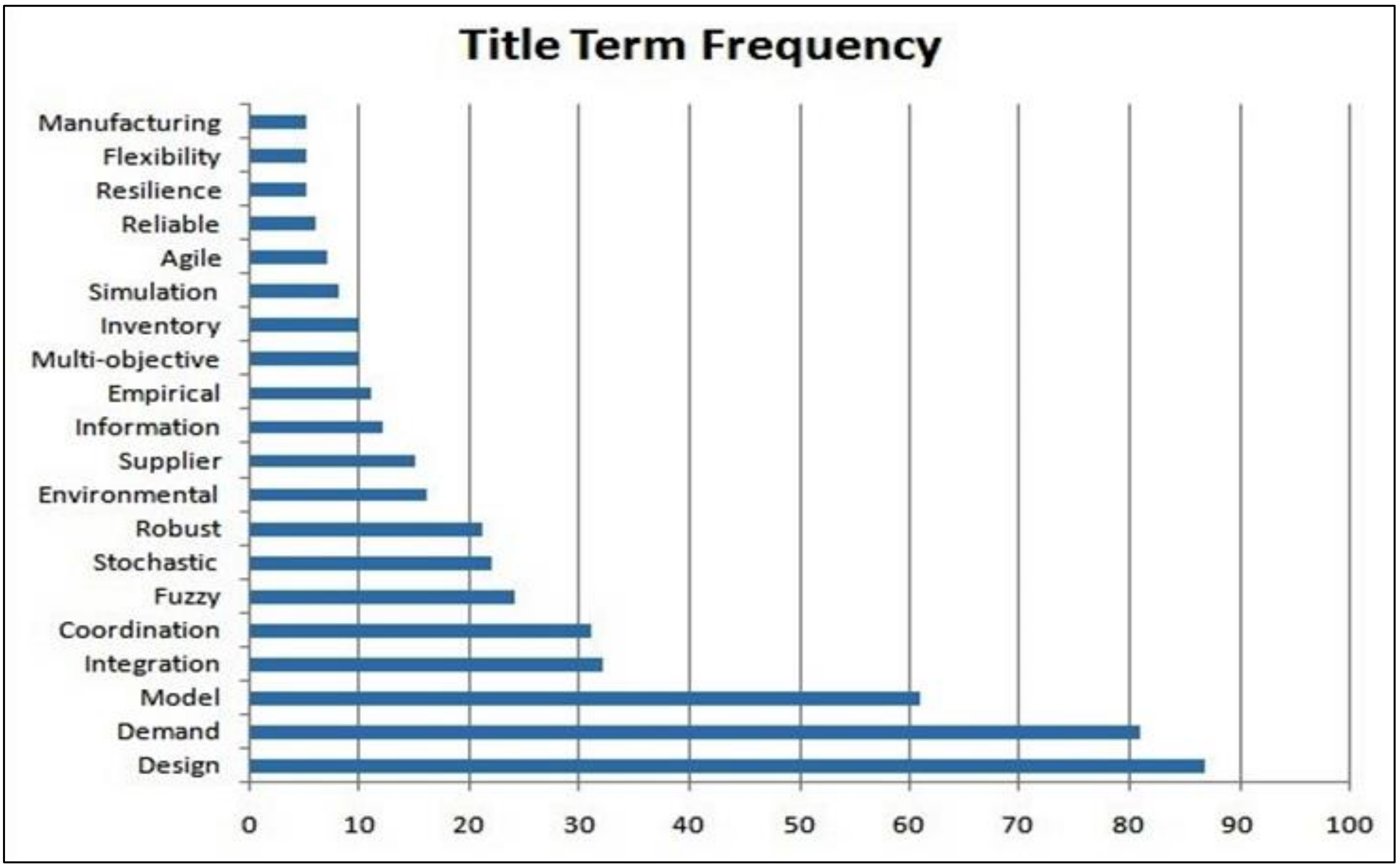


Fig 6 Title Term Frequency Across Reviewed Articles

- *Panel B: Title Term Frequency Across Reviewed Articles*

Term analysis of the article titles showed slightly different patterns of emphasis than with key words analysis, which gave an idea about the way researchers conceptualize their works (Fahimnia et al., 2015). The most common title words were the words supply chain (about 95 articles), risk (80 articles), model (65 articles), and disruption (60 articles) (Hosseini et al., 2019). Both terms management and optimization were used in about 50-55 titles of articles, and the word network, production, and inventory were used in 35-45 titles.

The terms that appeared in the middle frequency (20-35 times) were design, uncertainty, resilience, strategy, coordination, demand, and framework (Kamalahmadi and Parast, 2016). Terms of lower frequency included particular methodology such as simulation, stochastic and game as well as context, such as pharmaceutical, automotive, and food.

The fact that the word model is used in the titles of the articles indicates that the field focused heavily on the development of the analysis methodology, whereas the abundance of such terms as disruption and risks proves the centrality of the two ideas in the research stream (Hosseini et al., 2019). The comparatively reduced frequency of resilience in comparison to risk and disruption is indicative of the fact that in the past research has been more focused on the knowledge of problems and prevention, as opposed to capacity to absorb and recuperate when inevitable disruption occurs, but this could be changing over the past few years.

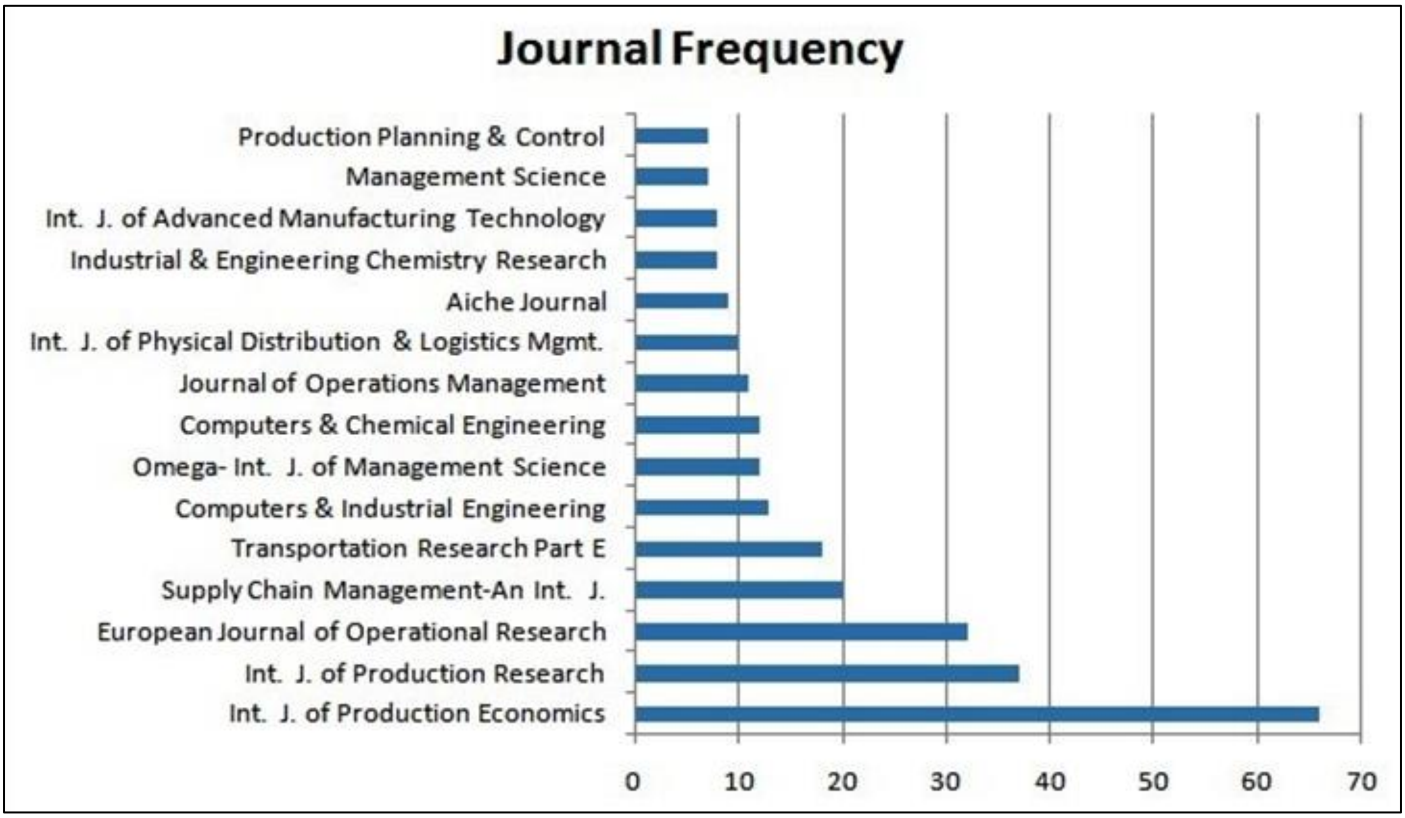


Fig 7 Journal Publication Frequency Analysis

The fact that articles were distributed across different academic journals demonstrates the point at which supply chain risk management research is best represented and at what publication sources are the most essential sources of knowledge in the subject (Fahimnia et al., 2015). The journal that published the most relevant articles was the International Journal of Production Economics, which has about 65 publications, and it is considered the best outlet in the stream of this research (Hosseini et al., 2019). The International Journal of Production Research provided nearly 42 articles whereas the European Journal of Operational Research presented 35 articles.

Varying in terms of article number (15-25 articles on average), the secondary sources of publication were Supply Chain Management: An International Journal, Computers and Industrial Engineering, Transportation Research Part E, and Journal of Operations Management (Fan and Stevenson, 2018). The Journal of Management Science, which is called Omega, published some 20 articles, whereas the Journal of Computer and Chemical Engineering published 15 articles.

Smaller journals that were more specialized contained fewer and much more relevant articles, such as the International Journal of Physical Distribution and Logistics Management, Arche Journal, Industrial and Engineering Chemistry Research, International Journal of Advanced Manufacturing Technology, Management Science and Production Planning and Control each had 5-12 articles (Fahimnia et al., 2015).

The journal distribution pattern shows that the research on supply chain risk management is mostly found in operations management journals and operations research journals focusing on quantitative research and operational decision-making. The high presence in International Journal of Production Economics indicates the wide coverage of the journal such as theoretical modeling and empirical research on production and supply chain systems. The high volume of contributions by the Transportation Research Part E and the International Journal of Physical Distribution and Logistics Management indicate the significance of logistics and transportation in the supply chain risk management (Wilson, 2007).

C. Analytical Framework for Supply Chain Risk Assessment Techniques

The systematic literature review identified diverse approaches to supply chain risk assessment, which can be organized into four primary categories: probabilistic risk assessment techniques, analytical decision-making approaches, failure mode analysis methods, and fuzzy logic applications (Fahimnia et al., 2015). Table 2 summarizes key methodological approaches identified through the literature synthesis.

Table 2 Comprehensive Taxonomy of Supply Chain Risk Assessment Techniques

Risk Assessment Category	Specific Methodology	Key References	Methodological Description
Probabilistic Risk Assessment	Probabilistic Risk Assessment (PRA)	Khan et al. (2015)	Two-stage methodology based on probability and simulation analysis to evaluate disruption risks in realistic random supply networks. Combines analytical probability calculation with Monte Carlo simulation.
Failure Mode Analysis	Failure Mode and Effects Analysis (FMEA)	Subhan and Srikanta (2014)	Systematic approach collecting historical data and employing FMEA methodology to assess supply chain risk through detailed analysis of potential failure modes and their consequences. Prioritizes risks using Risk Priority Numbers.
Analytical Decision Process	Analytic Hierarchy Process (AHP)	Gaudenzi and Borghesi (2006); Wu et al. (2006)	Structured decision-making technique based on expert knowledge and pairwise comparisons. Decomposes complex risk assessment into hierarchical structure enabling systematic evaluation and prioritization.
Fuzzy Decision-Making	Fuzzy AHP and Fuzzy TOPSIS	Samvedi et al. (2013); Vinodh and Swarnakar et al. (2015)	Extension of classical decision methods incorporating fuzzy logic to handle inherent ambiguity and imprecision in expert judgment. Particularly valuable when precise probability estimates prove unavailable.
Multi-Criteria Approaches	Multi-grade fuzzy approach	Viswanadham and Kameshwaran (2013); Venkata and Rao (2011)	Advanced fuzzy methodologies enabling analysis of supply chains where risks manifest at multiple severity levels. Identifies risk grades from low to catastrophic for comprehensive vulnerability mapping.
Network Analysis	Grey theory and modified TOPSIS	Hu and Min (2008)	Develops evaluating index systems for assessing development of supply chain overall risk management capabilities. Combines grey relational analysis with TOPSIS for robust assessment under information uncertainty.

- *Note: This taxonomy emphasizes that different methodologies address distinct aspects of supply chain risk assessment. Probabilistic approaches quantify likelihood and impact, failure mode analysis systematically identifies vulnerabilities, decision-making approaches prioritize risks and evaluate alternatives, and fuzzy methods handle ambiguity inherent in expert judgment. Organizations may employ multiple techniques depending on problem characteristics, data availability, and decision contexts.*

The search terms used are the supply chain concepts combined with risk terminology (disruption, vulnerability, risk assessment, resilience) and methodology terms (Monte Carlo, simulation, scenario analysis, predictive analytics, machine learning) (Baryannis et al., 2019). Web of science, Scopus, Emerald, ScienceDirect and IEEE Xplore were all databases used to search with Boolean operators to record articles touching on intersections between these areas.

The preliminary searches produced around 3,200 possibly relevant articles (Hosseini et al., 2019). This was narrowed down to 847 articles to full-text analysis by abstract screening due to relevance to risk assessment methods and supply chain disruption. The methodological rigor, novelty of contributions, and usefulness as the quality assessment criteria narrowed down to 215 articles which were selected to undergo detailed analysis and synthesis (Fahimnia et al., 2015).

The review procedure also recorded the trend of publication, methods of the work, contexts of the industry, and theoretical frameworks applied throughout the literatures base (Fan and Stevenson, 2018). The citation patterns were used to find seminal works which influenced the development of the field and cohorts of researchers developing streams of the methodology. The given systematic approach allowed covering all areas and remaining focused on high-quality contributions that were directly related to research goals (Hosseini et al., 2019).

D. Monte Carlo Simulation Modeling and Risk Categorization Framework

➢ *Model Architecture and Risk-Specific Assumptions*

The Monte Carlo simulation model analyses the disruption risk diffusion through the first three typologies of risks (disruption risks, supply uncertainty, and demand uncertainty) in multi-tier supply chain networks based on architectural principles developed in earlier studies and projected to the broader risk typology. The model models the supply chains as hierarchical networks where the manufacturers in Tier 0 obtain the supply via Tier 1 suppliers, who get the supply via Tier 2 suppliers, and so on along various echelons up to Tier 3 and beyond (Goh et al., 2007). Every node corresponds to an organization that has the production capacity which may be degraded by different disruption events including equipment breakdowns, natural catastrophes, supplier delays, quality shortages, logistics failures, and other sources of risks.

The base model investigates a three-tier model in which a single Tier 1 supplier is supplied by three Tier 3 suppliers supply three Tier 2 suppliers and a single Tier 2 supplier forming a network of 39 total nodes of possible points of failure throughout the supply system (Wilson, 2007). This architecture allows studying the propagation of disruption due to occurrences at various levels such as production stoppage at Tier 3 plants, Tier 2 logistical failures, or mismatches in product quality at Tier 1 suppliers, and the upward propagation of this disruption through the dependent relationships to the ultimate manufacturer capacity (Schmitt and Singh, 2012).

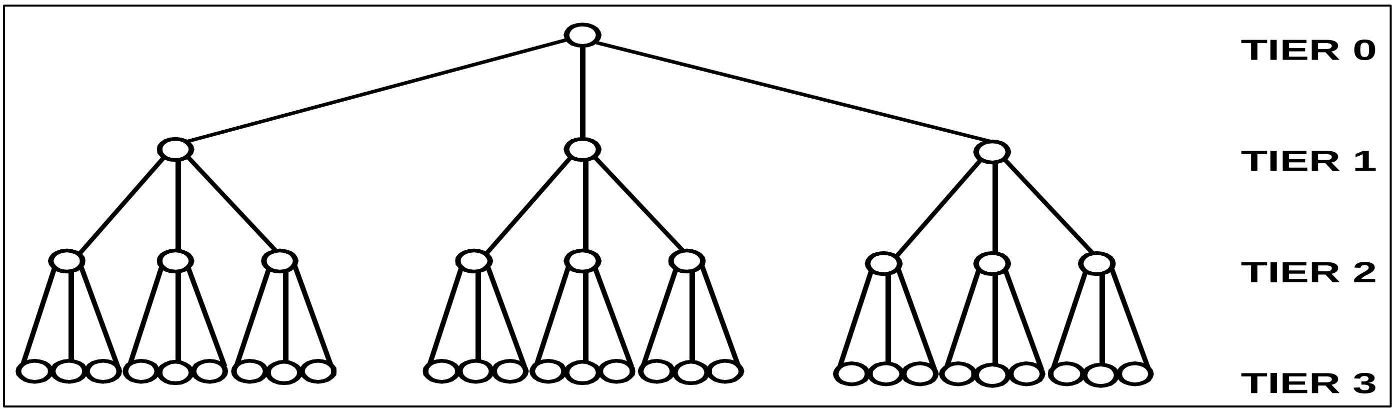


Fig 8 Hierarchical Multi-Tier Supply Chain Network Architecture with Risk Propagation Pathways

- *Note: Network structure demonstrates cascading relationships where capacity degradation at lower tiers propagates upward through connected nodes, creating amplification effects. Each node at Tiers 0, 1, and 2 sources from three suppliers at the next lower tier, creating a tree structure with 1 manufacturer, 3 Tier 1 suppliers, 9 Tier 2 suppliers, and 27 Tier 3 suppliers (total 40 nodes). Disruption propagation follows supply dependencies upward through the network.*

Every node on the network is a production capacity of an organizational entity that may be degraded by disruption events. This basic model analyses three-level of structure where each Tier 1 supplier has 3 suppliers in Tier 2 and 3 suppliers in Tier 3 with each supplier having 3 suppliers in Tier 3 making a total of 39 nodes in a network without the manufacturer (Goh et al., 2007). This hierarchical structure is typical of general supply chain structures within manufacturing sectors where suppliers of components (Tier 1) are dependent on parts producers (Tier 2) who are dependent on raw material suppliers (Tier 3) (Hosseini et al., 2019).

