Logist. Res. (2016)9:1
DOI 10.1007/s12159-015-0128-1

ORIGINAL PAPER

Topological robustness of the global automotive industry

Alexandra Brintrup[1,2] · Anna Ledwoch[1,2] · Jose Barros[1,2]

Received: 28 May 2015 / Accepted: 7 December 2015

Abstract The manufacturing industry is characterized by large-scale interdependent networks as companies buy goods from one another, but do not control or design the overall flow of materials. The result is a complex emergent structure with which companies connect to each other. The topology of this structure impacts the industry's robustness to disruptions in companies, countries, and regions. In this work, we propose an analysis framework for examining robustness in the manufacturing industry and validate it using an empirical dataset. Focusing on two key angles, suppliers and products, we highlight macroscopic and microscopic characteristics of the network and shed light on vulnerabilities of the system. It is shown that large-scale data on structural interdependencies can be examined with measures based on network science.

Keywords Complex network · Supply · Manufacturing · Robustness

1 Introduction and background

A supply network is created when companies buy and sell goods to each other, transferring necessary parts downstream to create a final product. Often, companies do not have visibility beyond their immediate buyers and suppliers, which results that these networks are not designed but emerge [10]. These networks can become large scale, with many thousands of companies becoming interdependent without their knowledge of being so. Due to these interdependencies, disruptions in the network can cascade, and the implications can be catastrophic. For example, the March 2011 Tohoku earthquake caused the Japanese auto industry to temporarily shut down, forcing European and North American manufacturers to halt production as their inventories from Japan were exhausted. Goldman Sachs estimated that the shutdowns cost Japanese automakers 200 million USD a day [17]. Daily global automotive production dropped by one-third, resulting in an overall loss of 5 million vehicles worldwide, out of the 72 million planned for 2011 ($\sim$7 % loss). Both in terms of risk management for the entire network, and from the perspective of individual firms planning and coordinating with different suppliers, a better understanding of interdependencies would help create better strategies for robustness.

The field of supply chain planning has a long history of creating sophisticated operational models that describe the flow of materials between organizations. While these models capture low-level dynamics with accuracy, they increasingly lose accuracy and become hard to construct as system size grows. Typical simulation and analytical models include detailed state variables of each individual production step such as inventory levels, bills of materials, throughput, and lead times for production. In the context of robustness to failures, several inventory and optimization

This article is part of a focus collection on "Robust Manufacturing Control: Robustness and Resilience in Global Manufacturing Networks".

✉ Alexandra Brintrup
alexandra.brintrup@gmail.com; ab702@cam.ac.uk

[1] Manufacturing and Materials, Cranfield University, Cranfield, Bedfordshire MK43 0AL, UK

[2] Institute for Manufacturing, University of Cambridge, Cambridge CB3 0FS, UK

Published online: 28 December 2015

models have been proposed [9, 26, 28]. However, these models cannot be extended to include the whole system because state variables are often not available because of a lack of visibility and unwillingness of suppliers to share data. Furthermore, these models are not practical for implementation at large scales due to computational limitations and the frequency with which state variables change. Several researchers have stressed the need for alternative methods to analyse system robustness that can complement low-level dynamical analysis (an excellent review can be found by Snyder et al. [24]). This inevitably means letting go of local detail, and focusing on statistical properties of the system.

In this respect, the last decade has seen the emergence of a substantial body of techniques under the broad heading of "network science" ([27], [21]), which provides tools for understanding the characteristics of large-scale networks and complex systems. Network science abstracts systems as a set of nodes and links, the former representing agents (such as companies), and the latter interactions among them (such as buy and sell relationships). In doing so, it reveals structure and infers the governing rules of the system. This development meant that supply networks could now be analysed as a whole system rather than isolated parts.

Choi et al. [10] pioneered the application of these ideas to supply networks (see also [5, 8, 14]). Empirical studies include Kim et al. [16] efforts to map part of the Honda, Acura, and Daimler Chrysler, which consisted of 70 members; Lomi and Pattison [18] analysis of 106 automotive firms in southern Italy; and Keqiang et al. [15] examination of the Guangzhou automotive industry, Saveedra et al. [23] study on the New York Garment Industry, and Brintrup et al. [7] study on Airbus. These studies examined network structure and proved that supply networks are complex systems and that their robustness properties would be affected by structure, but did not find empirical consensus on universal properties ([12], Brintrup et al. [7]).

The above studies on large-scale supply networks force us to revisit long assumed models of isolated parts and think about the bigger system picture when robustness is examined. In this respect, Thadakamaila et al. [25] used the preferential attachment model to generate a scale-free network, from which they interpreted robustness properties. Nair and Vidal [19] examined robustness against disruptions under random, small-world, and scale-free network topologies using multi-agent simulation. Zeng and Xiao [29] proposed network load entropy as a measure to detect spreading dynamics of cluster supply chain networks under cascading failures. Basole and Bellamy [3] applied the classical SIR model from epidemiology for understanding risk diffusion in supply networks.

As previous researchers demonstrated, network science is a promising approach in modelling whole system robustness in supply networks. However, the extant literature ignored a crucial ingredient for modelling supply network robustness, which is their dualistic topology, containing (1) the structure with which suppliers connect to each other and (2) the structure with which production is distributed among suppliers. A supplier might be in a periphery position in the network, but its product list might contain products that are unique. Hence, network modelling based only on supplier connections would not capture this supplier as an important node, although disruptions in this supplier would halt the production of an assembly. For a supply network to be robust, not only the supplier connections should remain intact, but also all products needed for an assembly should subsist.

In this article, we close this gap by proposing a comprehensive framework for the analysis of robustness in supply networks. The framework borrows ideas from network science extending them within the supply network context for both static and dynamic assessment of robustness. Firstly, the dualistic supplier–product perspective is created. Then, a review of network disruption scenarios is collated and modelled. This is followed by the development of damage assessment measures, which help identify the impact of disruption scenarios. The framework is then tested using large-scale empirical data from the global automotive industry.

2 A framework for robustness assessment in supply networks

2.1 Two perspectives

The framework we propose includes two distinct modes of analysis: structural and simulation based. The structural analysis includes the examination of as-is topology, whereas the simulation-based analysis includes subjecting the topology to disruption scenarios and extracting statistical properties relating to possible failure types. Both structural and simulation-based analysis include examining two key perspectives of supply networks, which are intertwined, but their connection has been hitherto ignored in the literature.

2.1.1 Supplier network

As Kim et al. [16] point out, links in a supply network can be of various forms, including contractual relationships and material flow. It might be that companies have a contractual obligation to an assembler to deliver certain goods, but the physical goods come from another company. As our query is on the robustness of the network, links of actual goods delivery are of interest. If these companies fail, then the final assembly cannot be completed. One can also argue that if a contracted company is disrupted, this would affect the flow of goods just as much as the disruption at the physical goods producer, as it essentially acts as an intermediary to deliver goods downstream. In that case, the assembler needs to find the producer and procure directly. Another argument would be the consideration of the logistics network. More often than not, producers rely on external logistics and warehousing providers to deliver goods downstream. If disruptions occur in these intermediaries, the supply network would fail. The producers would need to find alternative modes of transportation and storage. For the sake of simplicity, in this paper we focus on the physical production network between companies and capture the most dramatic disruption mechanism—that of failures of producers. Hence, in this network nodes represent production companies, and directional links capture material flow relationships between them. Each node is assigned a vector of products that it offers. Topology of this network defines its robustness to company failures. Let us call this perspective a supplier network.

2.1.2 *Product network*

In a supply network, there are interdependencies between components that make sub-systems, which themselves make an assembly. An actual bill of materials map would be the most accurate representation in understanding how products traverse in the system and come together to make up the assembly. However, in large-scale supply networks, as companies entrust each other with sub-assemblies, they do not necessarily have visibility of the entire sub-system down to the component level. In the absence of such data, other forms of representation must be used to approximate interdependencies between products. We thus propose a representation where each product category that exists in the network is represented by a node. The more two products occur within the same supplier, the more likely these two products would be related and interdependent. Nodes are connected to one another if they coexist in a supplier's product portfolio. The total weight w on a link represents how many times the two products co-occur in the same portfolios. In other words, $w \geq 1$, where w is an integer. We shall use the term product as an all-encompassing term that includes sub-components and sub-systems (please see Table 4 for examples). Thus, this network perspective helps us understand potential relationships among product categories. Let us call this perspective a *product network.*

Clearly, for robustness in a supply network the two perspectives cannot be separated because each node produces one or more types of products and supplies them to other firms, eventually ending with the manufacturer, which assembles the products. For a supply network to remain functional, both the supplier and product network should be robust and contain redundancies at system level. In subsequent sections, both these perspectives are used for the assessment of robustness.

