

# Disruptions in supply networks: a Probabilistic Risk Assessment approach

Anssi Käksi, Ahti Salo and Srinivas Talluri

October 24, 2013

## **Abstract**

Supply disruptions have received growing attention among academics and practitioners. Even companies in geographically and politically stable locations are exposed to disruptions, because they depend increasingly on their suppliers and suppliers' suppliers. Analyzing the impact of disruptions in different locations of the supply network helps mitigate risks more effectively: for example, instead of local measures such as safety stock or insurance, a company can introduce new supply contracts or back-up risky suppliers. In this paper, we develop a methodology for analyzing risks caused by supplier disruptions and, specifically, introduce concepts from probabilistic risk assessment (PRA), which is a widely employed methodology in the risk analysis of complex engineering systems. We apply the methodology to simple networks such as triads, and analyze disruption risks by simulating realistic-size random networks. We also illustrate how PRA-based approach can support strategic decisions, such as when to use single or multiple suppliers; how to identify risky and non-risky suppliers; and how to assess the impact of supply base complexity on network risk or reliability.

# 1. Introduction

Supply networks have become more complex due to the growth of global supply alternatives and strategic outsourcing. While the expansion of company's supply base can decrease costs, it also affects the risks, responsiveness, and suppliers' innovation capabilities (Choi and Krause 2006). Thus, in many companies, the goal of supply network management has shifted from short term cost savings to the pursuit of long term strategic benefits and, from the risk perspective, the improvement of resilience (Christopher and Peck 2004; Simchi-Levi 2010). Also Zsidisin et al. (2005) propose that

[...] supply risk management will evolve toward being embedded in the everyday strategic practices of purchasing organizations.

Yet it is challenging to quantitatively analyze risks caused by disruptive events in supply networks. First, there are strong dependencies among the supply network participants, and disruptive events can often be tracked down to disruptions at supplier, supplier's supplier, or even further upstream in the network (see various examples in Sheffi 2005). Second, a typical supply network has a large number of nodes (suppliers, tiers) and arcs (supplier relationships). Third, there are myriad of improbable events that can cause operational, environmental, or financial risks (Wagner and Bode 2008). In their recent review, Snyder et al. (2010) present various models for disruption management that account for these challenges. Still, most of these models are used in very specific decision making situations, such as where to locate inventory buffers.

In this paper, we develop a generic methodology for the assessment of risks caused by supplier disruptions in a supply network. The methodology is based on probabilistic risk analysis (PRA), which is a standard paradigm for the analysis of complex technical systems such as nuclear power plant or spacecraft (Bedford and Cooke 2001; Stamatelatos et al. 2011). PRA has also been applied to analyze electric power networks (Holmgren 2006; Koonce et al. 2008),

to perform stress tests of financial networks (Amini et al. 2012), and to manage risks in process control networks (Henry and Haimes 2006). As a rule, these applications follow the same process: i) create a sufficient structural model of the system; ii) identify the key risks and their likelihood; and iii) conduct a quantitative risk analysis to find the critical (most risky) parts of the system. Following this process, we develop a model of how disruptions at supply base contribute to company's disruption risk in operations management context, and, in particular, how i) the supplier's reliability and ii) the supplier's position in the supply network both impact the supplier's relative importance. The importance is evaluated by introducing probabilistic risk importance measures to supply networks.

At the strategic level, the proposed methodology provides input to the planning of supply network design. For example, it can be used to assess whether to use single or multiple suppliers, or what impacts the complexity of the network has on its reliability. In tactical decisions such as designing supplier contracts, the methodology can be used to identify best candidates for improving or relaxing reliability, for instance, by implementing contractual incentives for improved quality or by imposing requirements for contingency planning. At the operational level, the methodology can be used for risk mapping and monitoring, and to take informed decisions on how closely a particular supplier should be monitored.

The rest of this paper is structured as follows. In Section 2, we review the literature related to risk analysis in supply networks. In Section 3, the context for disruptions and the risk management process are discussed. Section 4 presents the methodology and risk importance measures. In Section 5, we illustrate the methodology by providing analytical results for triad networks and, moreover, numerical results for networks of more realistic size. Section 6 discusses managerial implications and Section 7 concludes.

## 2. Earlier approaches to disruptions in supply networks

The focus of sourcing and supplier management literature has recently expanded from buyer-supplier dyads and supply chains to supply networks: a review of supply network studies by Bellamy and Basole (2012) listed 19 papers between 1995-2003 and 107 papers 2004-2011. Wu and Choi (2005) and Choi and Wu (2008) study triad structures which account for supplier-supplier relationships in addition to buyer-supplier relations. Choi et al. (2001) conceptualize supply networks as complex adaptive systems, and derive several proposals related to supply network structure and behavior. Choi and Hong (2002) study three real supply networks for a strategic component in car manufacturing. Kim et al. (2011) complement these results with social network analysis for the same networks.

The network perspective has received growing attention in risk management as well: Christopher and Peck (2004) encourage companies to adopt supply chain strategies that lead to higher degree of resilience; Buhman et al. (2005) and Choi and Krause (2006) list risk management as one of the fundamentals of network management; and Zsidisin et al. (2000) and Simchi-Levi (2010) discuss the strategic importance of risk-informed procurement. Sheffi (2005) presents various cases that highlight the importance of supply chain risk management, and Hendricks and Singhal (2005) present evidence of how “supply chain glitches” impact company share price negatively. Wagner and Bode (2008), however, found that the link between supply chain performance and disruptions is not necessarily very strong, based on their empirical investigation of a random sample of German companies.

Manuj and Mentzer (2008) propose a risk management and mitigation framework that consists of five steps: i) Risk identification, ii) Risk assessment, iii) Risk management strategy formation, iv) Strategy implementation, and v) Risk mitigation. Most papers reviewed by Tang (2006), Snyder et al. (2010) and Sodhi et al. (2012) are risk management or risk mitigation studies that are motivated by the need to support specific decisions, such as inventory sizing and location (Schmitt and Singh 2011), order allocation (Tomlin 2006), or facility location

decisions (Qi et al. 2010). Instead of risk management, our focus in this paper is primarily on risk analysis. Typically, risks are divided into two categories (Kleindorfer and Saad 2006): demand-supply mismatches and risks arising from disruptive events; out of these we focus on the latter.

Supply risk analysis seeks to identify the most important risk factors in the supply network (Deleris and Erhun 2011). Different approaches have been developed: Zsidisin et al. (2000) interviewed eight companies about the maturity of their risk analysis practices and found that qualitative approaches dominate. Quantitative approaches have also been proposed: the case study by Schmitt and Singh (2011) employs a simulation approach which accounts for dynamic and structural complexity of supply networks. Wu et al. (2007) present Petri nets for large-scale, dynamic network environments; their methodology gives insights into how the impact of a disruption can propagate through a complex network. Deleris and Erhun (2011) develop a probabilistic model of a supply chain of a product family with various disruption sources, such as natural disasters, geopolitical instability, and operational and financial risks. They use simulation to investigate how different variables contribute to lead time and cost distributions.

The two studies most relevant for this paper are Craighead et al. (2007) and Adenso-Diaz et al. (2012). Craighead et al. (2007) discuss the impact of supply network design characteristics (network complexity, network density, and node criticality) on the severity of a possible disruption in the network. Based on a case study and expert interviews at nine companies, they propose that these three factors are positively related to the severity of the disruption. Adenso-Diaz et al. (2012) employ these characteristics, as well as several others, in their study of relationship between i) network characteristics, and ii) reliability in a large-scale simulation study. They postulate that the most important determinants of network reliability are the number of nodes, the number of arcs, network density, and node criticality. Except for the number of arcs, these determinants are positively linked to network risk (i.e., the risk level of the company that is being analyzed), which confirms most of the propositions by Craighead et al. (2007).

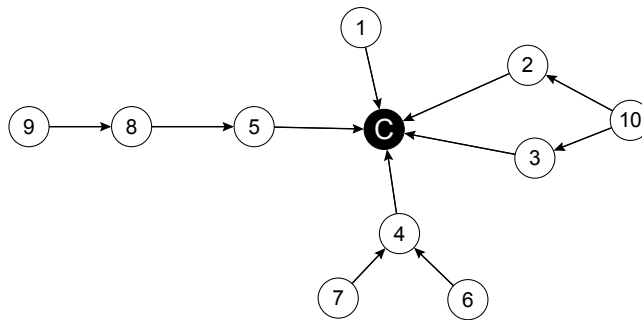
Some previous studies (Kao et al. 2005; Lockamy and McCormack 2010; Deleris and Erhun

2011) utilize *Bayesian networks* (BNs) to model the probability distributions and dependencies of risky variables. BNs are probabilistic graphical models used for structuring probabilistic information (Darwiche 2010). Langseth and Portinale (2007) state that reliability analysis must be mathematically sound, easy for the decision maker to understand, capable of handling low quality information (such as estimates based on few data points or vague expert opinions), and efficient for the calculation of probabilistic queries. They advocate the use of BNs for reliability analyses and argue that BNs are intuitive, flexible and effective for this purpose. Even in industrial risk management literature, the need to address risks comprehensively by taking dependencies into account has been recognized (e.g., Paté-Cornell 1996). BNs seem useful tool in this regard, because they can represent multiple uncertainties with dependencies (Darwiche 2010).

Specifically, we model supply networks as BNs and propose *risk importance measures* to identify risky suppliers. In PRA, there are many importance measures for supporting risk management decisions; for a comprehensive review, see Zio (2011). According to Van der Borst and Schoonakker (2001), the traditional uses for importance measures are i) optimization of system design, ii) optimization of system performance, and iii) controlling system configuration. We primarily focus on i) and ii), and use measures similar to risk reduction (decrease in risk when some entity of the system is assumed to function) and risk achievement (increase in risk when an entity is assumed to fail) which are common in PRA applications (Cheok et al. 1998; Van der Borst and Schoonakker 2001; Stamatelatos et al. 2011). Some extensions to these measures have been proposed: Borgonovo and Apostolakis (2001) introduce a differential importance measure which is additive and applicable to groups of entities; Toppila and Salo (2013) develop a methodology that accounts for epistemic uncertainties related to event probabilities; and Ramirez-Marquez and Coit (2005) extend these measures for systems with multi-state components.