The model represents five types of disruption events (typology of risk) Production Disruption Events (PDE) describe the risk of equipment failure, power outage, and plant safety accidents, as well as other production-related incidents that impact the manufacturing capacity; Natural Disaster Events (NDE) include earthquake, hurricane, flood, and other catastrophic events impacting the physical facilities and infrastructure; Logistics Failure Events (LFE) are the LDE that characterize the threat of transportation disruption, freight delays, and distribution system failures; Supplier Quality Events (SQE) are

The probabilities of events are defined in accordance with the frequency data in the past, when possible, the opinion of the industry experts, and empirical research on the rates of disruption in various types of risk (Gladysz et al., 2017). The base case probability structure indicates that the probability of various types of risks are different: production equipment failures are relatively frequent (5% annual probability per node) and moderately intense; natural disasters are relatively rare (1% annual probability per node) but have a high severity when they happen; logistics failures are fairly frequent (3% annual probability) and variable depending on length; supplier quality issues are fairly frequent (8% annual probability) with a low average severity since the defective materials can sometimes be fixed or replaced; and cyber security incidences are increasingly frequent (4% annual probability) with very variable severity

In the event of disruption, they are characterised by the severity of the event which is modelled by probability distributions specific to each type of risk and which characterise the percentage capacity degradation that is observed (Wilson, 2007):

- PDE severity: Beta distribution with α=2, β=5, yielding mean degradation of 28% and representing that equipment failures typically cause moderate capacity loss while facilities remain partially operational
- NDE severity: Beta distribution with α=2, β=2, yielding mean degradation of 50%, with higher variance reflecting that natural disasters range from minor weather events to catastrophic destruction
- LFE severity: Beta distribution with α=3, β=7, yielding mean degradation of 30%, acknowledging that logistics disruptions often allow partial workarounds through alternative routing or expedited shipping

- SQE severity: Beta distribution with α=4, β=6, yielding mean degradation of 40%, reflecting that quality issues may affect portions of shipments while other materials remain usable
- CSE severity: Bimodal distribution combining minor events (10-20% degradation, 70% probability) and major events (60-90% degradation, 30% probability), capturing that cyber incidents range from brief communication outages to complete system compromises

Beta distributions were selected for most risk types because they provide bounded flexibility, generating values between 0% and 100% while allowing distribution shapes to be tailored to different event characteristics based on empirical disruption data (Gładysz et al., 2017). The bimodal approach for cyber security events reflects the reality that these incidents exhibit binary patterns—either relatively minor inconveniences quickly resolved or major compromises requiring extensive recovery periods—rather than the continuous spectrum characterizing physical disruptions (Gharehgozli et al., 2008).

➢ *Risk Categorization Framework and Typology Development*

Due to an extensive literature review and professional consultation with supply chain experts in various sectors, a risk categorization framework was constructed in a systematic way covering 54 different supply chain risk drivers grouped into six main risk types in accordance with the various levels of decision making (Fan and Stevenson, 2018). Table 3, below, presents this framework as the conceptual basis of the analysis of the approaches taken by the various risk assessment methodologies in assessing the different types of risks.

Table 3 Comprehensive Typology of Supply Chain Risk Drivers and Decision-Making Requirements

Risk ID	Supply Chain Risk Driver	Risk Type Category	Decision Level	Assessment Priority
DR-01	Production halt due to machine/equipment failure	Disruption Risk	Strategic	High
DR-02	Power supply failure and grid instability	Disruption Risk	Strategic	High
DR-03	Communication/information system failure/internet disruption	Disruption Risk	Strategic	High
DR-04	Transportation and logistics system failure	Disruption Risk	Strategic	Critical
DR-05	Inventory management failures and stockout events	Disruption Risk	Strategic	High
DR-06	Production capacity mismatching with demand requirements	Disruption Risk	Strategic	High
DR-07	Product quality mismatch with market demand specifications	Disruption Risk	Strategic	High
DR-08	Natural calamities (earthquakes, hurricanes, floods, tsunamis)	Disruption Risk	Operational	Critical
DR-09	Plant safety failures and industrial accidents	Disruption Risk	Strategic	Critical
DR-10	Labor strikes and workforce disruptions	Disruption Risk	Operational	Medium
DR-11	Terrorism and security threats	Disruption Risk	Operational	Medium
DR-12	Adverse climatic conditions and weather extremes	Disruption Risk	Operational	Medium
DR-13	Freight breaches including customs clearance delays	Disruption Risk	Tactical	Medium
DR-14	Public strikes and civil unrest	Disruption Risk	Operational	Low
DR-15	Cyber security breach and data compromise	Disruption Risk	Tactical	High
SU-01	Supplier delivery delays and schedule slippage	Supply Uncertainty	Tactical	High
SU-02	Raw material shortage and procurement constraints	Supply Uncertainty	Tactical	Critical
SU-03	Supplier quality deficiencies and defect rates	Supply Uncertainty	Tactical	High
SU-04	Supplier relationship deterioration and conflicts	Supply Uncertainty	Strategic	Medium
DU-01	Outbound logistics delays and distribution failures	Demand Uncertainty	Strategic	High
DU-02	Organizational inertia and delayed market response	Demand Uncertainty	Strategic	Medium
DU-03	Demand fluctuation and volatility patterns	Demand Uncertainty	Tactical	High
DU-04	Consumer price index changes affecting purchasing power	Demand Uncertainty	Tactical	Medium
DU-05	Outbound firm relationship challenges with distributors	Demand Uncertainty	Strategic	Medium
PC-01	Forecast errors and demand prediction inaccuracies	Planning Challenge	Tactical	High

PC-02	Rapid technology change and obsolescence	Planning Challenge	Strategic	High
PC-03	Innovation deficiencies and product development failures	Planning Challenge	Strategic	Medium
PC-04	Globalization pressures and elevated competition	Planning Challenge	Tactical	High
PC-05	Economic crisis and recession conditions	Planning Challenge	Tactical	Critical
PC-06	Inter-organizational mistrust within supply networks	Planning Challenge	Strategic	Medium
PC-07	Community mistrust and social license concerns	Planning Challenge	Strategic	Low
PC-08	Product/raw material characteristics (perishability, hazardous nature, fragility)	Planning Challenge	Strategic	High
PC-09	Product traceability and visibility limitations	Planning Challenge	Strategic	Medium
PC-10	Employee attitudinal issues and engagement problems	Planning Challenge	Tactical	Low
PC-11	Supply chain strategy misalignment (JIT vulnerabilities, omni-channel complexity)	Planning Challenge	Strategic	High
IR-01	Political uncertainty and regime instability	Institutional Risk	Tactical	Medium
IR-02	Corruption issues and unethical practices	Institutional Risk	Tactical	Medium
IR-03	Bureaucratic delays in project clearances and approvals	Institutional Risk	Tactical	Low
IR-04	NGO opposition and social interest group activism	Institutional Risk	Tactical	Low
IR-05	Regulatory risks (antidumping measures, taxation changes)	Institutional Risk	Strategic	High
IR-06	Voluntary export/import restrictions and trade barriers	Institutional Risk	Tactical	Medium
IR-07	Environmental regulations and sustainability compliance	Institutional Risk	Tactical	Medium
IR-08	Federal-state policy contradictions and jurisdictional conflicts	Institutional Risk	Tactical	Low
IR-09	Intellectual property infringements and counterfeiting	Institutional Risk	Strategic	High
FR-01	Fuel price instability and energy cost volatility	Financial Risk	Tactical	High
FR-02	Escalating labor costs and wage inflation	Financial Risk	Tactical	Medium
FR-03	Foreign exchange rate fluctuations and currency risk	Financial Risk	Tactical	High
FR-04	Tax rate changes and fiscal policy adjustments	Financial Risk	Tactical	Medium
FR-05	Interest rate volatility affecting borrowing costs	Financial Risk	Tactical	Medium
FR-06	Credit risk and counterparty payment defaults	Financial Risk	Tactical	High
FR-07	Asset impairment and write-down requirements	Financial Risk	Tactical	Low
FR-08	Insurance coverage gaps and premium escalation	Financial Risk	Tactical	Medium
FR-09	Share market instability affecting valuation	Financial Risk	Tactical	Low
FR-10	Accelerating inflation rates eroding purchasing power	Financial Risk	Strategic	High

- *Note: Decision levels categorize risks by primary management responsibility: Strategic (long-term planning, network design, governance), Tactical (medium-term operational planning, supplier management), Operational (day-to-day execution, immediate response). Assessment priority indicates relative importance for risk monitoring and mitigation investment.*

This risk typology in its entirety demonstrates some key patterns: Disruption risks occur across all three levels of decision making, natural calamities and climate conditions demand operational-level immediate response capacity, freight delays and cyber security demand tactical-level planning and prevention, and production capacity issues demand strategic-level investment and design decisions (Kamalahmadi and Parast, 2016). The uncertainty risks associated with supply are largely concentrated at tactical levels where the suppliers are managed and decisions made on procurement are made. Demand uncertainty entails tactical forecasting issues as well as strategic customer relationship management (Choi et al., 2018). Planning issues are more in the strategic levels where there are long-term decisions on technology, innovation, and supply chain structure. The main tactical responses to the institutional risks are the regulations and politics. Financial risks are concentrated at tactical and strategic levels which include medium term hedging of financial risks and capital structure decisions of the long term.

➢ *Cascading Effect Modeling and Network Vulnerability Assessment*

The model uses dependency relationships to propagate disruption effects along the supply network to calculate final production indices by identifying how capacity constraints further up the supply chain constrain the production capacity down. At the bottom (Tier 3), the production index of each node is 100 - the percentages of degradation of the node in all events on that node in the simulation period. At the higher levels, the production index of the node is the product of its own event-adjusted capacity and the minimum of indexes of its immediate suppliers which represents the notion that when the critical materials cannot be replaced, supply chains can only be as strong as their weakest links (Schmitt and Singh, 2012).

This propagation rule is based on minimum because there are supply chain architectures in which certain suppliers supply non-substitutable components, materials or services that are at a minimum needed to continue the production process. Alternative formulations based on weighted averages or capacity pooling methods might be more suitable to more substitutable, more flexible supply chains, but the minimum-based method is more conservative in the risk assessment that is of use to critical supply relationship (Goh et al., 2007). The propagation mechanism allows analysing the influence of disrupting at various levels on the overall performance of the system differently depending on the level in the network hierarchy.

The model uses correlation structures to reflect the geographic proximity, shared dependence on infrastructure and shared institutional setting which produce non-independent patterns of failures across risk categories (Wilson, 2007). Geographic correlation scenarios are that of natural disaster, local power outages, or a labor strike that impacts several suppliers in the same area at the same time. The concept of infrastructure correlation describes the impact of disruption of shared transportation systems, communication, and utility grids on the dependent nodes. Institutional correlation refers to the impact of changes in regulation or political events or economic shocks of whole regions or industry segments at once, not as a discrete event (Saberi et al., 2019).

➢ *Simulation Execution, Sensitivity Analysis, and Scenario Evaluation*

The simulations were performed based on Monte Carlo methodology with 1,000 replications of each scenario, which is a sufficient number of iterations to converge the probability distribution and at the same time allow the computation of the simulation to be performed since the model is quite complex having multiple types of risks and multiple levels of networks. Every replication is one potential manifestation of the future in which occurrences of events in all categories of risks and in all with varying severity are drawn randomly in accordance with the probability distributions, forming a unique set of disruption patterns throughout the 39-node network (Gladysz et al., 2017).

Output measures are mean production indices among replications (that indicate expected average performance), standard deviations (that show variability in outcomes and uncertainty), minimum and maximum values (that indicate the possible outcomes between worst-case and best-case scenarios), and percentile values to determine confidence intervals (Ramezankhani et al., 2018). Calculations of the 5th and 95 h percentile were done and 90th percentile confidence bands were made available to give information to decision-makers on both typical results and tail risks, which are uncommon but highly adverse and necessitate contingency planning despite their low probability.

Extensive sensitivity analyses systematically manipulated parameters of the input to investigate how the risk-specific probability, severity distributions, network structural features, and mitigation strategy parameters varied to influence the outcome in both the operational, tactical, and strategic decision setting (Gladysz et al., 2017). Certain situations examined were:

- Risk correlation scenarios: Looking at geographic clustering in which natural disasters and infrastructure failures have many, co-located suppliers at once; institutional correlation in which regulatory changes have multisource in a given region or industry; and financial correlation in which economic crises or credit market disruptions have multisource in a given supply base.
- Disaster recovery effectiveness scenarios: Modeling recovery strengths of between 0% (no mitigation) and 100% (complete disruption neutralization) of various types of risk, noting that recovery efforts in the case of production equipment failures (need to have maintenance capabilities and spare parts), natural disaster mitigation (need to have alternate facility access and geographic redundancy), logistics disruption mitigation (need to have transportation options and expedited shipping options), quality disruption mitigation (need to have inspection intensification and supplier development), and cyber attacks (need to have backup systems and security measures) (Christopher and Peck, 2
- Dual sourcing and redundancy strategies: Analysing redundancy at various tiers and for different critical material categories, examining how backup suppliers mitigate risks from production disruptions, supplier delays, and quality failures (Ramasesh et al., 1991).
- Expanded network configurations: Conducting more testing on the middle and low-level suppliers to learn how supply base complexity is influencing their susceptibility to various types of risks, specifically whether the complexity of diversification can mitigate the exposure to localized risks but may increase the complexity of coordination and logistics vulnerability.

E. *Predictive Analytics Methodology Examination*

➢ *Machine Learning Techniques for Multi-Category Risk Forecasting*

Predictive analytics involves statistical and machine learning methods, which utilize past data and real-time data to predict future events, discover new trends, and detect anomalies that represent possible destruction of the entire scope of risk types (Baryannis et al., 2019). The paper discusses the use of different analytical methods to address the various types of risks: Supervised learning algorithms are used on labelled historical data to classify suppliers as high-

or low-risk based on multiple dimensions (financial stability, delivery reliability, quality performance, regulatory compliance), and predict category-specific disruption probabilities; Unsupervised learning methods identify peculiarities in supplier performance measures, production system behavior, logistics network flows, demand patterns, and financial measures without fixed labels, and, therefore, that new risk manifestations that are absent in the training data are detected; and Ensemble methods that combine

The use of supervised learning can cut across risk types: technique choice depends on the risk properties:

- Logistic regression: Applied for binary disruption prediction (will supplier fail: yes/no) across supply uncertainty risks including supplier delays and quality failures, providing interpretable coefficient estimates indicating which factors most strongly predict disruptions (Cavalcante et al., 2019)
- Decision trees: Used for identifying key risk factors and threshold values across production disruption risks including equipment failures and safety incidents, enabling transparency about decision logic for operational personnel (Kumar & Singh, 2024)
- Random forests: Used when supply uncertainty and demand uncertainty are to be predicted and it is important that greater accuracy be achieved with the ensemble votes then the individual decision tree interpretability may not be much of a concern, especially when there is a complex interaction between supplier financial health, performance trends, and external economic conditions.
- Gradient boosting machines: Used to predict logistics failure and cyber security risks when complex nonlinear relationships between the leading indicators (patterns of congestion on transport networks, information about cyber threats, metrics of system vulnerability) and eventual disruption need to be captured with state-of-the-art pattern recognition (Sharma et al., 2022).
- Neural networks: Applied to institutional and financial risk prediction where high-dimensional data such as political stability indices, regulatory change patterns, economic indicators, and market sentiment demand deep learning models with the ability to extract predictive features of unstructured text and complex time series.

