# Identification of Critical Groups and Other Supply Chain Vulnerabilities

Tim vor der Brück
*Department of Computer Science*
*Distance University of Switzerland (FFHS)*
Brig, Switzerland
email: tim.vorderbrueck@ffhs.ch

***Abstract*—The impact of a supplier or transportation link breakdown in a supply chain can strongly differ depending on which nodes/links are affected. While the breakdown of producers of rarely needed products or backup suppliers might result in no or only minor repercussions, the breakdown of central suppliers or transportation links, also called critical nodes/links, can be fatal and may cause a severe delivery delay or even a complete production failure of certain product lines. Therefore, it is of high importance for a company to identify its critical nodes/links in the supply chain and take precautionary actions such as organizing additional backup suppliers or alternative ways of transportation. In this paper, we describe a novel method to identify critical groups, nodes, and links in a supply chain based on robust optimization, which has the advantage that supply chain risks are considered, and also precise risk cost estimates regarding the possible breakdown of each supplier node are provided. Afterwards, we introduce the concept of *Critical Groups*, which is a generalization of *Critical Nodes* to potentially more than one supplier. Finally, we demonstrate this method on an example supply chain and discuss its distribution of critical nodes, links, and groups.**

***Keywords*—supply chain management; critical nodes; critical groups; critical links; robust optimization; supply chain risks.**

## I. Introduction

Note that this paper is an extended version of [1]. In comparison to the original paper, we revised and extended our optimization model to include change-over costs and fixed penalties. In addition, we discuss an important generalization of *critical nodes* that we term *critical groups*.

Supply chain disruption may cause severe loss of sales and revenue. Therefore, a thorough risk analysis of the supply chain is of high importance. Falasca et al. [2] identified three major determinants of supply chain risks, which are:

- Density (cf. Figure 1)
- Complexity (cf. Figure 2)
- Critical Nodes (cf. Figure 3)

The first determinant of supply chain risks according to Falasca et al., supplier density relates to the number of suppliers residing inside a certain region. In this paper, we slightly generalize the concept of density according to Falasca and Craighead [2], [3] and also refer to a high density if a high number of suppliers reside in the same country even if these suppliers might not be geographically located close to each other. A high density increases the probability of joint supplier failures due to similar geological, economic, or political influences on neighboring suppliers. We will call a group of neighboring suppliers with a high joint dropout impact a critical group.

Craighead et al. [3] assess the complexity of a supply chain, which is the second determinant of supply chain risks, by the number of its nodes (suppliers) and edges (transportation links). The more complex the supply chain is, the higher can be the supply chain risk since a highly complex supply chain structure can complicate the logistics as well as the production processes. However, the authors point out that a high complexity can also mean that the supply chain contains redundancies and backup suppliers, which would increase its resilience. Consider as an example the supply chain in Figure 2. If supplier *A* breaks down on the low-complexity supply chain on the left subfigure, the whole chain is interrupted and non-operational because the goods on the left side of the subfigure can no longer be transported to any of the suppliers on the right side. However, on the more complex supply chain on the right subfigure, supplier *A* can partly be bypassed by nodes *B* and *C*, which effectively mitigates a potential failure of node *A*. Thus, the effect that a high complexity has on the supply chain risk is not as clear as for the other two determinants (density and critical nodes). Therefore, we chose not to propose an assessment measure for supply chain complexity and will not discuss this topic any further in the remainder of this paper.

Finally, the third determinant of supply chain risk is given by its critical nodes. Craighead et al. [3] define criticality as the relative importance of a given node or set of nodes within a supply chain (see Figure 3). A breakdown of a critical node has typically severe implications, such as serious delay or even a complete collapse of the production process for certain product lines, which can result in non-fulfillment of customer demand. Consequently, the affected company suffers lost revenue and faces a potential non-delivery contract penalty. Thus, it is of great importance to identify the critical nodes in the supply chain and mitigate their possible breakdown risks by implementing precautionary measures such as organizing backup suppliers.