### 3. Scope of study

We focus on inbound supply risks which arise from events in the supply base that have a negative impact on the focal company, i.e., the company from whose perspective risks are analyzed. Such an event can prevent the company from meeting its customers' demands, thus inducing a supply risk (similar definition is used by, e.g., Wu et al. 2006; Choi and Krause 2006). In PRA terms, the undesirable end state of the system is a disruption in the activities of the focal company, and so-called the basic events are disruptions at suppliers. These disruptions are high-impact events which have significant adverse impact on the supplier's performance, and they may be caused by natural events such as earthquakes, but also by less obvious causes such as supplier becoming a competitor. As a rule, these events are unexpected, can cause a severe dysfunction of a supplier, and, moreover, have an impact than can propagate in the network. For example, a fire at supplier's plant is a disruption only in case the company does not have a back-up that can replace the original plant, thus causing a break in the material flow. Like Craighead et al. (2007) and Adenso-Diaz et al. (2012), we do not differentiate between disruption types, but rather consider disruptions in general, and their ability to "contaminate" the supply network so that the focal company will be affected. Each node in the network is either fully disrupted, or fully operational. This binary approach is a typical way to model supply network disruptions (Snyder et al. 2010).

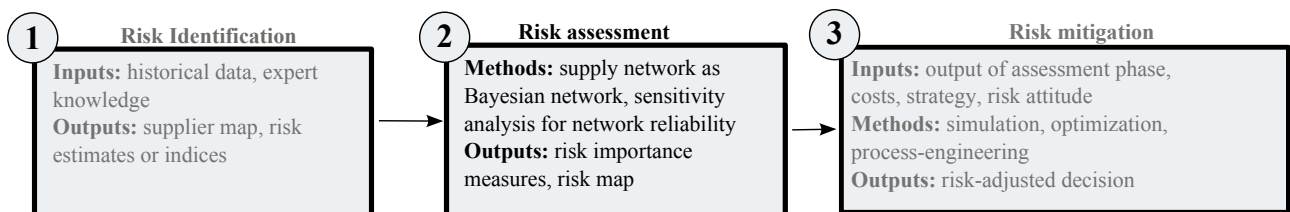


**Figure 1** Example supply network.

We do not differentiate between node types but consider all nodes as suppliers. In the network of Figure 1, the focal company  $C$  has ten suppliers: the first tier suppliers are 1-5 and,

e.g., second tier suppliers 6 and 7 are called parents of 4. Suppliers 2 and 3 are referred to as siblings, because they share a common parent supplier 10 whose customers they are. We treat the network as a static probabilistic network where *risk is measured by the probability of disruption at the focal company*. This probability depends on what the status of the other nodes in the network is. In particular, we seek to assess how this probability depends on possible disruptions at other nodes; this leads us to define the importance (or, criticality) of these other nodes.

Our methodology supports the risk assessment phase of the risk management process in Figure 2, adapted from the SCOR-model by the Supply Chain Council (SCC 2010). The purpose of the first phase, risk identification, is to list potential risk sources, to create a cause-effect diagram, and to estimate the likelihood of disruptions by using, e.g., historical data, expert workshops, or supplier audits and site visits. The second phase, risk assessment, provides information about the distribution of risks in the network. Here, we use Bayesian networks to model the supply network and to provide risk importance measures that enable sensitivity analyses; supplier risk importance measures and risk maps are the key outcomes of this phase. Finally, the third phase, risk mitigation, provides support for decision making: here, optimization can be used to evaluate specific decision options using risk analysis as input. For example, multi-criteria optimization models can be used to select suppliers by treating risk importance as an additional criterion beyond other relevant factors, such as cost and capacity (Narasimhan et al. 2006).



**Figure 2** The supply network risk management process (adapted from SCC 2010).



## 4. Methodology

### 4.1. Bayesian networks and notation

*Bayesian networks* (BNs; see Pearl 2000; Darwiche 2009) are probabilistic graphical models in which random variables are represented by a directed acyclic graph. A material flow based supply network can readily be represented by such a graph: material flows have a direction and –assuming return flows and recycling are negligible– there are no cycles in the network. In a BN, an arc denotes causality between two nodes. In the supply risk context, the relationship  $A \rightarrow B$  is interpreted as: *disruption at A is a direct cause for disruption at B*. We assume that a company downstream does not cause disruptions upstream. This is in line with typical supply network dynamics where materials flow downstream. In principle, a customer can cause a disruption at a supplier, but such a possibility is beyond the scope of this paper.

We denote suppliers with numbers  $i = 1, \dots, N$  and node  $C$  is the focal company (this is also the global sink of the graph, to which all paths eventually lead). Node  $X$  can have two states: it is either *disrupted* ( $X = true$ , or simply  $X$ ) or *functional* ( $X = false$ , or  $\bar{X}$ ). Generally, for a single node  $X$  with parents  $\mathbf{U}$ , the probability of state  $x$  when parents are in state  $\mathbf{u}$  is  $\Pr(x|\mathbf{u})$ , and it must hold that  $\sum_x \Pr(x|\mathbf{u}) = 1$  for every instantiation  $\mathbf{u}$  (realization of the states of parent companies). The probabilities  $\Pr(x|\mathbf{u})$  are called network parameters or, in our case, risk parameters. With binary states, there are  $2^n$  parameters to be defined for a node with  $n$  parents.

We employ a so-called *noisy-OR* model (Pearl 1988) for modeling the relationship between disruptions at parents and child nodes. This is done because of two reasons. First, the computational challenges can be reduced: in supply networks nodes can have tens of parents (high  $n$ ), which can pose serious challenges with the standard Bayesian network formulation, where the number of network parameters grows exponentially ( $2^n$ ). Second, reducing the parameters also makes the methodology more attractive for applications: often expert knowledge must be

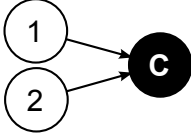
utilized in probability elicitation and to do this successfully, the amount of probabilities to be estimated must be rather limited. In this model, each parent can independently cause a disruption at a child node and, in addition, there is a “leak variable” that can cause a disruption of this node even if the parent nodes are functional. Interactions, i.e., disruptions due to more than one supplier being disrupted simultaneously are not omitted, but their impact is calculated implicitly. The implicit treatment of interactions reduces some accuracy: e.g., it is not possible to set an exact value for the risk parameter of event “suppliers 2,3,6 and 9 (out of 10) are disrupted”, but the inaccuracies caused by this simplification are likely to be small as the probability of such event is typically small and, in any case, the risk is approximated by the event “2 or 3 or 6 or 9 is disrupted”. The noisy-OR model decreases the number of parameters required for a node with  $n$  parents to  $n + 1$ , which makes it easier to model large networks. We introduce next the notation and a numerical example of the noisy-OR model; further technical details are provided in the Appendix.

Three types of notations are used: the probability that parent  $j$  causes disruption at node  $i$  is  $\beta_{i|j}$ ; the probability of disruption due to the leak variable (i.e., independent of parents) is  $\alpha_i$ ; and the marginal probability that node  $i$  is disrupted is denoted with  $F_i$ . For nodes without parents, we have  $F_i = \alpha_i$ . If the set of parents of node  $i$  is  $\mathcal{P}$ , then  $F_i = f(\alpha_i, \beta_{i|p}, F_p) \forall p \in \mathcal{P}$ . This function  $f$  is a multilinear function of the network parameters and can be calculated recursively (for details, see Appendix). A simple example of how to calculate  $F_C$ , i.e., the probability that the focal company  $C$  is disrupted is in Table I. This probability is central in further analyses in that  $F_C$  describes the supply risk and the sensitivity analysis of this probability motivate the development of risk importance measures.

## 4.2. Risk importance measures and sensitivity analysis

To identify suppliers whose disruptions have the greatest impact on the focal company, we characterize how  $F_C$  depends on the changes in the network parameters. For example, to assess the importance of a given supplier, it is possible to calculate how much

**Table I** An example with node  $C$  and two suppliers. In numerical examples, all independent disruption probabilities are 5% ( $\alpha_i = 0.05 \forall i$ ) and disruption at supplier  $i$  induces 50% probability of disruption at  $C$  ( $\beta_{C|i} = 0.50 \forall i$ ). Note that due to the noisy-OR assumption, there is no need to specify separately the probability for  $C$  being disrupted if *both* 1 and 2 are disrupted.

Network	States $\mathbf{u}$	$\Pr(C \mathbf{u})$	$\Pr(\mathbf{u})$
	$u_1 = \{\bar{1}, \bar{2}\}$	$\alpha_C = 0.05$	$(1 - \alpha_1)(1 - \alpha_2) \approx 0.90$
	$u_2 = \{\bar{1}, 2\}$	$1 - (1 - \alpha_C)\beta_{C 2} \approx 0.53$	$(1 - \alpha_1)\alpha_2 \approx 0.05$
	$u_3 = \{1, \bar{2}\}$	$1 - (1 - \alpha_C)\beta_{C 1} \approx 0.53$	$\alpha_1(1 - \alpha_2) \approx 0.05$
	$u_4 = \{1, 2\}$	$1 - (1 - \alpha_C)\beta_{C 1}\beta_{C 2} \approx 0.76$	$\alpha_1\alpha_2 \approx 0.00$

$$F_C = \sum_{\forall \mathbf{u}} \Pr(C|\mathbf{u}) \Pr(\mathbf{u}) \approx 0.097$$

$F_C$  increases when the probability of a disruption at a given supplier grows. In Table I, the updated risk level under the event “supplier 1 is disrupted with probability 1” is  $\underbrace{0}_{u_1} + \underbrace{0}_{u_2} + \underbrace{(1 - (1 - \alpha_C)\beta_{C|1})(1 - \alpha_2)}_{u_3} + \underbrace{(1 - (1 - \alpha_C)\beta_{C|1}\beta_{C|2})\alpha_2}_{u_4} \approx 0.54$ , which means an increase of 44 percentage points in the risk of disruption at  $C$  from the initial 9.7% risk of disruption.