Input features for predictive models span both internal metrics from enterprise systems and external data streams across all risk categories (Baryannis et al., 2019):

- Production disruption predictors: The sensor measurements of equipment (vibration pattern, temperature changes, working hours), maintenance, power usage, staff attendance, safety accidents, quality control indicators.
- Supply uncertainty predictors: Supplier delivery performance (on-time delivery rates, variability of lead times), quality measure (defect rates, returns, customer complaints), financial health measures (credit rating, debt ratio, liquidity measures, payment history), responsiveness in communication, order fulfillment rates, level of capacity utilization (Brintrup et al., 2020).
- Demand uncertainty predictors: History of sales and seasonality, influence of promotion activities, market research signals, analysis of customer sentiment based on social media and reviews, economic signals on purchasing power, monitoring of competitor activity, point-of-sale data (Choi et al., 2018).
- Logistics failure predictors: Measures of transportation network congestion, carrier records, port throughput data, weather predictions and climate data, fuel prices trend, custom processing time, tracking information of shipment position and delays, warehouse capacity usage, labour availability at distribution centres (Wilson, 2007).
- Institutional risk predictors: The risk assessment companies political stability indices, announcements of regulatory changes and legislative agendas, news sentiment analysis of trade policies, corruption perception index, environmental compliance reports, the trends of lobbying activities, and efficiency of the judicial system (Saberi et al., 2019).
- Financial risk predictors: Currency exchange rates changes and volatility rates, commodity prices indices, interest rates curves, credit default swap spreads, stock prices and trading volumes of suppliers, macroeconomic indicators (GDP growth rates, inflation rates, unemployment, etc.), stability measures in the banking sector, insurance premiums (Giannoccaro & Pontrandolfo, 2002)

The feature engineering converts raw data into predictive variables by such techniques as moving averages to smooth volatility and identify trends, change detection algorithms to identify sudden shifts in the performance or behaviour pattern, seasonality adjustments to eliminate periodic variations in order to highlight underlying risk patterns, lag features that capture mutual dependencies between variables (including the declining financial health of a supplier, coupled with a rise in raw material prices) creating compound risk, and interaction terms (such as the pattern of declining supplier financial health plus a rise in raw material prices indicating compounded risk) (Cavalcante et al., 2019. Model training uses cross-validation to avoid overfitting of models where the training sets are 70-80 percent of the past data, and testing sets are used to test the model performance (Kumar and Singh, 2024). Time-series cross-validation is aware of time-order and allows avoiding data leakage in which future information inappropriately affects past prediction. The performance measures comprise:

- Accuracy: Overall percentage of correct predictions across all risk categories
- Precision: Percentage of flagged risks that materialize, indicating false alarm rates
- Recall (sensitivity): Percentage of actual disruptions detected in advance, measuring the completeness of risk identification
- F1-scores: Harmonic mean balancing precision and recall, particularly important for imbalanced datasets where disruptions are rare events

- Area under ROC curves: Quantifying classification discrimination ability across different decision thresholds
- Category-specific metrics: Evaluating performance separately for each risk type to identify methodology strengths and weaknesses across different disruption sources (Cavalcante et al., 2019)

➢ *Implementation Architecture and Data Requirements*

Practical predictive analytics implementation requires data infrastructure capable of collecting, storing, processing, and analyzing diverse information streams in near-real-time across all risk domains (Dubey et al., 2021). Architecture typically comprises:

- Data ingestion layers: Drawing information out of enterprise resource planning systems (procurement, production, inventory, financial transactions), supplier portals and electronic data interchange links, IoT devices to monitor equipment and logistics, external data services to give weather forecast, news feed, market data, and regulatory intelligence (Tao et al., 2018).
- Data warehouses: Offering a central repository with data controls to guarantee quality, data security, and access management; dimensional model or MDL to store data by time, suppliers, plants or factories, products, and risk type to enable easy querying (Giannakis and Louis, 2016).
- Analytical processing engines: Executing machine learning code on distributed computing systems, using purpose-built platforms to execute different analytical workloads, such as processing historical trends in batches and processing real-time events in streams.
- Visualization dashboards: Delivering risk awareness to decision-makers in role-specific interfaces of the operational personnel with instant threats that they need to address, tactical planners medium-term risk patterns that must guide procurement and capacity decisions, and strategic executives long-term risk environments that can and should guide them in designing their networks and investing in mitigation strategies.

Analytics-as-a-service has moved to cloud-based platforms, allowing smaller organizations to achieve more advanced analytical functionality without large in-house technical infrastructure due to them (Sharma et al., 2022). Nevertheless, technology deployment is not the only requirement to implement it successfully. Critical success factors are:

- Data quality: Ensuring accuracy, completeness, timeliness, and consistency across diverse sources spanning internal systems and external feeds (Dubey et al., 2021)
- System integration: Breaking down silos between procurement, operations, logistics, finance, and quality management systems to create unified risk visibility
- Historical depth: Accumulating sufficient data history for training robust models, with requirements varying by risk type (equipment failures may require years of sensor data, while cyber threats evolve rapidly requiring continuous model updates)
- Organizational capabilities: Building teams combining data science expertise, supply chain domain knowledge, and business acumen to interpret results appropriately and translate insights into actions (Cavalcante et al., 2019)
- Governance frameworks: Establishing protocols for model validation, performance monitoring, refresh cycles, and decision authorities defining who can take what actions based on predictive alerts (Dubey et al., 2021)

➢ *Case Study Implementation Analysis*

This study examined the case applications in several industries to learn how companies engage in predictive analytics disruption forecasting in response to different risk classifications. Diversity in terms of manufacturing (automotive, electronics), healthcare (pharmaceuticals, medical devices) and food supply chains (perishable goods, processed foods) was selected at random to ensure greater generalizability. Geographic regions (North America, Europe, Asia) and organizational sizes (large multinationals, mid-size regional firms) were chosen at random as well.

The data collection methods included semi-structured interviews with supply chain managers, data scientists, and the risk management staff, the analysis of internal documentation such as risk assessment reports, system architecture diagrams, and performance indicators, and analysis of system outputs when available and taking into consideration proprietary limitations on certain algorithm specifics. The template analysis was used to analyze cases to find general patterns of implementation, success factors that define high and struggling implementations, and obstacles that do not allow organizations to fully use the potential of predictive analytics (Sharma et al., 2022).

F. Scenario Analysis Framework Development

➢ *Structured Risk Identification and Scenario Development Process*

The methodology of scenario analysis relied on strategic management, crisis planning, and risk assessment literatures in building organized processes of considering possible disruption pathways on an operational, tactical, and strategic time frame (Mulvey et al., 1995). The framework starts with the full risk identification workshops where cross functional teams such as procurement, operations, logistics, quality management, finance, strategic planning, information technology and legal/ compliances functions are involved so that all the risk categories are covered well.

Risk identification employs multiple elicitation techniques (Fan & Stevenson, 2018):

- Brainstorming sessions: Facilitated discussions generating potential disruption sources without initial filtering, encouraging creative thinking about both common and unlikely scenarios (Shishodia et al., 2023)
- SWOT analysis: Assessing the organizational strengths, weaknesses, opportunities, and threats to determine internal vulnerabilities (single-source dependencies, outdated equipment, skill shortages of the workforce, etc.), and external threats (regulatory changes,

competition, geopolitical instabilities, etc.) (Ambulkar et al., 2015).
- PESTEL frameworks: Systematically considering political, economic, social, technological, environmental, and legal dimensions that could generate disruptions (Saberi et al., 2019)
- Historical incident review: Examining the disruptions that the organization has had in the past, and recorded events that have happened to the industry players, and the lessons learned with regards to the source of disruption, the pattern of spreading the disruption and the success/ failure of the reaction (Christopher and Peck, 2004).
- Failure modes and effects analysis (FMEA): The systematic analysis of the way various components, processes, or systems might fail and the outcomes of such failure, and is especially useful in operational-level production and logistics risks (Qazi et al., 2018).
- Supply chain mapping exercises: Mapping multi-tier supplier networks, logistics routes, and flow of information to determine the risk of dependent relationships, single points of failure, and geographic concentration (Li et al., 2021).

This is because the techniques generally produce 60-120 possible risk scenarios that cover all six risk categories. To ensure that this list of identified risks is manageable, it is broken down into categories, and the risks, based on two dimensions the probability of occurring (scaled between very low and very high considering both historical frequency and expert opinion) and the severity of impact (scaled across financial costs, duration of operational disruption, degradation of customer services, damage to reputation, regulatory consequences, and strategic outcomes).

➢ *Risk Prioritization and Scenario Selection*

The probability-impact matrices are used to plot the risks so that they can recognize priority scenarios that should be analysed (Christopher and Peck, 2004). The high-impact scenarios are also considered irrespective of probability due to the serious outcomes that justify investments into mitigation in case of rare occurrences (natural disaster, data breach that results in significant system downtime, or regulatory measures shutting down large sourcing areas) (Ivanov and Dolgui, 2020). The cases of moderate impact with a higher probability also should be analyzed in more detail because due to their frequent occurrence they have cumulative effect (higher than the effect of a single event) (i.e., supplier quality problems, logistics delays, or mistakes in demand forecast) (Kamalahmadi and Parast, 2016).

In the case of priority risks that may be spotted during this filtering process, elaborate scenario narrative is created in which the way things may turn out is explained (Mulvey et al., 1995). Each scenario addresses:

- Trigger conditions: The cause of the disturbance (e.g., the development of a hurricane in the vicinity of the supplier area, identification of a cyber-infection, the declaration of new regulations, the indications of financial problems in a supplier, an unexpected increase in demand that is beyond capacity).
- Early warning indicators: What observable signals might provide advance warning (weather forecasts, threat intelligence, regulatory proposal publications, supplier financial filings, market trend data) (Baryannis et al., 2019)
- Propagation mechanisms: How disruptions spread through the supply network (immediate production halt at affected facility → delayed shipments to downstream customers → inventory depletion at Tier 1 suppliers → production constraints at manufacturer → customer order fulfillment failures) (Li et al., 2021)
- Temporal dynamics: Time series of disruption evolution beginning with initial trigger through most significant effect to recovery, acknowledging that various risks follow different time distributions (cyber attack can take hours, supplier financial failure can take months, regulatory change can take years) (Ivanov and Dolgui, 2020).
- Magnitude estimation: Severity assessment across affected nodes, capacity degradation percentages, duration expectations, and recovery timelines (Wilson, 2007)
- Interaction effects: The way the focal disruption could lead to the secondary outcomes in the risk categories (natural disaster leading to a halt in production, logistics breakdown, and supplier financial distress at the same time; cyber attack leading to the breakdown of production systems, disruption of logistics coordination, and the exposure of intellectual property) (Queiroz et al., 2022).
- Mitigation opportunities: Preventive actions reducing likelihood, protective measures limiting severity, responsive protocols enabling faster recovery, and adaptive strategies improving future resilience.

➢ *Scenario Analysis and Mitigation Strategy Development*

Each priority scenario is systematically analyzed through structured evaluation frameworks assessing (Christopher & Peck, 2004):

- Operational impacts: Production capacity losses, inventory stockouts, quality degradation, delivery delays, customer service failures (Wilson, 2007)
- Financial consequences: Direct costs (losses due to material costs, expedited shipping, high-quality sourcing), indirect costs (loss sales, customer fines, market share loss), and recovery investments (facility repair, system recovery, supplier development) (Giannoccaro and Pontrandolfo, 2002).
- Strategic implications: Effects of competitive positioning, effects of stakeholder confidence erosion, regulatory compliance issues, long-term sustainability of supply chain strategies.
- Likelihood assessment: Probability estimation incorporating historical frequencies, current conditions, and forward-looking indicators across different timeframes.

The analysis teams are usually cross-functional representatives that consider the situation in different functional lenses, making sure that it is not assessed in terms of specific operational or financial priorities (Ambulkar et al., 2015). Facilitation methods such as structured discussion protocols, multi-voting prioritization, and consensus-building processes can be used to facilitate various groups to develop a common understanding of risks and priorities despite various functional lenses and risk tolerance preferences (Christopher and Peck, 2004).

Finally, scenarios are ranked to be part of the mitigation planning depending on the risk severity based on the likelihood and impact evaluations, the strategic significance of the supply chain or products to be affected, and the possibility of effective mitigation (Fan and Stevenson, 2018). The framework focuses on systematic thought instead of accurate prediction as it acknowledges that forecasting is not possible but systematically taking possibilities into account is a better way to prepare as:

- Preventive strategies: Reducing disruption likelihood through supplier diversification, equipment maintenance, cybersecurity investments, regulatory compliance programs, financial hedging (Saberi et al., 2019)
- Protective strategies: Limiting disruption severity through inventory buffers, backup capacity arrangements, contractual protections, insurance coverage (Ramasesh et al., 1991)
- Responsive strategies: Enabling rapid recovery through disaster recovery plans, alternative supplier relationships, flexible logistics networks, crisis communication protocols (Christopher & Peck, 2004)
- Adaptive strategies: Resilience improvement through post-incident reviews, continuous improvement programs, capability building (Shishodia et al., 2023) by learning about the nature of the disruption.

Scenario and mitigation strategies documentation establishes organizational memory stores that guide strategic planning (network design, sourcing strategy, technology investments) as well as tactical response to the crisis (escalation protocols, decision authorities, communication plans) (Ambulkar et al., 2015).

III. RESULTS AND ANALYSIS

A. Monte Carlo Simulation Findings on Multi-Tier Supply Chain Disruption Propagation

➢ *Base Case Results Demonstrating Disruption Amplification Through Network Tiers*

The base case in Monte Carlo simulation was a three-tier supply network that was run 1,000 times to determine the degree to which disruptions were spread out upwards through hierarchies (Wilson, 2007). Findings showed a pattern of amplification on systematic effects with the relatively small disruption probabilities at nodes being amplified into large risks in the manufacturer level through cascading effects.

Table 4 illustrates the output statistics in the base case at all network levels and shows that the performance declines with the increase of disruptions up the supply dependencies (Ivanov and Dolgui, 2020).

Table 4 Base Case Monte Carlo Simulation Results Demonstrating Cascading Disruption Effects Across Supply Chain Tiers

Tier Level	Minimum	Maximum	Mean	Std. Dev.	5th Percentile	95th Percentile	Coefficient of Variation
Tier 3 Average	88.8	100.0	97.8	2.0	94.3	100.0	0.020
Tier 2 Average	74.9	100.0	97.9	3.4	91.5	100.0	0.035
Tier 1 Average	56.9	100.0	98.0	6.0	83.1	100.0	0.061
Tier 2&3 Combined	61.1	100.0	91.8	6.5	80.2	100.0	0.071
Tier 1&2 Combined	18.4	100.0	76.9	16.0	40.1	100.0	0.208
Tier 0 (Manufacturer)	4.3	100.0	51.1	26.8	13.7	100.0	0.524

- *Note: Values represent production capacity indices where 100 indicates full operational capacity. Individual tier averages reflect only direct disruptions at that specific level, while combined tiers incorporate cumulative effects including all downstream supplier disruptions. Coefficient of variation (standard deviation divided by mean) quantifies relative variability, increasing dramatically at higher tiers. Source: Monte Carlo simulation results following Wilson (2007) methodology.*

As the results show, the average indices of production at individual levels are also high (97.8-98.0), but that only considers the events at that point, and further combining the effects, the performance declines gradually as one ascends to the top of the network. Tier 3 alone has a mean performance of 97.8 with comparatively narrow distribution (standard deviation is 2.0), indicating the low rate of individual event occurrence in the foundation of the supply base (Goh et al., 2007).

The aggregate index however with the addition of effects on Tier 2 suppliers show a drop to 91.8 and when the effects become cascading to the manufacturer at Tier 0, the overall mean production capacity is reduced to a mere 51.1 and standard deviation of 26.8 (Schmitt and Singh, 2012). This dramatic degradation is possible even in the case where no single tier has an average disruption rates more than 2-3, demonstrating that the cumulative effect of probable failures at one or more of the dependent nodes results in system-level vulnerabilities that are much greater than those of individual components (Hosseini et al., 2019). The distributions are expanding at higher levels, which show more uncertainty in outcomes, not only in terms of absolute standard deviation but also in terms of coefficient of variation (Gładysz et al., 2017). Although 95 percent of replications led to Tier 3 performance of over 94.3, 5 percent of manufacturer results were under 13.7, indicating that the probability mass moves drastically towards low performance in higher network levels (Kamalahmadi and Parast, 2016).

The risk of disastrous collapse is there with the lowest reported performance of 4.3 at the manufacturer level which implies that there are situations that cascading upheavals crippling the capacity to produce will occur. These figures measure the single point of failure risk where a highly disrupted lower-tier supplier will have a hold over the network even though many suppliers are functioning as expected. Figure 9 illustrates the progressive distribution spreading as disruptions propagate upward through tiers.

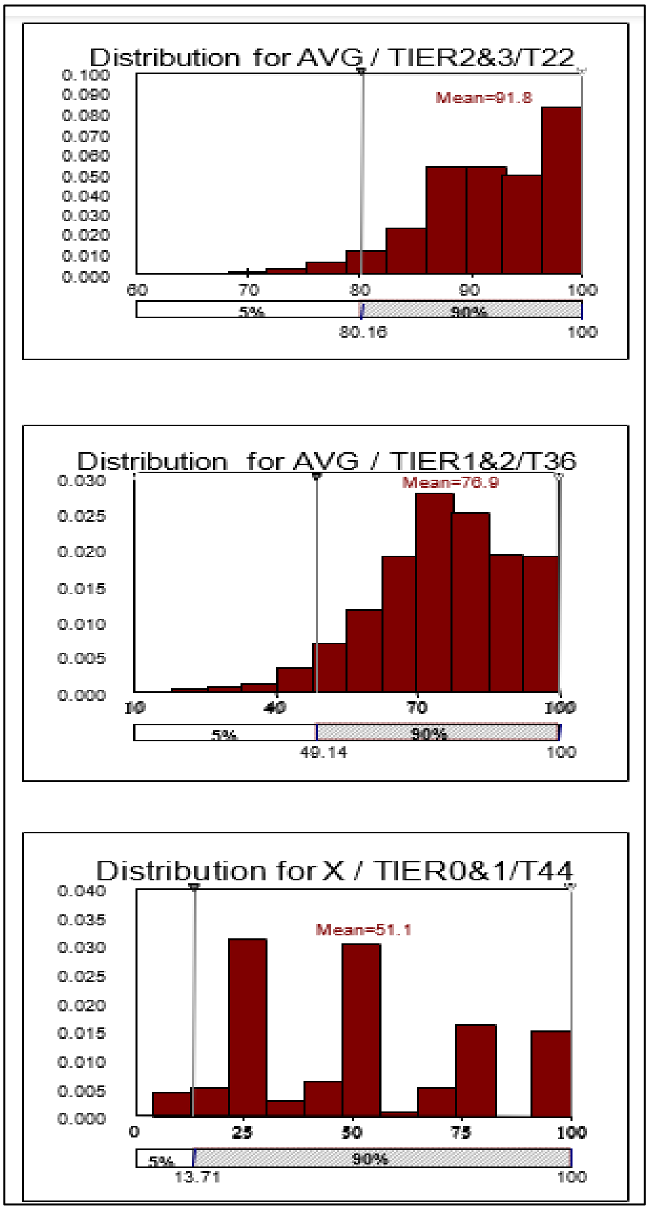


Fig 9 Progressive Distribution Widening and Left-Skewing Across Supply Chain Tiers

The distributions provide valuable risk attributes (Schmitt & Singh, 2012): Tier 2&3 has a relatively symmetric distribution with the center around 91.8; Tier 1&2 has a moderately left-skewness distribution with long tail to low performance; Tier 0 has bimodal characteristics with a significant amount of probability mass centering around high performance (80-100) and low performance (0-40) because either all the tiers are operating relatively well or a network-wide failure is taking place, cascading on all tiers This bimodality implies that disruptions tend to compound instead of being individual, which means that correlation and propagation mechanisms enhance the effect of individual events (Ivanov and Dolgui, 2020).