The concept of critical nodes can also be transferred to important transportation links. A link in a supply chain denotes a certain transport mode (e.g., airplane, truck, or ship transportation) and a route between two suppliers or between a supplier and a customer. Analog to the definition of critical nodes, a critical link denotes a link that is of high importance for the total supply chain. Critical links should therefore be secured by identifying alternative means of transportation.

The rest of the paper is structured as follows. Related work is given in the upcoming section (Section II). The employed optimization model is given in Section III. In Section IV, we

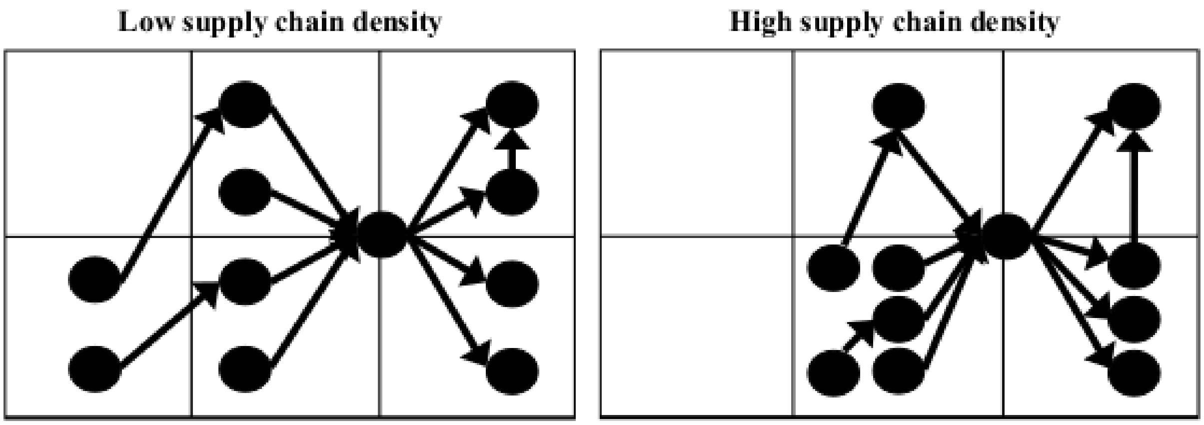


Fig. 1. Different degrees of supply chain density [2].

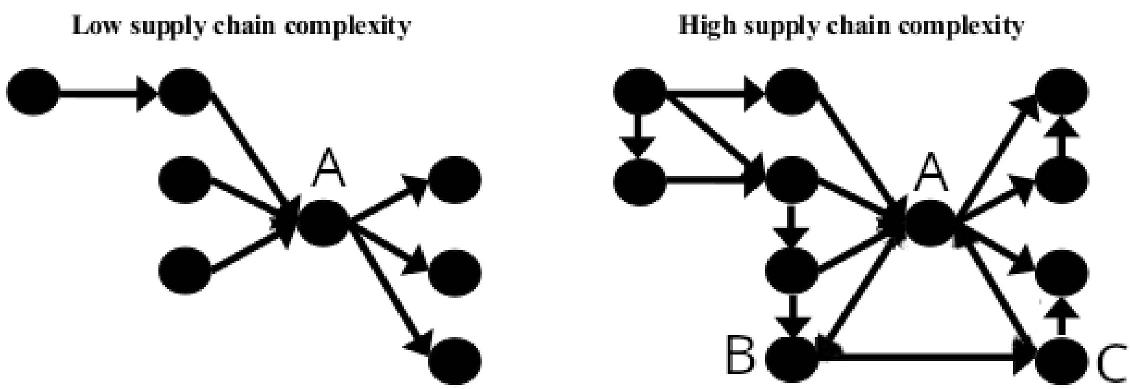


Fig. 2. Different degrees of supply chain complexity, slightly modified from [2].

