

Systemic Risk Assessment in Complex Supply Networks

Anna Ledwoch, Alexandra Brintrup, Jörn Mehnen, Ashutosh Tiwari

Abstract—The growth in size and complexity of supply chains has led to compounded risk exposure, which is hard to measure with existing risk management approaches. In this study, we apply the concept of systemic risk to show that centrality metrics can be used for complex supply network risk assessment. We review and select metrics, and set up an exemplary case applied to the material flow and contractual networks of Honda Acura. In the exemplary case study, geographical risk information is incorporated to selected systemic risk assessment metrics and results are compared to assessment without risk indicators in order to draw conclusions on how additional information can enhance systemic risk assessment in supply networks. Katz centrality is used to measure the node's risk spread using the World Risk Index. Authority and hub centralities are applied to measure the link risk spread using distances between geographical locations. Closeness is used to measure speed of disruption spread. Betweenness centrality is used to identify high risk middlemen. Our results indicate that these metrics are successful in identifying vulnerabilities in network structure even in simplified cases, which risk practitioners can use to extend with historical data to gain more accurate insights into systemic risk exposure.

Index Terms—Complex supply networks, systemic risk, network science, Katz centrality, HITS, closeness centrality, radiality, betweenness centrality

I. INTRODUCTION

A supply chain can be defined as a set of companies that share the production and delivery responsibility of the material flow, from raw materials to the finished product delivered to end-users [1]. Supply chains spontaneously change and emerge without a single entity controlling it, thus they can be considered a Complex Adaptive System (CAS) [2]. During recent decades supply chains became global and intertwined, increasing their complexity and risk exposure.

Globalisation resulted in increased competition, which lead to pressure to decrease costs through practices such as reducing inventory or supplier base, outsourcing, factories tend to focus on core capabilities [3]–[9]. Global sourcing encouraged manufacturing in sites in few places in the world, which made companies vulnerable to disruptions like natural disasters and terrorism [3]. Risk assessment has thus become an important part of successful supply chain management [8], [10], [11].

Several risk assessment practices exist, but none of these embody the structural complexities supply chains face today. Although the term *complexity* has many definitions, in this

context it shall denote that a structure has numerous interconnected components with non-trivial interactions [12], [13]. Recent empirical studies show that supply chains comprise of inter-tier connections, cycles and feedback loops [14], [15], thus can be represented as a network rather than a chain [16]. Interconnectedness, complexity and uncertainty have increased [4], [8], [11], [17] and so did risk exposure [11], [18], [19].

Supply chains became extended networks, they became susceptible to disruptions cascading through complex interactions and interdependencies. This implies that their risks have systemic nature [20]. Increased risk exposure necessitates extended supply network visibility, where the term extended refers to the visibility beyond direct business partners. Supply network visibility is often limited or unavailable [21]–[25]. Current tools do not always consider the extended supply network and are not enough to capture vulnerabilities [26], [21]. There is a need for better methods to identify and measure risks [11], [27], including supply chain dynamics, flows and interdependencies [26].

This research aims at identifying new methods for systemic risk assessment in supply networks. We argue that network theory is a suitable tool for systemic risk evaluation, when risk practitioners do not have an access to detailed supply chain data. First, we review the concept of systemic risk and recent advances in the domain of supply chain risk assessment. Next, we give an overview of statistical tools available in the interdisciplinary field of network theory to assess their applicability for systemic risk assessment. We split the metrics in three groups: degree-like, closeness-like and betweenness-like. We choose amongst them ones that are a good representation of the others, based on the correlation study. Five metrics are chosen to be applied in the case study: eigenvector centrality, hub, authority, closeness and betweenness. Katz centrality (a type of eigenvector centrality) is used to evaluate transmission of the node risk; hub and authority centralities are applied to measure how the risk associated with links transmits to nodes; closeness is used to assess speed of disruption spread; betweenness centrality is used to identify the high risk firms amongst the intermediaries. We highlight how these metrics can be used through a case study that assesses the risk of firms embedded in the Honda-Acura supply network and how incorporating supply network specific information to centrality measures can enhance systemic risk view.

II. RELATED WORK

Risk is the probability of a negative event occurring multiplied by the impact of this event [28]; or the variability of possible outcomes [29].

Manuscript received (...); accepted (...). Date of publication (...)

A. Ledwoch, J. Mehnen and A. Tiwari are with the Manufacturing Department, Cranfield University, MK43 0AL (email: a.m.ledwoch@cranfield.ac.uk)

A. Brintrup is with the Institute for Manufacturing, Cambridge University

As risk in supply chains increase, risk assessment practices gain more popularity. Example of risk assessment methods are conceptual frameworks [30], [31]. However these are usually subjective and time-consuming. Other methods include risk optimization and evaluation. Roncoli et al. (2013) developed a model for risk minimization for transport of dangerous goods by road [32]. Raj et. al. (2015) developed a model measuring resilience using Cox-PH model [33]. These approaches are usually NP-hard [34], and become computationally expensive as extended supply networks can reach to thousands of nodes and tens of thousands of links [24].

Traditional risk practices were developed for supply chains having in mind their hierarchical properties and simplicity. The growth in their complexity, interconnectedness and interdependency made old techniques outdated [35], [36]. Traditional risk concepts are being replaced by the idea of systemic risk, a risk on the systems level.

According to Helbing (2013), systemic risk is “*the risk of having not just statistically independent failures, but inter-dependent, so-called ‘cascading’ failures in a network of N interconnected system components*” [35]. While thinking about systemic risk one needs to ask questions such as: who is most likely to fail? How will it affect other parts of the system? Who is most likely to fail next?

An intuitive way to measure systemic risk in a complex system is through the use of simulation. Examples include measurement of the disruption impact in the Portuguese automotive industry [37] or risk assessment using timed Petri nets [38]. The main drawback of such approaches is that simulations are data driven. In cases where supply network visibility is limited data might not be easy to obtain. There is a need for methods that enable the assessment of risk of a complex system, without the need of long and laborious data collection.

The interdisciplinary field of complex networks focuses on the identification and study of patterns that occur in complex networks such as social, computer, technological or brain networks. Complexity science helps to analyze risk propagation with the use of methods like cascading failures, percolation or epidemiology. It has begun with the field of social sciences and biology, where phenomena such as *information cascades*, *diffusion of innovations* or *spread of diseases* are studied. In these systems an individual in a society is able to influence other’s behavior, decisions and beliefs [39], [40] or health [41].

Systemic risk has been seen from the lens of cascading failure, which happens when a disruption in one node triggers failures in neighboring nodes [42]–[44], applied across range of fields such as transportation networks [45], power-grids [42] or supply networks [43], [44]. It was observed that cascades in many systems happen rarely, yet with surprising high impact [46]. There are various cascade propagation models available in the literature and each of which deal with different damage scenarios taking into account the same initial conditions [47].

Another view on systemic risk in complex systems can be taken from epidemiology, a science of understanding risk spread in networks. It has been applied to many disciplines ranging from transmission of infectious diseases in biological systems, power-grid failures or computer viruses spread.

Epidemiology studies how network topology influences propagation of a disease and answers the question what is the possibility of an outbreak in the system [48]. It expanded its view from disease spread to systemic risk profiles, especially in financial networks studying unexpected shocks and bankruptcy propagation [49], [50]. In supply networks Hertz et al. (2008) studied the effects of firm bankruptcy [51] and Basole and Bellamy (2014) used classical epidemic model to measure risk diffusion [21].

Another network science method is *percolation*, which is the process of removing some part of the network: nodes, links or both [52], to determine network robustness and resilience [48], but can be successfully applied as a systemic risk proxy. It has been used in numerous applications including communication networks [53] and supply chains, where Thadakamalla et al. (2004) and Zhao et al. (2012) applied the classical preferential attachment model to generate a supply network, and used percolation for supply network survivability and resilience assessments. Their work highlights that different topologies result in different network vulnerabilities - for example scale-free network structures are robust against random attacks, but vulnerable against targeted ones [34], [54].

So far we have mentioned dynamical processes used for risk assessment, but the domain of complex science is also wealthy in static methods originating from graph theory. Examples of such metrics include shortest paths [55]–[57], degree distribution [58], [59] or clustering coefficient [59]. In supply networks Reniers et al. (2012) have studied systemic risk of the chemical industry, by developing the risk indexes based on the shortest path metric [60].