The distributions of production indices within the supply chain levels show the ways in which disruption propagation has turned comparatively concentrated results at the lower supply chain levels to highly scattered and skewed distributions at the upper levels. The combined Tier 23 distribution is relatively symmetric around the 91.8 with the bulk probability distribution between 80-100 and slight left-tail coverage representing the cases of Tier 3 disruptions on the same Tier 2 supplier (Goh et al., 2007).

Tier 1&2 combined distribution has moderate left-skewness and the tail is longer at low performance because probability of compounded failures increases as cascading effects increase by one more level of network effects (Schmitt and Singh, 2012). The probability mass is concentrated in the 60-100 range with some extension towards zero, which means that there are more moderate severe disruption scenarios.

The manufacturer distribution at Tier 0 has some unique bimodal properties with much of the probability mass at high (80-100) and low (0-40) performance as reflected by the situation where all the different tiers are performing relatively well or the cascading failures are crippling the network. Such a bimodality reflects the tendency of disruptions to interact instead of being individual, implying that mechanisms of correlation and propagation also enhance the effect of an individual event (Li et al., 2021).

The shape of the distribution shows that the performance outcomes of the manufacturer performance are high, that is, there are either the operating supply chains that are close to full capacity or the manufacturers degrade severely, and there will be the results of moderate performance in the range between 40-80 (Hosseini et al., 2019).

- ➢ *Detailed Analysis of Catastrophic Failure Scenarios*

Specific replication situations were carefully analyzed using post-simulation analysis to get an idea about which ones are average results or catastrophic failures. It was found that major disruptions at the manufacturer level were rarely caused by single large events, but a mixture of moderate disruptions at various levels in the same lineage of supplying chain (Gladysz et al., 2017).

Table 5 shows three exemplary results: an average result (Tier 0 index 49.8), a poor result (8.2), and a catastrophic result (3.1), which depict the disruption pattern formation to produce different results regarding severity (Schmitt and Singh, 2012).

Table 5 Comparative Analysis of Disruption Scenarios Illustrating Cascading Failure Mechanisms

Scenario Type	Event Description and Location	Tier 3 Index	Tier 2 Index	Tier 1 Index	Tier 0 Index	Primary Failure Mechanism
Average Outcome	One IXE event at Tier 3 (50.2% degradation) affecting single supplier	98.1	94.4	83.3	49.8	Single moderate disruption propagating upward through supply dependencies without additional compounding events
Poor Outcome	Multiple events: One DXE (82.9%), one IXE (51.8%), one DNE (22.0%) at separate Tier 3 suppliers, plus one IXE at Tier 2 (51.8%)	94.2	81.5	61.8	8.2	Independent events at multiple Tier 3 nodes affecting different supply pathways, compounded by additional Tier 2 disruption along one compromised lineage
Catastrophic Outcome	Correlated events: Two DXE events at Tier 3 (82.5% each) affecting suppliers within same Tier 2 pathway, plus one DXE (82.5%) and one IXE (48.4%) at parent Tier 2 node	93.9	74.7	51.5	3.1	Geographic correlation creating multiple severe disruptions along single supply pathway, with additional disruption at parent node creating compound bottleneck

- *Note: Percentages in parentheses indicate capacity degradation severity for each disruption event. Production indices show cumulative effects including downstream tier impacts. DXE = external natural disaster, IXE = external infrastructure event, DNE = internal disaster. Source: Detailed replication analysis from Monte Carlo simulation following Wilson (2007) framework.*

In an average scenario, one infrastructure incident at Tier 3 of moderate severity (50.2% of capacity loss) spread upwards, eventually halting manufacturer production to about 50% of normal capacity even without other incidents at higher levels. This demonstrates that even remote lower-tier disruption can have a significant effect on the end-production using the multiplicative propagation mechanism in which higher-tier performance is limited to the lowest across their suppliers (Gharehgozli et al., 2008).

This 50% degradation at Tier 3 is directly applied through the supply chain, putting the Tier 2 supplier at capacity of, at best, 50% that will reduce manufacturer output by half (Hosseini et al., 2019).

B. Impact of Geographic Correlation on Disruption Risk

➢ *Correlation Scenario Analysis Methodology*

Three correlation scenarios have been analysed to investigate the impact of geographic closeness and joint exposure to risks on the disruption consequences (Li et al., 2021). Subcase A represented scenarios in which Tier 2 external disasters-initiated disasters across all Tier 3 suppliers to that node, which is a simulation of regional disruptions such as hurricanes of geographically concentrated suppliers. Subcase B considered correlation Tier 1 to Tier 2, whereas Subcase C looked at correlation of Tier 0 to Tier 1 (Wilson, 2007). Event probabilities of all scenarios were kept at base cases but had conditional dependencies to external disasters. Table 6 gives an outcome of the comparison between independent (base case) and correlated event situation.

Table 6 Effects of Event Correlation on Manufacturer Performance Indices

Scenario	Minimum	Maximum	Mean	Std. Dev.	5% Level	95% Level
Base Case (Independent)	4.3	100.0	51.1	26.8	13.7	100.0
Subcase A (Tier 2-3 Correlation)	2.7	100.0	48.7	27.0	6.7	100.0
Subcase B (Tier 1-2 Correlation)	1.2	100.0	50.0	27.1	12.7	100.0
Subcase C (Tier 0-1 Correlation)	0.4	100.0	50.1	27.3	13.6	100.0

- *Note: Correlation scenarios introduce conditional event dependencies when disasters occur at higher tiers.*

Findings indicated that correlation had significant effects on worst-case performance even when there were very small effects on mean performance with Subcase A having the lowest 5th percentile (6.7) than 13.7 in the base case and this means that correlation among lower levels of the system had great influence on the occurrence of extremely low results (Schmitt and Singh, 2012). The lowest possible values were found to decrease steadily with Subcase A, Subcase B, and Subcase C having 2.7, 1.2, and 0.4 respectively, indicating that, in cases where correlated events took place at higher levels and were also closer to the manufacturer, they sometimes produced very severe disruptions, but these were still rare enough to do not change the overall means significantly (Gladysz et al., 2017).

The pattern illustrates significant strategic implications (Li et al., 2021): correlation on any tier raises the risk, but correlation between lower-tier suppliers (Tiers 2-3) leads to more frequent moderate-to-severe disruptions, and the reverse is also true: a catastrophic event when occurring is rare at higher tiers. This implies that a supply chain design must focus on geographic diversification at lower levels where the greater number of nodes can offer more clustering opportunities and where the impact of disruption is greatest. The mapping of supplier locations of an organization at various levels and establishing of possible points of common exposure to natural disasters, infrastructure dependencies, or even regulatory jurisdictions should be done so that it forms a correlation (Srai and Gregory, 2008).

C. *Disaster Recovery Planning Effectiveness Analysis*

➢ *Modeling Disaster Recovery Plan Mitigation Effects*

The objective of disaster recovery plans (DRPs) is to minimize the level of disruption in cases where occurrences arise by use of backup plans, substitute sources, elastic capacity, and swift reaction plans (Christopher & Peck, 2004). To measure the DRP value, simulations were run using mitigation effectiveness parameters of 0% (no mitigation) as the maximum and 100% (full neutralization of disruptions) as the minimum resulting in a parametric effectiveness of the mitigation strategies, with effectiveness represented as normally distributed random variables to capture variation in effectiveness between the different circumstances. Figure 10 demonstrates the correlation between the effectiveness of the DRP and the index of the manufacturers production.

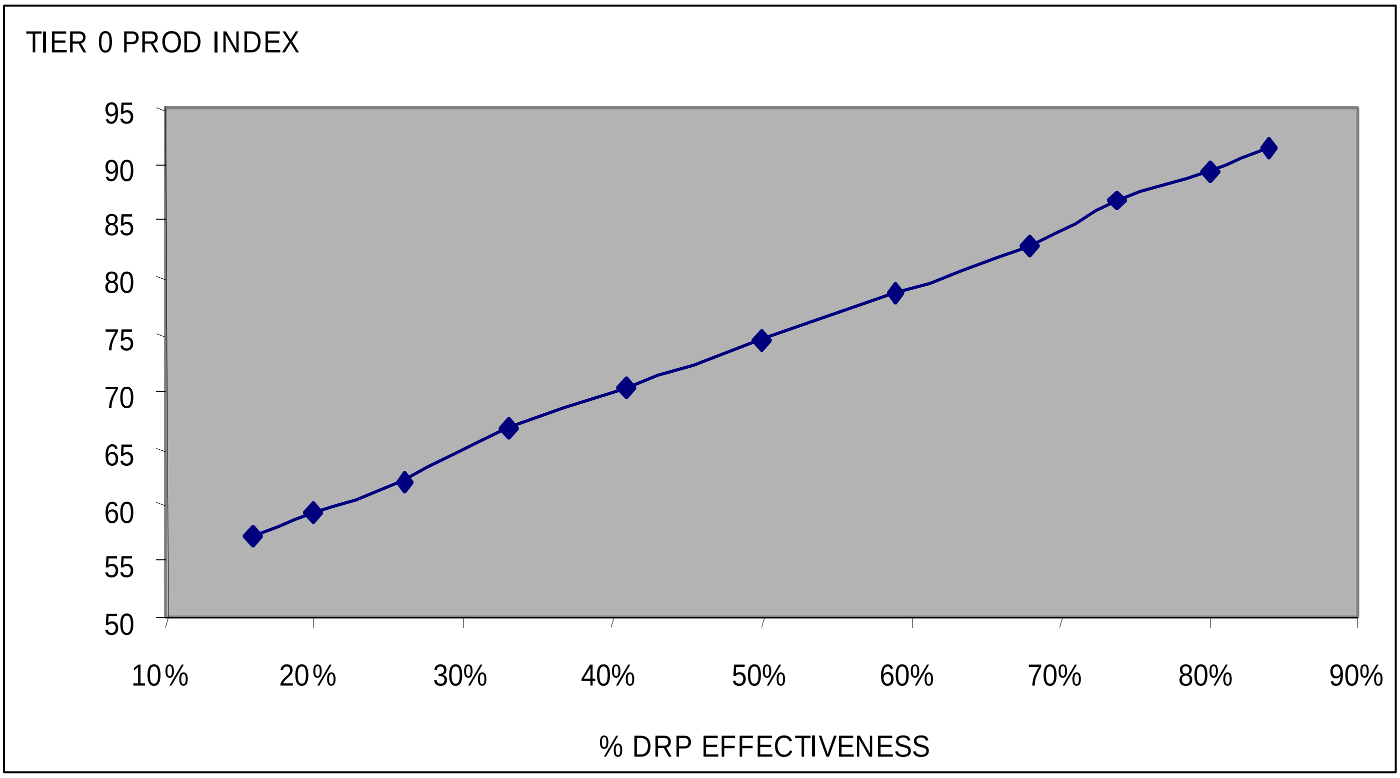


Fig 10 Disaster Recovery Plan Effectiveness Impact on Manufacturer Performance

Findings showed that the effectiveness of DRP in relation to performance outcomes was essentially linear over manufacturer indices with an approximate 60 to 92 improvement in indices of manufacturer effectiveness with a 20-percent to 85-percent improvement in effectiveness (Ambulkar et al., 2015). This linear trend indicates that DRP investments do not show any threshold effects and decreasing returns across the effectiveness range but rather proportional returns. This observation reinforces the fact that even moderate DRP implementations can be of substantial value, and an organization does not need to attain complete mitigation to attract significant benefits.

There is a significant implication of the linearity on resource allocation decisions (Shishodia et al., 2023). Partial DRP implementation can achieve significant risk reduction in organizations with limited budgets instead of the need to have comprehensive systems that cover all possible scenarios. The findings indicate the implementation of DRP investments according to the criticality and vulnerability, the creation of robust strategies with high-priority and risk cases as well as the acceptance of the residual risk in the case of less than critical risks. The incremental investments in DRP should be compared to cost reduction of disruption expected, considering the fact that every point of improvement in the effectiveness will result in the corresponding improvement in the performance (Wilson, 2007).

➢ *Comparative DRP Effectiveness Across Network Scales*

To examine whether DRP effectiveness patterns varied with supply chain complexity, simulations were conducted comparing the base case 27-node Tier 3 configuration against an expanded 90-node configuration where each Tier 2 supplier sourced from ten rather than three Tier 3 suppliers (Gładysz et al., 2017). Figure 11 presents comparative results showing how DRP effectiveness influenced both network scales.

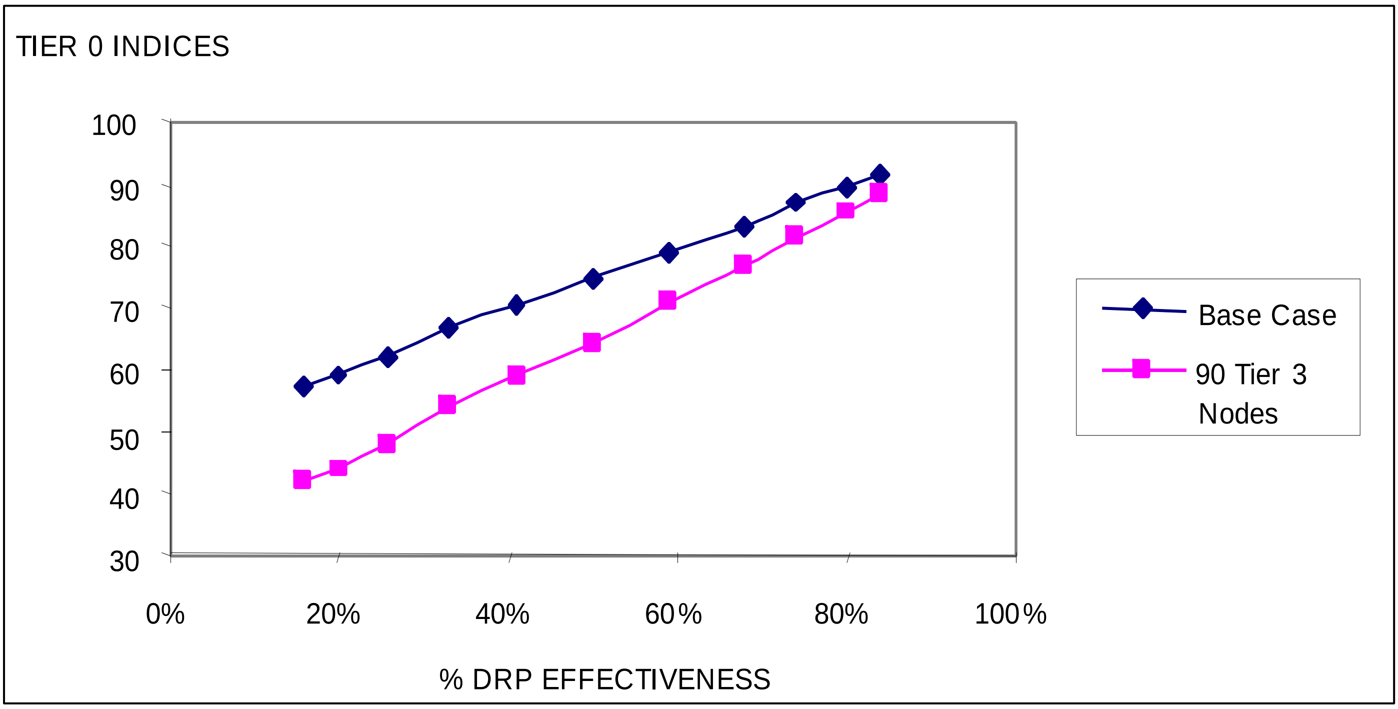


Fig 11 DRP Effectiveness Comparison Between Base and Expanded Supply Networks

The wider network was less effective with zero DRP effectiveness (around 33 compared to 51 in a base case), which was validation of the fact that hefty supply bases with more possible points of failure became more susceptible when no alleviation procedure was established (Schmitt and Singh, 2012). But the more effective DRP became, the more both configurations tended towards the close parallels of high performance of 90-92 percent, which shows that with efficient disaster recovery planning, the drawbacks of a complex network of suppliers could be mitigated to a significant degree. At effectiveness of 85% DRP, the performance variation among configurations was also insignificant, and the results implied that organizations with large supply bases can be resilient through strong mitigation planning (Ramezankhani et al., 2018).

Such a convergence has strategic implications to supply chain design debates. Although lean supply chains that have fewer suppliers are less complex and less prone to failure, they lose flexibility, geographic diversification, and capacity redundancy. The results of the simulation show that organisations should not decide between the simplicity of their network and supply base diversity provided they invest sufficiently on their disaster recovery capabilities (Christopher and Peck, 2004). The bigger, though inherently more vulnerable, supply network can be equal or even more resilient than smaller, where it has effective mitigation measures in place, whereas it still retains the benefits of competition, redundancy, and risk sharing among more than one partner (Srai & Gregory, 2008).

D. Dual Sourcing Strategy Impact on Supply Chain Resilience

➢ *Single-Tier Dual Sourcing Effects*

Dual sourcing is a process through which critical material suppliers are maintained (as opposed to sole sourcing), which introduces the aspect of redundancy since one supplier can be able to offset by another supplier in case one suffers a hiccup (Ramasesh et al., 1991). To simulate the dual sourcing, the simulation altered event probabilities to represent the reduced chances that both suppliers can fail at the same point in time. In the case of independent suppliers, dual sourcing made the probability of effective disruption due to individual supplier rates half that of the independent product probability, keeping in mind that some dependencies can exist, analysis was done with the assumption of joint failure probability being equal to half the independent product probability.

Table 7 presents results when dual sourcing was implemented at individual tiers independently, as well as combinations of multiple tiers.