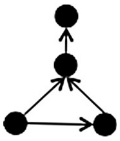
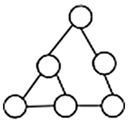
2.2 Structural analysis

The field of network science offers a toolset to analyse topology with respect to robustness, using a minimal set of parameters, in the form of nodes and links. In what follows, we use and explain some relevant measures reported in the literature and propose new ones to capture intricacies of supply networks (Table 1). In both supplier and product network perspectives, both the network (system) level and the node (company or product) level are analysed. The first present us with a macroscopic view of how the network is interconnected, pinpointing structural vulnerabilities. The second examines how key actors and their roles can be identified using centrality measures, which help understand suppliers that act as network connectors, integrators, and mediators. In the case of the product network, the network level helps understanding the interconnectivity and scarcity of products, while the node level helps identify products that are most frequently used for the assembly and bring together various different sub-systems.

2.2.1 *Supplier network metrics: in-, out-, total degree centralities and distributions*

These measures refer to the number and distribution of relationships across firms in the network. Since supply networks are directed networks, we can distinguish between in- and out-degree centralities, with the first being the number of suppliers a company has, and the latter being the number of clients a company has. Nodes with high in-degree centrality are integrators that assemble components that go into a final product and are integral to the architectural design of the product, whereas nodes with high out-degree centrality are concerned with distributing limited resources among several customers (Kim et al. [16]). High in-degree centrality relates to a firm's supply load, whereas high out-degree centrality relates to its demand load (Kim et al. [16]). The total degree is the number of clients and suppliers a node has. Distributions are plots showing the frequencies of these centralities across the network and are used to highlight variations. A homogeneous distribution would show that

Table 1 Metrics used for structural analysis of the supplier and product networks

	Supplier network	Product network
		
Node	Company	Product
Link	"Supplies to"	"Jointly supplied by"
Properties	Directional, unweighted	Bidirectional, weighted
Most relevant network-level metrics	In-, out-, total degree distribution Assortativity Modularity Average path length Clustering coefficient	Weighted degree distribution
Most relevant node-level metrics	In-, out-, total degree centrality Betweenness centrality Closeness centrality	Degree centrality Betweenness centrality Closeness centrality
Additional metrics proposed	Product degree distribution (network level) Product centrality (node level)	

most suppliers have similar numbers of relationships, affecting the overall connectivity in similar ways. A heterogeneous distribution would mean some suppliers affect connectivity more than others. Degree, in-degree and out-degree are defined as:

$$k_i = \sum_{j=1}^{n} A_{ij} \tag{1}$$

$$k_i^{\text{in}} = \sum_{j=1}^{n} A_{ij} \tag{2}$$

$$k_i^{\text{out}} = \sum_{i=1}^{n} A_{ij} \tag{3}$$

where A_{ij} corresponds to the element (ith and jth) of the adjacency matrix. The event, or probability of outcome, of degree k can be represented by:

$$p_k = \frac{n_k}{n} \tag{4}$$

where n_k is the number of nodes with degree k, and n is the number of all nodes in the network. The degree distribution can be analysed in a (k, p_k) plot.

2.2.2 *Average path length*

The average path length is the sum of lengths of shortest path between all nodes divided by the number of all pairs, defined as [21]:

$$l = \frac{1}{n^2} \sum_{ij} d_{ij} \tag{5}$$

where d_{ij} is the shortest path length between vertices i and j, and n is the number of nodes in the network. It can be associated with the distance the products and materials need to travel on average. Here a path refers to a geodesic path, meaning the number of nodes one must traverse to reach to a destination; and is not related to actual distance. The shorter the average path length, the more efficient the flow of materials will be (Kim et al. [16], [6]).

2.2.3 *Clustering coefficient*

This metric quantifies the extent to which two random nodes with links between them are also connected through common third parties and is defined as the ratio of the number of existing links between a given node's nearest neighbours and the maximum possible number of such links, averaged over all nodes in the network. Clustering coefficient is defined as:

$$C = \frac{1}{n} \frac{\left[k^2 - k\right]^2}{k^3} \tag{6}$$

where n is number of nodes in the network, and $\langle k^m \rangle$ is kth moment defined as:

$$\langle k^m \rangle = \sum_{k=0}^{\infty} k^m p_k \tag{7}$$

where k is the degree of the network and p_k is the degree distribution. From a robustness perspective, the higher the clustering coefficient, the more dependent suppliers are on each other for production.

2.2.4 Modularity

Network structure can be affected from geographical and industrial influences, forming into substructures called communities. Modularity essentially investigates the goodness of specific subgroup formations in a network. Biological and social networks have been shown to have high modularity [20]. Communities are important in understanding the dynamics of a network. For instance, in epidemiology the resistance of connections between communities determine the rate of transfer of diseases throughout the network of humans. Similarly, in a supply network, modularity can point to the extent where failures can be contained within communities. Modularity is defined as:

$$Q = \frac{1}{2m}\sum_{ij}\left(A_{ij} - \frac{k_i k_j}{2m}\right)\delta\left(c_i, c_j\right) \tag{8}$$

where m is the number of edges, A_{ij} is the element in the adjacency matrix in the ith row and jth column, k is the degree of the node, and $\delta(c_i,c_j)$ is the Kroneker delta, which is 1 if two nodes belong to the same community, 0 otherwise. Modularity has its maximum at $Q = 1$, where all nodes are separated into communities. If $Q = 0$, the whole network becomes a single community. We use the popular community detection method described by Girvan and Newman [13].

2.2.5 Assortativity

Social networks have been observed to show "assortative mixing", which means that high-degree nodes have a tendency to connect to other high-degree nodes. The concept is important as something that affects a single high-degree node could quickly cascade to other high-degree nodes. For example, in the field of epidemiology an assortative network means that diseases will spread faster than disassortative networks, whereas in the latter type of network targeting vaccinations to high-degree nodes, i.e. persons with a large social network, would be an effective strategy. To characterize assortativity, the behaviour of the average nearest neighbour's degree of the firms of degree k is studied:

$$k_{nn}(k) \equiv \sum_{k'} k' P(k'|k) \tag{9}$$

where $P(k'|k)$ is the conditional probability that a firm of degree k is connected to a firm of degree k'. Here k includes both suppliers and customers and thus considers all firms connected to the node in question. If k_{nn} increases with k, the network is assortative. If k_{nn} decreases with k, network is disassortative. Assortativity could point to several dynamics at play in a supply network. Firms with high numbers of links could be managing sub-communities in certain areas of production and then connect to other high-degree firms doing the same thing, creating subassemblies that they pass on downstream. Although efficient, the structure also would mean that disruptions at any one of the connector nodes could bring the whole network to a standstill quickly, as they will quickly cascade to other high-degree nodes.

2.2.6 Closeness centrality

This metric provides a measure of how close a firm is to other firms in the network by counting the total geodesic distance between a node and all other nodes in the network. This could be used as a proxy for the speed with which disruptions from a disrupted node can affect others. Closeness centrality is defined as:

$$C_i = \frac{n}{\sum_j d_{ij}} \tag{10}$$

where n is the number of nodes and d_{ij} is the length of the shortest path between vertices i and j.

2.2.7 Betweenness centrality

This metric measures how often a node will sit on the shortest paths that connect different nodes to each other in the network. Nodes with high betweenness centrality have been shown to control the flow of materials and communication in the network (Kim et al. [16]). Consequently, they can control the speed with which information and material can be disseminated in the network and act as bottlenecks during disruptions. Kim et al. [16] relate betweenness centrality to a firm's operational criticality. It is important to point out that betweenness centrality counts shortest paths, whereas all paths are in use in a supply network as firms work towards a bill of materials. A more refined measure should include all the paths; however, in this paper we base our discussions on the conventional definition of this measure so that comparisons with other empirical work can be made by researchers. Betweenness centrality is defined as:

$$x_i = \sum_{st} \frac{n^i_{st}}{g_{st}} \tag{11}$$

where n^i_{st} is 1 if vertex i lies on the shortest path between s and t, and g_{st} is the number of all shortest paths between s and t.