Percolation, cascading failures and epidemiology are tools that help detecting vulnerabilities in the network and they have been extensively applied in many domains, including supply networks. But so far they have been used mainly to assess the overall system health. The focus of this paper is to investigate how an individual node in the complex system is exposed to systemic risk and how its vulnerability is affected by its direct and indirect neighbors, which requires more in-depth analysis on the node level. Based on this gap, we will draw from the field of Social Network Analysis (SNA), which is a sub field in complex networks rich with statistical tools specifically, centrality metrics, that enable the assessment of topological properties of a network from an individual node perspective. Centrality measures explain the nodes that play a significant role in the general structure of a given network [61], [48]. In addition, there are various types of interpretations for centralities such as power, exposure, risk, control, autonomy or other [62]. Centralities has been used for vulnerability and risk assessment in various fields, ranging from electrical grids and financial systems to supply networks. Wang et al. (2010) have used centrality measures such as degree, eigenvector centrality, betweenness and closeness to assess the vulnerability of the electric power grid [63].

Systemic risk assessment has become popular in financial systems mainly after the 2008 financial crisis [64]–[66]. Hu et al. (2012) built a framework that incorporates individual bank level information with hub and authority centralities in order to predict contagious bank failures and determine capital

injections to stop those failures [64].

In supply networks the focus has been on identification of critical business partners [8], [15], [67], [68]. Bezuidenhout et al. (2012) used degree centrality in the cause-and-effect network to identify critical issues in the sugar cane supply network [15]. Mizgier et al. (2013) used radiality, betweenness and degree centrality as an aid in bottleneck identification [8]. Basole and Bellamy (2014b) used betweenness centrality as a risk measure in their visualisation framework [68].

Network perspective is a powerful way to systematically understand the complex supply network dependencies and flows [21], especially when detailed data are not available. We found that many network approaches focus on the overall system health, ignoring what is the vulnerability of a node embedded in a complex supply network. Centrality measures can help to assess the compounding of risks residing in various parts of topology to create a systemic view [34], but have found limited application in supply networks [8], [15], [67], [68]. Literature highlights its potential in risk assessment and the need for further study [8], [15]. In the following sections we first review node-level network theory metrics drawing from various fields to assess whether they can serve as a useful systemic risk proxy. We then illustrate how chosen centrality measures can be used by applying them in an empirically informed case study, whereby geographical risk is incorporated to the network. We conclude by discussing how additional insights can be gained and outline future opportunities for research.

III. SYSTEMIC RISK ASSESSMENT BASED ON CENTRALITY MEASURES

Network theory is the study of networks. A network is a combination of *nodes* and *links*, where nodes represent entities of the system and links their relationships. In the supply chain context nodes can represent companies or geographical locations whereas links can represent contractual relationships or material flow. There are different networks types such as: undirected, directed and weighted. Directed networks imply that there is a direction of the relationship between nodes. For example, this could be used when there is a need to represent a material flow from a supplier to a customer. Weighted networks are used when the links or nodes themselves can be characterized by some value, such as inventory or goods transferred.

A. Node-level metrics overview

This section consists of an overview of node-level metrics with their applicability for supply chain systemic risk assessment, based on the relevant literature. To define centrality metrics we use adjacency matrix with the following definition:

$$A_{ij} = \begin{cases} 1 & \text{if there is an edge from } j \text{ to } i \\ 0 & \text{otherwise.} \end{cases} \quad (1)$$

1) *Degree centrality*: The degree of a node it is the number of nodes connected to it [48]. It depicts the connectivity and immediate chance for a node to exert its influence to the rest of the network [63]. In the literature the degree is associated also with prestige, status [48] or access to knowledge [69]. It is represented by the following formula:

$$C_{D_i} = \sum_j A_{ij} \quad (2)$$

where A is an adjacency matrix, and C_{D_i} is a degree centrality of a node i .

The measure has been applied in vulnerability assessment in various domains from power-grids, disease networks to supply chains. Wang et al. (2010) uses degree with the domain related information to find the vulnerable nodes in power-grid network [63]. Bell et al. (1999) uses the metric to assess the vulnerability of individuals defining it is a probability of being infected by HIV [70]. Laxe et al. (2012) links degree with the operational capacity of each port in transportation network [58]. Correa and Yusta (2013) use the measure to define the operational functionality of the power grid components, e.g. low-degree nodes are capacitors, high-degree are buses [55]. Borgatti and Everett (2006) relate to the degree centrality as the volume measure and discuss that it is associated with certainty of arrival [62]. There are many applications for this centrality measure and it has a fair background in vulnerability assessment [71], being a good indicator of the exposure of the node to whatever is flowing through the network [63], [72].

In a supply chain context degree specifies the number of business partners. It has been used to identify specific roles of firms within the supply network: integrators and allocators. An integrator is a company assembling or transforming materials into value-added products, whereas an allocator's responsibility is resource distribution [73]. It has been used by Bezuidenhout et al. (2012) and Mizgier et al. (2013) for bottleneck identification [15], [8], and by Dong (2006) to assess supply chain robustness [67].

Although a useful measure to assess the vulnerability, we argue that it is not enough to assess the systemic risk. Mizgier et al. (2013) mention that it accounts only partially for network topology [8]. Niu et al. (2015) mentions that the degree consider limited information and there are better metrics that include the global information [74].

2) *Eigenvector centrality*: Eigenvector centrality measures node importance based on the importance of its neighbors [75]. It can be represented as:

$$C'_{EI_i} = \kappa_1^{-1} \sum_j A_{ij} C_{EI_j} \quad (3)$$

where A is an adjacency matrix, C_{EI_i} is eigenvector centrality of the node i and κ_1 is the largest eigenvalue of the adjacency matrix.

High eigenvector centrality means that a node has more power [72], [74]. Borgatti and Everett (2006) relate eigenvector centrality with certainty of arrival and highlight the link with risk assessment [62]. It was used in pattern analysis in

fMRI data of the human brain [76] and applied to electric power grid for vulnerability analysis [63].

In a supply chain context it might be regarded as a measure of how important a focal company is, based on the importance of its business partners. The node or link characteristics can be substituted by the risk factor, which enables the assessment of how local risk influence risk of company's neighbors. Examples of such risk factors are natural disaster index, terrorism index, or inventory risks.

3) *Hub and Authority Centrality*: Hubs are nodes that point to many authorities. Authorities are nodes that are pointed to by many hubs [77]. They can be expressed by equations:

$$C_{H_i} = \beta \sum_j A_{ji} C_{A_j} \quad (4)$$

$$C_{A_i} = \alpha \sum_j A_{ij} C_{H_j} \quad (5)$$

where α and β are positive constants, A is an adjacency matrix, C_A is authority centrality and C_H is hub centrality.

Hub and authority centrality has been used in financial systems to identify which banks need a capital injection in order to stop contagious failures [64]. Carlos (2013) argues that authority and hub centralities are successful proxies to measure systemic risk and are able to identify different systemic risk types: coming from the out-going and in-coming links [78].

In a supply chain context this measure can be interpreted as a metric identifying firms having many customers or firms having many suppliers, either direct or indirect. Different weights associated with the links and nodes can be applied such as volume, any cost or lead time variance for links, and natural disaster index, inventory risks for nodes. Weights could help identify companies that have many supplier or customer relationships with firms having high local risk.

4) *Closeness centrality*: Closeness centrality is the inverse of the mean distance from a node to other nodes [48], introduced by Bavelas (1950) [79]. It is denoted by equation:

$$C_{C_i} = \frac{n}{\sum_j d_{ij}} \quad (6)$$

where C_C is closeness centrality, n is number of nodes and d_{ij} is length of the shortest path between nodes i and j [48].

Closeness centrality indicates how long it takes for information to spread from the node to the rest of the network [74], is associated with the influence on other nodes [72] and independence [69]. It is regarded as a proxy for social capital and information spread [80], [81]. Closeness centrality-like measures are natural choice when dealing with risk of something arriving on time [62]. Closeness is used by Nguyen et al. (2013) for the vulnerability analysis in the electric power network [82].

The highest closeness value for a company embedded in the supply chain indicates that the firm has the smallest average distance to the other parts of the network. Companies with high centrality have been classified as navigators, who collect information more autonomously [73].