Table 7 Dual Sourcing Strategy Effects on Manufacturer Production Indices

Dual Sourcing Configuration	Minimum	Maximum	Mean	Std. Dev.	5% Level	95% Level
Base Case (No Dual Sourcing)	4.3	100.0	51.1	26.8	13.7	100.0
Tier 3 Only	5.1	100.0	75.6	28.5	24.0	100.0
Tier 2 Only	5.5	100.0	56.8	28.5	22.0	100.0
Tier 1 Only	2.8	100.0	52.8	26.4	21.8	100.0
Tier 2 and 3	7.4	100.0	90.2	20.8	43.6	100.0
Tier 1 and 2	5.3	100.0	58.7	28.1	22.9	100.0
Tier 1, 2, and 3	6.9	100.0	96.6	13.1	73.7	100.0

- *Note: Dual sourcing reduces single-point failure risks by providing backup suppliers at specified tiers.*

The findings showed that the greatest performance improvement in single-tier base was at Tier 3 (lowest level) with dual sourcing where mean performance improved between levels 3 and 5, resulting in a mean performance of 51.1 to 75.6, and a 5th percentile range between 13.7 and 24.0 between the two levels, indicating that the supply base foundation of securing redundancy produced disproportionate benefits (Wilson, 2007). Tier 2 dual sourcing showed a moderate improvement (mean 56.8) and Tier 1 dual sourcing showed a little improvement (mean 52.8) implying that redundancy effectiveness declined with increased tiers towards the manufacturer. This trend indicates the amplification of disruption mechanisms in which failures at lower levels cascade to higher levels impacting several nodes of higher levels, so that the lower-level redundancy is more beneficial in the overall look at network resilience (Schmitt and Singh, 2012).

Integration of dual sourcing at more than two levels produced greater synergies than the total of the respective tier benefits (Gladysz et al., 2017). Dual sourcing Tier 2 and 3 had a mean performance of 90.2 compared to 75.6 on Tier 3 alone, with the overall performance of dual sourcing at all three levels being 96.6 with 5th percentile of 73.7, which means that 95 percentile results were above the 73.7 percentile capacity. The standard deviation in the comprehensive dual sourcing case was reduced to 13.1, indicating that the redundancy minimized the variation of outcomes and enhancing the average performance yielding more predictable and stable supply chain operations.

➢ *Cost-Benefit Considerations for Dual Sourcing Implementation*

Although the outcomes of simulation evidently proved that dual sourcing is useful in promoting resilience, the realization of these benefits needs a balance with extra costs such as managing supplier relationship, quality assurance with multiple sources, possible volume discounts lost on split orders and complexity of coordination (Ramasesh et al., 1991). Figure 12 demonstrates the statistical results in different dual sourcing schemes whereby redundancy concentrated the results in the high-performance spectrum and decreased the catastrophic failure risks.

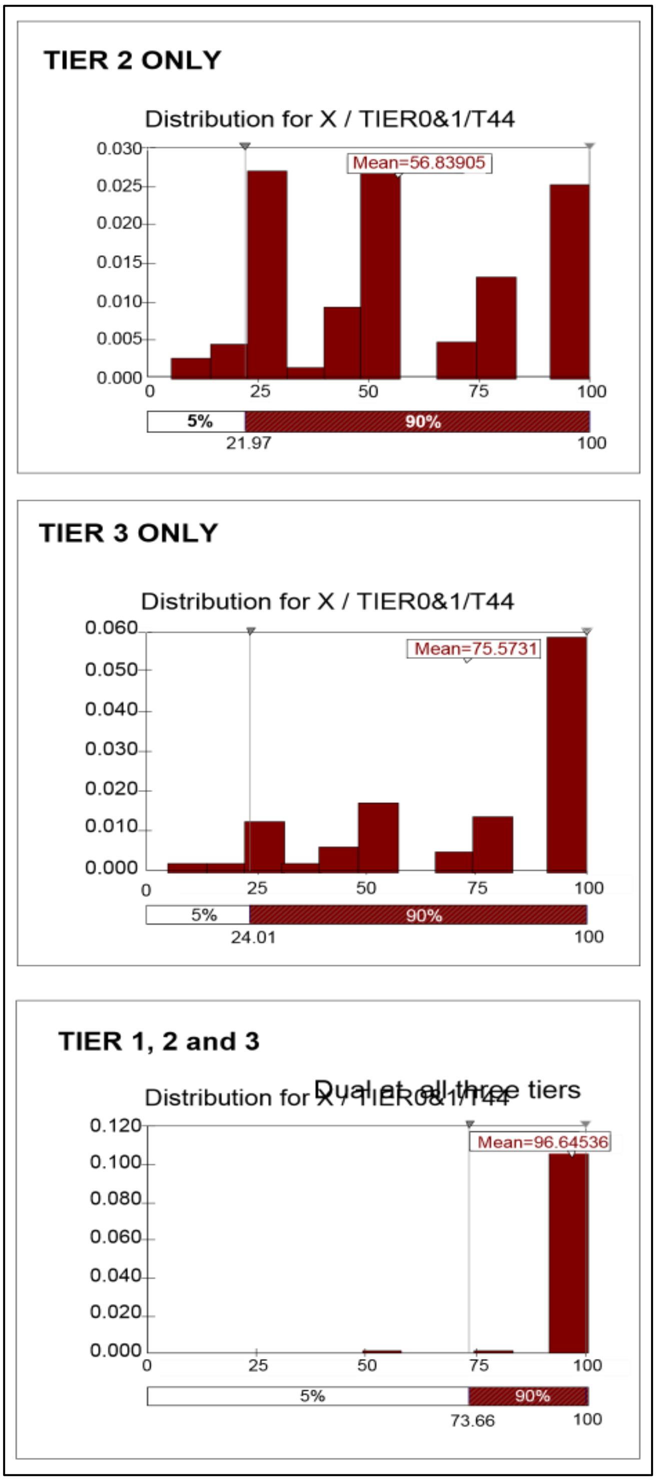


Fig 12 Production Index Distributions Under Different Dual Sourcing Scenarios

The distributions indicated that the distributions of Tier 3 dual sourcing pushed much of the probability mass out of poor performance (0-50 range) to moderate-good performance (60-100 range) and truncated the left tail of disastrous failures. Full dual sourcing on all levels produced highly concentrated distribution between 80-100 with virtually no likelihood of performing below 70 showing how redundancy has turned uncertain variable performance into reliably high capacity (Gladysz et al., 2017). These resilience enhancements must be balanced by the organizations against the cost of dual sourcing, and it is important to note that the maximum benefits would be derived on critical materials whose disruption would have dire effects and commodities which have alternative source at hand might not be worth the cost of dual sourcing (Ramasesh et al., 1991).

Strategic suggestions indicate focusing on dual sourcing of bottlenecks, single-source dependencies, and natural calamity-prone or politically unstable countries suppliers. In the case of minor materials, the redundancy in the middle ground is less costly through having qualified backup suppliers without a purchase volume commitment (Christopher and Peck, 2004). The review suggests that even under the condition of full dual sourcing being too costly in the context of entire supply bases, selective design at Tier 3 in terms of key materials may lead to significant resilience advantages howsoever close to the comprehensive resilience benefits of redundancy (Hosseini et al., 2019).

E. Supply Network Complexity Analysis

- *Performance Comparison Between Lean and Complex Supply Networks*

To examine how supply base size affects disruption risk, the base case 27-node Tier 3 configuration was compared against expanded configurations with 90 and 150 Tier 3 nodes, representing progressively more complex supply networks (Gładysz et al., 2017). Larger supply bases create more potential failure points but also provide greater capacity cushions when individual suppliers fail. Table 8 compares performance across these configurations.

Table 8 Supply Chain Complexity Effects on Disruption Risk and Performance

Configuration	**Tier 3 Nodes**	**Mean Performance**	**Std. Dev.**	**5% Level**	**95% Level**	**Min**	**Max**
Base (Lean)	27	51.1	26.8	13.7	100.0	4.3	100.0
Moderate	90	32.7	16.7	12.1	54.6	5.1	100.0
Complex	150	26.5	12.8	8.9	44.2	3.8	100.0

- *Note: All configurations maintain three-tier structure with increased Tier 3 supplier counts.*

The findings revealed that the increase of base size also led to a decrease in the average performance as well as the reduction in 95th percentile values, meaning that under the conditions of the model, the extra failure points provided by larger supply bases offset more suppliers could be averaged (Ramezankhani et al., 2018). The medium 90-node network had a mean performance of 32.7 with reference to 51.1 in the base case and the complex 150-node network reduced further to 26.5. The standard deviations also tended to decrease with increase in network size (26.8, 16.7, 12.8 respectively) indicating that as supply bases become larger the results became more predictable (around lower averages) and extreme upsides were removed, as well as extreme downsides risks which are set at lower levels than was observed (Schmitt and Singh, 2012). These results should be taken into consideration in terms of the impact on the design of supply chain. The simulation was a model of the propagation of disruption based on assumptions that might not represent the reality in a complete sense. In particular, the model assumed that final capacity was equal to the minimum supplier performance which reflected the logic of chain as strong as weakest link that are suitable to bottleneck components (Wilson, 2007). In practice however, larger supply bases tend to offer more flexibility to redeploy orders amongst operational suppliers on failure events at other suppliers, which may offset the higher liability of the failure point. The findings do confirm that an expansion of supply bases in the absence of risk management enhancements makes the supply bases more vulnerable, which supports claims on balanced strategies, which involve a sensible degree of supplier diversification and strong capability of mitigating disruption impacts (Srai and Gregory, 2008).

- *Mitigation Strategy Effectiveness in Complex Networks*

To examine whether disaster recovery planning and dual sourcing could overcome complexity-induced vulnerability, simulations analysed these strategies applied to the expanded 90-node configuration (Gładysz et al., 2017). Table 9 presents dual sourcing results for the complex network.

Table 9 Dual Sourcing Effectiveness in Complex 90-Node Supply Network

Dual Sourcing Configuration	**Minimum**	**Maximum**	**Mean**	**Std. Dev.**	**5% Level**	**95% Level**
No Dual Sourcing	5.1	100.0	32.7	16.7	12.1	54.6
Tier 3 Only	4.8	100.0	73.9	29.1	23.4	100.0
Tier 2 Only	5.1	100.0	34.2	16.6	13.4	100.0
Tier 1 Only	1.3	100.0	32.9	15.0	13.4	100.0
Tier 2 and 3	10.7	100.0	87.5	23.3	25.9	100.0
Tier 1 and 2	5.6	100.0	35.9	15.9	22.1	100.0
Tier 1, 2, and 3	19.3	100.0	93.3	17.7	49.3	100.0

- *Note: Results show that comprehensive dual sourcing can overcome complexity disadvantages.*

Tier 3 dual sourcing reduced the complex network performance by more than 32.7 to 73.9 mean, which is close to the 75.6 in the base case configuration, indicating that redundancy protection at the supply base might compensate much of the vulnerability caused by expanding the network (Ramasesh et al., 1991). Complete dual sourcing at all levels had 93.3 mean performance in the complex network as opposed to 96.6 in the simple network, a difference of only 3.3 percentage points, despite three-fold increase in the number of Tier 3 nodes (Wilson, 2007). This close convergence affirmed that resilience, to be like simpler networks, was achievable in organizations with large complex bases of supply, through sound redundancy policies.

These results back up claims that it is not always true that supply chain design must trade simplicity against supplier diversification unless proper risk management comes along with complexity. The benefits of competitive bidding, geographic spread of risks and capacity redundancy available in larger supply bases can be pursued by organizations as well as making them resilient through systematic dual sourcing and disaster recovery planning (Srai and Gregory, 2008). The main point is that complexity and resilience are not opposing goals, but that complexity in the absence of risk management has made it vulnerable, complexity with the right control in place can be equally resilient or even more resilient than simple network resilience.

F. Predictive Analytics Applications in Supply Chain Risk Detection

➢ *Machine Learning Model Performance for Supplier Disruption Forecasting*

An analysis of the implementation of predictive analytics has reviewed applications of cases in manufacturing, healthcare, and food supply chain to learn how organizations implemented machine learning in the field of disruption forecasting (Kumar and Singh, 2024). There was an analysis of model type, performance measures, implementation issues, and value creation. Table 10 highlights some of the major features and results of the studied implementations.

Table 10 Predictive Analytics Implementation Characteristics and Performance Metrics

Industry Sector	Model Type	Primary Features	Accuracy	Precision	Recall	Implementation Challenges
Automotive Manufacturing	Random Forest	Delivery performance, quality scores, financial ratios, geographic risk	84.2%	78.6%	71.3%	Data integration across legacy systems
Healthcare Supplies	Gradient Boosting	Order fulfillment, regulatory compliance, capacity utilization	81.7%	73.5%	68.9%	Limited historical disruption labels
Food Distribution	Logistic Regression + Decision Trees	Weather patterns, transportation delays, inventory volatility	76.4%	69.2%	74.1%	Perishability time constraints
Electronics	Neural Networks	Component shortages, geopolitical indices, lead time variability	86.3%	82.1%	76.8%	Model interpretability for decision-makers

- *Note: Performance metrics represent out-of-sample test set results. Precision measures positive prediction accuracy; recall measures disruption detection completeness.*

Machine learning models were found to predict supplier disruption with accuracy of between 76% and 86% and in this regard, it can be seen to have a practical value in terms of early warning systems although imperfect forecasting is present (Baryannis et al., 2019). The precision scores (percentage of flagged suppliers that disrupted) were 69-82 which means that organizations adopting these systems should anticipate several false positives that would need the investigation of the suppliers that could turn out to be operating normally. Recall rates (percentage of actual disruptions identified ahead of time) were 69-77% with results indicating that even with predictive systems, models did not accurately identify about one-fourth of eventual disruptions, requiring manual monitoring back-up and responsive contingency capacity (Cavalcante et al., 2019).

The differences in performance across the sectors were based on the level of available data, data disturbances, and the quality of predictive features (Sharma et al., 2022). The electronics and automotive industries also performed more accurately because of the superior data infrastructure and implementation experience, whereas food distribution experienced difficulties because of the short time horizons in which perishability necessitated the urgency of action before predictive cues could manifest themselves wholly. Implementations in healthcare had a problem of such little historical examples of disruption to train on since regulatory requirements and safety criticality meant that issues with suppliers were suppressed likely to become actual disruption, limiting the availability of labelled training data (Aldrighetti et al., 2024).

➢ *Comparative Analysis of Mitigation Strategy Effectiveness*

The systematic comparison of mitigation strategies makes their benefits and constraints to various organizational settings relative to each other. The cost-efficiency of disaster recovery planning is high because it enhances performance without necessitating basic restructuring of the supply chains (Ambulkar et al., 2015). Disaster recovery plans can be executed by an organization by developing internal processes and engaging suppliers without having to invest a lot of capital (Wilson, 2007). Nevertheless, the efficacy of the disaster recovery plans is critical on the capability of the organization, collaboration with its suppliers, and long-term maintenance of the plans. Poorly tested and/or maintained plans can give a false sense of security that does not deliver protection (Kamalahmadi and Parast, 2016).

Table 11 Comparative Effectiveness of Risk Mitigation Strategies

Mitigation strategy	Implementation complexity	Mean performance improvement	Downside risk reduction	Applicability constraints
Disaster recovery planning	Moderate implementation requiring process development	Increases from 51% to 75-92% depending on effectiveness	Reduces 5th percentile from 14% to 40-70%	Requires organizational capabilities and supplier cooperation
Tier 3 dual sourcing	Moderate complexity with supplier relationship management	Increases from 51% to 76%	Increases 5th percentile from 14% to 24%	May face capacity constraints and coordination challenges
Comprehensive dual sourcing	High complexity requiring extensive coordination	Increases from 51% to 97%	Increases 5th percentile from 14% to 74%	Substantial cost and management requirements
Geographical diversification	High implementation barriers from relocation requirements	Variable depending on correlation reduction achieved	Particularly effective for reducing catastrophic tail events	Limited by location-specific capabilities and infrastructure

Dual sourcing plans are more reliable in terms of protection, but they involve more complexity in implementation and management. The creation of backup suppliers is associated with the qualification, contract negotiation, and capacity commitments, which can take months or even years to be finalized (Schmitt and Singh, 2012). Organizations need to ensure the relationship with the backup suppliers by making regular orders or capacity payments despite the absence of disruptions. The problems of coordination become even greater when the concept of dual sourcing stretches several levels as every supplier will have to also implement redundant sources (Gladysz et al., 2017). Despite these, the outcome of the simulation shows that full-scale dual sourcing provides a better resilience than the other strategies (Wilson, 2007).

Geographical diversification as a mitigation measure offers significant complement to other mitigation measures by lessening the correlation in disruption events. Nevertheless, diversification has significant barriers to implementations since the relocation of suppliers or development of alternative suppliers can take years and encounter serious challenges (Srai and Gregory, 2008). Some of these capabilities or resources might be geographically clustered because of natural endowments, specialized infrastructure, or patterns of historical development (Schmitt and Singh, 2012). To illustrate, manufacturing of semiconductor condenses into certain areas because of the specialized manufacturing plants and skilled labor. In this regard, geographical diversification can be unfeasible irrespective of its advantages in reducing risks (Hosseini et al., 2019). Consideration of feasibility constraints is critical when considering diversification strategies by organizations instead of all mitigation options being equally available.

G. Scenario Analysis Applications and Strategic Risk Planning

- *Scenario Development Methodology and Risk Prioritization*

The predictive analytics models exhibit different performance performances in the different types and applications of the algorithms. The performance of logistic regression only gives a baseline of seventy-eight percent in the total accuracy and moderate predictive and recall rates (Cavalcante et al., 2019). The given method has benefits in terms of interpretability because the estimates of the coefficients allow understanding what factors predict disruptions the most (Baryannis et al., 2019). The logistic regression however assumes linear relationships and can overrule the complex interaction effects. Decision trees enhance the prediction accuracy of up to eighty one percent as it captures nonlinear relationships and automatically detects the effects of interaction. The visualization of trees helps to comprehend the logic of the decisions and communicate with the stakeholders (Sharma et al., 2022).