The following two metrics we propose complementing the supplier network by examining how products are connected to suppliers in the form of a bipartite network.

2.2.8 *Product centrality*

We propose that disruptions at companies with large numbers of product types would have a higher impact on the network than companies with small numbers of product types, and we propose to measure the number of product types that each company has. Here a product is used to refer to distinct product categories that make up an assembly, rather than inventories of products. Product categorization could be a rather subjective measure that reflects a scale instead of distinct types. For example, a distinction can be made between diesel and petrol engines, or between slightly different engine models. The level of differentiation between categories would need expert input and consideration of substitutions between categories. For example, product categories that can be substituted between each other can be bundled together to demonstrate redundancies in the network. Product centrality can be defined as:

$$\mathrm{pc}_i = \sum_j n_{ij} \tag{12}$$

where pc_i is the product centrality of vertex i, n_{ij} is 1 when company i has product j, 0 otherwise.

2.2.9 *Product degree distribution*

We propose this measure to capture the variations among suppliers' product portfolio sizes. A homogeneous distribution would show that most suppliers have similar numbers of products, affecting the overall assembly in similar way. A heterogeneous distribution would mean some suppliers affect the assembly more than others. Product degree distribution is defined as:

$$p_{\mathrm{pc}} = \frac{n_{\mathrm{pc}}}{n} \tag{13}$$

where n_{pc} is the number of companies with product centrality pc and n is the number of nodes in the network.

A summary of each metric and its relevance is given in Table 2.

Table 2 Description of metrics used for structural analysis

Metrics	Description
Supplier network	
In-, out-, total degree distribution	A homogeneous distribution shows most suppliers affect overall connectivity in similar ways. A heterogeneous distribution means some suppliers affect connectivity more than others
Assortativity	Assortative network means disruptions at any one of the connector nodes can halt production quickly, as they will quickly cascade to other high-degree nodes
Modularity	Modularity can point to the extent where failures can be contained within communities
Average path length	The shorter the average path length, the more efficient the flow of materials
Clustering coefficient	The higher the clustering coefficient, the more dependent suppliers are on each other for production
Total degree centrality	Integrators that assemble components
In-degree centrality	Supply load
Out-degree centrality	Demand load
Betweenness centrality	The speed with which information and material can be disseminated in the network and suppliers that act as bottlenecks during disruptions
Closeness centrality	Speed with which disruptions from a disrupted node can affect others
Product degree distribution (network level)	A homogeneous distribution shows most suppliers have similar numbers of products, affecting the overall assembly in similar way
Product centrality (node level)	Companies with large numbers of product types would have a higher impact on the network than companies with small numbers of product types
Product network	
Weighted degree distribution	Ubiquity of products. Highly ubiquitous products are least likely to disappear, but can cause a lot of disruptions, as many components including this product cannot be made
Degree centrality	Redundancy of a product in the network
Betweenness centrality	High betweenness centrality for a product highlights how commonly it is needed to bring sub-systems together
Closeness centrality	High closeness centrality relates to how soon product would be needed to create other products in the network, and how soon its lack would affect the making of the assembly

2.2.10 *Product network metrics: weighted degree distribution*

We propose to examine the likelihood of a product to be coupled with other products in a supplier's portfolio. A large weight represents a ubiquitous product, and although its lack would affect many suppliers, its ubiquity means there will be many instances of it across the network. While least likely to disappear, if a product with a large degree disappears, it can cause a lot of disruptions, as many components including this product cannot be made. Here the frequency of weights across the product network are plotted to highlight variations.

2.2.11 *Degree centrality*

Similar to the supplier network, here we measure the number of connections a node has. The connections refer to the number of companies co-producing that product. If a node has no connections, the product is made by only one supplier. If it has many connections, the product is made by multiple suppliers. The degree centrality therefore can be an indicator of the redundancy of the product in the network.

2.2.12 *Betweenness centrality*

In the context of the product network, this measure accounts for the number of times a product sits on shortest paths between products. As the paths represent interrelatedness in this network, the closer products are to each other, the more interrelated they will be. High betweenness centrality for a product can thus highlight how ubiquitously it is needed to bring sub-systems together.

2.2.13 *Closeness centrality*

In the context of the product network, this measure accounts for the distance a product is from other products. A high closeness centrality would relate to how soon this product would be needed to create various other products in the network, and how soon its lack would affect the making of the assembly.

2.3 Risk scenarios

Research has shown that supply networks face various types of risks whose frequency and impact severity differ widely [22]. Analysing the relationship between network structure and risk scenario should therefore involve linking risk scenarios into their structural impact and thus outlining how the impact can be simulated.

Table 3 shows a variety of risk scenarios gathered from the literature. Although this is not a comprehensive list, a variety of examples can be considered in this vein. For example, a natural catastrophe such as a volcano eruption would affect a region or a country. To simulate the effect of the eruption on the network, all companies that fall within

Table 3 Risk scenarios in the supplier network

Risk scenarios	Impact level	Simulation procedure	Damage assessment	Attack scenarios
Humanitarian crisis	Region/country	Remove all companies in the country or countries and associated product instances	LCC	Targeted single
Political violence			APL	
Geopolitical conflicts			AC	
Climate catastrophe			CFP	
Disease outbreak			CFC	
Natural/environmental catastrophe				
Financial issues	Group of companies	Remove all companies and associated product instances		Random single
Reputation damage				
Hazard on premises	Factory	Remove company location and associated product instances		Targeted
Financial issues	Company	Remove company and associated product instances		
Quality issues				
Reputation damage				
Machine breakdowns	Product instance	Remove product instance from the network	AC	Progressive
Quality issues				
Resource scarcity				
Resource scarcity	Product type	Remove all product instances associated with a product type from the network		Random progressive

the impacted region or country are removed from the network along with the products they supply. Financial issues such as bankruptcy can affect a group of companies that belong to the same corporation. These can be simulated by removing all companies that belong to the impacted corporation. Similarly, problems at a factory such as a fire hazard at a premise or at a company as a whole entity such as damaged reputation can be simulated by removing singular premises or companies.

An important difference needs to be made between product types and product instances. A product type is a category of products that needs to exist in the network for an assembly to be made. If a given product category no longer exists in the network, the assembly cannot be made, and hence, the production fails. A product instance, on the other hand, is a specific realization of a product category within a supplier's portfolio of products. The more instances of a product category there is in the network, the more robust the network would be. When a supplier is disrupted, the product instances that it holds in the network are no longer available. On the other hand, it is possible that a single product instance only is affected. For example, problems in a single production line such as the breakdown of a machine can mean that a certain product instance, say a gearbox from a supplier, is not available; however, the other products of the supplier are. It is also possible that a product category, capturing all gearboxes in the network, is no longer available, because a certain raw material necessary to make the product can no longer be sourced. In this scenario, all product categories that contain this raw material would cease to exist in the network.

To evaluate the impact of the different risk scenarios, we adopt a computational procedure which involves "stress testing" the network by assessing how the system would cope with failures, a summary of which is given in Table 3. The stress testing involves triggering a potential crisis by exogenously failing a node and investigates the spread of this failure within the system. Failing a node does not imply physical removal but that the node is dysfunctional in some way. To investigate maximum impact, we make sure the nodes that fail do not become functional, but remain dysfunctional throughout the simulation period.

Simulation can be undertaken in many ways. In the simplest case, a single attack is carried out at random. Depending on the risk scenario under consideration, this could be a company, a product instance, a whole product category, a whole country, or group of companies. This would help answer questions such as:

- Would my network function if there was a freeze event in northern Europe, disrupting all companies in this region?

Another option might be progressive removal. Here, the network is repeatedly attacked by random removal of nodes, until the network fails. This would help understand the failure threshold of the network and answer questions such as:

- How many companies need to be disrupted at random before my network ceases to function?

A popular alternative to random removal is targeted removal, during which a node or set of nodes are attacked according to some criterion. The criterion could include a ranking order with respect to a node's centrality. Again, under this attack type, removal can be progressive or targeted at a single node. Targeted progressive removal would put the network under the most pressure, as the network is attacked using intelligent choices. Research has shown that different network structures respond to attack types differently. In scale-free networks, the network remains connected in the face of random disruptions as these will most likely affect those firms that connect to large hubs. If, on the other hand, large hub firms are disrupted, the overall network will most likely suffer, given that they are integral to the functioning of the network (Barabási and Albert [2]).