5) *Radiality centrality*: Radiality centrality is a measure of how a node is connected and reachable within a network [83], and can be denoted by equation:

$$C_{R_i} = \frac{\sum_j d - d_{ij} + 1}{n - 1} \quad (7)$$

where d is the network diameter, d_{ij} is the length of the shortest path between nodes i and j , and n is the number of nodes.

In a supply chain context it denotes how closely the company is located to its partners in the neighborhood. It is a natural choice when dealing with risk of something arriving on time [62]. Mizgier et al. (2013) used radiality to identify suppliers that if disrupted affect the most companies [8]. The measure can be used with weights such as lead time, or distance.

6) *Betweenness centrality*: Betweenness centrality measures the extent to which a node lies on paths between other nodes [84]. It can be denoted by:

$$C_{BT_i} = \sum_{j,k} \frac{st_{j,k}(i)}{st_{j,k}} \quad (8)$$

where $st_{j,k}(i)$ indicates number of shortest paths between j and k going through i and $st_{j,k}$ number of all shortest paths between j and k .

Betweenness centrality is associated with the global importance of the node and the influence it has over the flow in the network [71], [74] including spread [72] and cut-off of information [69]. Bompard et al. (2011) argue that the higher the betweenness, the higher number of geodesic paths coming through the node and therefore higher criticality [85]. Laxe et al. (2012) link betweenness centrality with relative geographical importance [58]. Nguyen et al. (2013) use the metric for vulnerability assessment in power networks [82]; Tang (2013) for IP multimedia subsystems [59].

Betweenness centrality in a supply chain context might indicate companies that act as a middleman, important in passing a product from a supplier to a customer. Those companies are intermediaries, controlling the flow of goods [73]. Mizgier et al. (2013) used it to identify bottlenecks in the supply network [8]; Basole and Bellamy (2014) used betweenness in risk visualisation model [68]. The metric can be used with supply related information, such as material flow volume or cost variance, which can help in identifying the sites in the network lying on the paths with highest fluctuations.

B. Summary

Metrics that are suitable for systemic risk assessment are eigenvector centrality, authority, hub, closeness, radiality and betweenness centrality. Summary of related work in supply chains and other fields is presented in Table I. Borgatti and Everett (2006) mention that these metrics complement each other and are needed for creating a complete picture of various roles played by each node in the network [62].

TABLE I
APPLICATIONS OF CENTRALITY MEASURES IN SYSTEMIC RISK
ASSESSMENT

| Measure | Supply network | Other fields |
|--------------------|-----------------|--|
| Degree | [8], [15], [67] | [55], [58], [59], [63], [69], [70], [71], [72], [82] |
| Eigenvector centr. | | [63], [72] |
| Hub and authority | | [64] |
| Closeness | | [55], [63], [69], [72], [82] |
| Radiality | [8] | |
| Betweenness | [8], [68] | [58], [59], [63], [69], [71], [72], [82], [85] |

TABLE II
PEARSON COEFFICIENT CALCULATED FOR THE CENTRALITY VALUES FOR
MATERIAL NETWORK OF HONDA ACURA

| | C_{EI} | C_H | C_A | C_C | C_R | C_{BT} |
|----------|----------|-------|-------|-------|-------|----------|
| C_D | 0.93 | 0.00 | 0.95 | 0.83 | 0.65 | 0.98 |
| C_{EI} | - | 0.31 | 0.84 | 0.96 | 0.86 | 0.89 |
| C_H | | - | -0.17 | 0.50 | 0.69 | -0.05 |
| C_A | | | - | 0.72 | 0.52 | 0.95 |
| C_C | | | | - | 0.96 | 0.81 |
| C_R | | | | | - | 0.61 |

Shaded cells are used to indicate the correlation that has passed the t-test at 99.95% confidence interval

IV. CASE STUDY

In this section we use the material flow and contractual relationship supply networks of Honda Acura presented by Choi and Hong (2002) and used by Kim et al. (2011) as a case example to illustrate how systemic risk concepts could be applied to supply networks [14], [73]. A correlation study is carried out to identify centrality measures that might carry similar information. From those we will select metrics that can be used to illustrate how systemic risk can be measured.

A. Correlation

After the calculation of each metric reviewed in Section III, Pearson correlation coefficient and the significance t-test at 99.95% confidence interval of each coefficient pair is performed (Table II). Pairs of centralities in Table II that have high correlation and have passed the t-test are shaded.

Three categories of metrics emerge: degree-like measures, closeness-like measures and betweenness-like measures [62]. Degree-like measures consist of degree centrality, eigenvector centrality, hub and authority centralities. Closeness-like measures consist of closeness centrality and radiality. Betweenness-like measures family consists of betweenness centrality. We analyze the correlation of those measures within the group and decide which metrics will be applied for the case study of Honda Acura.

Degree centrality is not considered in the case study, because it accounts for network topology only partially [8], [74]. Since eigenvector centrality and authority centralities are not correlated with hub centrality, we consider all three for the case study. Closeness and radiality are highly correlated with each other, thus we choose one to apply in Honda Acura network. Closeness centrality is chosen since it has numerous applications in the risk assessment literature. One needs to bear in mind that the results of the correlation study is specific to

the network of Honda Acura - as different supply networks might bear different topological features the resulting metrics might have different correlations.

B. Experiment description

We perform two experiments for each metric for unweighted and weighted network to highlight how incorporating domain related information can enhance risk analysis. To measure systemic risk we use two different risk types: node risk and link risk. As a node risk we apply World Risk Index (WRI), as a link risk we use a distance between two geographical locations. We assign the WRI to nodes in the study of Katz centrality (a type of eigenvector centrality), to identify risk spread in the undirected contractual supply network. We assign the distance between geographical locations to links in the study of hub and authority to assess supplier and customer risk exposure in the directed material network, and in the study of closeness to assess the speed of disruption spread in the undirected material network. The inverse of distance is used for betweenness centrality study to identify the critical intermediaries. There are in total 8 experiments and their summary is presented in Table III.

WRI and distance are not part of the original Choi and Hong (2002) case study, thus the Marklines¹ automotive database is used to extract companies headquarters locations, which helps to evaluate node and link weights. The care has been taken to be as accurate as possible, although due to the fact that the data provided in the study of Choi and Hong (2002) is not the most recent, we made some assumptions. Therefore values retrieved from the on-line database and geographical locations found should be taken as guidance only, not the actual state of the current Honda Acura supply chain.

Data are incomplete as names of five companies are changed in order to protect the identity of the firms: Intek, JFC, J1, J2, and J3. For those cases Intek and JFC are assumed to be suppliers located in China, as Marklines suggests. Choi and Hong (2002) highlights that J1, J2 and J3 are suppliers located in Japan, but we were unable to find additional information in Marklines database, thus we assume that the headquarters are located in Tokyo.

Calculations were performed using NetworkX library for Python 3.4.

C. Katz centrality for assessing undirected node risk spread

Katz centrality is applied to the contractual network of Honda Acura to assess undirected node risk spread. It is a variation of eigenvector centrality, denoted by the following equation [86]:

$$C'_{K_i} = \kappa_1^{-1} \sum_j A_{ij} C_{K_j} + \beta_i \quad (9)$$

where C_{K_i} is Katz centrality of a node i , A is the adjacency matrix of the network, κ_1 is the biggest eigenvalue of the adjacency matrix and β_i is the constant. We use Katz, since original eigenvector centrality does not account for including

¹http://www.marklines.com/en/supplier_db/, accessed on August 2015

TABLE III
CASE STUDY EXPERIMENT SUMMARY

| Experiment | Measure | Network type | Direction | | Weights | | |
|------------|-------------------|---------------|------------|----------|------------|-------------|-------------|
| | | | Undirected | Directed | Unweighted | Node weight | Link weight |
| 1 | Katz centrality | Contractual | x | | x | | |
| 2 | Katz centrality | Contractual | x | | | x | |
| 3 | Hub and authority | Material flow | | x | x | | |
| 4 | Hub and authority | Material flow | | x | | | x |
| 5 | Closeness | Material flow | x | | x | | |
| 6 | Closeness | Material flow | x | | | | x |
| 7 | Betweenness | Material flow | x | | x | | |
| 8 | Betweenness | Material flow | x | | | | x |