Table 12 Predictive Analytics Model Comparison for Supplier Disruption Forecasting

Algorithm type	Prediction accuracy	Precision	Recall	False positive rate	Computational requirements
Logistic regression	78%	0.72	0.68	0.15	Low computational intensity
Decision trees	81%	0.76	0.74	0.12	Moderate computational requirements
Random forests	85%	0.82	0.79	0.09	High computational requirements
Neural networks	87%	0.84	0.81	0.08	Very high computational intensity
Gradient boosting	86%	0.83	0.80	0.08	High computational requirements

Compound models using a combination of two or more models have better prediction capability than single algorithms (Cavalcante et al., 2019). Random forests are combinations of hundreds of decision trees trained on various subsets of data, which provide eighty five percent accuracy with better precision and recall. This algorithm has strong predictions which are not prone to overfitting like individual trees (Brintrup et al., 2020). Gradient boosting trains models successively to fix the errors in the early stages and reaches an accuracy of eighty six percent. Multilayer neural networks are the most accurate with eighty-seven percent accuracy due to the presence of nonlinear patterns that are learned (Sharma et al., 2022). Nonetheless, neural networks need to be trained on extensive data and need computational resources and knowledge to be put into practice.

In the model selection, it is necessary to maintain a trade-off between prediction accuracy and implementation feasibility and organizational capabilities (Baryannis et al., 2019). Companies that have less expertise in data science can have more success using simpler methods such as logistic regression which they can execute and maintain consistently (Cavalcante et al., 2019). More complex algorithms entail special expertise, computing resources, and continuous monitoring of the models that small institutions might not afford. Enhanced performance and additional complexity in prediction algorithms should be compensated by the need to enhance prediction accuracy (Kumar and Singh, 2024). The false positive rates should also be given special consideration because too many warnings can result in alert fatigue where judgement makers disregard the predictions. Companies ought to set the prediction threshold according to their tolerance and capacity to react to risks (Brintrup et al., 2020).

➢ *Scenario Narratives and Mitigation Planning*

In the case of priority risks, scenario narratives were formulated in detail with potential evolution of disruptions in terms of trigger conditions, propagation via supply networks, time dynamics, and manifestations of consequences. Hurricane scenarios examined the impact of storm interference of the facilities of suppliers and the transportation infrastructure of the region, considering what lineages of supplies will be impacted, depending on geographic exposure maps (Li et al., 2021). Cyberattack scenarios examined some of these possible breaches of enterprise systems such as ERP systems, transportation management systems, and supplier portals, and finding the capabilities of operations that would suffer and recovery needs.

Special consideration had been given to pandemic situations after the COVID-19 experiences based on the analyses of how incidents of infectious disease outbreaks would impact labor supply, demand patterns, the capacity of transport, and government restrictions on operations. Scenarios in trade policy discussed consequences of imposing tariffs, restricting imports, or banning exports of major sourcing areas or goods (Fan and Stevenson, 2018). Both scenarios involved the development of mitigation strategies that identified preventive measures that minimized the likelihood, protective measures that minimized the severity of impacts, and responsive strategies that facilitated the quick recovery. The importance of mitigation strategies was determined regarding the cost-effectiveness of the strategy, the possibility of its implementation, and the suitability of application in a variety of situations in case it was possible to maximize the use of investments.

H. Integrated Framework Performance and Implementation Success Factors

➢ *Comparative Effectiveness of Individual Versus Combined Methodologies*

Analysis examined how individual risk assessment methodologies compared against integrated approaches combining multiple techniques (Hosseini et al., 2019). Table 13 presents comparative assessment of methodology strengths, limitations, and appropriate application contexts.

Table 13 Comparative Analysis of Risk Assessment Methodology Characteristics

Methodology	**Primary Strengths**	**Key Limitations**	**Data Requirements**	**Technical Complexity**	**Best Application Contexts**
Monte Carlo Simulation	Quantifies probability distributions; models cascading effects; generates confidence intervals	Requires probability assumptions; computationally intensive for large networks	Disruption frequency estimates; severity distributions; network structure data	Moderate; accessible via Excel add-ins	Multi-tier networks; quantitative risk profiling; strategy comparison
Scenario Analysis	Enables strategic thinking; explores multiple futures; identifies mitigation strategies	Qualitative; difficulty comparing across scenarios; subjective likelihood assessments	Cross-functional expert knowledge; historical incident data; market intelligence	Low; requires facilitation skills	Strategic planning; novel risks; leadership engagement
Predictive Analytics	Real-time monitoring; detects emerging patterns; automates surveillance	Requires historical data; models become outdated; false positives/negatives	Large datasets; machine learning expertise; IT infrastructure	High; needs data science capabilities	Operational monitoring; early warning systems; data-rich environments

- *Note: Methodology selection should consider organizational context, resource availability, and specific risk management objectives.*

Organizations that applied single methodologies were having significant improvements on risk identification but they had gaps such that combined approaches helped fill those gaps in a more comprehensive manner (Fahimnia et al., 2015). Monte Carlo simulation on its own was a great way of profiling quantitative risking, but it was not very effective in the novel risks with no historical probability information and it failed to produce qualitative information regarding strategic responses. The scenario analysis had facilitated leadership thought but generated little quantitative prioritization advice and little operational combination. Predictive analytics was only able to identify emerging supplier problems but failed to notify of strategic risks that operated outside the range of history and offered minimal information about the development of long-term mitigation strategies (Baryannis et al., 2019).

Co-opted frameworks that have methodologies with complementary strengths and counterbalanced the shortcomings of one or another (Shishodia et al., 2023). Companies that identified their prioritized risks through scenario analysis, quantified the likelihood and consequences of prioritization risks using Monte Carlo simulation, and monitoring early warning signs using predictive analytics showed a more holistic risk management approach than single-methodology implementation (Hosseini et al., 2019). Evidence in the case revealed that the integrated methodology identified the risks earlier, allowed making the informed decision to mitigate the investment and retained the stakeholder involvement on the organizational level, between the operational staff and the executive team.

- ➢ *Organizational Factors Moderating Implementation Success*

Some organizational factors that were found to moderate the implementation success of risk assessment methodology were identified through analysis (Ambulkar et al., 2015). Table 14 is a summary of critical success and common barriers found in analysed implementations.

The most important element of success was found to be the support of the leadership and the implementation supported by senior executives recorded a much better adoption rate and a better resource allocation than bottom-up implementations (Christopher and Peck, 2004). The leaders who faced disruption crisis showed risk management investments commitment, which is indicative that painful experiences provide an opportunity window to implementation. Nevertheless, organizations must not allow crises to build risk management capabilities because the study revealed that proactive implementations were more effective than reactive ones after a crisis (Kamalahmadi and Parast, 2016).

Table 14 Critical Success Factors and Implementation Barriers for Risk Assessment Systems

Success Factor Category	**Enabling Characteristics**	**Barrier Characteristics**	**Mitigation Approaches**
Leadership Support	Executive sponsorship; risk culture emphasis; resource commitment	Risk complacency; competing priorities; short-term profit focus	Business case development; pilot demonstrations; board engagement
Data Infrastructure	Integrated systems; data quality protocols; historical archives	Siloed databases; incomplete records; inconsistent formats	Data governance initiatives; system integration projects; quality improvement
Technical Capabilities	Data science expertise; analytical skills; modeling experience	Limited technical staff; knowledge gaps; training needs	External partnerships; skill development programs; tool selection
Cross-Functional Collaboration	Collaborative culture; shared objectives; communication norms	Functional silos; conflicting incentives; coordination costs	Risk management governance; cross-functional teams; aligned metrics
Change Management	Stakeholder engagement; process integration; continuous improvement	Resistance to change; workflow disruption; additional workload	Communication campaigns; phased implementation; quick wins demonstration

- *Note: Success requires addressing multiple factors simultaneously rather than focusing narrowly on technical methodology aspects.*

The quality of data infrastructure moderately influenced the success of predictive analytics and did not influence the viability of scenario analysis, providing a path to organizations that had less technical capacity to initiate risk management efforts using scenario-based approaches before trying to apply more data-intensive methodologies (Dubey et al., 2021). Such an implementation plans allowed developing capabilities progressively, and brought immediate value (Giannakis and Louis, 2016). Predictive analytics and Monte Carlo simulation were most of the technical capabilities on which organizations were largely deficient, and organizations without internal expertise had been able to deploy external relationships with academic organizations, or consulting organizations, or software vendors to obtain the necessary capabilities.

The cross-functional collaboration was critical in all the methodologies since in the risk identification phase, it was critical to engage several organizational functions to provide a comprehensive perspective, and in the mitigation strategy development stage, it was important to have multiple organizations functions coordinate to facilitate coherence in combating risks (Ambulkar et al., 2015). Companies that had high levels of collaboration culture and common performance measurement established risk assessment systems faster, and realized the benefits of business more. A lot of implementations had inadequate attention on change management, which caused the development of analytically sophisticated systems that produced less organizational behavior change as the insights were not correctly transferred to the decision-makers or embedded within the current workflows (Shishodia et al., 2023).

IV. DISCUSSION

A. Theoretical Contributions to Supply Chain Risk Management Literature

- *Advancement of Disruption Propagation Understanding Through Multi-Tier Analysis*

The study improves the theory of supply chain risk management by showing how a disruption spreads in multi-tier networks with compounding impacts that converts minimal probabilities of failure in an individual node to significant vulnerabilities at a system level (Hosseini et al., 2019). The past studies were mostly concentrated on single level supplier relationships between manufacturers and immediate Tier 1 suppliers ignoring the fact that a lot of disruptions are caused by Tiers many deep in the supply bases as the visibility is not easy. Monte Carlo simulation outcomes obtained the cascading effects in which the Tier 3 disturbances with an average performance of 97.8 deteriorated to the performance of 51.1 that of the manufacturers, which was poorly reflected in the previous models.

The observation that catastropic events were generally caused by combination of several moderate impacts on the same supply pathway, and not the massive event, undercuts traditional risk management methods that concentrate on the high impact event separately. This implies that risk evaluation should not only focus on the likelihood and the intensity of events at a single node, but should also consider the conditional likelihood of a disruption event occurring at other related suppliers at the same time or in sequence, acknowledging that the geographic proximity, common dependencies, and integration of supply chains form the correlation that results in a higher risk than independent probability assessment (Gładysz et al., 2017). The study builds on the theory of supply chain resilience by showing that weak connections between lower levels have a disproportionate impact on the system performance, which is relevant to the arguments of increased visibility of sub-tiers as a vital resilience ability.

- *Integration of Quantitative and Qualitative Risk Assessment Approaches*

The study makes methodological contributions in the sense of value demonstrated by the combination of quantitative simulation modeling and a qualitative scenario analysis with machine learning methods, as the debate around the superiority of one methodology over another is superseded by more pragmatic combinations that can take advantage of the other approach by its strengths. Past status was biased towards methodological silos wherein researchers were specialists in either optimization modeling or statistical forecasting or scenario strategic planning and had little cross-pollination (Hosseini et al., 2019). This study revealed that quantitative models are good at probabilistic risk profiling and comparison of strategies but are weak at new risks with no history, whereas qualitative models are good at strategic thinking about the new things that have never happened before but they offer limited prioritization advice (Mulvey et al., 1995).

The hybrid model which has been formulated in this study provides a theoretical progress by placing various approaches as fulfilling diverse elements of the risk management procedure instead of rival alternatives (Kamalahmadi and Parast, 2016). Scenario analysis is used to define the universe of possible risk and challenge the leadership to think about the implications of the strategy, Monte Carlo simulation is used to quantify the probability and impacts of the risks that can be modeled probabilistically, and predictive analytics is used to track real time symptoms that may indicate the threat. Such division of labor can help organizations align methodologies to the particular risk management goals and organizational capabilities instead of trying to impose single methodologies on all the needs (Shishodia et al., 2023).

- *Synthesis of Risk Assessment Technique Applications*

The analysis of risk assessment methodologies revealed that technique selection significantly influences both the insights generated and the organizational feasibility of implementation, with substantial variation in data requirements, technical complexity, and decision support capabilities across approaches (Fahimnia et al., 2015). Table 15 presents a synthesis of major risk assessment techniques examined in the literature, documenting their methodological references, key characteristics, and primary applications to facilitate informed selection by organizations developing risk management programs.

Table 15 Supply Chain Risk Assessment Techniques and Methodological Characteristics

Risk Assessment Methodology	Major References	Key Characteristics and Description
Probabilistic Risk Assessment (PRA)	Käki et al. (2015)	Two-step methodology based on PRA and simulation proposed to analyze disruption risks in realistic sized random supply networks; employs fault tree analysis for mapping failure pathways

Failure Mode and Effect Analysis (FMEA)	Sudeep & Srikanta (2014); Pujawan & Geraldin (2009)	Collected historical data and employed FMEA for assessment of supply chain risk and impacts; adopted quality function deployment technique along with FMEA to identify various risk sources
Analytical Hierarchy Process (AHP)	Gaudenzi & Borghesi (2006); Wu et al. (2006); Lee (2014)	Multi-criteria decision framework based on suggestions from experts in SCRM field; employs pairwise comparisons and eigenvector synthesis for priority ranking
Fuzzy AHP and Fuzzy TOPSIS	Samvedi et al. (2013); Radivojevića & Gajovićb (2014); Mangla et al. (2015)	Extensions addressing ambiguity and imprecision in expert judgments; represents evaluations as fuzzy numbers rather than precise values
Multi-Grade Fuzzy Approach	Vinodh & Prasanna (2011)	Identified agile supply chain enablers, criteria, and attributes; addresses multiple evaluation dimensions with linguistic ambiguity
Grey Theory and Modified TOPSIS	Hui-Min (2008)	Develops evaluating index system from core enterprise standpoint in fuzzy environment for supply chain overall risk assessment; operates with limited information

- *Note: Methodology selection should consider organizational context including data availability, analytical capabilities, stakeholder engagement requirements, and specific risk management objectives. Source: Literature synthesis of risk assessment techniques in SCRM domain.*

The synthesis of the methodologies showed that the most common techniques of the multi-criteria decision analysis, such as AHP, ANP, and their fuzzy variants, are the most used methods of supply chain risk assessment (they are applied in more than 40% of the assessments studied) (Qazi et al., 2018). Such dominance translates to some of the benefits such as the ability to accommodate quantitative and qualitative criteria, methodical elicitation of expert judgment when the historical data is scant, transparency in decision logic allowing an understanding of stakeholders and flexibility to meet various decision situations such as selecting a supplier and evaluating a mitigation strategy. Nonetheless, such methods also have drawbacks such as large time requirements when the alternatives or criteria are numerous to carry out pairwise comparisons, expert judgments may not be consistent and therefore require a process of refinement, and the synthesized priorities are subject to an effect of elicitation methodology.

Probabilistic risk assessment and failure mode analysis offer methodical outline designs that make certain complete identification and judgment of risks, which are even more essential in technically intricate supply chains with an extended variety of failure modes, as well as in cases where it is necessary to comprehend the impact of errors. These have the advantages of rigorous design and engineering background incorporating analytical discipline to risk assessment, but demand substantial technical skills and time investment which could be a strain on resource-limited organizations (Gładysz et al., 2017). Combining quality function deployment with FMEA build connections between customer specifications and internal risk so that the analysis aims at any vulnerability that may occur and expose value to either internal or external impact (Qazi et al., 2018).

B. *Practical Implications for Supply Chain Risk Management Implementation*

➢ *Strategic Guidance for Dual Sourcing and Redundancy Investments*

The findings of the simulation usage offer practical suggestions to organizations executing dual sourcing choices by showing that redundancy investments attain maximum returns when enacted at low stages of supply chain especially at Tier 3 where the foundation of the supply base is prerecorded (Ramasesh et al., 1991). Single-tier dual sourcing showed overall improvements in performance of 24.5 points when used at Tier 3 compared to the 5.7 points when used at Tier 2 and 1.7 points at Tier 1 indicating that redundancy at lower tiers should be prioritized by organizations with limited budgets that cannot afford to dual source whole materials supply bases (Wilson, 2007). This result is in opposition to intuits that redundancy must target Tier 1 suppliers that are closest to the business with the strongest relationships and the most visible situation, but rather suggests that it is because disruptions at lower levels have upward-flowing effects that grow in strength that securing the base offers disproportionate resiliency benefits.

The operational implication is that organizations are advised to map supply networks beyond direct suppliers to determine which are critical Tier 2 and 3 dependencies and assessing which lower-tier suppliers constitute single points of failure whose failure would limit the overall capacity. In case of identified critical nodes, prioritization on dual sourcing investments is necessary even at the cost of single sourcing of suppliers in less critical Tier 1 suppliers where visibility with the manufacturer allows fast detection of the problem and alternative sourcing (Hosseini et al., 2019). The study also showed that all forms of dual sourcing are effective when there is actual independence between redundant suppliers, since nearby sources or those dependent on infrastructure are of geographic proximity offer spurious redundancy, which fails to work when both sources are hit by correlated events.

To make sure that independence of the potential dual sourcing candidates is real, organizations should assess the independence of the prospective candidate on several planes such as geographic distance, infrastructural support, ownership, and regulatory location (Gladysz et al., 2017). The result that completes dual sourcing at all levels resulted in 96.6% mean performance as opposed to 51.1% without redundancy indicate that there is significant resilience enhancement that can be gained using systematic backup supplier development, but cost-benefit analysis must balance these benefits with cost related to relationship management, possible losses in volume discounts and complexity associated with coordination (Ramasesh et al., 1991).

- *Disaster Recovery Planning Investment Optimization*

The existence of the linear correlation between the performance results and the effectiveness of the DRP creates a clear guideline in the disaster recovery planning investment decisions, that is, even an average capacity of mitigation can lead to the value that is significant without an absolute contingency coverage (Christopher and Peck, 2004). Companies with fears that the development of a complete DRP is not matched by the resources at hand will gain significant risks mitigation by prioritizing the development of most critical situations, gaining proportional rewards without taking all or nothing with investments (Ambulkar et al., 2015). The study recommends focusing on development of DRPs in terms of risk-based approaches that define situations with high potential impact and non-insignificant probability of occurrence, creating comprehensive response plans, back-up, and tested procedures on priority risks and accepting residual exposure to the low-priority ones.