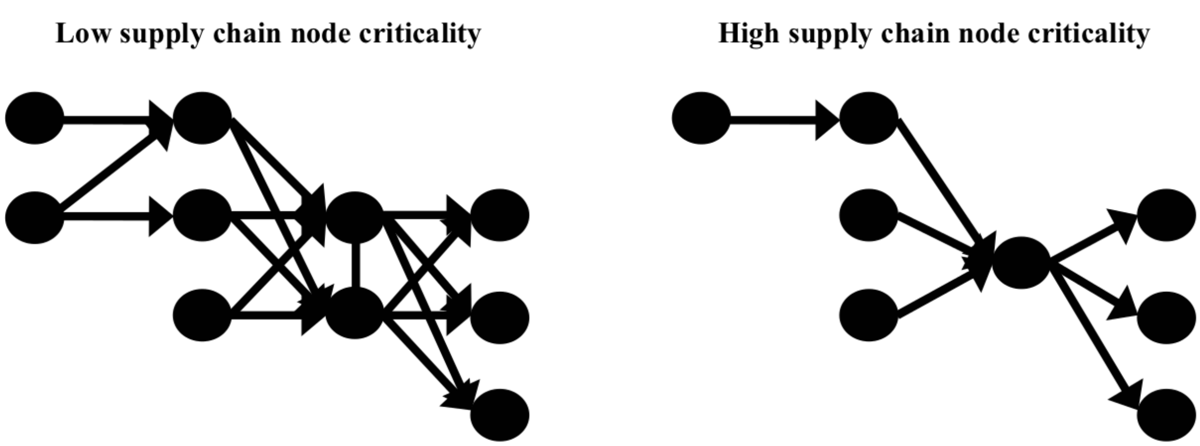


Fig. 3. Supply chain with (right) and without a critical node (left) [2].

describe how the node criticality is assessed and discuss the obtained results. Critical groups are discussed in Section V. Finally, we conclude the paper with Section VI where we summarize our contribution and give potential future work.

## II. Related work

Zhang and Han [4] as well as Yan et al. [5] propose to use network centrality (especially degree, betweenness centrality, and eigenvalue centrality) as indicators for the criticality of a node in a supply chain.

Gaura et al. [6] assess the criticality of a certain network node by determining the decrease in network efficiency when this node is removed from the network. The network efficiency is measured by the normalized sum of the reciprocal of graph distances between any two nodes in the network. Prior to applying their approach, nodes with low clustering indices are removed from the network, wherefore the authors termed their approach clustering-based.

The approaches described so far assess a node's criticality alone by topological network measures. In contrast, Falasca et al. [2] propose to also consider throughput through the supply chain but fail to suggest a concrete measure. Sabouhi et al. [7] consider a node as critical, if the throughput through this node as determined by solving a linear optimization problem, exceeds a certain predefined threshold. However, this measure does not take the use of backup suppliers into account as we do here, which can de facto reduce the node criticality of alternative suppliers.

There are also some existing approaches to identify critical links. Scotta et al. [8] introduce the so-called Network Robustness Index (NRI), "for evaluating the critical importance of a given highway segment (i.e., network link) to the overall system as the change in travel-time cost associated with rerouting all traffic in the system should that segment become unusable." Note that the NRI only takes costs into account that are directly transportation-related but disregards repercussions of item non-delivery for downstream production processes as we considered in our proposed method.

We chose to use a robust optimization model as a basis for our risk cost estimation. Such a model is oftentimes employed for supply chain optimization under uncertainties. Kim et al. introduce [9] such a model, which maximizes profit in a closed-loop supply chain scenario also considering repairs and recycling of products and materials. The uncertainty arises since the available budget for uncertainties and repairs is unknown and can assume one of possible three values. Babazadeh and Jafar Razmi [10] propose a mixed integer linear programming model based on robust optimization that minimizes production, inventory, and transportation costs under 4 different economic growth scenarios.