The risk importance measures (or briefly, importance measures) indicate how the total risk  $F_C$  depends on changes in the disruption probabilities in the supply base. We introduce two such measures: Supplier Fortification Impact ( $F_I$ ) and Supplier Disruption Impact ( $D_I$ ). These are analogous to Risk Reduction and Risk Achievement which are commonly used importance measures in PRA (Van der Borst and Schoonakker 2001). Both measures follow the same principle: they measure the absolute change in  $F_C$  when the state of a given supplier node is fixed, i.e., the probability of disruption at that node is either zero or one.

**Supplier fortification impact** ( $F_I$ ) measures *the decrease in total risk*  $F_C$  when possibilities of disruption at supplier  $n$  are eliminated, i.e.,  $F_n = 0$ . It is defined as follows:

$$F_I(n) = \left\{ F_C - F_C(\bar{n}) : F_C(\bar{n}) \text{ is the total risk with } \alpha_n = \beta_{n|i} = 0 \forall i \text{ parent of } n \right\} \quad (4.1)$$

**Supplier disruption impact** ( $D_I$ ) measures *the increase total risk*  $F_C$ , when supplier  $n$  is disrupted for sure, i.e.,  $F_n = 1$ . It is defined as follows:

$$D_I(n) = \left\{ F_C(n) - F_C : F_C(n) \text{ is the total risk with } \alpha_n = 1 \right\} \quad (4.2)$$

When comparing, we use notation  $i \overset{F}{>} j$  when  $F_I(i) > F_I(j)$ , and  $i \overset{D}{>} j$  when  $D_I(i) > D_I(j)$ .

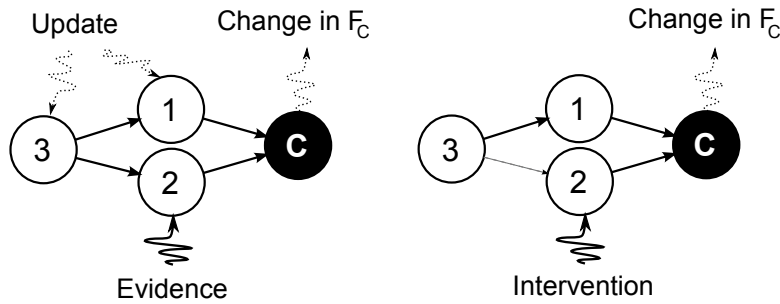
No single importance measure is suitable for all purposes (Van der Borst and Schoonakker 2001). Fortification Impact is a measure of *risk-significance*: it represents the maximum decrease in the total risk that can be achieved by improving the reliability of a supplier. If this measure is relatively high, the supplier in question is a big contributor to the current risk level (i.e., is a probable cause for disruption) and thus, is a good candidate for improvement actions. Disruption Impact, on the other hand, is a measure of *reliability-significance*: it measures how much the disruption risk grows if the supplier is no longer available. This indicates the importance of ensuring the current level of reliability of the supplier. If this measure is low in comparable terms, the supply network can resist a disruption at this supplier rather well, and thus, the supplier is a good candidate for reliability relaxation actions. In our examples, we focus mostly on risk-significance ( $F_I$ ), because it is more suitable for risk management in existing supply networks, i.e., in cases where network design is fixed.

The calculation of risk importance measures requires probabilistic queries where dependencies need to be accounted for. Note that directed acyclic graphs are not necessarily *trees* and, consequently, a node can be dependent of another node even though it is not a descendant of it. This is exemplified by the networks in Figure 3, where company  $C$  has two suppliers that are both dependent on a single parent supplier. Here, if one were to observe that supplier 1 is disrupted, one would readily infer that parent supplier 3 is a possible cause so that supplier 2 could be or become disrupted. This exemplifies a case where a node can be dependent of another node, even though it is not a descendant of it. The condition for independence between two nodes is called d-separation:

**D-separation** : Let  $\mathbf{X}$ ,  $\mathbf{Y}$  and  $\mathbf{Z}$  be disjoint sets of nodes in a directed acyclic graph. Iff

every (undirected) path between a node in  $\mathbf{X}$  and a node in  $\mathbf{Y}$  is blocked by  $\mathbf{Z}$ ,  $\mathbf{X}$  and  $\mathbf{Y}$  are d-separated, or  $\text{dsep}(\mathbf{X}, \mathbf{Z}, \mathbf{Y})$ . Further,  $\text{dsep}(\mathbf{X}, \mathbf{Z}, \mathbf{Y})$  implies that  $\mathbf{X}$  and  $\mathbf{Y}$  are independent given  $\mathbf{Z}$  and gaining information about  $\mathbf{X}$  does not influence our beliefs about  $\mathbf{Y}$ . (For proof and details, see Chapter 4 in Darwiche 2009).

Details on d-separation are provided in the Appendix, and some implications for supply network risks are covered in Section 5.2.



**Figure 3** Difference between insertion of evidence and intervention in an example network with two suppliers and one supplier’s supplier.

In effect, two sorts of modifications can be introduced to a BN (Pearl 2000): observations (insertion of evidence) and interventions. The difference between these is that an observation calls for an update of state probabilities in all nodes that are dependent on the node in question, whereas an intervention requires such an update only on its descendants. In Figure 3, there are two ways to update the probabilistic model after the event “there is a disruption at supplier 1 with probability 1”: i) inserting evidence of supplier 1 being disrupted so that the disruption probability of parent node 3 also increases (because it is a possible cause of disruption at node 1), making the disruption probability of the other sibling 2 is also higher; and ii) updating only nodes 1 and C. In the latter, the manipulated node (in this case 1) becomes uniquely determined by the intervention, and dependence on other variables vanishes as illustrated in Figure 3.

As noted by Pearl (2000), following the principle of Occam’s razor, the fewer assumptions the better and thus, sensitivity analyses should be performed primarily using interventions. As an example, consider again Figure 3: if one were to observe that supplier 1 is disrupted, one

would infer that parent supplier 3 is a possible cause and thus, supplier 2 could also be or become disrupted. Yet, in typical planning related to risk management, disruptions are not *de facto* observed. Instead one may, for example, be interested in exploring what would happen if supplier 1 would end the business relationship (and thus, become disrupted). In this case, the parent supplier is not impacted at all, and thus, supplier 2 is not impacted either. This suggests that when the cause for disruption at a given supplier is not known, only its descendants should be updated. This is also the case for when importance measures are calculated.

## 5. Results for Bayesian supply networks

### 5.1. Single vs. multiple sourcing

We analyze first tier suppliers, which are often the most important nodes of a supply network. Consider two simple “networks”, where all materials (or, sub-assemblies, services, etc.) are sourced either from one or two suppliers as in Figure 4. The probability of disruption at  $C$  in the single-supply case (denoted with  $G'$  in the Figure) is

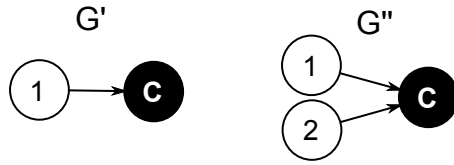
$$F'_C = \alpha'_C + (1 - \alpha'_C)F'_1\beta'_{C|1}$$

and in the dual-supply case ( $G''$ )

$$F''_C = \alpha''_C + (1 - \alpha''_C)[\beta''_{C|1}F''_1(1 - F''_2) + \beta''_{C|2}F''_2(1 - F''_1) + (\beta''_{C|1} + \beta''_{C|2} - \beta''_{C|1}\beta''_{C|2})F''_1F''_2].$$

If we assume that  $\alpha'_C = \alpha''_C = 0$  meaning that all disruptions at  $C$  are caused by suppliers, we can compare the riskiness of these two structures with a simple equation:

$$F'_C - F''_C = \beta'_{C|1}F'_1 - (\beta''_{C|1}F''_1 + \beta''_{C|2}F''_2) + \underbrace{\beta''_{C|1}\beta''_{C|1}F''_1F''_2}_{\text{small}} \approx \beta'_{C|1}F'_1 - (\beta''_{C|1}F''_1 + \beta''_{C|2}F''_2)$$



**Figure 4** Single ( $G'$ ) and dual supplier ( $G''$ ) networks.

This means that single-supply is more risky, if the supplier's marginal risk ( $F'_1$ ) multiplied by the probability that disruption at a supplier causes disruption at  $C$  ( $\beta'_{C|1}$ ) exceeds the sum of same terms of suppliers in the dual-supply case. This intuitive result highlights the duality in comparing single vs. multiple suppliers: it is essential to account for i) how reliable the suppliers are, and ii) how the focal company depends on its supplier(s).

In their discussion of single vs. multiple sourcing, Blome and Henke (2009) emphasize that supplier reliability and dependency on suppliers are critical in supply risk management. They argue that, in the single supply case, the relation with the supplier is typically deeper and thus supplier risk (in our case  $F'_1$ ) is lower, but dependency on the supplier ( $\beta'_{C|1}$ ) is also higher so that there can be “painful consequences” if the disruption occurs. On the other hand, using multiple suppliers may lead to order allocation (and smaller orders per supplier) so that the buying company is not a top customer for any of its suppliers; thus, the risk of supply disruption can increase (larger  $F''_i$ ). Then again, due to alternative suppliers, buying company's dependency on any particular supplier should be lower (low  $\beta''_{C|i}$ ). In keeping with our quantitative result above, Blome and Henke (2009) conclude that neither single or multiple sourcing leads automatically to lower supply risks, but, rather, these risks vary depending on supplier reliability and relationship.

## 5.2. Impact of parents, siblings and children on supplier importance

The position of the supplier in the network has a big impact on how significant of a risk it poses to the focal company. For example, one could conclude that the smaller the distance (tier) to the focal node, the more important the supplier. But this is not always the case: a typical assembler of a high-technology consumer product can have several first tier suppliers of, say,

flat screen modules. These suppliers can select their own suppliers from few companies that have fabrication centers for the special glass required for such modules. But these fabrication plants could all be dependent on a specific raw material – in this case indium (Patel-Predd 2009). If the second tier suppliers of special glass depend on one or two indium suppliers, these (third tier) raw material suppliers might be the most critical ones in the supply network. So, in supply network risk analysis, both the number of parents (suppliers) and the number of children (customers) matter. Next, we analyze how supplier’s position in the network impacts its (Supplier Fortification Impact) importance, when the risk parameters are otherwise identical.