2.4 Damage assessment

Following risk and attack scenarios, a procedure for detecting network failure needs to be established. There are several damage assessment measures that could be used to detect when a network fails. Of these, most used are *decrease of size of the largest connected component* (LCC) and *increase of the average path length* (APL) (Table 3).

A component is composed of nodes that are directly or indirectly connected to each other. The LCC contains the highest number of nodes that are connected to each other. The criterion of size decrease therefore investigates how fast a network becomes disconnected into isolated clusters, and there is no longer a guarantee that two random nodes will be connected through traversing intermediary nodes. This metric is useful in networks such as the Internet or social networks. In supply networks, the measure can be useful to understand the extent of the contracted, established network. However, unlike communication networks, the existence of disconnected clusters does not mean that companies cannot procure goods from them. Existing contracts allow companies to simply rewire their network to procure goods from elsewhere. The measure thus could be useful to identify when, on average, the network will need to be reorganized.

The second measure, APL, investigates how the average path, which must be traversed by products to reach to the assembler, increases in length, as nodes are deleted. If the network is disconnected, APL becomes infinitely long. This is a somewhat useful measure for supply networks, as the addition of each node on the average path will mean an additional contract and thus increased transaction cost and time for the procurement of products.

While informing to some extent, none of the above measures readily capture the intricacies of supply networks during robustness analysis. We thus introduce an additional damage assessment measure, called *assembly completeness* (AC) (Table 3), which is concerned with the product distribution on the network. To build a final assembly, in this case a car, all product categories that are necessary for the assembly to be built need to come together. Hence, there needs to be at least one instance of each product category that is necessary for the assembly in the network. This criterion therefore analyses how quickly the network loses the ability to build an assembly under sustained failure. Let us define assembly completeness γ_i as:

$$\gamma_i = \frac{p - p_i}{p}, \tag{14}$$

where p is the total number of product categories that are needed in the network; p_i is the number of product categories that supplier i produces.

LCC and APL could be examined during removal of nodes that represent companies or products, as these examine the connectance of the topology of the network, whereas AC is applicable throughout.

Another consideration we propose is *cascades of failures*. A cascading failure is a failure that can trigger the failure of successive parts in a given system. In ours, a supplier's failure can cause other suppliers to fail in delivery of their goods, cascading throughout the network. Two measures of cascading failure can be considered here: *cascading failures of companies* (CFC) and their *products* (CFP) (Table 3). CFC measures how many firms fail due to the disruption of a single company. CFC can be considered by a company's level of impact on the environment, from first degree of cascades, where the removed company affects its customers and suppliers, second degree, where neighbours of neighbours of removed company are considered, and so on. CPC takes the products portfolios of these companies into account, measuring the theoretical maximum number of products that can be affected. We followed (Costa et al. [11]) to formulate the CFC and CFP concepts. Consider a bidirectional network build from our direct network that is represented by $g \overset{\text{def}}{=} \left(\vec{n}, \vec{l}, \vec{p}\right)$, where n is the list of nodes, l is the list of links, and p is the list of products. Such as, p_1 is the list of products belonging to the company n_1. Hence, if we want to analyse a cascading effect starting in node, n_1, we have to define first the radius R_k^i. Radius R_1^1 is the list of nodes separated by distance 1 of node 1:

$$R_1^1 = \{n_i \in g : d(n_1, n_i) = 1\} \tag{15}$$

Then, to determine the nodes at radius $d = 2$ from node n_1, i.e. R_2^1, we need to remove all elements from R_1^1:

$$R_2^1 = \left\{n_i \in g \backslash R_1^i : d(n_1, n_i) = 2\right\} \tag{16}$$

So in general, for a distance k from a node i:

$$R_k^i = \left\{n_i \in g \backslash R_{k-1}^i : d(n_i, n_k) = k\right\} \tag{17}$$

Now, to obtain a quantity for the number of cascading failing companies, we just need to write the cascading number C, for a cascade range of k layers starting at node i, which is the sum of the number of elements of each radius:

$$C_k^i = \sum_k \# R_k^i \tag{18}$$

In the same way, for the cascading of products, the union of the lists of products in each set of companies belonging to each radius is:

$$P_k^i = \bigcup_j \left\{p_j : n_j \in R_k^i\right\} \tag{19}$$

To write the full list of products that belong to all failing companies put together, we have the union of products of every company at distance k from node i. So, all cascading products are the union of this union for all distances:

$$P^i = \bigcup_k P_k^i \tag{20}$$

and the total number of products unavailable, is then simply $\# P^i$.

In the product network described earlier, risk scenarios can be represented in a similar vein. Each weight represents a product instance. By reducing weights from the links, we can observe risks relating to the disappearance of individual products from suppliers' portfolios. To simulate resource scarcity, we would need to delete a node. To simulate disruptions at companies, the weights of all links associated with products in a supplier's portfolio are reduced. If a product node becomes isolated, this means the product is no longer reachable. However, in the product network isolated company nodes cannot be observed readily. Hence, we shall use the supply network for the simulation of risk scenarios.

3 An empirical illustration: the global automotive industry

In this section, we test a part of the risk assessment framework proposed in the previous section using large-scale empirical data. First, the dataset and network creation are described, followed by topological and simulation-based analysis.

3.1 Data and methods

To illustrate the analysis proposed, the automotive industry is mapped by querying a private industry database (Marklines Automotive Information Platform). The database collects data populated through surveys sent to about 40,000 automotive supplier firms and is primarily used by member firms to search for suppliers and advertise their capabilities. The data are agglomerative, in that once a supplier has identified itself as a supplier to a certain firm, it will remain so, unless either the customer firm or the supplier firm requests a removal of the relationship from the database. Therefore, the data are cross-sectional and might show relationships that are not continuous, although most data were gathered after 2007.

Data were downloaded from the databases during August–October 2014. The search process involved downloading data on products, customers and suppliers of firms that advertise themselves on the database. The customer and supplier data were then used to create links between companies. Every supplier was coded with a unique identification. Hence inter-tier linkages, and supplier links to multiple clients could be identified. First, the supplier network was constructed. Following data collection and the creation of the network, we isolated the largest connected component, ignoring clusters of firms that are not connected to the network. This resulted in 18,943 companies with 103,632 links between them. Of these, 16,469 are suppliers and the remainders are assemblers. One of the challenges in modelling supply networks is to define its boundaries. The companies on the network view themselves as connected to the automotive industry, given that they advertise their services to this particular industry. This, however, could mean companies such as raw material producers are missing from the network. The dataset also does not include non-production suppliers (for example, those providing maintenance, repair, and operating supplies, or capital equipment).

After the construction of the supplier network, we construct the product network by listing all distinctive product categories advertised by the suppliers and then creating linkages between the products with weights that signify how many times a product pair appears in the same portfolios of suppliers. There are a total of 934 product types in the network, produced by 16,469 supplier firms.

The products listed by companies are chosen from standard categories provided by the database and hence are consistent. A product refers to one of the product categories in the network, which are generic automobile components and sub-systems, rather than model specific. These could include categories such as gearbox, air conditioner, wiper switch. Product categories are thus viewed as substitutable. Generic processing capabilities such as forging and plastic moulding were ignored. Our view is that suppliers that create these generic product categories could be substitutable as they have the general capability and tools to produce a given product.

The networks constructed are shown in Fig. 1. The open source graph visualization manipulation software Gephi (available at http://gephi.org/) was used to visualize the two networks. Gephi was used also to identify network- and node-level metrics. The metrics proposed by the authors and simulation scenarios were implemented using the JGraphT library. The simulation experiments were carried out on two 2.8 GHz Intel Core i5 Apple computers with 8 GB 1600 MHz DDR3 memory. To achieve statistically significant results, we compared topological metrics with 100 random realizations of networks of the same numbers of nodes and links. The random realizations are created using Gephi, based on Erdős and Rényi networks (Erdős and Rényi 1960). Of course, a random network is likely to be a poor match with real supply chains.