TABLE IV
KATZ CENTRALITY FOR CONTRACTUAL NETWORK OF HONDA ACURA

| Unweighted | | Node-weighted | |
|-------------|--------|---------------|--------|
| Company | C_K | Company | C_K |
| Intek | 0.3759 | Intek | 0.3302 |
| Honda | 0.3113 | Iwata Bolt | 0.2948 |
| Arkay | 0.2377 | Microtech | 0.2528 |
| Select Ind. | 0.2169 | Nihon | 0.2528 |
| Tobutsu | 0.1873 | Honda | 0.2515 |
| HFI | 0.1741 | J1, J3 | 0.2493 |

TABLE V
HUB CENTRALITY FOR MATERIAL FLOW NETWORK OF HONDA ACURA

| Unweighted | | Link-weighted | |
|--------------|--------|---------------|--------|
| Company | C_H | Company | C_H |
| Iwata Bolt | 0.0617 | Select Ind. | 0.0988 |
| Select Ind. | 0.0575 | Tobutsu | 0.0980 |
| Tobutsu | 0.0575 | IPG | 0.0591 |
| Milliken | 0.0544 | Milliken | 0.0609 |
| Arkay | 0.0544 | Honda Trading | 0.0583 |
| Garden State | 0.0544 | Jergens | 0.0580 |

node characteristics and Katz does [48]. We substitute β_i by 1 for unweighted case and by WRI for weighted case to incorporate geo-political risk.

The WRI is an index that measures risk on the natural hazard and social level. It consists of four components: exposure, susceptibility, coping and adaptation. Exposure is a natural disaster risk, susceptibility is a *likelihood of suffering harm*, coping is a *capacity to reduce negative consequences*, and adaptation is a *capacity for long-term strategies for societal change*, as defined by [87]. The index is appointed per country and is the highest for Vanuatu (36.43), and the lowest for Qatar (0.1). The ranking consists of 173 countries with 7.40 as the average. WRI is assigned to each node according to their headquarters location taken from on-line automotive database Marklines. The metric is calculated for unweighted and WRI node-weighted case. Table IV presents results for the six highest Katz centralities in the contractual relationship network.

In the unweighted case, the highest Katz is for Intek and Honda. This is because they manage most of the business relationships in the supply network. Intek can be regarded as the most critical company, because it has the highest number of business partners and its partners have numerous relationships themselves. Katz centrality score of other companies is also proportional to their degree.

In the node-weighted case, the highest Katz centrality has Intek. The second score belongs to Iwata Bolt because together with its two business partners they are located in high risk region, creating a *high risk cluster*. The other companies that have high Katz centrality are Intek's business partners with high local WRI.

Traditional unweighted Katz centrality evaluates the risk of the node based mainly on its degree and degree of its neighbors. Incorporating additional information, such as WRI, enables to identify firms vulnerable to geo-political risk that

TABLE VI
AUTHORITY CENTRALITY FOR MATERIAL FLOW NETWORK OF HONDA ACURA

| Unweighted | | Link-weighted | |
|---------------|---------|---------------|---------|
| Company | C_A | Company | C_A |
| Intek | 0.6656 | Intek | 0.5830 |
| Arkay | 0.1589 | Arkay | 0.3359 |
| HFI | 0.1153 | HFI | 0.0465 |
| Select Ind. | 0.0602 | Select Ind. | 0.0345 |
| Honda Trading | 0.0000* | Honda Trading | 0.0001 |
| Iwata Bolt | 0.0000* | Honda | 0.0000* |

* approximation

would not be identified using the traditional approach. Iwata Bolt, Microtech, Nihon, J1 and J3 are firms having relatively small degree compared with the other companies, thus are omitted by unweighted Katz centrality measure. High WRI and the proximity to other high geo-political risk exposure locations makes them worth attention for risk practitioner. For network visualisations please see Figures 1a and 1b.

As presented above, Katz centrality can be used with local risk factors to identify high risk firms clustered together. This shows how local risks impact those of its neighbors, to generate the systemic view.

D. Hub and authority centrality for assessing directed link spread

Hub and authority centralities can be used to assess the directed link spread of failure. Directed network of material flow of Honda Acura is used for this example. Two cases are considered: unweighted and weighted with transportation risk assigned to the links. We calculate transportation risk based on the distance - the higher distance the higher risk. Results for both cases are presented in Table V and VI.

Nodes with high authority and hub centrality can be regarded as the ones having high risk suppliers and high risk

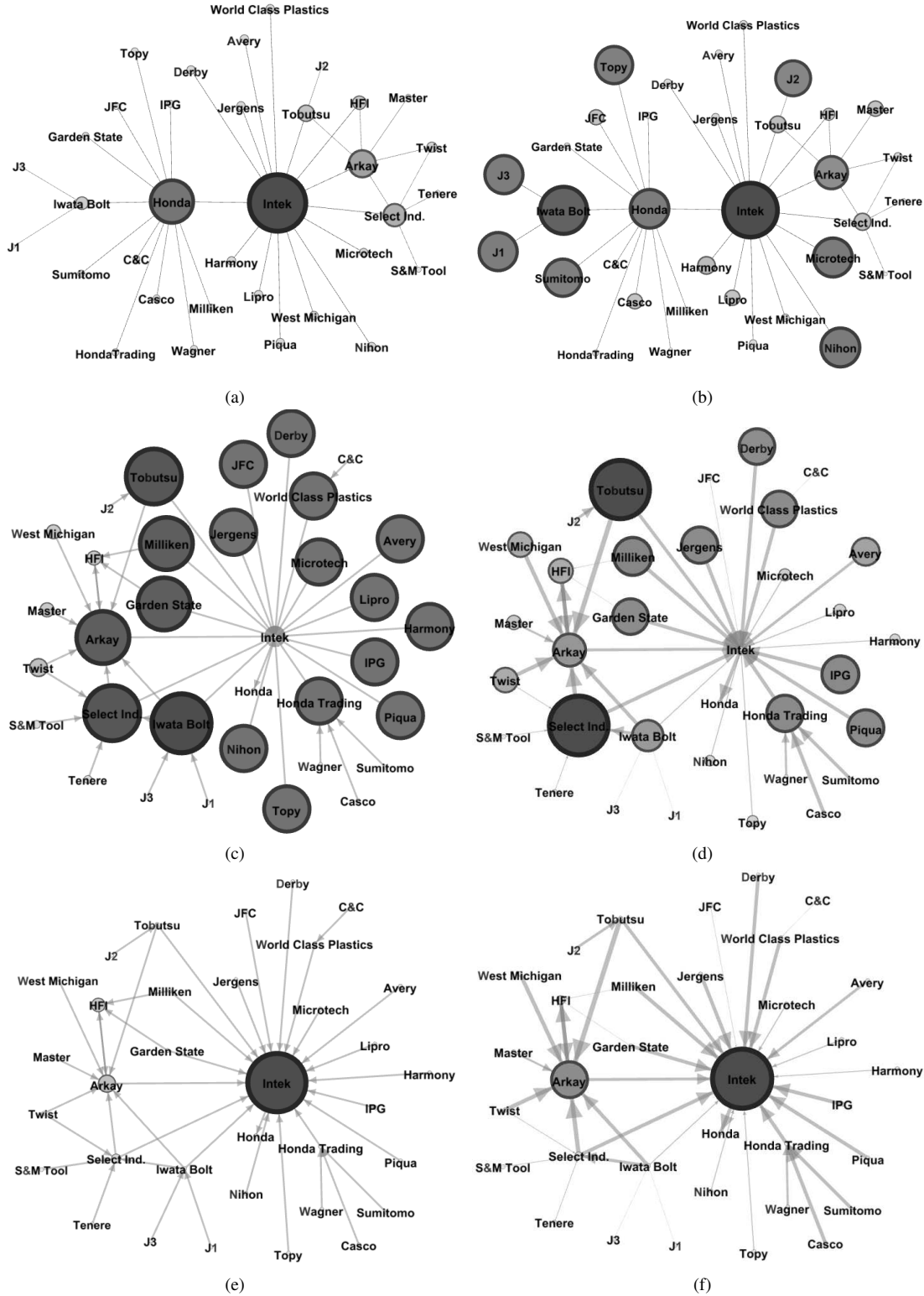


Fig. 1. Network visualisations: a) unweighted Katz centrality, b) node-weighted Katz centrality, c) unweighted hub centrality, d) link-weighted hub centrality, e) unweighted authority centrality, f) link-weighted authority centrality. Each node and link are sized and shaded according to the respective centrality value. The darker and bigger node/link, the higher value.

customers respectively. Unweighted hub centralities are low, because there is no dominant hub in the network and the ones having the highest score are the ones with the highest out-degree and having Intek as a customer. Intek has the

highest authority because it has many suppliers and is the last assembler before delivering to Honda.