D-separation can be used to study a sequential (chain) structure  $j \rightarrow i \rightarrow C$ . Because  $i$  d-separates  $C$  and  $j$ ,  $\Pr(C \text{ disrupted} | \alpha_i = 0, \beta_{i|j} = 0) = F_C(\bar{i})$  is independent of supplier  $j$  and its ancestors. However,  $F_C(\bar{j})$  is dependent on  $i$ , and because supplier  $i$  can only increase this disruption risk, it follows that  $F_C(\bar{j}) \geq F_C(\bar{i})$ . In the Fortification Impact measure  $F_I(n) = F_C - F_C(\bar{n})$ , the importance of  $n$  becomes higher with smaller  $F_C(\bar{n})$  values and thus  $F_C(\bar{j}) \geq F_C(\bar{i}) \Rightarrow i \stackrel{F}{\geq} j$ . Also with the convergent structure  $k \rightarrow i \leftarrow j$ , where  $i$  is a first tier supplier of  $C$ , supplier  $i$  is more important than  $k$  or  $j$ . This is because  $i$  d-separates both  $j$  and  $k$  from  $C$ . But the importance order between  $j$  and  $k$  cannot be defined directly. The risk of disruption at  $i$  in convergent structure is:

$$\begin{aligned} F_i &= \alpha_i + (1 - \alpha_i) [\beta_{i|j} F_j (1 - F_k) + \beta_{i|k} F_k (1 - F_j) + (\beta_{i|j} + \beta_{i|k} - \beta_{i|j} \beta_{i|k}) F_j F_k] \\ &\Rightarrow F_C(\bar{k}) - F_C(\bar{j}) = \beta_{i|j} F_j - \beta_{i|k} F_k, \end{aligned}$$

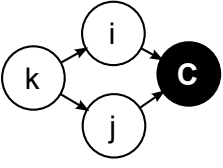
so the importance order between  $j$  and  $k$  can be defined by investigating the sign of  $\beta_{i|j} F_j - \beta_{i|k} F_k$ . If this is positive,  $j \stackrel{F}{>} k$ , and vice versa.

In divergent structures with one supplier and multiple customers, the number of siblings matters, too. Namely, if a node has a sibling, it does not d-separate the parent supplier from the downstream node. For example with  $i \leftarrow k \rightarrow j$ , where  $i$  and  $j$  are first tier suppliers of  $C$  (see also Table II), they do not d-separate  $k$  from  $C$  individually. It follows that  $F_C(\bar{i})$ , i.e., the disruption risk of  $C$  when  $i$  is blocked, is dependent on  $k$ , which can still increase the



disruption risk at  $C$  through supplier  $j$ . When compared to a sequential structure with one supplier and one supplier’s supplier,  $F_C(\bar{i})$  is equal or higher and, other things being equal, it follows that a sibling makes a supplier less important compared to a sequential structure. Divergent structure is analogous to a dual-supply situation, where both (first tier) suppliers have a common (second tier) supplier. Here, the first tier suppliers  $i$  and  $j$  are not necessarily the most important ones: consider the numerical example in Table II where any kind of importance ranking can be achieved in a setting where marginal risks are equal.

**Table II** Examples of the divergent structure with varying node importance rankings. As highlighted below, all chosen parameter values imply (approximately) equal marginal risks. In all cases,  $\alpha_k = F_k = 0.10$ ,  $\alpha_C = 0.05$ ,  $\beta_{C|i} = 0.50$ , and  $\beta_{C|j} = 0.50$ .

Network	$\alpha_i$	$\alpha_j$	$\beta_{i k}$	$\beta_{j k}$	$F_C$	$F_i$	$F_j$	Fortification Importance
	0.08	0.05	0.25	0.50	0.14	<b>0.10</b>	<b>0.10</b>	$i(4.4\%) \stackrel{F}{>} j(4.2\%) \stackrel{F}{>} k(3.0\%)$
	0.01	0.05	0.90	0.50	0.13	<b>0.10</b>	<b>0.10</b>	$k(5.4\%) \stackrel{F}{>} i(3.6\%) \stackrel{F}{>} j(3.5\%)$
	0.10	0.01	0.00	0.95	0.14	<b>0.10</b>	<b>0.10</b>	$j(4.7\%) \stackrel{F}{>} i(4.5\%) \stackrel{F}{>} k(4.2\%)$

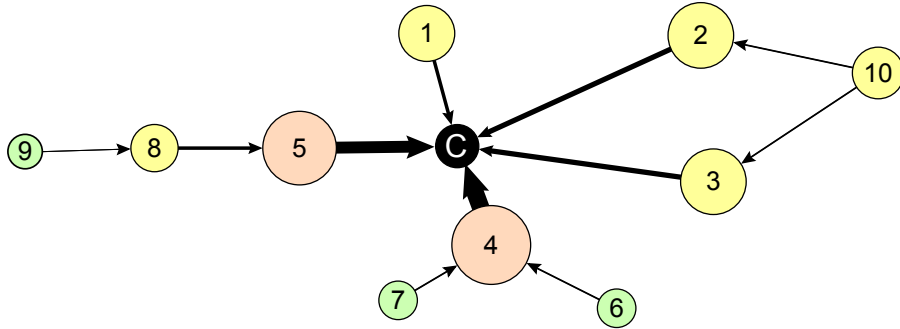
In the view of the above, it is not easy to make generic conclusions about how the risk importance of a supplier is linked to its position in the network. For example, first tier suppliers are not always the most important ones. Some rules of thumb, however, can be summarized:

**Each supplier increases total supply risk:** a supplier can be thought as a gate that amplifies the “disruption flow” that originates from the leaf suppliers (i.e., suppliers without parents). Compared to a supplier with one parent, a supplier with multiple parents is more risky and thus more important (measured by the Fortification Impact), if all other parameters are equal.

**Distance decreases importance:** if node  $i$  d-separates its suppliers  $\mathbf{X}$  from  $C$  (sequential and convergent structures), this node is more important than any of  $\mathbf{X}$ . Because being close to  $C$  increases the probability of separating other suppliers from  $C$ , closeness increases the relative importance of  $i$ .

**Divergent structures do not decrease risks:** divergence divides parent’s disruption risk into branches. Thus, supplier is relatively less important if it has siblings. The supplier cannot fully “block” its parent’s disruption, which can still “flow” towards  $C$  through the sibling.

Figure 5 illustrates these concepts in the network of Figure 1 with identical parameters  $\alpha = 0.05$  and  $\beta = 0.5$  for all nodes. The size of each node represents its Fortification Impact (the larger the more important) and colors are used for additional highlighting of the differences. Here,  $4 \stackrel{F}{>} 2$ , because 4 can “block” two parents, whereas 2 cannot “block” the one parent it has. Also,  $1 \stackrel{F}{>} 8$ , even though its marginal risk is smaller ( $F_1 = 5\% < F_8 = 7.4\%$ ). This is because 1 is closer to  $C$  than 8. Note that the weights of flows illustrate the “disruption flow” that is independent of node parameters; because 4 gathers the disruption probability from two parents, it cause more weight to the flow compared to, e.g., 1 which is not an amplifier of any further tier disruption sources.



**Figure 5** Example supply network with Fortification Impact importance illustrated.

### 5.3. Large networks

Supply networks tend to be large: Choi and Hong (2002) note that car manufacturers can have 40-1500 suppliers in the supply base. They analyze selected sub-assemblies, for which the supply networks consist of some 30 to 80 suppliers. To conduct probabilistic risk analysis in such large networks, a numerical approach is required because the network risk  $F_C$ , as any marginal probability in a Bayesian network, is a multilinear function of network parameters

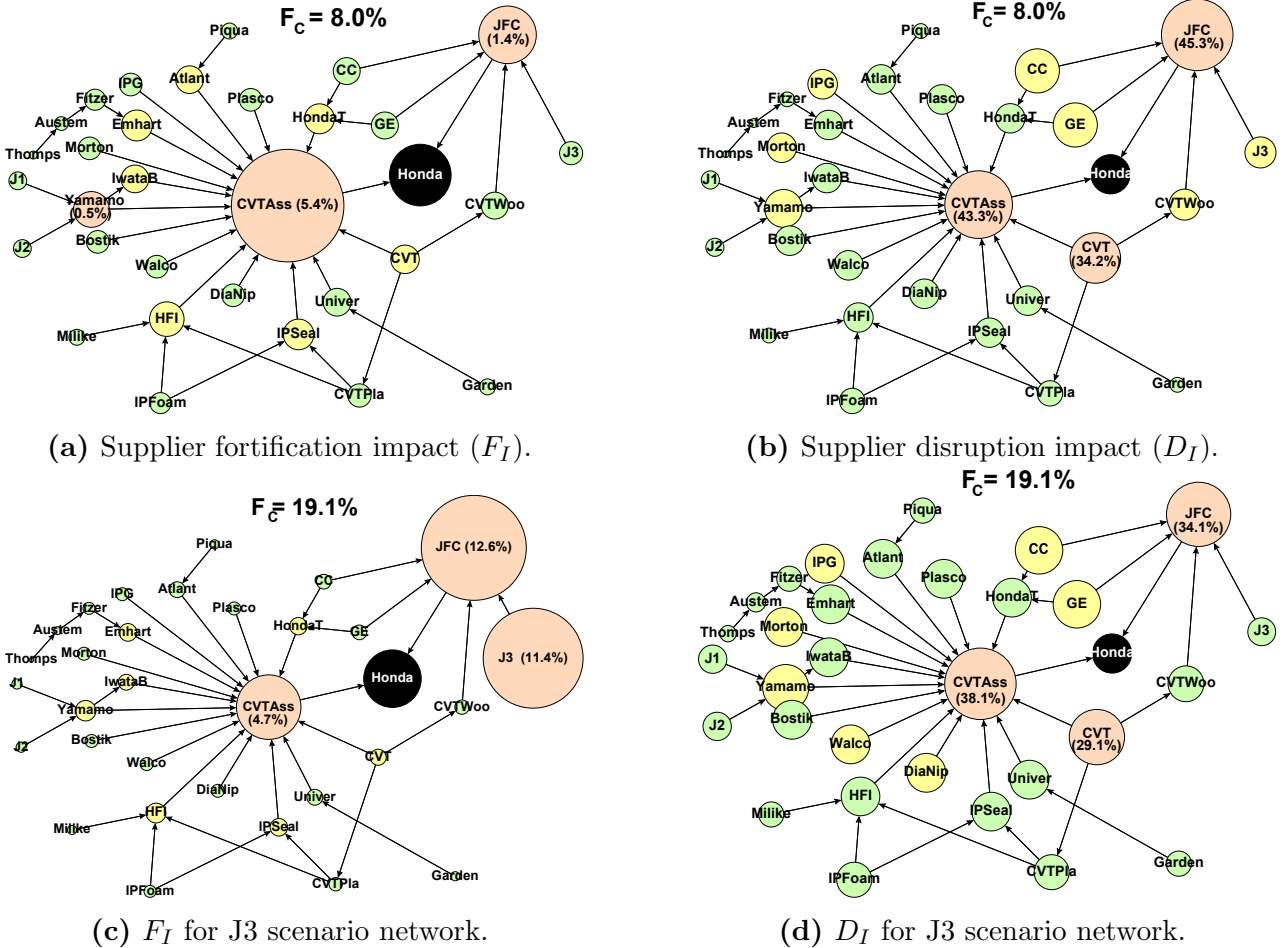
whose number grows exponentially as a function of the number of nodes (Darwiche 2003). There are efficient algorithms for the numerical analysis of large networks. We use the jointree (or, junction tree) algorithm of the Bayes net toolbox for MATLAB (Murphy 2001). All network graphics are produced with Pajek (Batagelj and Mrvar 2003).