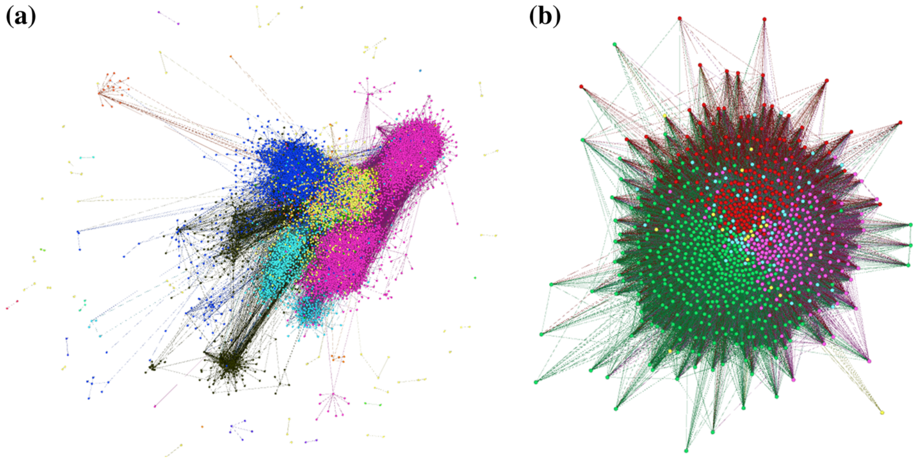


Fig. 1 **a** Supplier and **b** product networks constructed. Nodes are colour-coded according to communities

Table 4 Supply and product network metrics

	Global automotive industry	Random network
Supply network		
Network level		
Assortativity	Assortative ($r = 0.52$)	Disassortative
Modularity	0.44	0.14 ± 1e−5
Average path length	3.92	3.67 ± 0.001
Clustering coefficient	0.17	0.001 ± 1e−7
Node level		
In-degree centrality (supply load)	Ford Motor Company (1), Toyota (0.93), Honda (0.88)	
Out-degree centrality (demand load)	Magna International (1), Robert Bosch GmbH(0.64), Denso Corporation (0.59)	
Total degree centrality	Ford Motor Company (1), Toyota (0.93), Honda (0.88)	
Betweenness centrality (operational criticality)	Toyota (1), Ford (1), Honda(1), General Motors(0.8), Nissan (0.7), China FAW (0.7)	
Closeness centrality (informational independence)	Mitsubishi Heavy Industries Philippines (1), Sanko Electronics America (1), Mitsubishi Heavy Industries	
Product centrality (assembly criticality)	Magna International Inc.(1), Denso Corporation(0.95), Robert Bosch GmbH (0.84), TRW Automotive Holdings Corporation (0.66), Delphi Automotive PLC (0.65), Aisin Seiki Co. Ltd. (0.64)	
Product network		
Network level		
Assortativity	Assortative ($r = 0.76$)	Disassortative
Modularity	Not highly modular (0.179)	0.023 ± 1e−5
Average path length	1.51	1.43 ± 0.001
Clustering coefficient	0.76	0.57 ± 1e−7
Node level		
Degree centrality	Pipe (1), Bearing (0.97), Fastener (0.97), Spring (0.97), Sensor (0.96), Seal (0.95), Wire Harness (0.95)	
Betweenness centrality	Pipe (1), Spring (0.82), Bearing (0.76), Wire Harness (0.76), Sensor (0.66), Fastener (0.74)	
Closeness centrality	Fuel Filter (0.94), Fuel Gallery (0.92), Automatic Choke (0.92), Interior Trim (0.92)	

Companies and products scoring highest in centrality measures are shown with normalized measures given in parentheses

However, given that there is a lack of real-world empirical data in the supply chain literature, it is not appropriate to speculate on alternative null models without having to resort to significant assumptions. Similarly, there is no empirical example of the product network representation in the literature, and thus, no assumptions can be made regarding its structure.

3.2 Structural analysis of the global automotive industry

Table 4 shows metrics obtained for the automotive supplier network. The network is assortative as there is a clear increase in k_{nn} as k grows and the correlation between k and k_{nn} is reasonably high (Fig. 3e). Assortativity could point to several dynamics at play in a supply network. It could be an artefact of a bill of materials flow. Firms with high numbers of links could be leading their communities in certain areas of production and then connect to other high-degree firms doing the same thing, creating sub-assemblies that they pass on downstream. From a robustness perspective, connection of hubs to hubs would mean disruptions can cascade faster than a non-assortative network. This would pinpoint a need to keep contingency plans in place at hubs, such as inventories from vulnerable suppliers.

Modularity is high in our network and close to that of networks reported in the literature, including metabolic networks, collaboration networks of scientists, and jazz musicians [20]. We find 21 communities in the network detected by the algorithm given in Blondel et al. [4]. Figure 1a shows the communities found. Although the community detection algorithm does not have any industrial intelligence embedded within it, it is able to find logical patterns solely based on topological data. The existence of communities in a network could act as a buffer for disruptions as communities can prevent cascades to leak outside.

The average path length is not shorter than what we would expect to occur by chance, as comparison with the random model reveals. The supply network does not appear to be tightly knit, on the whole. Though of course, specific communities, perhaps those of some assemblers, might be more closely positioned than others. However, the clustering coefficient is higher than that of random networks, meaning that companies are indirectly connected to one another. Rather than the unitary pathways that would define a strictly hierarchical network, a firm may have many dozens of potential routes, whereby its output can reach the final customer. The overall average number of connections is 9.2. But here the issue is not the average number of links, but the distribution of links, as shown in Fig. 2.

The distributions of *in-* , *out-* , and *total* number of links demonstrate that the number of relationships maintained by firms in the network is not characterized by some random value, such as the Poisson distribution that we would expect for a random network (Erdős and Rényi 1960). However, contrary to some prior claims about supply networks ([25, 30]), we do not find a power-law degree distribution as would be the case in a scale-free network [2]. A scale-free structure would imply that a significant proportion of all relationships are associated with firms that act as hubs. Instead, the supply network follows an exponential degree distribution, with some firms maintaining significantly more relationships than others, but a clear upper bound on how many relationships a firm can maintain. An exponential degree distribution is typically observed in networks generated by a trade-off evolutionary process that involves nodes incurring costs for obtaining links [1]. This would put the supplier network somewhere in between a random network and a scale-free network in terms of its robustness to random and targeted failures. While the