For the link-weighted case, high hub values have companies that are supplying directly to Intek and have higher number of high transportation risk relationships with other customers.

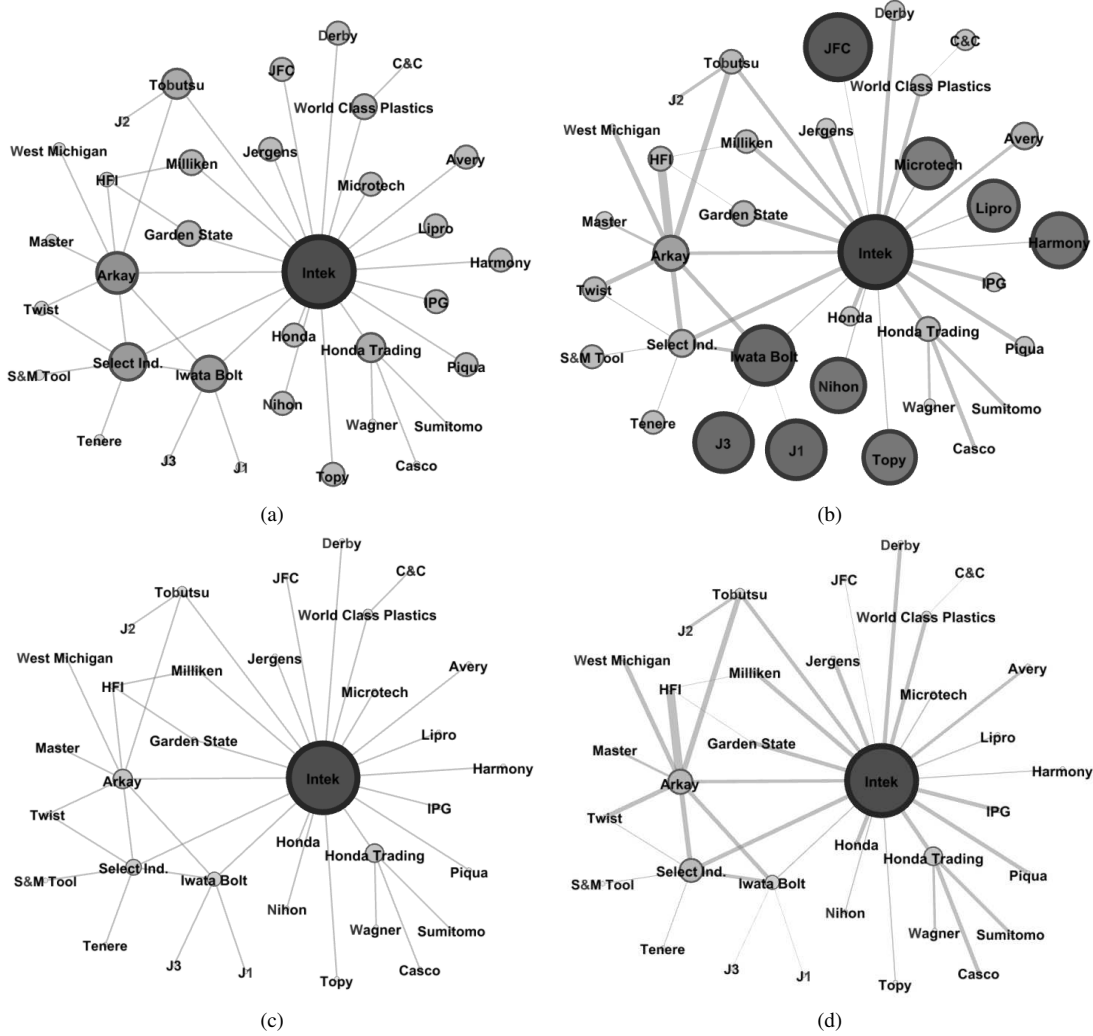


Fig. 2. Network visualisations: a) unweighted closeness, b) link-weighted closeness, c) unweighted betweenness centrality, d) link-weighted betweenness centrality. Each node and link are sized and shaded according to the respective centrality value or link weight. The darker and bigger node/link, the higher value.

The companies with the highest authority are the ones having the highest number of high transportation risk supplier links.

Unweighted hub identifies companies mainly according to their out-degree: the higher number of customers, the higher risk. Weighted hub centrality assigns the highest risk to companies having high out-degree and having high risk relationships with their customers. Tobutsu and Select Ind. are important for product assembly with many high risks supplier relationships, but their criticality for Honda operations is not highlighted enough by the unweighted hub centrality. Weighted and unweighted authority result in the same companies identified as the ones having high risk. This is because in order to be an authority a node cannot have zero in-degree. There are only few nodes that fulfil this condition, thus there are not many nodes that can have high authority. For network visualisations please see Figures 1c, 1e, 1d and 1f.

Hub and authority centralities can be used for assessing the systemic risk in the supply network. The authorities are vulnerable to disruptions from supplier side, hubs are vulnerable to disruptions from customer side.

E. Closeness for assessing the speed of disruption across a network

We use closeness to calculate the speed of failure spread across the network. The assumption that it is a good measure for speed of risk spread is based on the fact that it measures the topological proximity of a node to the rest of the network. The closer the node to the rest of the network, the higher the probability that it will affect the network quicker. Topological proximity is of course a single factor in the spread of risk. For example, delivery frequencies, lead times between suppliers, and the volume of delivery would all have mediating affects on topological proximity. Since operational variables frequently change, and are often invisible to extended members of the network, topological proximity to the source of a disruption could serve as a preliminary indicator of how soon a company could be impacted. Metric is used for undirected material flow network of Honda Acura. Two different cases are applied: unweighted and weighted with the distance as a link weight. Table VII presents the results for both cases. In order to find the most vulnerable companies in the network, we look at the highest closeness.

TABLE VII
CLOSENESS CENTRALITY FOR UNDIRECTED MATERIAL FLOW NETWORK
OF HONDA ACURA

| Unweighted | | Link-weighted | |
|---------------|-----------|---------------|-----------|
| Company | Closeness | Company | Closeness |
| Intek | 1.0000 | Intek | 1.0000 |
| Arkay | 0.7419 | JFC | 0.9433 |
| Select Ind. | 0.7077 | Iwata Bolt | 0.8747 |
| Iwata Bolt | 0.6970 | J1 | 0.8747 |
| Tobutsu | 0.6479 | J3 | 0.8747 |
| Honda Trading | 0.6389 | Harmony | 0.8312 |

Intek, Arkay, Select Ind., Iwata Bolt, Tobutsu, and Honda Trading have the highest unweighted closeness. These companies are located at the heart of Honda Acura operations and are the most involved in the product assembly.

In the link-weighted case, the highest centralities have the following companies: Intek, JFC, Iwata Bolt, J1, J3 and Harmony. Other companies with high score, but not included in the tables are Nihon, Lipro, Topy and Microtech. This is because all the companies mentioned are located in Asia with Intek being the main assembler. The close localization means that if a disruption happens in any of these companies, its effect might be transferred quicker through Intek to the rest of the supply network. For network visualisations of unweighted and weighted closeness centralities please see Figure 2a and 2b.

JFC, J1, J3 and Harmony are not identified as critical by the traditional unweighted closeness, because the proximity of those companies to Intek is not considered in unweighted case. This means that incorporating distance related information enables to identify high risk clusters of nodes close to each other.

F. Betweenness centrality for the identification of high risk intermediaries

We use betweenness centrality for the identification of high transportation risk intermediaries. We apply the centrality measure to undirected material flow network for Honda Acura. There are two cases: unweighted and weighted. We set the inverse of the distance as the link weight and we assume that the higher the distance, the higher probability of something going wrong during transportation. The inverse is used because betweenness centrality is based on the idea of counting how many times the node lies on the shortest path between all the other nodes. Since we are interested in the nodes lying on the high risk paths, we inverse the risk, because the shortest path with inversed risk is equivalent to the highest risk path. Results for betweenness centrality are presented in the Table VIII and Figures 2c and 2d.