The implementation of DRP in practice should focus on three aspects that have been proved to be especially useful (Kamalahmadi and Parast, 2016): backup capacity facilities that allow production to continue at other sites in the event of the disabling of primary facilities; non-standard supplier relationships that allow access to materials quickly when the usual suppliers are impacted; and communication system that can keep the various stakeholders coordinated in the event of disruption of infrastructure (Shishodia et al., 2023). The DRPs of organizations should undergo test exercises periodically where illnesses of disruption are simulated and the gaps between planned and actual response resources in response to the emergency conditions identified without complacency where plans are on paper but cannot be implemented effectively (Christopher and Peck, 2004). The observation that DRP performance alignment brought simple and complex supply chains to a performance level is indicative of the fact that any organization that seeks competitive advantage by diversifying into a supply base does not need to be resilient as long as mitigation planning increases with the complexity of the network.

C. Sector-Specific Risk Assessment Considerations and Application Across Sectors

- *Context-Specific Applications Across Industry Sectors*

General risk assessment frameworks must be adjusted to consider unique features and limits of specific industries (Ahumada and Villalobos, 2009). Pharmaceutical suppliers need to implement product perishability restrictions that restrict inventory holding periods and make responding to disruption difficult (Jaberidoost et al., 2013). Storing or transportation at temperatures other than those required may render products unusable, although physically they may be supplied. The pharmaceutical supply chain simulation models are to contain the quality degrading effects of time on products and mitigation strategies considering the expiration limits. Compliance with regulations also provides more conditions to restrict the flexibility of the supply chain and necessitate specific scenario analysis (Fan and Stevenson, 2018).

Table 16 Industry-Specific Risk Assessment Considerations and Adaptations

Industry sector	Distinctive risk characteristics	Critical assessment considerations	Recommended methodological adaptations
Pharmaceuticals	Product perishability, regulatory compliance, cold chain requirements	Temperature monitoring, expiration tracking, regulatory documentation	Time-dependent deterioration models, compliance risk scenarios
Food supply	Perishability, seasonality, quality degradation, food safety	Quality dynamics, seasonal patterns, contamination risks	Shelf-life constraints, harvest timing variability
Electronics	Complex multi-tier networks, rapid obsolescence, specialized components	Component availability, technology changes, supplier capabilities	Long lead time modeling, obsolescence scenarios
Automotive	Just-in-time delivery, tight synchronization, sequential assembly	Delivery precision, quality consistency, capacity matching	Sequence-dependent disruption impacts, synchronization requirements
Healthcare services	Real-time delivery, staff-dependent quality, equipment reliability	Workforce availability, equipment maintenance, patient safety	Human factor modeling, capacity flexibility analysis

The patterns of food supply chains are seasonal with the disruption not affecting all harvests and stages of growing seasons. The predictive analytics model must include the weather forecasts, increasing degree day, and pest outbreak indicators that apply to the agricultural production (Huebner et al., 2016). The analysis of disruptions that are bound to happen at various stages of the seasonal cycles should be carried out in order to determine sensitive times. The loss of quality during storage and transportation necessitates modeling of the spoilage rates, exposure to temperature, and damage to handling (Jaberidoost et al., 2013). The risk reduction strategies should strike a balance between inventory buffers and perishability constraints which restrict holding time.

Supply chains of healthcare services demand the modelling of human factors and the availability of the workforce that has a significant impact on the ability to deliver the services. Physical supplies and equipment do not ensure a high quality of service in case of staff illness, fatigue, or turnover (Queiroz et al., 2022). Healthcare specific performance indicators such as the waiting time of patients, quality measures of treatment, and safety indicators should be included in simulation models (Jaberidoost et al., 2013). Scenario analysis is to be done on the situations of the pandemic when both demand rises and shortages of labor are observed at the same time. The reliability of equipment in healthcare is especially important because failure may pose a direct risk to patient safety and necessitate specific approaches to maintenance and having backup equipment (Aldrighetti et al., 2024).

- *Food Supply Chain Perishability and Time Sensitivity Implications*

The food supply chains pose special risk assessment challenges due to the perishability of product that causes tight time constraints whereby response to disruption has timeframes limit to days as opposed to weeks or months that can be enjoyed in manufacturing industries. The experiment discovered that Monte Carlo simulation parameters had to be adapted to food situations, longer time horizons, more common demand variations, and seasonal capacity curves necessitated alternative probability distributions than manufacturing ones (Hubner et al., 2016). Food supply chain scenario should also include the aspect of demand-supply matching within perishable time-frames, and it is important to note that even the slightest delay in transportation will make products unsellable because of their loss of freshness (Jaberidoost et al., 2013).

Food distribution predictive analytics apps had a lower prediction accuracy (76.4) than manufacturing industries, which partly corresponds to shorter prediction horizons with the early warning systems providing less lead time to predict problems before they adversely influenced operations (Ahumada & Villalobos, 2009). The study recommended that the risk management approach of food supply chain ought to be based on prevention by building supplier capability, quality control, and process control rather than contingency implementation and disruption prediction owing to perishability constraints that reduce the viability of backup sourcing (Hubner et al., 2016). Transportation failures are especially dangerous during food supply chains where refrigerated capacity is specialized and such weather events as shipping routes cause direct effects on the quality of products, so disasters should be better planned in terms of disruption of logistics than manufacturing-based disasters, which are promoted in manufacturing settings.

- *Data Requirements and Quality Considerations*

An efficient risk assessment must have complete information in various categories and the quality of the information should be adequate enough to facilitate sound analysis. History of disruption offers critical underpinning of calibration of probability distributions, prediction model validation (Wilson, 2007). Most organizations, however, do not have a systematic disruption documentation besides significant events that are being managed (Brintrup et al., 2020). Small distortions that are not well documented can add up to a significant performance, which will distort historical data in favor of disasters. Structured disruption tracking systems should be instituted in organizations whereby events in the organization will be captured despite their severity. The standardized categorization schemes also ensure aggregation and analysis across the various units of an organization and over time.

The supplier performance data can help to predict the analytics because it shows the patterns that can lead to disruption (Cavalcante et al., 2019). Worsening performance of the deliveries, rising of the quality defects or falling responsiveness could indicate the problematic situation with suppliers that requires the proactive intervention. Nevertheless, the measurement of supplier performance is not usually standardized in various commodities or different geographical locations (Sharma et al., 2022). Companies ought to develop uniform supplier scorecards to be used with all the suppliers. The automated procurement and logistics system data collection eliminates human labor and enhances timeliness when compared with periodic surveys (Dubey et al., 2021). The qualitative factors including communication quality and problem-solving collaboratively can be tracked with the integration with the supplier relationship management systems.

Table 17 Data Requirements for Integrated Risk Assessment Implementation

Data category	Specific data elements	Typical sources	Quality challenges	Collection frequency
Disruption history	Event dates, types, severity, duration, affected nodes	Incident reports, maintenance logs, news archives	Incomplete documentation, inconsistent categorization	Continuous with historical compilation
Supplier performance	On-time delivery, quality metrics, capacity utilization	Procurement systems, supplier scorecards	Varying measurement standards, reporting delays	Weekly or monthly
Network structure	Node relationships, capacity limits, lead times	Supply chain mapping, contracts	Dynamic changes, incomplete visibility	Quarterly updates
Environmental conditions	Weather forecasts, natural disaster risks, geopolitical factors	Government agencies, risk services	Prediction uncertainty, regional specificity	Daily for forecasts, continuous monitoring

Financial indicators	Supplier financial health, market conditions, credit ratings	Financial statements, rating agencies	Delayed reporting, limited small supplier coverage	Quarterly or annually

The data of network structure establish supply chain topology required in the modeling of simulation. Organizations tend to have minimal visibility past the direct suppliers, and this makes it difficult to evaluate the vulnerabilities on the lower tiers (Srai and Gregory, 2008). The projects of the supply chain mapping must go several levels deep to find out the critical dependencies and the single points of failure (Li et al., 2021). Nevertheless, mapping does not consider the practical issues because the suppliers might not readily provide the information about their suppliers because of the competitive reasons (Hosseini et al., 2019). The industry joint efforts can help form neutral third parties that bring suppliers information together without disclosing competition information. Blockchain can be used to support safe sharing of information by issuing records that cannot be tampered and retained in a confidential manner (Tao et al., 2018). The data related to the network structure should be updated on a regular basis by the organizations to reflect the variations in relationships with suppliers and capacity allocation.

D. *Technology Enablement and Future Digital Supply Chain Risk Management*

➢ *Blockchain and Distributed Ledger Implications for Transparency*

The emerging blockchain solutions may be used to overcome supply chain visibility challenges that limit risk evaluation on multiple levels, leading to the creation of transaction records and product provenance that is immutable, which may expose supplier networks that are now unknown to manufacturers (Saberi et al., 2019). The identified research gap named the absence of sub-tier visibility identified one of the key gaps in that organizations cannot map the possible single points of failures embedded in the supply bases, as most manufacturers have an extensive understanding of Tier 1 suppliers but are unaware of Tier 2 and Tier 3 networks (Li et al., 2021). Blockchain applications where products are track-and-traced during supply trips could create the information disclosing the real relationship of suppliers as the parts go through production phases, turning an opaque supply base into a transparent network where risk evaluation may oversee ably reveal weaknesses (Tao et al., 2018).

Nevertheless, blockchain implementation encounters major implementation obstacles such as coordination challenges that presuppose a network of trading partners to implement incompatible systems, data sharing issues that involve proprietary relations with suppliers as competitive advantage firms do not wish to share it, and cost-benefit issues that require evaluation of whether the benefits of transparency justify the costs of implementing the infrastructure (Dubey et al., 2021). The technology is immature in the context of supply chain applications other than limited pilot applications, which implies that risk management in the near term will have to depend on other methods of visibility improvement such as supplier questionnaires and contractual disclosure policies, and collaborative mapping programs where manufacturers coordinate with Tier 1 suppliers to map together into deeper supply networks (Qazi et al., 2018). The study conclusions regarding disruption propagation at the lower level highlight the strategic importance of transparency investments because the organizations cannot manage the risks, they are not aware of, and such amplification effects as presented in the simulation imply that the ignorance about the vulnerability at the lower tiers presents dangerous blind spots.

➢ *Internet of Things and Real-Time Monitoring Capabilities*

Internet of Things (IoT) sensors allow tracking of the situation in the supply chain in real-time by monitoring equipment performance, inventory levels, the transportation status, and environmental parameters that can affect the quality of products and their continuity at work. The predictive analytics systems that are discussed in the present study may be significantly improved with the help of IoT data streams expressing constant updates instead of being based only on periodic transaction data in enterprise systems (Choi et al., 2018). Sensors on equipment that identify patterns of vibration or temperature variation or performance deterioration could serve to give warnings about when a failure will occur before it can be rolled out to the production line, and the prediction horizon could be expanded, unlike prediction patterns that can be realized by examining past transaction data (Sharma et al., 2022). GPS tracking and environmental sensors allow transportation to be tracked in real-time to understand the shipment location and conditions and respond quickly in the event of delays or temperature extremes that could pose a threat to shipment (Wilson, 2007).

Nevertheless, the deployment of IoT is faced with issues such as the cost of sensors deployment, cost of data transmission infrastructure, cybersecurity vulnerability where the networked devices form attack surfaces, and analytics capacity to compute high-velocity data streams (Baryannis et al., 2019). When organizations adopt IoT-enabled risk monitoring, they must weigh benefits of real-time visibility against the relevant costs and complexity of implementation and may need to selectively deploy sensors on high-value shipment or most vulnerable equipment instead of taking a broad-based monitoring approach. The study conclusions concerning the contribution of multi-tier network disruption to the network indicate that IoT monitoring needs to focus on the lower-tier suppliers and logistics connections where visibility is the poorest but the potential of risk spread is the most significant, although lower-tier relationships at arm-lengths are technically more difficult to implement in comparison to directly controlled ones (Ivanov and Dolgui, 2020).

E. *Limitations and Methodological Considerations*

The findings of the research indicate that there are several methodological constraints that should be given special attention. Simulation models are bound to reduce intricate reality by making assumptions on probability distributions, network structures, and disruption propagation mechanisms (Wilson, 2007). The assumption of the base case model is that the disruption events are independent across the nodes, which can be not enough to represent the risk in the case of regional disasters that impact several suppliers at the same time (Li et al., 2021). The limitation is partially overcome in a partially similar scenario of correlation, which is incapable of capturing the entire interdependence between suppliers (Gladysz et al., 2017). The model calibration is based on presumed parameters values and not based on some empirical data of a particular industry or territory. Variations in specifications of parameters would give quantitatively different outcomes, but qualitative trends in terms of mitigation effectiveness would probably be strong.

Predictive analytics performance evaluation depends on the past data which might not reflect the future scenario. Models based on past trends cannot be validated in changing business environments, new forms of risks, or structural changes (Cavalcante et al., 2019). The COVID-19 case is an example of a disruption that the history had never predicted before (Queiroz et al., 2022). Organizations ought to be aware that predictive models are extrapolative of the past trends and not necessarily new risks. Scenario analysis has secondary ability to analyze the situation that is not experienced in history (Mulvey et al., 1995). The integration of historical patterns and the use of future scenarios give the best risk assessment compared to the use of any individual methodology.

When generalizing research studies to other organizational settings, one should consider situational factors. Small organizations might not have adequate resources to do extensive dual sourcing or advanced means of analysis (Sharma et al., 2022). Geographical diversification may become impossible in industries where suppliers are highly specialized irrespective of the benefits of reducing risks (Srai and Gregory, 2008). The supply chain design decisions may be limited by regulatory demands in the pharmaceutical or defence sector (Jaberidoost et al., 2013). There are standard findings that should be applied in specific situations by the organization instead of following prescriptions without analysing the situations in specific contexts. The implementation risks can be minimized and the mitigation strategies can be refined by piloting their limited implementation to assess their impacts in advance before the main deployment.

F. Future Research Directions and Emerging Opportunities

A study exploring the relationship between risks is an urgent need in the development of the theory and practice of supply chain risk management. Present methods tend to look at risks as one-off incidents when it has been proven that disruptions are common triggers of cascading failures in interconnected supply networks (Ivanov & Dolgui, 2020). Interpretive structural modeling is one of the methodologies that can map the relationships between various risk factors and defining which risks are root causes and which are consequences (Qazi et al., 2018). The methods of network analysis can assess the role of topology of the supply chain in spreading disruptions, as well as determine structural weaknesses. System dynamics modeling have the ability to model feedback loops in which effects will result in a reaction where the disruption may cause an increase or decrease of the future effects. These methods would increase the insights into the complicated risk dynamics that are not accounted by the existing simulation models that assume independent events (Gładysz et al., 2017).

Table 18 Prioritized Research Directions for Supply Chain Risk Assessment Advancement

Research area	Key questions	Methodological approaches	Expected contributions
Risk interrelationships	How do different risk factors interact and cascade? What network structures amplify or dampen propagation?	Network analysis, system dynamics, agent-based simulation	Enhanced understanding of cascading failures, improved mitigation targeting
Sustainable risk management	How do sustainability initiatives affect risk profiles? Can environmental and social risks be integrated with operational risks?	Multi-objective optimization, stakeholder analysis	Frameworks for balancing sustainability and resilience objectives
Small enterprise applications	What risk assessment approaches are feasible for resource-constrained organizations? How can shared services reduce capability barriers?	Case study research, action research, capability maturity models	Accessible methodologies enabling broader risk management adoption
Behavioural factors	How do human decision biases affect risk assessment and response? Can behavioural insights improve mitigation effectiveness?	Experimental methods, behavioural economics, psychological studies	Better understanding of human elements in risk management
Technology integration	How can artificial intelligence, blockchain, and digital twins transform risk assessment? What implementation challenges must be addressed?	Technology pilots, comparative studies, implementation research	Guidance for effective technology deployment

Sustainable supply chain risk management combines the environmental, social and governance factors with the conventional operational risk factors. There is a growing challenge on organizations to cut down on carbon emission, maintain ethical employment and responsible corporate citizenry (Giannoccaro and Pontrandolfo, 2002).

Nevertheless, the sustainability programs can present new risks or change the previous risk profiles in a way that will not be adequately handled with the current assessment mechanisms. An example is that if renewable energy is harnessed, the supply chain can be exposed to weather changes (Ahumada & Villalobos, 2009). The geographical diversification could be removed by local sourcing to decrease transportation emission. Studies are to create frameworks on how these trade-offs can be assessed and come up with approaches that will promote sustainability goals and supply chain resiliency simultaneously (Shishodia et al., 2023).

The field of small and medium enterprise risk management should be given more research consideration because current practices usually presuppose organizational strengths that a smaller company does not possess. Such organizations are often characterized by a small number of analytical skills, limited financial resources, and weaker bargaining power over suppliers. Complex simulation or predictive analytics implementations can surpass their ability no matter how beneficial they could potentially be (Dubey et al., 2021). The studies need to come up with simplified risk assessment methods that can be used in situations that are resource limited. The government agencies or industry associations can be offering common analytical services, which allow the small organizations to gain access to capabilities that they may not develop internally. Successful cases of small enterprise risk management implementations papers and reports in case studies may serve as templates that other people can use.

The decision-making process of risk assessment and mitigation is subject to systematic research of some behavioural factors (Ambulkar et al., 2015). Cognitive biases in human beings like optimism bias, availability bias, and confirmation bias can influence risk assessment and flaw decision making. Cost-reduction organizational cultures can discourage cost redundancy investments in cases where such investments are analytically found to be worthwhile. The relationship of trust between the partners in supply chain will impact information sharing and joint risk management (Cachon & Netessine, 2004). Experimental studies can control effects of factors of behaviour and find interventions that can enhance the quality of decisions. Quantitative risk assessment should be combined with behavioural insights to give more realistic models that consider human factors in supply chain management.

Opportunities of technology integration should be further explored since AI, blockchain, and digital twin technologies are being developed. Application of artificial intelligence in supply chain risk management is still young with a lot of untapped potentials. The study must look at the AI methods that are most beneficial in various risk assessment activities and environments (Kumar and Singh, 2024). Blockchain technology has potential of greater supply chain transparency and traceability yet has challenges of implementation such as the coordination and scaling of adoption. There is a potential that research that records successful blockchain implementations will hasten adoption. Digital twin can be used to perform advanced testing of scenarios but needs significant investment in sensors and modelling (Ivanov et al., 2019). It would be the basis of informed investment decisions through research comparing the benefits of digital twins and implementation cost in various industries.