### 5.3.1. Illustrative example: Honda Accord center console

We consider the Honda Accord center console network presented in Choi and Hong (2002) and Kim et al. (2011). The network has 32 suppliers (two first tier, 19 second tier, 8 third tier, and two further tier suppliers) and 38 arcs. With the basic formulation, the corresponding BN would have 65 682 parameters. We use the noisy-OR formulation, which has 216 parameters. We do not have probabilistic risk data for this network and thus, for illustrative purposes, we assume that the independent probability for disruption at each supplier ( $\alpha_i$ ) is 1%, and that each parent supplier’s disruption spreads to a customer ( $\beta_{i|j}$ ) with 50% probability. We note that the first value corresponds to “high reliability” in the similar approach by Adenso-Diaz et al. (2012), the second is not directly comparable because Adenso-Diaz et al. model dependencies with a deterministic model ( $\beta_{i|j} = 0$  or 1). With our setup, the risk of disruption at Honda  $F_C = 8\%$  and at first tier suppliers CVTAssembly  $F_{CVTAss} = 11\%$  and JFC  $F_{JFC} = 3\%$ , respectively.

Figure 6 illustrates the importance of each supplier measured with Supplier Fortification Impact ( $F_I$ ) and Supplier Disruption Impact ( $D_I$ ). The numerical values of these measures are given to Top-3 suppliers in each case. In the upper networks, each supplier has the same parameter values. In this case, the first tier supplier CVT Assembly is the best candidate for improvement actions:  $F_I(CVTAss) = 5.4\%$ -points which means that Honda’s disruption risk would drop from 8.0% to 2.6%, in case the disruption risk at CVT Assembly would be zero. CVT Assembly is also important from structural perspective, i.e., the rest of the network cannot protect its disruption well:  $D_I(CVTAss) = 43.3\%$  points which means that a sure disruption at this supplier increases Honda’s disruption risk from 8.0% to 51.3%. Note, however, that the supplier JFC is more important when measured with supplier disruption impact  $D_I$ . But it is

also far more reliable, which explains why potential improvement actions are more effective at (less reliable) CVT Assembly. The most important second tier supplier when measured with  $F_I$  is Yamamoru. It has two parent suppliers and two customers which makes it relatively more risky than, e.g., Bostik, Walco, or J3, who have only one customer and no parents at all.



**Figure 6** Risk importances of suppliers in the Honda Accord network. Upper figures are for network with  $\alpha_i = 0.01$  and  $\beta_{i|j} = 0.5$ . In lower figures,  $\alpha_{J3} = 0.5$ .

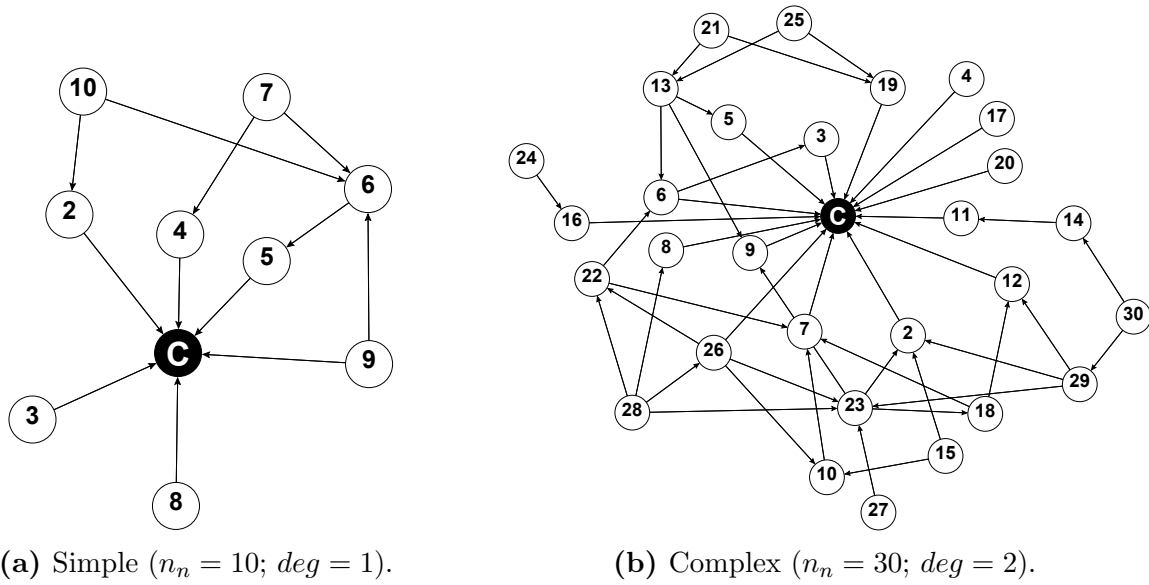
The risk maps in the bottom of Figure 6 have the same network and parameters except for supplier J3, whose risk of disruption  $F_{J3} = 50\%$  instead of 1%. This exemplifies a situation where J3 becomes very risky but is not yet disrupted (e.g., there is a severe risk of disruptive labor strike in the company). This would increase Honda’s risk from 8.0% to 19.1%, because its first tier supplier JFC would become more risky (3.2%  $\rightarrow$  27.0%). As a result, as can be seen from the  $F_I$  risk map in Figure 6, the focus of risk mitigation should be moved from CVT Assembly to JFC or J3. Note that this risky J3 scenario gives largely similar ranking of nodes

when ordering with  $D_I$  risk measures. This is because the system structure does not change and thus the system’s ability to resist disruption at a certain node has not changed significantly.

### 5.3.2. Simulation-based results: Impact of complexity

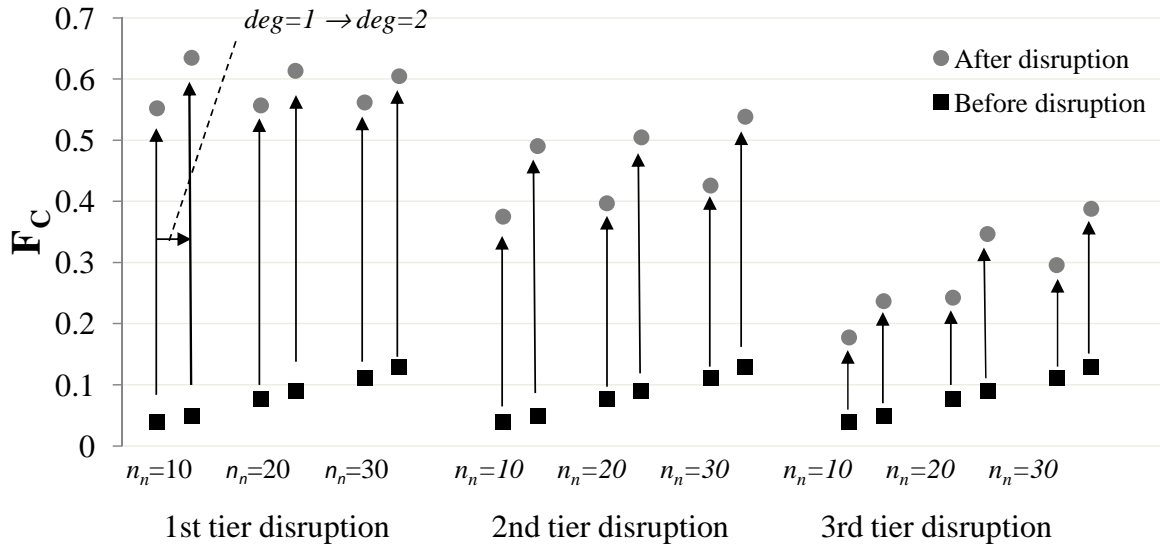
The Honda example illustrates how risk maps can be used to identify risky suppliers in a specific supply network. Next, we study how network complexity, in general, impacts the disruption risks. Craighead et al. (2007) study supply chain disruptions empirically and propose that a disruption in a complex supply chain is likely to be more severe than a disruption in a less complex supply chain. They measure complexity by the number of nodes and arcs. The logic is that the more interdependencies there are among the nodes, the more probable it is that a disruption propagates in the network (and vice versa). In their study of network complexity and reliability, Adenso-Diaz et al. (2012) identify which design parameters impact the static network reliability the most. This differs from our approach in that we are more interested in the change in reliability (or, risk) due to a possible disruption or the elimination of the possibility of disruption, not only the reliability of a network in *status quo*.