The companies with the highest betweenness centrality for unweighted and weighted cases are Intek and Arkay. This is because they are located at the heart of this supply network operations, managing multiple relationships. Select Ind. has higher centrality in the weighted case, because it is managing more business relationships with high risk than the other nodes identified as critical. Originally there are few nodes having non-zero betweenness not included in the Table VIII as Garden

TABLE VIII
BETWEENNESS CENTRALITY FOR IDENTIFICATION OF HIGH RISK
LOCATIONS

| Unweighted | | Link-weighted | |
|---------------|----------|---------------|----------|
| Company | C_{BT} | Company | C_{BT} |
| Intek | 0.8387 | Intek | 0.8390 |
| Arkay | 0.1869 | Arkay | 0.2538 |
| Honda Trading | 0.1761 | Select Ind. | 0.2386 |
| Select Ind. | 0.1414 | Honda Trading | 0.1761 |
| Iwata Bolt | 0.1193 | Iwata Bolt | 0.1193 |
| Tobutsu, WPC | 0.0606 | Tobutsu, WPC | 0.0606 |

State, HFI and Miliken. Their betweenness reduces to zero for weighted network, on the account of Select Ind. World Class Plastics gets high betweenness, but does not score high in experiments performed with other centrality metrics. It is because it has low degree and is located relatively far way on the average from the other nodes in the network. Still it is topologically important firm, as it plays an important role for C&C as a material delivery proxy.

Betweenness centrality applied with the transportation risk indicators can be used to identify nodes that lie on the highest transportation risk paths. These nodes are critical for the supply chain operations, because they often behave as a proxy, enabling communication and goods transportation between two ends of the supply network. Incorporating supply chain domain information enables to highlight the most critical firms amongst the intermediaries, although in the Honda Acura case did not bring many additional insights.

V. CONCLUSIONS AND FUTURE WORK

Alternative supply chain risk management frameworks are gaining attention in the post-financial crisis era. Cost reduction strategies such as outsourcing, offshoring, inventory minimization and supply base can result in increased risk exposure [18], [26]. Companies extend their supply chain boundaries globally, often leading to a lack of understanding on how risk is compounded at the system level. While cost reduction strategies will continue to prevail, new methods for assessing and planning for compounded risk need to be developed. Those methods should have in mind the invisibility of operational variables for the extended members of the network. In this paper we contribute to the extant literature by arguing that the new science of networks makes this possible. Our contributions are as follows:

- We interpret centrality metrics in the supply chain risk context, building on the literature from the other fields. Eigenvector centrality, hub and authority centrality, closeness centrality, radiality and betweenness centrality can be used for supply chain systemic risk assessment to evaluate how local risk of either the relationship or the business partner can spread across the network. Amongst those metrics we have chosen the ones that lead to complimentary considerations of risk:
 - Katz centrality can be used to calculate systemic risk for a site taking into account the local risks of neighboring business partners.

- Hub centrality can be used to identify the sites that have high-risk customer relationships.
- Authority centrality can be used to identify sites that have high-risk supply relationships.
- Weighted closeness can be used to identify the companies that if disrupted will make the cascading failure to progress the quickest.
- Weighted betweenness centrality can be used to identify the highest risk companies amongst intermediaries.
- We devised methods to analytically incorporate risk exposure into the centrality metrics, showing that additional information enhances assessment of systemic risk in supply chains and in doing so, it delivers helpful decision support. As an example of risk exposure information that can be added this way, we have chosen geographical risk indicators to identify clusters of companies that operate in areas with high geo-political or transportation risk. The insights can help risk practitioners in supply chain design and choice of their supply base.
- We compare centrality measures with and without their risk exposure embedded versions and concluded that incorporating additional information can enhance risk assessment. Although centrality measures are common in the literature, their risk embedded versions are absent to the best of authors knowledge. Pure metrics consider only number of business partners, e.g. authority centrality identifies sites with high number of suppliers, which have high number of suppliers themselves etc. But this information might not bring many insights about actual risk. We might have 20 suppliers, but if all of them are stable local suppliers, our risk will be smaller than if we had 5 very high risk and unstable ones. Incorporating risk exposure in the supply network helps to see additional information beyond topology only and is a useful tool for decision support where access to operational data is limited.

In using the above metrics for systemic risk assessment, the risk practitioner needs to define weights on nodes and links, where link weights can refer to risk related to the relationship between firms, and node weights can refer to the local risk of the company. In this study we have used geo-political risk and transportation risk as examples, but other risk exposures can be used by risk practitioner e.g. quality issues, reputation risks etc.

Future avenues for research include increased granularity and heterogeneity on node and link risk, through the compounding of different risk factors such as machine breakdowns, hazards, combined time delays, and production defects. Further analysis need to be made on increased network size and the applicability of different risk planning strategies in light of different vulnerabilities.

REFERENCES

- [1] B. La Londe and J. Masters, "Emerging logistics strategies: Blueprints for the next century", *Int. J. Phys. Distrib. Logist. Manag.*, vol. 24, no. 7, pp. 35, 1994.
- [2] T. Y. Choi, K. J. Dooley, and M. Rungtusanatham, "Supply networks and complex adaptive systems: control versus emergence", *J. Oper. Manag.*, vol. 19, no. 3, pp. 351-366, Sep. 2001.
- [3] P. R. Kleindorfer and G. H. Saad, "Managing disruption risks in supply chains", *Prod. Oper. Manag.*, vol. 14, no. 1, pp. 53-68, 2005.
- [4] A. Adhitya, R. Srinivasan, and I. A. Karimi, "Supply chain risk identification using a HAZOP-based approach", *AIChE J.*, vol. 55, no. 6, pp. 1447-1463, Jun. 2009.
- [5] G. Arzu Akyuz and T. Erman Erkan, "Supply chain performance measurement: a literature review", *Int. J. Prod. Res.*, vol. 48, no. 17, pp. 5137-5155, Sep. 2010.
- [6] S. Chopra and P. Meindl, "Supply chain management: strategy, planning and operation", Upper Saddle River, NJ: Pearson, 2010.
- [7] D. Diehl and S. Spinler, "Defining a common ground for supply chain risk management - a case study in the fast-moving consumer goods industry", *Int. J. Logist. Res. Appl.*, vol. 16, no. 4, pp. 311-327, Aug. 2013.
- [8] K. Mizgier, M. Jüttner, and S. Wagner, "Bottleneck identification in supply chain networks", *Int. J. Prod. Res.*, vol. 51, no. 5, pp. 1477-1490, 2013.
- [9] J. V. Vlajic, S. W. M. van Lokven, R. Haijema, and J. G. A. J. van der Vorst, "Using vulnerability performance indicators to attain food supply chain robustness", *Prod. Plan. Control*, vol. 24, no. 8-9, pp. 785-799, Sep. 2013.
- [10] M. Goh, J. Y. S. Lim, and F. Meng, "A stochastic model for risk management in global supply chain networks", *Eur. J. Oper. Res.*, vol. 182, pp. 164-173, 2007.
- [11] K. E. Steckel and S. Kumar, "Sources of supply chain disruptions, factors that breed vulnerability, and mitigating strategies", *J. Mark. Channels*, vol. 16, no. 3, pp. 193-226, Jun. 2009.
- [12] A. Ghadge, S. Dani, M. Chester and R. Kalowsky, "A systems approach for modelling supply chain risks", *Supply Chain Management: An International Journal*, vol. 18, no. 5, pp. 523-538, 2013.
- [13] T. J. Pettit, K. L. Croxson and J. Fiksel, "Ensuring supply chain resilience: development and implementation of an assessment tool", *Journal of Business Logistics*, vol. 34, no. 1, pp. 46-76, 2013.
- [14] T. Y. Choi and Y. Hong, "Unveiling the structure of supply networks: case studies in Honda, Acura and DaimlerChrysler", *J. Oper. Manag.*, vol. 20, pp. 469-493, 2002.
- [15] C. N. Bezuidenhout, S. Bodhanya, T. Sanjika, M. Sibomana, and G. L. N. Boote, "Network-analysis approaches to deal with causal complexity in a supply network", *Int. J. Prod. Res.*, vol. 50, no. 7, pp. 1840-1849, Apr. 2012.
- [16] T. Y. Choi and Z. Wu, "Taking the leap from dyads to triads: Buyer-supplier relationships in supply networks", *J. Purch. Supply Manag.*, vol. 15, no. 4, pp. 263-266, Dec. 2009.
- [17] R. Gaonkar and N. Viswanadham, "A conceptual and analytical framework for the management of risk in supply chains", in *International Conference on Robotics & Automation*, pp. 2699-2704, 2004.
- [18] C. Harland, R. Brenchley, and H. Walker, "Risk in supply networks", *Journal of Purchasing & Supply Management*, vol. 9, pp. 51-62, 2003.
- [19] S. M. Wagner and C. Bode, "An empirical investigation into supply chain vulnerability", *J. Purch. Supply Manag.*, vol. 12, no. 6, pp. 301-312, Nov. 2006.
- [20] J. Vilko, A. Rumpu, and J. Koivuniemi, "Risk management in supply chains: Information exchange, systemic motives and cognitive barriers", *Technology Management in the Energy Smart World (PICMET)*, 2011 Proceedings of PICMET '11: Portland, OR, 2011.
- [21] R. C. Basole and M. A. Bellamy, "Supply network structure, visibility, and risk diffusion: A computational approach", *Decis. Sci.*, vol. 45, no. 4, pp. 753-789, Aug. 2014.
- [22] A. Jeyaraj and V. Sethi, "Implementation of information systems infrastructures for supply chain visibility in organizations", *Journal of Information Science and Technology*, vol. 9, no. 1, pp. 3-23, 2013.
- [23] A. Brintrup, Y. Wang, and A. Tiwari, "Supply networks as complex systems: A network-science-based characterization", *IEEE Systems Journal*, 2015, In Press.
- [24] T. Kito, A. Brintrup, S. New, F. Reed-Tsochas, "The structure of the Toyota supply network: An empirical analysis", Saïd Business School WP, available at SSRN: <http://ssrn.com/abstract=2412512>, Mar. 2014.
- [25] S. New, "Supply chains: construction and legitimation", *Understanding Supply Chains: Concepts, Critiques & Futures*, pp. 69-108, 2004.
- [26] U. Jüttner, H. Peck, and M. Christopher, "Supply chain risk management: Outlining an agenda for future research", *Int. J. Logist. Res. Appl.*, vol. 6, no. 4, pp. 197-210, 2003.
- [27] S. M. Wagner and N. Neshat, "A comparison of supply chain vulnerability indices for different categories of firms", *Int. J. Prod. Res.*, vol. 50, no. 11, pp. 2877-2891, Jun. 2012.
- [28] M. Christopher and H. Peck, "Building the resilient supply chain", *Int. J. Logist. Manag.*, vol. 15, no. 2, pp. 1-14, 2004.