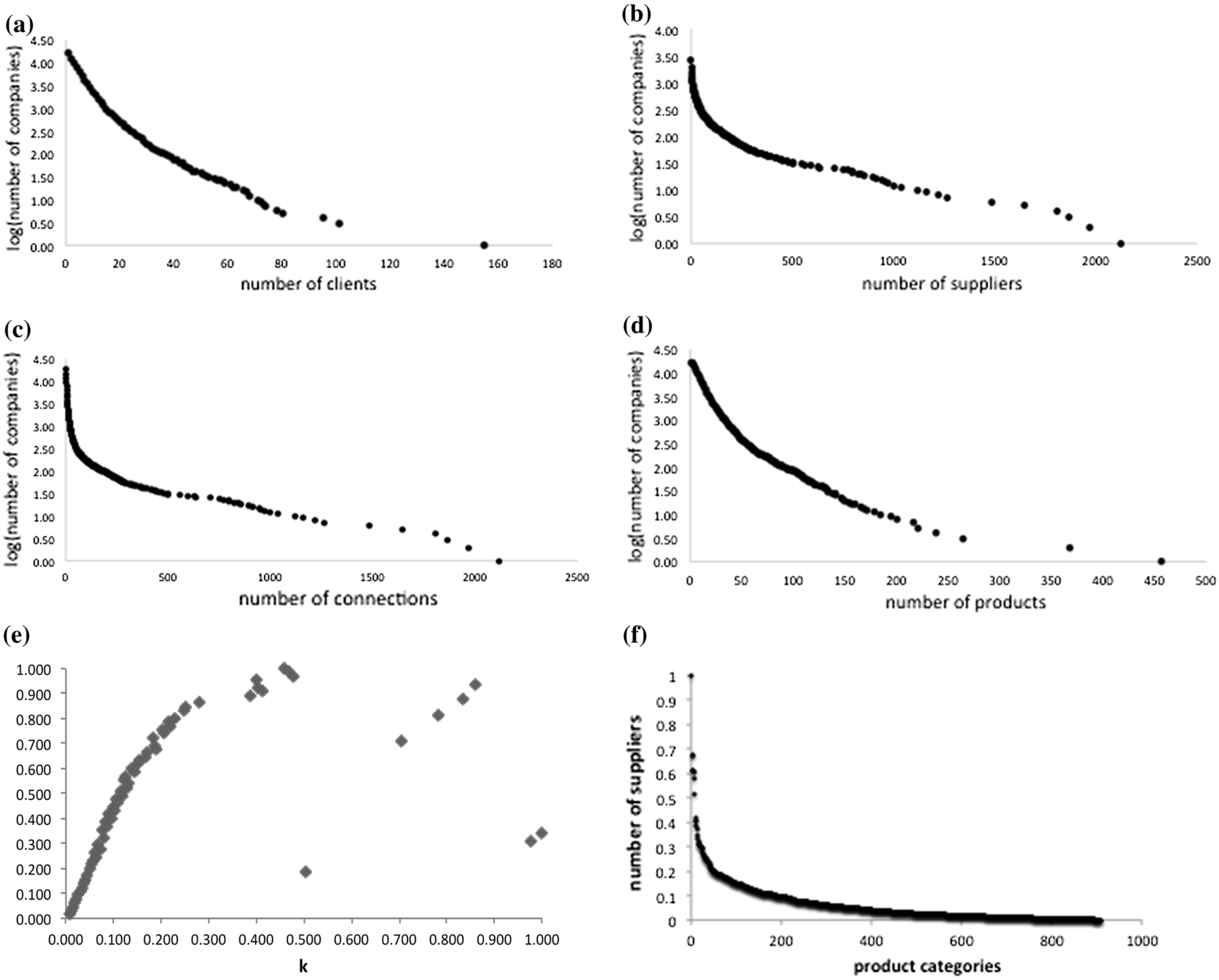


Fig. 2 Supply network distributions of **a** out-degree, **b** in-degree, **c** degree, **d** product degree, **e** assortativity and **f** product network weight distribution

network would be more robust to random failures than a random network, it would not be as robust as a scale-free network. On the other hand, it would be more robust to the failures of nodes with high numbers of links than a scale-free network, but not as robust as a random network. Probabilities associated with such attacks can be found using the simulation approach.

Product degree distribution shows a pattern in which some firms sell many products and most firms sell a few products. Although we cannot generalize a pattern to the distribution, given its low scale, we can assert that failures on those few firms with many products in their portfolio will likely affect the network more, provided that there is little redundancy. There is an average of 129 suppliers per product category out of 16,469 suppliers that supply products. Of course, this number is artificially high, as the product categories we work with are generic. The product weight distribution on the product network shows a different perspective (Fig. 2f). It appears that most product categories have multiple suppliers associated with them; however, a number of products are single- or double-sourced (2 %). These products need to be carefully inspected, and contingency plans for their scarcity need to be developed.

Next, we investigate centrality measures in both networks. In the previous section, we showed that the overall structure of the network is composed of hubs, to which most firms are connected. The network is vulnerable to disruptions on these hub firms but resistant to random disruptions. Furthermore, the network is composed of several sub-communities. Given the assortative network structure, we hypothesized that certain firms will connect these communities, providing the glue, which holds the network together. These firms will also act as bridges that transfer information and materials in the network. In this section, we identify these key actors by using network centrality measures and discuss how they impact the network. While network-level measures such as average path lengths and density provide macroscopic views of how the overall structure is organized, centrality measures provide a node-level view and examine how a certain node is embedded within a network, helping us identify firms with significant roles. Table 4 shows the companies scoring highest in out-degree, in-degree, betweenness, and closeness centrality measures. Following Kim et al. [16] terminology, we relate these measures to demand and supply load, operational criticality, and informational dependence, respectively. Several well-known automotive companies score highest in in-degree and total degree, forming the top of the network boundary. Overall, the correlation between the degree centrality of a company and its product centrality is 0.71. Therefore, it is highly likely that a supplier with many numbers of products in its portfolio will also be a hub in the network. However, the high correlation results from the out-degree and product centrality (0.70) rather than in-degree and product centrality (0.17). Suppliers with highest demand loads are multi-national corporations. Many of these, such as Magna and Denso, are not only highly connected, but also appear to be operationally critical. Magna has many links to many assemblers, but also is connected to high-degree suppliers such as Fuji Heavy, Cherry and Dongfeng. It consolidates many products from small suppliers and delivers goods downstream. If Magna was disrupted, the disruption would quickly cascade to multiple OEMs. Interestingly, it does not score highly in closeness centrality, possibly because of its assortative nature linking it to other Tier 1s but placing itself a hop away from Tier 3s. Magna needs to be closer to its extended network to be better informed of disruptions.

Examination of measures in the product network is revealing. This network has a slightly higher clustering coefficient, but average path length is not shorter than a random network. Many products in the network are coupled to one another. From a systems perspective, the system is not highly modular, meaning that there is little tolerance to disruptions to be contained within sub-systems before they reach other parts of the assembly. In terms of centrality measures scoring highly are usual suspects such as simple connectors and sensors. These are also the highest scoring in redundancy. It emerges that those products that are critical for many systems are also those products that have many suppliers.

3.3 Simulation of risk scenarios in the global automotive industry

Due to lack of data on groups of companies or factory locations and to exemplify as diverse set as possible, we opt for the simulation of two main attack scenarios out of the scenarios proposed in Table 3. These are progressive targeted disruptions at companies and targeted disruptions in countries. Figure 3 displays results. In the first scenario, we attempted to cause the most damage with the least removal of the nodes and thus select a targeted procedure. The nodes are ranked according to their total degree centrality and then nodes removed starting with the highest ranked node. When nodes are removed, all of its links are also removed. The size of LCC is observed upon each successive removal. As nodes with highest degree are removed, the largest component decreases and disappears at the removed fraction $f = 0.28$, deforming into disconnected clusters (Fig. 2a). This value is typical of exponential networks and is higher than scale-free networks but lower than random networks [2]. The network will thus be more tolerant to failures of highly connected nodes than a scale-free network but less tolerant than random networks.

The same pattern can be observed with the increase in the average path length, which increases with the removal of highly connected nodes as alternative paths are eliminated (Fig. 2b). After the LCC disappears, the APL will tend to infinity. Figures 4 and 5 show CFC and CFP as companies are deleted. In both scenarios, damage caused by deletion of individual companies are shown in decreasing logarithmic scale. In CFC, the number of affected buyers (Fig. 4a) and number of affected suppliers (Fig. 4b) are shown. In CFP, the number of affected buyers' products (Fig. 5a) and number of affected supplier products (Fig. 5b) are shown. Although in all cases third-degree cascades are exponentially larger in terms of impact, not all company deletions cause third-degree cascades. For example, the average number of products affected during a disruption at an individual supplier is 12 (Fig. 5b). The average number on the second-degree-cascade-affected products increases to an average of 101, and on third-degree cascade, this number increases to 768. However, out of all the suppliers, only the disruption of 0.002 % would cause a third-degree cascading failure although the third-degree cascading failure results in the loss of a large