We generate random networks of varying complexity level and simulate disruptions in these networks. The networks are generated with Pajek’s Bernoulli-Poisson algorithm (see Batagelj and Mrvar 2003 for details). The algorithm requires two inputs: i) the number of nodes ( $n_n$ ) and ii) the average degree ( $deg$ ). The latter is a measure of node connectivity and it is calculated with:  $deg = d \cdot (n_a - 1)$ , where  $d$  is the graph density (number of arcs divided by maximum amount of arcs) and  $n_a$  is the number of arcs; thus the higher the degree, the more arcs there are in the network. This kind of graph has from 1 to  $N$  sinks. To create a network with exactly one sink –the focal company– one of the sinks is selected at random and the other sinks are connected to it (making them first tier suppliers). We considered six different networks with  $n_n = \{10, 20, 30\} \times deg = \{1, 2\}$ , which are of the same scale as low and high levels of complexity in Adenso-Diaz et al. (2012). Examples of a simple network and a complex network are in Figure 7.



**Figure 7** Examples instances of random networks used in simulation.

To study disruptions, one node is selected at random, and it is then assumed that there is a disruption at this node. The impact of this disruption is then calculated as the increase in supply risk  $F_C$ . With same network parameters as in the Honda example ( $\alpha_i = 0.01$ ,  $\beta_{i|j} = 0.5$ ), the risk before the random disruption varies between 0.04 (average for the least complex networks) and 0.12 (the most complex networks). The results in Figure 8 are based on averages from 1000 simulations with each of the six network parameter pairs  $n_n \times deg$ . The  $y$ -axis shows the risk level  $F_C$  before and after a randomly selected supplier is disrupted. Separate results are given based on the supplier's tier (in case 3rd tier or less). With our modeling approach, the more nodes or arcs there are (other things being equal), the more risky a network is; this can be observed by the black squares in the Figure (complexity increases to the right). There is also a marked rise in both risk before the disruption and risk after the disruption when the average degree increases from one to two. This because a higher degree means that there are more links between suppliers so that disruptions spread more easily. The absolute increase in  $F_C$  is of the same scale for all networks. However, the relative risk increase (circle divided by square) differs by a large margin: for example, for a network with ten nodes the average increase in risk caused by disruption at a second tier supplier is tenfold, where for a network with 30 nodes, the risk is only four times higher.

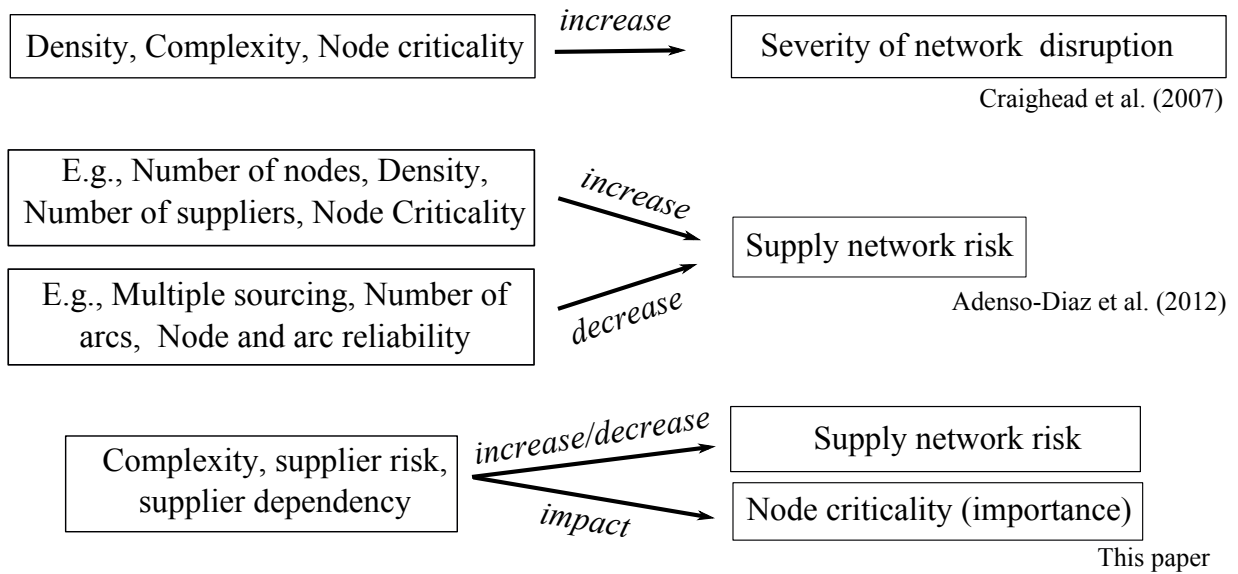


**Figure 8** Average impact of random distribution for focal company's risk  $F_C$ .

These results suggest that network complexity can either increase or decrease the severity of a disruption. Results based on analysis with constant parameter values for  $\alpha$  and  $\beta$  across simulations indicate that complex networks tend to be riskier because they contain more possible disruption sources and/or links for propagation of the disruption. Indeed, the risk of disruption at the focal company after a random disruption in the network seems to be higher in complex networks. On the other hand, the relative increase in focal company's risk level is higher for less complex networks. In the above example, in the case of high connectedness ( $deg = 2$ ) and first tier disruption, even the absolute risk level is higher for network with ten nodes, compared to  $n_n = 20$  or 30. This is intuitive: a streamlined supply chain, where most supplier relationships are deep and collaborative, has fewer disruption sources but in the less likely event of something disruptive happening, such a supply network may be less able to recover than a more complex supply chain which is less dependent on individual suppliers. This has also been proposed by Choi and Krause (2006) who argue that *both* the non-complex end and the high-complexity end of the complexity continuum are risky. They propose that it is less risky to be in the middle, where dependencies are not overly high but there is still a manageable number of suppliers. Adenso-Diaz et al. (2012), on the other hand, argue that increasing the number of nodes increases risks as well, whereas high number of arcs decreases the probability of disruption.

## 6. Discussion

The results show that, on one hand, the supply network’s total risk is dependent on both the network structure and individual supplier’s attributes and, on the other hand, that the importance that a supplier has for network reliability depends on the supplier’s reliability and its position in the network relative to other suppliers. In earlier studies (Craighead et al. 2007; Adenso-Diaz et al. 2012), node criticality has been one of the inputs of network risk. In our approach, however, node criticality is defined after the node’s impact on the network risk is analyzed. This is done by assessing how a node’s disruption or fortification would impact the total network risk. The difference between the earlier approaches and ours is illustrated in Figure 9.



**Figure 9** Supply network characteristics and their impact on supply network risk in earlier studies and this paper.

We provide next a classification matrix for supplier criticality based on reliability and dependency. Then, some guidelines about the impact of supplier’s position in the network are provided. Finally, it is discussed how risk importance measures can support managerial decision making related to risk mitigation.



**Reliability and dependency are critical in supplier evaluation.** As discussed in Section 5.1, even the most reliable supplier can be risky if the dependency on the supplier is high; this is often the case in single-supply situations. Then again, with multiple suppliers, a particular supplier can be unreliable but also dependency on it is, on average, lower. When the risk level of a supplier is evaluated, its reliability ( $\alpha_i$ ) and dependency ( $\beta_{i|j}$ ) are equally critical attributes to consider. Table III can be used to classify suppliers based on these two attributes.

**Table III** Supplier classification based on reliability and dependence.

Low reliability	Risky supplier, but dependency is low; e.g., one-out-of-many, back-up supplier available, material or service not critical	Critical supplier; e.g, sole supplier of unreliable technology or otherwise context specific material or service
High reliability	Non-critical supplier	Supplier is a potential risk-source because of high-dependency; e.g., single-supplier, access to scarce technology or raw material
	Low dependency	High dependency

**Network structure and supplier’s position are critical in supplier evaluation.**

These attributes can have either increasing or decreasing impact on supplier’s importance, and Adenso-Diaz et al. (2012) even conclude that the design of network is more important than the reliability of network components. We considered some basic network structures in Section 5.2 and introduced the concept “disruption flow”. This analysis suggested, for example, that closeness to focal company increases risk importance, but that a second tier supplier can still be more important than a first tier supplier. The Honda example also illustrated how the fact that a node has many parents, i.e., serves as a hub in a network (like CVT Assembly in Honda’s supply base) can make it critical. Simulations of disruptions in large networks indicated that complexity can make disruptions less severe compared to a simple network, if one considers the relative increase in risk. These simulations also show that even a third tier disruption can increase the disruption risk at the focal company. To summarize:

- Suppliers who are closer to the focal company tend to pose greater risks
- High number of parents makes a supplier more risky compared to a supplier with less or no parents (all other things equal), and thus high amount of parents increases supplier importance
- If a node is a supplier for many other nodes, it is also a potential disruption source for these nodes, which makes it more important
- Nodes which have more siblings are less important compared to ones with fewer siblings, because these nodes are unable to “block” disruptions of parent supplier(s)

**There are two complementary ways to prioritize suppliers for risk mitigation actions.** Consider two kind of risk mitigation actions: i) those that are targeted for improving the reliability of existing suppliers, and ii) those that aim to improve reliability by changing the network configuration or design. Examples of reliability improvement actions include quality improvement programs, supplier contracts with reliability incentives, or increasing safety stock at a supplier. The latter category consists of actions such as introduction of new suppliers or back-up suppliers, or acquisition of a critical supplier (vertical integration). Also in this

category, one could include considerations related to risks of outsourcing: for example, if one out of three supplier nodes is to be outsourced, it can be critical to assess how the total absence of the node (bankruptcy, acquisition) would impact the network risk.

In probabilistic risk analysis, Fortification Impact types of measures are used to rank components (Cheok et al. 1998; Zio 2011): high Fortification Impact implies that the failure of a supplier contributes significantly to the total risk, so the improvements are most efficient here. High Disruption Impact implies that the supplier has a big role in preventing the occurrence of a disruption at the focal company, or that the rest of the system does not protect well from a disruption at the supplier. Thus, it can be used in decisions related to outsourcing above, i.e., to find critical suppliers (the removal of which would be critical). Disruption Impact is also suitable for supply network design decision at large, but for such high impact decisions it is advisable to use  $D_I$  and  $F_I$  combined (Van der Borst and Schoonakker 2001).