- [29] J. G. March and Z. Saphira, "Managerial perspectives on risk and risk taking", *Management Science*, vol. 33, pp. 1404-1418, 1987.
- [30] T. J. Pettit, J. Fiksel, and K. L. Croxton, "Ensuring supply chain resilience: development of a conceptual framework", *J. Bus. Logist.*, vol. 31, no. 1, pp. 1-22, 2010.
- [31] K. Scholten, P. S. Scott, and B. Fynes, "Mitigation processes –antecedents for building supply chain resilience", *Supply Chain Manag. An Int. J.*, vol. 19, no. 2, pp. 211-228, 2014.
- [32] C. Roncoli, C. Bersani, and R. Sacile, "A risk-based system of systems approach to control the transport flows of dangerous goods by road", *IEEE Syst. J.*, vol. 7, no. 4, pp. 561-570, Dec. 2013.
- [33] R. Raj, J. W. Wang, A. Nayak, M. K. Tiwari, B. Han, C. L. Liu, and W. J. Zhang, "Measuring the resilience of supply chain systems using a survival model", *IEEE Syst. J.*, vol. 9, no. 2, pp. 377-381, Jun. 2015.
- [34] K. Zhao, A. Kumar, T. P. Harrison, and J. Yen, "Analyzing the resilience of complex supply network topologies against random and targeted disruptions", *IEEE Syst. J.*, vol. 5, no. 1, pp. 28-39, Mar. 2011.
- [35] D. Helbing, "Globally networked risks and how to respond", *Nature*, vol. 497, pp. 51-59, May 2013.
- [36] M. Christopher, "Managing supply chain complexity: Identifying the requisite skills", *Supply Chain Forum: An International Journal*, vol. 13, no. 2, pp. 4-9, 2012.
- [37] H. Carvalho, A. P. Barroso, V. H. Machado, S. Azevedo, and V. Cruz-Machado, "Supply chain redesign for resilience using simulation", *Comput. Ind. Eng.*, vol. 62, no. 1, pp. 329-341, Feb. 2012.
- [38] G. Tuncel and G. Alpan, "Risk assessment and management for supply chain networks: A case study", *Comput. Ind.*, vol. 61, no. 3, pp. 250-259, Apr. 2010.
- [39] A. Banerjee, "A simple model of herd behavior", *Quarterly Journal of Economics*, vol. 107, pp. 797-817, 1992.
- [40] D. Easley and J. Kleinberg, "Networks, crowds and markets: Reasoning about a highly connected world", *Cambridge University Press*, New York, 2010.
- [41] J. S. Coleman, H. Menzel, and E. Katz, "Medical innovations: A diffusion study", *Bobs Merrill*, 1996.
- [42] Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, Dec. 2014.
- [43] L. Tang, K. Jing, J. He, and H. E. Stanley, "Complex interdependent supply chain networks: Cascading failure and robustness", *Physica A*, vol. 443, pp. 58-69, Feb. 2016.
- [44] Y. Zeng and R. Xiao, "Modelling of cluster supply network with cascading failure spread and its vulnerability analysis", *International Journal of Production Research*, vol. 52, no. 23, pp. 6938-6953, 2014.
- [45] Z. Zhao, P. Zhang, and H. Yang, "Cascading failures in interconnected networks with dynamical redistribution of loads", *Physica A*, vol. 433, pp. 204-210, 2015.
- [46] D. J. Watts, "A simple model of global cascades on random networks", *Proceedings of the National Academy of Sciences*, vol. 99, no. 9, pp. 5766-5771, Apr. 2002.
- [47] J. Lorenz, S. Battiston, and F. Schweitzer, "Systemic risk in a unifying framework for cascading processes on networks", *European Physical Journal B*, vol. 71, no. 4, pp. 441-460, 2009.
- [48] M. E. J. Newman, "Networks: An introduction", *Oxford University Press*, 2010.
- [49] P. Gai and S. Kapadia, "Contagion in financial networks", *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, vol. 466, no. 2120, pp. 2401-2423, 2010.
- [50] S. Battiston, D. Delli Gatti, M. Gallegati, B. Greenwald, and J. E. Stiglitz, "Credit chains and bankruptcy propagation in production networks", *Journal of Economic Dynamics and Control*, vol. 31, no. 6, pp. 2061-2084, 2007.
- [51] M. G. Hertz, Z. Li, M. S. Officer, and K. J. Rodgers, "Inter-firm linkages and the wealth effects of financial distress along the supply chain", *Journal of Financial Economics*, vol. 87, no. 2, pp. 374-387, 2008.
- [52] T. N. Dinh and M. T. Thai, "On approximation of new optimization methods for assessing network vulnerability", *Proceedings in IEEE Infocom*, Jan. 2010.
- [53] M. Jorgic, I. Stojemnovic, M. Hauspie, and D. Simplot-Ryl, "Localized algorithms for detection of critical nodes and links for connectivity in ad hoc networks", *Mediterranean Ad Hoc Networking Workshop*, Turkey, 2004.
- [54] H. P. Thadakamalla, U. N. Raghavan, S. Kumara, and R. Albert, "Survivability of multiagent-based supply networks: A topological perspective", *Intell. Syst.*, vol. 19, no. 5, pp. 24-31, Sep. 2004.
- [55] G. J. Correa and Y. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models", *Electric Power Systems Research*, vol. 11, pp. 71-79, 2013.
- [56] G. J. Correa-Henao and J. M. Yusta-Loyo, "Representation of electric power systems by complex networks with applications to risk vulnerability assessment", *DYNA*, vol. 82, no. 192, pp. 68-77, Aug. 2015.
- [57] R. A. El-Rashidy and S. M. Grant-Muller, "An assessment method for highway network vulnerability", *Journal of Transport Geography*, vol. 34, pp. 34-43, 2014.
- [58] F. G. Laxe, M. J. F. Seoane, and C. P. Montes, "Maritime degree, centrality and vulnerability: port hierarchies and emerging areas in containerized transport (2008-2010)", *Journal of Transport Geography*, vol. 24, pp. 33-44, 2012.
- [59] X. Tang, "Vulnerability evaluation on multimedia subsystem based on complex network", *Journal of Multimedia*, vol. 8, no. 4, Aug. 2013.
- [60] G. L. L. Reniers, K. Sørensen, and W. Dullaert, "A multi-attribute systemic risk index for comparing and prioritizing chemical industrial areas", *Reliability Engineering and System Safety*, vol. 98, no. 1, pp. 35-42, 2012.
- [61] C. Lozares, P. Lopez-Roldan, M. Bolibar, and D. Muntanyola, "The structure of global centrality measures", *International Journal of Socioal Research Methodology*, vol. 18, no. 2, pp. 209-226, 2015.
- [62] S. P. Borgatti and M. G. Everett, "A Graph-theoretic perspective on centrality", *Social Networks*, vol. 28, no. 4, pp. 466-484, 2006.
- [63] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical centrality measures for electric power grid vulnerability analysis", *49th IEEE Conference on Decision and Control*, pp. 5792-5797, Dec. 2010.
- [64] D. Hu, J. L. Zhao, and Z. Hua, "Network-based modelling and analysis of systemic risk in banking systems", *MIS Quarterly*, vol. 36, no. 4, pp. 1269-1291, Dec. 2012.
- [65] H. Chen, J. D. Cummins, K. S. Viswanathan, and M. A. Weiss, "Systemic risk and the interconnectedness between banks and insurers: An econometric analysis", *The Journal of Risk and Insurance*, vol. 81, no. 3, pp. 623-652, 2013.
- [66] X. Zhang, B. Podobnik, D. Y. Kenett, and H. E. Stanley, "Systemic risk and causality dynamics of the world international shipping market", *Physica A*, vol. 415, pp. 43-53, 2014.
- [67] M. Dong, "Development of supply chain network robustness index", *Int. J. Services Operations and Informatics*, vol. 1, no. 1-2, pp. 54-66, 2006.
- [68] R. C. Basole and M. A. Bellamy, "Visual analysis of supply network risks: Insights from the electronics industry", *Decis. Support Syst.*, vol. 67, pp. 109-120, Nov. 2014.
- [69] S. Rana and N. E. Allen, "Centrality measures to identify key stakeholders in family violence councils", *Psychosocial Intervention*, vol. 24, pp. 167-176, 2015.
- [70] D. C. Bell, J. S. Atkinson, and J. W. Carlson, "Centrality measures for disease transmission networks", *Social Networks*, vol. 21, pp. 1-21, 1999.
- [71] S. S. Chopra and V. Khanna, "Understanding resilience in industrial symbiosis networks: Insights from network analysis", *Journal of Environmental Management*, vol. 141, pp. 86-94, 2014.
- [72] T. U. Kuzubas, I. Omercikoglu, and B. Saltoglu, "Network centrality measures and systemic risk: An application to the Turkish financial crisis", *Physica A*, vol. 405, pp. 203-215, 2014.
- [73] Y. Kim, T. Y. Choi, T. Yan, and K. Dooley, "Structural investigation of supply networks: A social network analysis approach", *Journal of Operations Management*, vol. 29, no. 3, pp. 194-211, Mar. 2011.
- [74] Q. Niu, A. Zeng, Y. Fan, and Z. Di, "Robustness of centrality measures against network manipulation", *Physica A*, vol. 438, pp. 124-131, 2015.
- [75] P. Bonacich, "Factoring and weighting approaches to status scores and clique identification", *Journal of Mathematical Sociology*, vol. 2, no. 1, pp. 113-120, 1972.
- [76] G. Lohmann, D. S. Margulies, A. Horstmann, B. Pleger, and J. Lepsien, et al., "Eigenvector centrality mapping for analyzing connectivity patterns in fMRI data of the human brain", *PLoS ONE*, vol. 5, no. 4, e10232-e10232, 2010.
- [77] J. M. Kleinberg, "Authoritative sources in a hyperlinked environment", *Journal of the ACM*, vol. 46, no. 5, pp. 604-632, 1999.
- [78] L. Carlos, "Authority centrality and hub centrality as metrics of systemic importance of financial market infrastructures", Available at SSRN: <http://ssrn.com/abstract=2290271>, Jul. 2013.
- [79] A. Bavelas, "Communication patterns in task-oriented groups", *The Journal of the Acoustical Society of America*, vol. 22, no. 6, 1950.
- [80] E. Otte and R. Rousseau, "Social network analysis: a powerful strategy, also for the information sciences", *Journal of Information Science*, vol. 28, no. 6, pp. 441-453, 2002.
- [81] S. P. Borgatti, C. Jones, and M. G. Everett, "Network measures of social capital", *Connections*, vol. 21, no. 2, pp. 27-36, 1998.