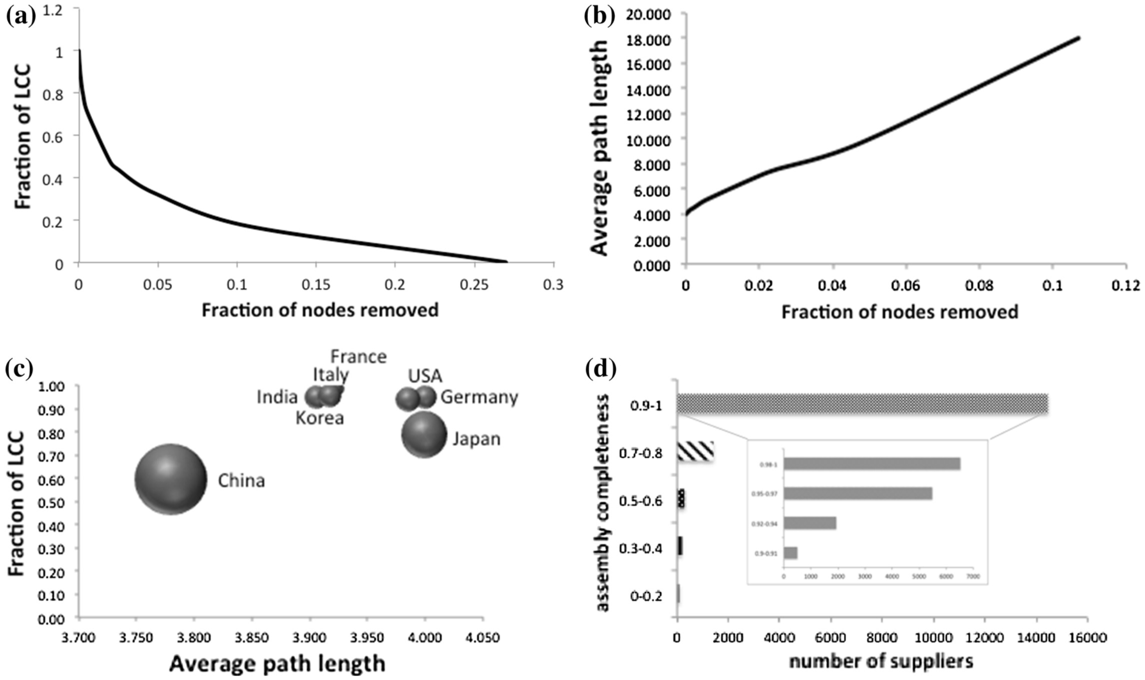


Fig. 3 **a** Reduction in largest connected component size as nodes with highest numbers of connections are targeted. **b** Increase in average path length as nodes with highest numbers of connections are targeted. **c** Reduction in largest component size and corresponding increase in average path length as companies from different countries are disrupted. Marker size is proportional to the number of companies removed from a country. **d** Number of suppliers failing versus assembly completeness if they are lost. Disruptions of majority will have little impact as most of the assembly can still be procured from elsewhere

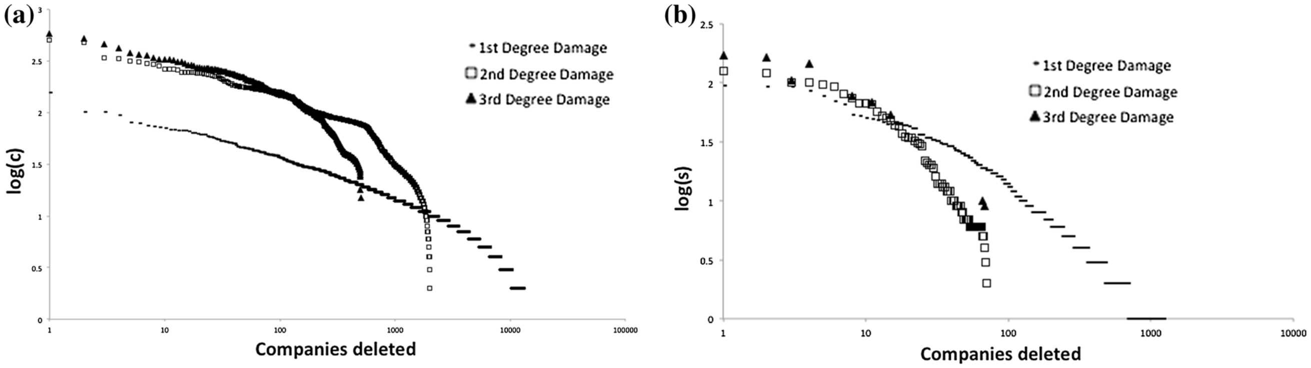


Fig. 4 Number of affected **a** clients and **b** suppliers, as companies are deleted

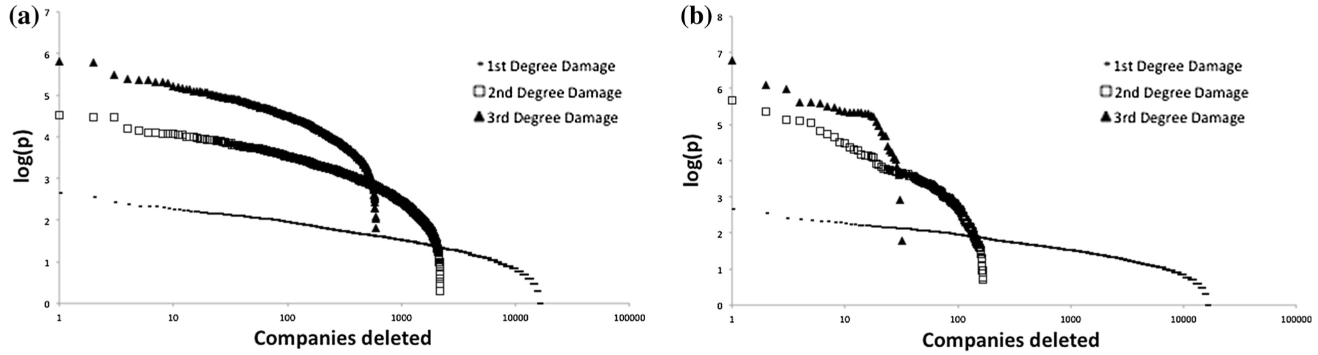


Fig. 5 Number of affected product instances **a** clients and **b** suppliers, as companies are deleted

number of products. Additionally, it is not necessarily the damage done by the first-degree disruption that determines the total amount of damage. For example, Magna's disruption would cause the most clients to be disrupted at the first degree because this company has the largest client base in the network. But when we look at second-degree damage, i.e. the clients of clients that are disrupted, Kamax's failure is the most damaging, and at the third-degree level, most damaging are Gibbs Die Corporation and Michigan Spring and Stamping. Interestingly, Magna also causes the most CFP damage at the first-degree level, but at the third-degree level, ZF Friedrichshafen AG, Panasonic Corporation, and Cummins Inc are most damaging. For network-level robustness, highly connected suppliers and suppliers with highest CFC and CFP levels need to be made more robust. For individuals in the network, the degree of spillover damage would depend on the containment measures taken at each successive supplier.

Equally interesting lessons emerge when countries are targeted for failure (Fig. 3c). China causes the highest damage to the LCC, but relative to its size, does not increase the average path length as much as Germany and Japan does. This means that China has many nodes the removal of which cause the size of LCC to decrease; however, these nodes are at the periphery of the network and thus are not highly connected. In contrast, Germany, USA, and Japan have fewer nodes, but those nodes provide most of the cohesiveness to the network. No single country's removal results in the disappearance of the LCC. Of course, note that many automotive assemblers such as Ford, Volkswagen, and Toyota are from these countries, to which many suppliers around the globe are connected, whereas companies in China are mostly sub-tier producers. When the AC is observed, no country except Japan and Germany causes any loss. Disruptions in Japanese and German suppliers result in an AC level of 0.98.

Next, we examine assembly completeness. Again we attempt to cause the most damage with the least removal of the nodes, in order to observe how fast breaking point would occur. This time suppliers are ranked according to their product centrality rather than degree centrality, with the assumption that the removal of suppliers with many products, rather than highly connected suppliers, would likely result in disappearance of products necessary to make the assembly. High-ranking suppliers are removed successively, and AC is noted. The plotted distribution shows the frequency of suppliers removed and the resulting AC. It is observed that removal of the vast majority of companies have little effect, whereas only a handful of suppliers cause the assembly to be severely incomplete. There is much redundancy in the network, and AC remains robust to majority of supplier failures.

4 Concluding remarks

4.1 Summary of findings

Supply chains emerge as large-scale complex networks, the interwoven topology of which makes them vulnerable to systemic risk. At large scales, accurate robustness analysis using operational details is not possible, not only because the variable space becomes infeasible to be solved analytically, but also because operational details such as buffer sizes, capacities, or throughput frequently change, making the analysis not worthwhile. In this paper, we proposed a network science-based framework as a powerful abstraction tool that captures some of the macroscopic features of disruption dynamics. This simplification captures what happens at the level of the network, rather than within the individual members of the population. Contrary to prior works, we used two network perspectives, namely those of suppliers and those of products, for a more complete analysis. The framework includes both existing and new metrics to capture static robustness and dynamic response to disruptions. We tested the framework with empirical data from the global automotive industry. Several conclusions have been drawn:

- Topological analysis showed that at large scales, the supply chain is structured as a complex network with multiple pathways between suppliers, rather than hierarchically organized simple chains. Thus, network science-based tools are appropriate for robustness analysis of the system.
- The network has an exponential degree distribution in terms of suppliers' in-, out-, total degrees as well as the product distribution among suppliers. This makes the network vulnerable to failures on companies with proportionally large numbers of clients, suppliers, total number of links, and products. The network, however, will be robust to random failures. As a comparison, the network will be more robust to failures on such hubs than on a scale-free network, but more vulnerable than on a randomly organized network.
- Assortative nature of both the product's and the supplier's network means that hubs tend to connect to hubs, making cascades of disruptions more damaging than that of disassortative networks.
- The supplier's network is organized into communities, with bridging suppliers connecting them. Disruptions at these central firms need to be prevented to contain cascades.
- If hubs fail in the supplier network, the largest connected component quickly disappears forming the network into disconnected clusters. Of course, in real life the network can be rewired; however, this will mean contractual rearrangements, which might take time, and result in increased costs.
- Considering the LCC mechanism, the removal of single countries do not result in the disconnection of the network; hence, topologically speaking, the network is robust to this kind of critical phenomena. However, the node-level damage of country removal and rewiring rates to avoid major catastrophes have not been analysed.
- Examination of cascades of disruptions in the supplier network showed that not only first-degree cascades but further degrees need to be taken into account as companies that score highly in first-degree damage are not necessarily the same companies that may result in secondary or tertiary damage. The degree to which cascades can happen may be estimated using operational variables such as buffers.
- Both the topology of the supplier network and distribution of production on the topology are important components of robustness. While the network may be topologically still connected, products that need to be procured for the car assembly might disappear. In this respect, our analysis showed that there is a high amount of multi-sourcing, making the network robust to supplier failures.
- The product network showed the existence of certain central products, such as fuel filters, which have high closeness centrality. Disruptions to the delivery of these products will affect the assembly of many products quickly, and these need to be carefully monitored. Products such as pumps have high betweenness and degree centrality. Although they have high redundancy in the network, disruptions to their delivery would cause issues for sub-systems to be brought together.

4.2 Limitations

Our results should be taken as a suggestive example due to limitations concerning the dataset. These are:

- Data correspond to a cross-sectional map, with companies advertising themselves as automotive parts manufacturers. Hence, at least the raw material layer is missing from the network.
- Data are agglomerative in that once a supply relationship or production capability is declared, it remains in the dataset, although ties can be broken and production capabilities may change over time.
- Analysis on product capabilities used standard product categories given by the dataset provider, the granularity of which might affect the resulting robustness analysis. For example, gearboxes for all models are grouped under one category, whereas products for different car models might vary. Robustness analysis using the framework should include expert input for product categorization to enable more accurate examination.
- By its nature, the framework offers an abstract analysis that develops statistical insights at large scales for which detailed operational data are not available. Therefore, the framework does not require exact bills of materials and material flow. Rather, it is aimed to complement operational analysis with a minimal set of parameters. For example, detailed analysis on a specific producer could include a discrete event simulation-type analysis. Our framework could serve as a statistical tool that informs such analysis with likely disruption cascades and vulnerabilities in the extended network.

4.3 Future outlook

Several avenues for future research are envisaged. First of these is an extension of this study to include other risk scenarios presented earlier and comparison with other industrial networks. Second is the automation of data collection. Current developments in intelligent products, automated supply chain management systems, and the Internet of Things can pave the way for intelligent systems that automatically gather and analyse risk data from large-scale supply networks in real time. Third, more studies need to be conducted on the use of network science-based analysis in supply chains. For example, after vulnerabilities are highlighted at the large scale, operational details can be introduced to pursue more in-depth questions such as levels of inventory needed to prevent cascades of failures within certain timeframes. Context-specific metrics that marry network science and operations need to be developed for a more complete understanding of robustness in supply chains. Furthermore, while this study focused exclusively on robustness properties of supply networks, the study of resilience is also important. Longitudinal data would be necessary to examine the relationship between structure and dynamical response of supply networks to perturbations.

References

1. Amaral LAN, Scala A, Barthélémy M, Stanley HE (2000) Classes of small-world networks. Proc Natl Acad Sci USA 97(21):11149–11152
2. Barabási A, Albert R (1999) Emergence of scaling in random networks. Science 286(5439):509–512
3. Basole R, Bellamy MA (2014) Supply Chain Risk Diffusion. Decis Sci 45(4):753–789
4. Blondel VD, Guillaume J, Lambiotte R, Lefebvre E (2008) Fast unfolding of communities in large networks. J Stat Mech Theory Exp10(2008):P10008
5. Borgatti S, Li X (2009) On social network analysis in a supply chain context. J Supply Chain Manag 1(1):7–22
6. Brintrup A, Kito T, New S, Reed-Tsochas F (2011) From transaction cost economics to food webs: a multi-disciplinary discussion on the length of supply chains. EUROMA, Cambridge
7. Brintrup A, Wang Y, Tiwari A (2015) Supply networks as complex systems: a network-science-based characterization. IEEE Sys. doi:10.1109/JSYST.2015.2425137
8. Carter CR, Ellram LM, Tate WL (2007) The use of social network analysis in logistics research. J Bus Logist 28(1):137–168
9. Chaturvedi A, Martínez-de-Albéniz V (2011) Optimal procurement design in the presence of supply risk. Manuf Serv Oper Manag 13(2):227–243
10. Choi TY, Dooley KJ, Rungtusanatham M (2001) Supply networks and complex adaptive systems: control versus emergence. J Oper Manag 19(3):351–366
11. Costa LDF, Rodrigues FA, Travieso G, Villas Boas PR (2007) Characterization of complex networks: a survey of measurements. Adv Phys 56(1):167–242
12. Dueñas-Osorio L, Craig JI, Goodno BJ, Bostrom A (2007) Interdependent response of networked systems. J Infrastruct Syst 13(3):185–194
13. Girvan M, Newman MEJ (2002) Community structure in social and biological networks. Proc Natl Acad Sci USA 99:7821
14. Kähkönen AK, Virolainen VM (2011) Sources of structural power in the context of value nets. J Purch Supply Manag 17(2):109–120
15. Keqiang W, Zhaofeng Z, Dongchuan S (2008) Structure analysis of supply chain networks based on complex network theory. In: Proceedings of the fourth international conference on semantics, knowledge and grid. IEEE Computer Society, Washington, pp 493–494
16. Kim Y, Choi TY, Yan T, Dooley K (2011) Structural investigation of supply networks: a social network analysis approach. J Oper Manag 29(3):194–211
17. Kurtenbach E, Karty SS (2011) As Japan shutdowns drag on, auto crisis worsens, Bloomberg Business Week. http://www.businessweek.com
18. Lomi A, Pattison P (2006) Manufacturing relations: an empirical study of the organization of production across multiple networks. Organ Sci 17(3):313–332
19. Nair A, Vidal JM (2011) Supply network topology and robustness against disruptions–an investigation using multi-agent model. Int J Prod Res 49(5):1391–1404
20. Newman MEJ (2006) Modularity and community structure in networks. Proc Natl Acad Sci USA 103(23):8577
21. Newman MEJ (2010) Networks: an introduction. Oxford University Press, Oxford
22. Punter A, Coburn A, Ralph D, Tuveson M, Ruffle S, Browman G. (2013) Evolving risk frameworks: modelling resilient business systems as interconnected networks. In: Proceedings of the think outside the risk, aon benfield hazards conference, gold coast, Australia, 22–24 September 2013
23. Saveedra S, Reed-Tsochas F, Uzzi B (2008) Asymmetric disassembly and robustness in declining networks. Proc Natl Acad Sci 105(43):16466–16471
24. Snyder LV, Atan Z, Peng P, Rong Y, Schmitt AJ, Sinsoysal B (2012) OR/MS models for supply chain disruptions: a review. Available at SSRN 1689882
25. Thadakamaila HP, Raghavan UN, Kumara S, Albert R (2004) Survivability of multi agent-based supply networks: a topological perspective. IEEE Intell Syst 19(5):24–31
26. Tomlin BT (2006) On the value of mitigation and contingency strategies for managing supply chain disruption risks. Manag Sci 52(5):639–657
27. Watts DJ (2004) The new science of networks. Annu Rev Sociol 30:243–270
28. Yang Z, Aydın G, Babich V, Beil DR (2009) Supply disruptions, asymmetric information, and a backup production option. Manag Sci 55(2):192–209
29. Zeng Y, Xiao R (2014) Modelling of cluster supply network with cascading failure spread and its vulnerability analysis. Int J Prod Res 52(23):6938–6953
30. Zhao K (2011) Analyzing the resilience of complex supply network topologies against random and targeted disruptions. IEEE Syst J 5(1):28–39