Alternatives to the scenario-based robust/stochastic optimization approach are the use of the value at risk and the conditional value at risk. The value at risk specifies a certain quantile of the probability density function of the production loss. The closer this quantile is to the expected value of the distribution, the less is the variance of the loss and therefore also the risk. In contrast, if this quantile is located far away from the expected value, the probability density curve must be quite flat and therefore the variance and also the supply chain risk are rather high. Thus, the distance between the value at risk and expected value should be minimized for obtaining a low-risk supply chain configuration. Khorshidi and Ghezavati [11] use the value at risk approach to obtain the best possible location of facilities to minimize production loss. The downside of the value at risk-based methods is that they consider only a single location on the probability density curve, which can make this measure unreliable as risk estimate in certain situations. Therefore, nowadays, the value at risk is oftentimes replaced by the conditional value at risk that considers the weighted average of the loss beyond the chosen quantile. A supply chain optimization approach based on the conditional value at risk is introduced by Azad et al. [12]. In particular, they minimize the conditional value at risk of the lost capacity to determine the optimal amount of investment for opening and operating distribution centers. We opted for the scenario-based robust optimization approach since value at risk as well as conditional value at risk require the probability distribution of the production loss/costs, which is difficult to obtain in practice.

## III. Employed optimization model

Our approach is based on robust optimization, which itself is based on stochastic optimization, which again is based on a deterministic optimization model.

We describe each of these three models subsequently in the following sections starting with the most basic one.

### A. Deterministic optimization model

The deterministic model disregards any potential risk for the supply chain and determines the minimum costs of the so-called "happy flow", which denotes the best-case situation that no supply chain disruption occurs. Since such a model contains no stochastic part, it can be computed very efficiently. Note that we use, due to the computational complexity of the stochastic and robust model, a single period of 12 months for all of our 3 optimization models, over which we aggregate the total customer demand.

The following constants must be specified beforehand:

- $d_{jz}$: demand at location $j$ for product $z$
- $c_{ij}$: cost to move one kg over one km from location $i$ to $j$
- $pc_{iz}$: cost to produce one item of product $z$ at supplier location $i$
- $a_{xz}$: number of items of product $x$ to produce one amount of product $z$
- $cap_{iz}$: production capacity of product $z$ at supplier location $i$
- $in_{iz}$: initial number of items of product $z$ contained in the inventory at supplier location $i$
- $ic_{iz}$: inventory cost for storing z at location $i$
- $dist_{ij}$: geographical distance between locations $i$ and $j$
- $weight_z$: weight of product $z$

- $coc_i$: change-over costs of supplier $i$. These costs arise if the supplier produces at least one item. Later on in the stochastic and robust optimization model, we assign change-over costs to all suppliers that are not part of the *Happy Flow* scenario, i.e., the scenario without any supply chain disruptions.

The following decision variables are to be determined by the optimizer:

- $T_{ijz}$: number of items $z$ that are moved from location $i$ to $j$
- $IT_{il}$: internal transfer of item $l$ from inventory at location $i$
- $P_{iz}$: number of items $z$ produced at supplier $i$
- $WT_{iz}$: number of items $z$ removed from the warehouse of supplier $i$
- $US_i$: use supplier $i$ in the supply chain

Model constraints:

- $d_{jz} \leq \sum_i T_{ijz}$: demand of item $z$ at location $j$ is met
- $\sum_z a_{lz} P_{iz} = IT_{il} + \sum_k T_{kil}$: number of items $l$ required to build items $z$ at location $i$
- $P_{iz} \leq cap_{iz}$: supplier at node $i$ can at most produce $cap_{iz}$ items for product $z$
- $P_{iz} + WT_{iz} \geq \sum_j T_{ijz} + IT_{iz}$: produced + removed from the inventory of supplier $i \geq$ number of items transported from supplier $i$
- $WT_{iz} \leq in_{iz}$ for each item $z$ and supplier $i$: inventory contents cannot become negative
- $US_i = 1 \Leftrightarrow \sum_z P_{iz} > 0$: A supplier $i$ is considered to be used in the supply chain if it produces at least one item. This constraint is implemented by means of the so-called big-M approach.