- [82] Nguyen, D. T and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment", *IEEE Transactions on Smart Grid*, vol. 4, no. 1, Mar. 2013.
- [83] T. W. Valente and R. K. Foreman, "Integration and radiality: measuring the extent of an individual's connectedness and reachability in a network", *Social Networks*, vol. 20, no. 1, pp. 89-105, 1998.
- [84] L. C. Freeman, "A set of measures of centrality based on betweenness", *Sociometry*, vol. 40, no. 1, pp. 35-41, 1977.
- [85] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach", *Electric Power Systems Research*, vol. 81, pp. 1334-1340, 2011.
- [86] L. Katz, "A new status index derived from sociometric analysis", *Psychometrika*, vol. 18, no. 1, pp. 39-43, 1953.
- [87] J. Butenop, T. Kistemann, M. Marx, P. Muehe, K. Rastke, et al., "WorldRiskIndex 2013", *World Risk Report 2013*, pp. 45-56, 2013.



Professor Ashutosh Tiwari is the Head of the Manufacturing Informatics Centre at Cranfield University (UK). His research focuses on the digitisation, simulation and optimisation of high-value manufacturing processes, such as wing manufacture and engine assembly. He is a fellow of the IMechE, the IET and the HEA, and a member of the EPSRC Peer Review College. He has produced 236 research publications including 93 refereed journal papers, 103 refereed conference papers, and 40 book chapters and research reports. He was awarded the IMechE Prize 2008/09 for the best journal paper in manufacturing. He has successfully supervised 24 PhD/EngD theses and 73 MSc theses, and secured over 10M of research funding from government grants and industry



Anna Ledwoch received the double M.Sc. degree in computer science from Cranfield University (UK) and Silesian University of Technology (Gliwice, Poland). Currently, she is pursuing the Ph.D. degree in the School of Aerospace, Transport and Manufacturing at Cranfield University. Her current research interests include complex networks, complex adaptive systems, multiagent systems and supply chain risk.



Dr. Alexandra Brintrup is lecturer in Digital Manufacturing at the University of Cambridge. Alexandra is interested in the modelling, analysis, and control of dynamical and functional properties of emergent manufacturing networks. She develops intelligent systems to help organizations navigate through complexity. Her broader work in this area includes system development for digitised product lifecycle management. She uses Artificial Intelligence paradigms, particularly for data analytics and automated decision making. Alexandra obtained her

PhD from Cranfield University, and held postdoctoral and fellowship appointments with the University of Cambridge and the University of Oxford. She teaches Operations Management and Decision Engineering.



Dr. Jörn Mehnen is Reader in Computational Manufacturing at Cranfield University (UK). His research focuses on application of computer science technologies in industry. Dr Mehnen holds the positions of Deputy Director of the Degradation Studies Laboratory and IoT Laboratory in the Through Life-Engineering Services Centre at Cranfield University. Dr Mehnen was awarded a prestigious EPSRC High Value Manufacturing Catapult Fellowship which concerns the practical application of IoT devices in manufacturing environments. He is working on various

national and EU sponsored projects concerning IoT, Big Data Analytics and Visualisation and Through-Life Engineering. With more than 100 journal, book and conference papers he has published extensively both in the field of computer science as well as manufacturing.