**Table IV** Implications of Supplier Fortification Impact ( $F_I$ ) and Supplier Disruption Impact ( $D_I$ ) (modified from Van der Borst and Schoonakker 2001).

High $D_I$	Supplier is not a big contributor to the overall risk, but its disruption can have severe implications; e.g., a supplier of customized screws, or the sole energy supplier in an isolated area	Supplier is critical and has a big impact on total risk and is important in preventing disruptions; key targets for improvement actions and supply network design.
Low $D_I$	Supplier is not significant; there is potential to relax reliability; e.g., lower quality requirements for cost savings)	Supplier is a big contributor for the overall risk, but the system can tolerate its disruption relatively well; a good candidate for reliability improvement actions.
	Low $F_I$	High $F_I$

Table IV summarizes the information in risk measures introduced in this paper. For decision making, especially the low-low and high-high corners of Table IV deserve emphasis: in the first, one can find potential candidates for reliability relaxations (where the objective is reducing costs, for example) and in the second, the best candidates for improvements.

## 7. Conclusions

We have developed a methodology based on Bayesian networks and Probabilistic Risk Analysis (PRA) for analyzing risks in supply networks. Properties of Bayesian supply networks were discussed and using various examples, managerial insights were drawn to support risk informed decision making. In particular, these insights relate to questions of whether single-supply is riskier than multiple-supply, and how complexity impacts the risks that stem from the supply base. The proposed methodology can be used to answer these questions quickly, effectively, and in an intuitive manner. We argue that the methodology could thus serve as a backbone for risk visualization, disruption management, and supply network redesign tool proposed for network reliability enhancements by Blackhurst et al. (2011). The use of methodology requires addressing challenges such as: How to estimate disruption probabilities? What is the adequate level of detail when modeling the supply network? There is, however, some evidence that these challenges can be addressed: Deleris and Erhun (2011) report a case study where supply chain managers participated successfully in PRA based supply risk management process.

Supply network analysis and supply risk analysis are recent streams in operations management and we argue that the latter can benefit enormously from the former: other fields such as finance or transportation have demonstrated that modern risk management in man-made systems require a systemic view, as exemplified by the expansion of US housing bubble to a global financial crisis in 2008, or the eruption of Icelandic volcano that caused a severe and global air travel disruption in 2010. Earlier supply network risk assessment studies that utilize PRA methodology (e.g., Lockamy and McCormack 2010; Deleris and Erhun 2011) have focused on detailed mapping of various sources of risk. Our approach differs from these in that we focus on suppliers as the sole disruption source, which allows us to study the relationship between supply network structure and supply risk. What is lost in details, is compensated for by gaining a more systemic view of the supply network and risk.

Our results can be extended in various ways. First, the time dimension could be added. Some disruptions might last for few days, whereas others might disable a supplier for months.

Dynamic Bayesian networks could be applied to take the length of disruption into account. Second, the methodology does not restrict the number of states a supplier could have. We have only considered 100% functional and 100% disrupted suppliers; it would be interesting to study, e.g., how adding a state for 50% functionality would impact suppliers' risk importance. Third, the methodology should be validated in a real business environment. Supply chain mapping has become increasingly important (Gardner and Cooper 2003), and combining supply maps with risk data from interviews, audits, and operations data would provide a straightforward way to test the proposed methodology in practice. Because risk management is a strategic function with long time horizon, longitudinal studies could be particularly valuable.

## References

- Adenso-Diaz, B., Mena, C., García-Carbajal, S., and Liechty, M. 2012. "The Impact of Supply Network Characteristics on Reliability." *Supply Chain Management: An International Journal* 17 (3): 263–276.
- Amini, H., Cont, R., and Minca, A. 2012. "Stress Testing the Resilience of Financial Networks." *International Journal of Theoretical and Applied Finance* 15 (1): 1–20.
- Batagelj, V. and Mrvar, A. 2003. "Pajek: Analysis and Visualization of Large Networks." In *Graph Drawing Software*, 77–103. Springer Series in Mathematics and Visualization.
- Bedford, T. and Cooke, R. 2001. *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, New York.
- Bellamy, M. A. and Basole, R. C. 2012. "Network Analysis of Supply Chain Systems: A Systematic Review and Future Research." *Systems Engineering* 16 (2): 1–20.
- Blackhurst, J., Dunn, K. S., and Craighead, C. W. 2011. "An Empirically Derived Framework of Global Supply Resiliency." *Journal of Business Logistics* 32 (4): 374–391.
- Blome, C. and Henke, M. 2009. "Single Versus Multiple Sourcing: A Supply Risk Management Perspective." In *Supply Chain Risk*, 125–135. Springer Science+Business Media, LLC, New York.

- Borgonovo, E. and Apostolakis, G. 2001. "A New Importance Measure for Risk-Informed Decision Making." *Reliability Engineering and System Safety* 72 (2): 193–212.
- Buhman, C., Kekre, S., and Singhal, J. 2005. "Interdisciplinary and Interorganizational Research: Establishing the Science of Enterprise Networks." *Production and Operations Management* 14 (4): 493–513.
- Cheok, M. C., Parry, G. W., and Sherry, R. R. 1998. "Use of Importance Measures in Risk-Informed Regulatory Applications." *Reliability Engineering and System Safety* 60 (3): 213–226.
- Choi, T. Y., Dooley, K. J., and Rungtusanatham, M. 2001. "Supply Networks and Complex Adaptive Systems: Control Versus Emergence." *Journal of Operations Management* 19 (3): 351–366.
- Choi, T. Y. and Hong, Y. 2002. "Unveiling the Structure of Supply Networks: Case Studies in Honda, Acura, and DaimlerChrysler." *Journal of Operations Management* 20 (5): 469–493.
- Choi, T. Y. and Krause, D. R. 2006. "The Supply Base and Its Complexity: Implications for Transaction Costs, Risks, Responsiveness, and Innovation." *Journal of Operations Management* 24 (5): 637–652.
- Choi, T. and Wu, Z. 2008. "Triads in Supply Networks: Theorizing Buyer-Supplier-Supplier Relationships." *Journal of Supply Chain Management* 45 (1): 8–25.
- Christopher, M. and Peck, H. 2004. "Building the Resilient Supply Chain." *International Journal of Logistics Management* 15 (2): 1–13.
- Craighead, C., Blackhurst, J., Rungtusanatham, M. J., and Handfield, R. B. 2007. "The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities." *Decision Sciences* 38 (1): 131–156.
- Darwiche, A. 2003. "A Differential Approach to Inference in Bayesian Networks." *Journal of the ACM* 50 (3): 280–305.
- . 2009. *Modeling and Reasoning with Bayesian Networks*. Cambridge University Press, New York.

- Darwiche, A. 2010. "Bayesian Networks." *Communications of the ACM* 53 (12): 80–90.
- Deleris, L. A. and Erhun, F. 2011. "Quantitative Risk Assessment in Supply Chains: A Case Study Based on Engineering Risk Analysis Concepts." In *Planning Production and Inventories in the Extended Enterprise*, edited by K. G. Kempf, P. Keskinocak, and R. Uzsoy. Springer Science+Business Media, LLC, New York.
- Druzdzel, M. J. and Van Der Gaag, L. C. 2000. "Building Probabilistic Networks: "Where Do the Numbers Come From?"" *IEEE Transactions on Knowledge and Data Engineering* 12 (4): 481–486.
- Gardner, J. T. and Cooper, M. C. 2003. "Strategic Supply Chain Mapping Approaches." *Journal Of Business Logistics* 24 (2): 37–64.
- Hendricks, K. B. and Singhal, V. R. 2005. "Association Between Supply Chain Glitches and Operating Performance." *Management Science* 51 (5): 695–711.
- Henry, M. H. and Haimes, Y. Y. 2006. "A Comprehensive Network Security Risk Model for Process Control Networks." *Risk Analysis* 29 (2): 223–248.
- Holmgren, Å. J. 2006. "Using Graph Models to Analyze the Vulnerability of Electric Power Networks." *Risk Analysis* 26 (4): 955–969.
- Kao, H.-Y., Huang, C.-H., and Li, H.-L. 2005. "Supply Chain Diagnostics with Dynamic Bayesian Networks." *Computers & Industrial Engineering* 49 (2): 339–347.
- Kim, Y., Choi, T. Y., Yan, T., and Dooley, K. 2011. "Structural Investigation of Supply Networks: A Social Network Analysis Approach." *Journal of Operations Management* 29 (3): 194–211.
- Kleindorfer, P. R. and Saad, G. H. 2006. "Managing Disruption Risks in Supply Chains." *Production and Operations Management* 14 (1): 53–68.
- Koonce, A., Apostolakis, G. E., and Cook, B. 2008. "Bulk Power Risk Analysis: Ranking Infrastructure Elements According to Their Risk Significance." *Electrical Power and Energy Systems* 30 (3): 169–183.

- Langseth, H. and Portinale, L. 2007. "Bayesian Networks in Reliability." *Reliability Engineering and System Safety* 92 (1): 92–108.
- Lockamy, A., III and McCormack, K. 2010. "Analysing Risks in Supply Networks to Facilitate Outsourcing Decisions." *International Journal of Production Research* 48 (2): 593–611.
- Manuj, I. and Mentzer, J. T. 2008. "Global Supply Chain Risk Management." *Journal of Business Logistics* 29 (1): 133–155.
- Murphy, K. P. 2001. "The Bayes Net Toolbox for Matlab." *Computing science and statistics* 33 (2): 1024–1034.
- Narasimhan, R., Talluri, S., and Mahapatra, S. K. 2006. "Multiproduct, Multicriteria Model for Supplier Selection with Product Life-Cycle Considerations." *Decision Sciences* 37 (4): 577–603.
- Paté-Cornell, E. 1996. "Global Risk Management." *Journal of Risk and Uncertainty* 12 (2–3): 239–255.
- Patel-Predd, P. 2009. "The Trouble With Touch Screens." *IEEE Spectrum* on-line. Available at <http://http://spectrum.ieee.org/consumer-electronics/gadgets/the-trouble-with-touch-screens>.
- Pearl, J. 1988. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann Publishers, San Mateo, CA.
- . 2000. *Causality: Models, Reasoning and Inference*. Cambridge University Press, Cambridge, UK.
- Qi, L., Shen, Z.-J. M., and Snyder, L. V. 2010. "The Effect of Supply Disruptions on Supply Chain Design Decisions." *Transportation Science* 44 (2): 274–289.
- Ramirez-Marquez, J. E. and Coit, D. W. 2005. "Composite Importance Measures for Multi-State Systems With Multi-State Components." *IEEE Transactions on Reliability* 54 (3): 517–529.
- SCC. 2010. *Supply Chain Operations Reference Model version 10.0*. Supply-Chain Council, Inc.