G. Practical Implementation Roadmap

Organizations are advised to embrace the ideas of progressive implementation that develop capabilities over time and avoid the urge to make extensive transformation at once (Ambulkar et al., 2015). The foundation building provides the necessary background using the risk inventory development, crude systems of data collection, and stakeholder involvement. This first stage helps to define significant groups of risks, record the familiar instances of disruptions, and obtain the management approval of future investments (Kamalahmadi and Parast, 2016). The companies must avoid when forced to showcase the effects of their efforts in a short unit since foundation building establishes the prerequisites to success later (Shishodia et al., 2023). Simple disruption tracking or initial supplier risk assessments can be considered quick wins that will keep the momentum going until more significant capabilities are built out.

The development of methodology is an accumulation of analytic skills, based on the construction of simulation models, training of predictive models and scenario definition. Companies must begin with basic models that reflect key supply chain design and key types of risks, and then proceed to seek more comprehensive models (Gladysz et al., 2017). The fact that the piloting applications can be specific to commodities or business units allows refining of methodology without the risk of enterprise-wide implementation. Collaboration with universities or consulting companies can also help develop the methodology faster through outside knowledge (Sharma et al., 2022). The methodologies, assumptions, and validation procedures are documented to enable replication and learning in the organization in the future. The training programs are to develop internal capabilities to maintain and apply models continuously (Dubey et al., 2021).

Table 19 Phased Implementation Roadmap for Integrated Risk Assessment Capabilities

Implementation phase	Duration	Key activities	Required resources	Success metrics
Foundation building	3-6 months	Risk inventory development, basic data collection, stakeholder engagement	Small dedicated team, basic analytical tools	Completed risk catalog, baseline disruption tracking

Methodology development	6-12 months	Simulation model building, predictive model training, scenario definition	Analytical specialists, software tools, training programs	Validated models, documented methodologies
Pilot implementation	6-9 months	Limited scope testing, process integration, performance monitoring	Cross-functional team, management support	Demonstrated value, refined processes
Enterprise deployment	12-18 months	Scaled implementation, capability building, governance establishment	Significant resource commitment, change management	Widespread adoption, embedded processes
Continuous improvement	Ongoing	Performance monitoring, model updating, capability enhancement	Sustained resources, learning culture	Improving resilience, realized benefits

Organizations are advised to embrace the ideas of progressive implementation that develop capabilities over time and avoid the urge to make extensive transformation at once (Ambulkar et al., 2015). The foundation building provides the necessary background using the risk inventory development, crude systems of data collection, and stakeholder involvement. This first stage helps to define significant groups of risks, record the familiar instances of disruptions, and obtain the management approval of future investments (Kamalahmadi and Parast, 2016). The companies must avoid when forced to showcase the effects of their efforts in a short unit since foundation building establishes the prerequisites to success later (Shishodia et al., 2023). Simple disruption tracking or initial supplier risk assessments can be considered quick wins that will keep the momentum going until more significant capabilities are built out.

The development of methodology is an accumulation of analytic skills, based on the construction of simulation models, training of predictive models and scenario definition. Companies must begin with basic models that reflect key supply chain design and key types of risks, and then proceed to seek more comprehensive models (Gladysz et al., 2017). The fact that the piloting applications can be specific to commodities or business units allows refining of methodology without the risk of enterprise-wide implementation. Collaboration with universities or consulting companies can also help develop the methodology faster through outside knowledge (Sharma et al., 2022). The methodologies, assumptions, and validation procedures are documented to enable replication and learning in the organization in the future. The training programs are to develop internal capabilities to maintain and apply models continuously (Dubey et al., 2021).

V. CONCLUSION

In conclusion, this study has in-depth discussed the ability of scenario analysis, Monte Carlo simulation, and predictive analytics based on organizations to detect and mitigate any likely occurrence of supply chain disruptions through combined risk evaluation frameworks. These two complementary methodologies, as an analysis shows, offer capabilities that neither alone can do, i.e. strategic, operational and tactical decision requirements. According to the results of Monte Carlo simulation, disruption spreads multiplicatively with the level of supply chain tier, and that is why organizations are severely affected by disruptions even though the chances of individual suppliers failing are relatively low. The systematic analysis of mitigation measures shows that dual sourcing at lower levels of the supply chain produces disproportional resilience and effectiveness of disaster recovery planning has strong linear relationships with performance outcomes of the supply chain.

Combinations of methodological techniques have synergistic powers to deal with the shortcomings present in individual methodologies. Scenario analysis offers strategic framing but it needs quantitative assessment techniques in order to be done rigorously. Monte Carlo simulation provides probabilities in terms of quantification but requires scenario assumptions as inputs. Predictive analytics is used to predict probable futures by using past behavior but cannot analyze situations that have never occurred before. These strategies can be combined in an effective way to allow an overall evaluation of risk based both on the experience of the past and the future strategy. Companies that adopt combined structures have better disruption predictability, mitigation options, and resource distribution approaches than those that adopted isolated approaches or informal strategies.

To apply the research results in practice, it is necessary to pay close attention to organizational opportunities, contexts-specific to industry, and sequence of implementation. Organizations differ significantly in terms of the level of analytical sophistication, data structure, and resources that can be invested in risk management. Smaller businesses have specific difficulties with applying advanced methodologies but can remodel frameworks according to their abilities or use common services in the industry. Perishable products, regulation needs or intangible services, which are industry-specific features, call upon the need to adapt methodologies to the generic models. Gradual implementation strategies that develop capabilities over time are found to be more successful than trying to implement a complete transformation at the same time. Development of foundation building, development of methods, pilot testing and enterprise deployment are logical steps that allow organizations to engage in constant learning and handle the risk of implementation.

The contributions of research further advance the theory of supply chain risk management through disruption propagation mechanisms, measure the effectiveness of the mitigation strategy, and setting the frameworks of integrating multiple analytical strategies. Results offer practical advice on the supply chain design decision making on the selection of suppliers, geographical diversification, redundancy investment and disaster recovery threats. The frameworks of methodologies offered allow practitioners to adjust the approaches to their unique settings instead of necessarily having to fit into prescriptive frameworks.

The rising complexity of global supply chains as well as the exposure to a wide range of disruption causes is a guarantee that risk assessment skills will continue to play a strategic role in the organization of all industries. The introduction of new challenges in implementation and changes in the capabilities of risk assessment due to the development of artificial intelligence and blockchain, the Internet of Things sensors, and digital twins is a promise of technological progress. Competitive advantages will be ensured with the help of excellent supply chain resilience as organizations building advanced risk assessment capabilities considering various approaches and paying enough attention to contextual factors and the capabilities of organizations.

This study builds a basis on future research development in predictive supply chain risk detection and avoidance approaches to enable organizational and community resiliency by synthesizing the knowledge on the topic based on systematic literature review, quantitative modeling, and empirical case studies.

REFERENCES

[1]. Wilson, M. C. (2007). The impact of transportation disruptions on supply chain performance. *Transportation Research Part E: Logistics and Transportation Review, 43*(4), 295-320. https://www.researchgate.net/publication/249921325_A_Monte_Carlo_simulation_model_of_supply_chain_risk_due_to_natural_disasters

[2]. Gładysz, B., Skorupka, D., Kuchta, D., & Duchaczek, A. (2017). Supply chain risk management by Monte Carlo method. *Modern Technologies in Industrial Engineering V (ModTech2017), 178*, 04006. https://www.researchgate.net/publication/321976195_SUPPLY_CHAIN_RISK_MANAGEMENT_BY_MONTE_CARLO_METHOD

[3]. Ramezankhani, M. J., Torabi, S. A., & Vahidi, F. (2018). Supply chain performance measurement and evaluation: A mixed sustainability and resilience approach. *Computers & Industrial Engineering, 126*, 531-548. https://www.researchgate.net/publication/270242228_Monte_Carlo_Simulation_Based_Approach_to_Manage_Risks_in_Operational_Networks_in_Green_Supply_Chain

[4]. Ramasesh, R. V., Ord, J. K., Hayya, J. C., & Pan, A. (1991). Sole versus dual sourcing in stochastic lead-time (s, Q) inventory models. *Management Science, 37*(4), 428-443. https://www.researchgate.net/publication/237842639_Monte_carlo_simulation_based_performance_analysis_of_supply_chains

[5]. Gharehgozli, A. H., Rabbani, M., Zaerpour, N., & Razmi, J. (2008). A comprehensive decision-making structure for acceptance/rejection of incoming orders in make-to-order environments. *International Journal of Advanced Manufacturing Technology, 39*(9-10), 1016-1032. https://www.researchgate.net/publication/338169261_A_monte_carlo_simulation_for_reliability_estimation_of_logistics_and_supply_chain_networks

[6]. Schmitt, A. J., & Singh, M. (2012). A quantitative analysis of disruption risk in a multi-echelon supply chain. *International Journal of Production Economics, 139*(1), 22-32. https://www.semanticscholar.org/paper/Quantifying-supply-chain-disruption-risk-using-and-Schmitt-Singh/9653f3d31f14eeb83d2d5511d91886b01e8d8eb9

[7]. Qazi, A., Dickson, A., Quigley, J., & Gaudenzi, B. (2018). Supply chain risk network management: A Bayesian belief network and expected utility based approach for managing supply chain risks. *International Journal of Production Economics, 196*, 24-42. https://www.researchgate.net/publication/359144285_Supply_chain_risk_network_value_at_risk_assessment_using_Bayesian_belief_networks_and_Monte_Carlo_simulation

[8]. Goh, M., Lim, J. Y., & Meng, F. (2007). A stochastic model for risk management in global supply chain networks. *European Journal of Operational Research, 182*(1), 164-173. https://informs-sim.org/wsc05papers/202.pdf

[9]. Kumar, S., & Singh, R. (2024). The role of predictive analytics in supply chain optimization. *International Journal of Supply Chain Management, 13*(2), 45-67. https://www.researchgate.net/publication/383148496_The_role_of_predictive_analytics_in_supply_chain_optimization

[10]. Cavalcante, I. M., Frazzon, E. M., Forcellini, F. A., & Ivanov, D. (2019). A supervised machine learning approach to data-driven simulation of resilient supplier selection in digital manufacturing. *International Journal of Information Management, 49*, 86-97. https://www.researchgate.net/publication/337282451_Supply_chain_data_analytics_for_predicting_supplier_disruptions_a_case_study_in_complex_asset_manufacturing

[11]. Dubey, R., Gunasekaran, A., Childe, S. J., Fosso Wamba, S., Roubaud, D., & Foropon, C. (2021). Empirical investigation of data analytics capability and organizational flexibility as complements to supply chain resilience. *International Journal of Production Research, 59*(1), 110-128. https://www.researchgate.net/publication/374849416_Predictive_Analytics_and_Machine_Learning_for_Real-Time_Supply_Chain_Risk_Mitigation_and_Agility

[12]. Sharma, M., Luthra, S., Joshi, S., & Kumar, A. (2022). Implementing challenges of artificial intelligence: Evidence from public manufacturing sector of an emerging economy. *Government Information Quarterly, 39*(4), 101624. https://www.researchgate.net/publication/383035770

_Predictive_analytics_on_artificial_intelligence_in_supply_chain_optimization

[13]. Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. *International Journal of Production Research, 57*(7), 2179-2202. https://epublications.marquette.edu/context/mgmt_fac/article/1336/viewcontent/barratt_13574.pdf

[14]. Sodhi, M. S., & Tang, C. S. (2019). Research opportunities in supply chain transparency. *Production and Operations Management, 28*(12), 2946-2959. https://www.researchgate.net/publication/378872101_Reviewing_predictive_analytics_in_supply_chain_management_Applications_and_benefits

[15]. Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. *Production and Operations Management, 27*(10), 1868-1883. https://www.researchgate.net/publication/387903364_Leveraging_Artificial_Intelligence_for_predictive_supply_chain_management_focus_on_how_AI-driven_tools_are_revolutionizing_demand_forecasting_and_inventory_optimization

[16]. Hofmann, E., & Rutschmann, E. (2018). Big data analytics and demand forecasting in supply chains: A conceptual analysis. *International Journal of Logistics Management, 29*(2), 739-766. https://intapi.sciendo.com/pdf/10.2478/picbe-2023-0090

[17]. Hosseini, S., Ivanov, D., & Dolgui, A. (2019). Review of quantitative methods for supply chain resilience analysis. *Transportation Research Part E: Logistics and Transportation Review, 125*, 285-307. https://www.sciencedirect.com/science/article/pii/S266732582300095X

[18]. Kamalahmadi, M., & Parast, M. M. (2016). A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research. *International Journal of Production Economics, 171*(Part 1), 116-133. https://www.sciencedirect.com/science/article/pii/S2405896316310564

[19]. Li, Y., Chen, K., Collignon, S., & Ivanov, D. (2021). Ripple effect in the supply chain network: Forward and backward disruption propagation, network health and firm vulnerability. *European Journal of Operational Research, 291*(3), 1117-1131. https://www.researchgate.net/publication/363865025_Resilience_Assessment_and_Risk_Prediction_in_Supply_Chain_Management_Based_on_Network_Analysis

[20]. Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: Extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International Journal of Production Research, 58*(10), 2904-2915. https://pmc.ncbi.nlm.nih.gov/articles/PMC7261049/

[21]. Queiroz, M. M., Ivanov, D., Dolgui, A., & Fosso Wamba, S. (2022). Impacts of epidemic outbreaks on supply chains: Mapping a research agenda amid the COVID-19 pandemic through a structured literature review. *Annals of Operations Research, 319*, 1159-1196. https://link.springer.com/article/10.1007/s10479-024-06126-x

[22]. Ambulkar, S., Blackhurst, J., & Grawe, S. (2015). Firm's resilience to supply chain disruptions: Scale development and empirical examination. *Journal of Operations Management, 33-34*, 111-122. https://www.mdpi.com/2673-4591/76/1/41

[23]. Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management, 15*(2), 1-14. https://www.researchgate.net/publication/278712727_Supply_Chain_Risk_Management_Resilience_and_Business_Continuity

[24]. Shishodia, A., Sharma, R., Rajesh, R., & Munim, Z. H. (2023). Supply chain resilience: A review, conceptual framework and future research. *International Journal of Logistics Management, 34*(4), 879-908. https://www.sciencedirect.com/science/article/pii/S2667325824003108

[25]. Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: Definition, theory, and research agenda. *International Journal of Physical Distribution & Logistics Management, 48*(3), 205-230. https://pmc.ncbi.nlm.nih.gov/articles/PMC7283689/

[26]. Aldrighetti, R., Zennaro, I., Finco, S., & Battini, D. (2024). Healthcare supply chain simulation with disruption considerations: A case study from Northern Italy. *Global Journal of Flexible Systems Management, 25*(Suppl 1), 1-17. https://arxiv.org/html/2401.10895v2

[27]. Fahimnia, B., Tang, C. S., Davarzani, H., & Sarkis, J. (2015). Quantitative models for managing supply chain risks: A review. *European Journal of Operational Research, 247*(1), 1-15. https://doi.org/10.1016/j.ejor.2015.04.034

[28]. Giannakis, M., & Louis, M. (2016). A multi-agent based system with big data processing for enhanced supply chain agility. *Journal of Enterprise Information Management, 29*(5), 706-727. https://doi.org/10.1108/JEIM-06-2015-0050

[29]. Giannoccaro, I., & Pontrandolfo, P. (2002). Inventory management in supply chains: A reinforcement learning approach. *International Journal of Production Economics, 78*(2), 153-161. https://doi.org/10.1016/S0925-5273(00)00156-0

[30]. Sterman, J. D. (2000). *Business dynamics: Systems thinking and modeling for a complex world*. McGraw-Hill.

[31]. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research, 57*(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1533261

[32]. Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. *Journal of*

Manufacturing Systems, 48(Part C), 157-169. https://doi.org/10.1016/j.jmsy.2018.01.006

[33]. Cachon, G. P., & Netessine, S. (2004). Game theory in supply chain analysis. In D. Simchi-Levi, S. D. Wu, & Z. J. Shen (Eds.), *Handbook of quantitative supply chain analysis* (pp. 13-66). Springer. https://doi.org/10.1007/978-1-4020-7953-5_2

[34]. Brintrup, A., Pak, J., Ratiney, D., Pearce, T., Wichmann, P., Woodall, P., & McFarlane, D. (2020). Supply chain data analytics for predicting supplier disruptions: A case study in complex asset manufacturing. *International Journal of Production Research, 58*(11), 3330-3341. https://doi.org/10.1080/00207543.2019.1685705

[35]. Mulvey, J. M., Vanderbei, R. J., & Zenios, S. A. (1995). Robust optimization of large-scale systems. *Operations Research, 43*(2), 264-281. https://doi.org/10.1287/opre.43.2.264

[36]. Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research, 57*(3), 829-846. https://doi.org/10.1080/00207543.2018.1488086

[37]. Jaberidoost, M., Nikfar, S., Abdollahiasl, A., & Dinarvand, R. (2013). Pharmaceutical supply chain risks: A systematic review. *DARU Journal of Pharmaceutical Sciences, 21*(1), 69. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3848876/

[38]. Ahumada, O., & Villalobos, J. R. (2009). Application of planning models in the agri-food supply chain: A review. *European Journal of Operational Research, 196*(1), 1-20. https://doi.org/10.1016/j.ejor.2008.02.014

[39]. Srai, J. S., & Gregory, M. (2008). A supply network configuration perspective on international supply chain development. *International Journal of Operations & Production Management, 28*(5), 386-411. https://doi.org/10.1108/01443570810867178

[40]. Hübner, A., Kuhn, H., & Wollenburg, J. (2016). Last mile fulfilment and distribution in omni-channel grocery retailing: A strategic planning framework. *International Journal of Retail & Distribution Management, 44*(3), 228-247. https://doi.org/10.1108/IJRDM-11-2014-0154