- Schmitt, A. J. and Singh, M. 2011. *A Quantitative Analysis of Disruption Risk in a Multi-Echelon Supply Chain*. Working Paper, Center for Transportation and Logistics, MIT. Available at: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1463417](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1463417).
- Sheffi, Y. 2005. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. The MIT Press, Cambridge.
- Simchi-Levi, D. 2010. "Operations Rules: Delivering Customer Value through Flexible Operations." Chap. 4: Procurement and supply contracts as competitive weapons in, First. The MIT Press, Cambridge, MA.
- Snyder, L. V., Atan, Z., Peng, P., Rong, Y., Schmitt, A. J., and Sinssoysal, B. 2010. "OR/MS Models for Supply Chain Disruptions: A Review." Submitted for publication. Available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1689882](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689882).
- Sodhi, M. S., Son, B.-G., and Tang, C. S. 2012. "Researchers' Perspectives on Supply Chain Risk Management." *Production and Operations Management* 21 (1): 1–13.
- Stamatelatos, M., Dezfuli, H., Apostolakis, G., Everline, C., Guarro, S., Mathias, D., Mosleh, A., Paulos, T., Riha, D., and Smith, C. 2011. "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners." Office of Safety and Mission Assurance, NASA, Washington, DC.
- Tang, C. S. 2006. "Review: Perspectives in Supply Chain Risk Management." *International Journal of Production Economics* 103 (2): 451–488.
- Tomlin, B. 2006. "On the Value of Mitigation and Contingency Strategies for Managing Supply Chain Disruption Risks." *Management Science* 52 (5): 639–657.
- Toppila, A. and Salo, A. 2013. "A Computational Framework for Prioritization of Events in Fault Tree Analysis Under Interval-Valued Probabilities." *IEEE Transactions on Reliability* 62 (3): 583–595.
- Van der Borst, M. and Schoonakker, H. 2001. "An Overview of PSA Importance Measures." *Reliability Engineering and System Safety* 72 (3): 241–245.
- Wagner, S. M. and Bode, C. 2008. "An Empirical Examination of Supply Chain Performance Along Several Dimensions of Risk." *Journal of Business Logistics* 29 (1): 307–324.

- Wu, T., Blackhurst, J., and Chidambaram, V. 2006. “A Model for Inbound Supply Risk Analysis.” *Computers in industry* 57 (4): 350–365.
- Wu, T., Blackhurst, J., and O’Grady, P. 2007. “Methodology for Supply Chain Disruption Analysis.” *International Journal of Production Research* 45 (7): 1665–1682.
- Wu, Z. and Choi, T. Y. 2005. “Supplier–Supplier Relationships in the Buyer–Supplier Triad: Building Theories from Eight Case Studies.” *Journal of Operations Management* 24 (1): 27–52.
- Zagorecki, A. and Druzdzel, M. J. 2004. “An Empirical Study of Probability Elicitation Under Noisy-OR Assumption.” In *FLAIRS Conference*, 880–886.
- Zio, E. 2011. “Risk Importance Measures.” In *Safety and Risk Modeling and Its Applications*, edited by H. Pham. Springer Series in Reliability Engineering, Springer-Verlag, London.
- Zsidisin, G. A., Melnyk, S. A., and Ragatz, G. L. 2005. “An Institutional Theory Perspective of Business Continuity Planning for Purchasing And Supply Management.” *International Journal of Production Research* 43 (16): 3401–3420.
- Zsidisin, G. A., Panelli, A., and Upton, R. 2000. “Purchasing Organization Involvement in Risk Assessments, Contingency Plans, and Risk Management: An Exploratory Study.” *Supply Chain Management* 5 (4): 187–197.

## Appendix

### Bayesian networks and noisy-OR model

Consider a simple triad network  $1 \rightarrow C \leftarrow 2$  (such as the example in Table I). Altogether, there are eight possible states of the world:  $\{\bar{C}, \bar{1}, \bar{2}\}, \{\bar{C}, \bar{1}, 2\}, \dots, \{C, 1, 2\}$ . For a single node  $X$  with parents  $\mathbf{U}$ , the probability of state  $x$  when parents are in state  $\mathbf{u}$  is  $\Pr(x|\mathbf{u})$  with  $\sum_x \Pr(x|\mathbf{u}) = 1$  for all  $\mathbf{u}$ . To resolve a probabilistic query for a particular network instantiation  $\mathbf{z}$ , one simply calculates the product of all probabilities  $\Pr(x|\mathbf{u}) = \theta_{x|\mathbf{u}}$  where  $x|\mathbf{u}$  is compatible with  $\mathbf{z}$

(denoted with  $\theta_{x|\mathbf{u}} \sim \mathbf{z}$ ), which means that they agree on the values of their common variables. For example, with network  $1 \rightarrow C \leftarrow 2$ , the probability of  $\mathbf{z} = \{C, \bar{1}, 2\}$  (focal company  $C$  and supplier 2 disrupted, supplier 1 functional) is  $\Pr(\mathbf{z}) = \Pr(\bar{1})\Pr(2)\Pr(C|\bar{1})\Pr(C|2)$ . The marginal probability of  $C$  being disrupted can be calculated as the sum of mutually exclusive instantiations  $\{C, 1, 2\}, \{C, \bar{1}, 2\}, \{C, 1, \bar{2}\}, \{C, \bar{1}, \bar{2}\}$ . In general, the semantics of a Bayesian network are given by a so-called chain rule (Darwiche 2009): if  $x\mathbf{u}$  denotes a family (node and its parents),  $\Pr(x|\mathbf{u}) = \theta_{x|\mathbf{u}}$ , and  $\theta_{x|\mathbf{u}} \sim \mathbf{z}$ , then

$$\Pr(\mathbf{z}) \stackrel{def}{=} \prod_{\theta_{x|\mathbf{u}} \sim \mathbf{z}} \theta_{x|\mathbf{u}}. \quad (7.1)$$

For a detailed discussion of calculating with Bayesian networks, we refer the reader to Darwiche (2009), Chapter 4.

In the noisy-OR model, interactions are treated implicitly. It is assumed that an “effect” (here, a disruption) at node  $X$  can happen independently (with probability  $\theta_x$ ) and because of parent  $i$  being “active” (w.p.  $\theta_{x|i}$ ). If node  $X$  has  $1\dots N$  parents and the set  $\mathcal{I}$  contains the indices of parents that are “active” (in our case, disrupted), then the probability of disruption at  $X$ , conditioned on  $\mathcal{I}$ , is

$$\Pr(X|\mathcal{I}) = 1 - (1 - \theta_x) \prod_{i \in \mathcal{I}} \theta_{x|i}. \quad (7.2)$$

For derivation of (7.2), see Darwiche 2009, Section 5.4. To emphasize the different nature of the two parameter types required for noisy-OR formulation, we denote:  $\theta_x = \alpha_x$  and  $\theta_{x|i} = \beta_{x|i}$ .

And example of a noisy-OR node with  $n = 2$  parents is in Table I. Note that the amount parameters required is not  $2^n = 2^2 = 4$  but  $n+1 = 2+1 = 3$ . What is lost in this approximation is the ability to model situations in which, e.g., two suppliers fail at the same time so that the resulting risk is higher than the risk of two suppliers failing independently. However, in other application it has been found that noisy-OR can even improve the model accuracy (Druzdzel and Van Der Gaag 2000; Zagorecki and Druzdzel 2004): when using expert knowledge in probability estimation, complex interaction terms might be impossible to assess and thus ignoring might

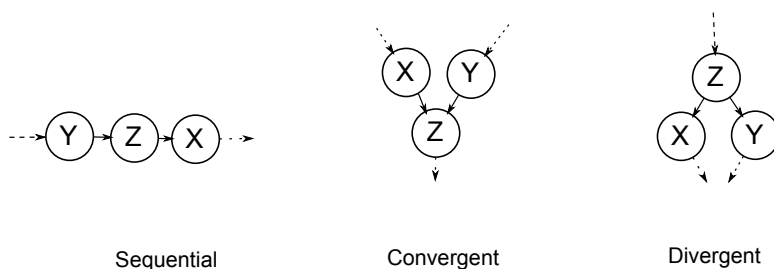
produce better input for the model. We model all nodes with multiple parents as noisy-OR nodes.

## Dependencies in Bayesian networks and d-separation

In the definition of d-separation, the term blocking requires further clarification. Darwiche (2009) uses the concept of valves and defines that  $\mathbf{Z}$  blocks a path if at least one valve in the path is blocked given  $\mathbf{Z}$ . The three types of valves are given in Figure 10. The rules for valve being closed are as follows:

- A sequential valve ( $\rightarrow \mathbf{Z} \rightarrow$ ) is closed given  $\mathbf{Z}$
- A convergent valve ( $\rightarrow \mathbf{Z} \leftarrow$ ) is closed if  $\mathbf{Z}$  is not given
- A divergent valve ( $\leftarrow \mathbf{Z} \rightarrow$ ) is closed given  $\mathbf{Z}$
- As a special case, a path with no valves (i.e.,  $\mathbf{X} \rightarrow \mathbf{Y}$ ) is never blocked

In the example of Figure 3, the path between 1 and 2 contains one valve  $1 \leftarrow 3 \rightarrow 2$  which is not closed unless 3 is known, and thus, 1 and 2 are not d-separated. D-separation implies



**Figure 10** Valves in a network.

all sorts of properties for Bayesian networks. We utilize mostly the implication of probabilistic independence between d-separated sets; for further properties and details of d-separation, see Darwiche (2009), Section 4.5.