The following objective is used:
Min. $costs_{total}$ with:

$$\begin{aligned} costs_{total} := &\sum_{ijz} T_{ijz} c_{ijz} dist_{ij} weight_z \\ &+ \sum_{iz} (P_{iz} pc_{iz} + in_{iz} ic_{iz}) + \sum_i US_i coc_i \end{aligned} \tag{1}$$

### B. Stochastic optimization model

The stochastic model takes supply chain risks into account and computes the expected value of the supply chain costs ($\mathbb{E}(C)$) determined over all generated risk scenarios. In a stochastic optimization setting, the set of risk scenarios describes the potential hazards for the whole supply chain. Hence, the nine scenarios from our case company's supply network are used as input for the stochastic optimization approach, which are given in Table I.

The stochastic optimization model determines the minimal supply chain costs under these risks and estimates the supply network resilience of the entire supply chain. Note that certain inventory costs are currently still disregarded in our model but may be considered for future work. We have expanded our initial deterministic optimization model as follows. First, each decision variable is assigned an additional index denoting the associated risk scenario. For instance: $P_{izs}$ denotes the number of item $z$ produced at location $i$ in risk scenario $s$. Furthermore, an additional decision variable named $Missed_{jzs}$ has been included to denote the shortfall of a produced item $z$ at location $j$ for risk scenario $s$ with respect to the actual demand. To represent the effect of a missed demand, we define a variable (per item) non-delivery penalty term $pen_{jz}$. The penalty is invoked when the demand for item $j$ and location $z$ cannot be met ($Missed_{jzs} > 0$). The non-delivery penalty comprises lost revenue and a possible contract penalty. As a result, the demand constraint changes as follows: $d_{jz} \leq Missed_{jzs} + \sum_i P_{izs} T_{ijzs}$ for every scenario $s$ and the objective function becomes:

TABLE I
SUPPLY CHAIN DISRUPTION RISK SCENARIOS FOR OUR EXAMPLE SUPPLY CHAIN.

| Number | Risk Scenario |
|---|---|
| 1 | Product line simplification of supplier 1 - supplier no longer delivers the component due to strategy change |
| 2 | Product line simplification of supplier 2 - supplier no longer delivers the component due to strategy change |
| 3 | Covid19 pandamic |
| 4 | Cyber attack |
| 5 | Transport disruption |
| 6 | Supplier disruption due to export restrictions |
| 7 | Delivery problems of a certain part from supplier 3 |
| 8 | Delivery problems of a certain part from supplier 4 |
| 9 | Happy Flow - no disruptions |

$$\text{Min. } \mathbb{E}(C) \tag{2}$$

where

$$\begin{aligned} \mathbb{E}(C) := &\sum_s C_s p_s \\ = &\sum_{ijzs} T_{ijzs} c_{ijz} dist_{ij} weight_z p_s \\ &+ \sum_{izs} (P_{izs} pc_{iz} + in_{iz} ic_{iz}) p_s \\ &+ \sum_{jzs} vp_{jz} Missed_{jzs} p_s \\ &+ \sum_{jzs} \mathbb{1}_{Missed_{jzs} > 0} fp_{js} p_s \\ &\text{( Missed demand is penalized.)} \\ &+ \sum_{is} US_{is} coc_i p_s \end{aligned} \tag{3}$$

with $p_s$ specifying the probability of occurrence of risk scenario $s$ and $C_s$ denoting the total supply chain cost in the broad sense (see Section III-C) as follows

$$\begin{aligned} C_s := &\sum_{ijz} T_{ijzs} c_{ijz} dist_{ij} weight_z \\ &+ \sum_{iz} (P_{izs} pc_{iz} + in_{iz} ic_{iz}) \end{aligned} \tag{4}$$

$$+\sum_{jz} vp_{jz} Missed_{jzs}$$
$$+\sum_{jz} \mathbb{1}_{Missed_{jzs}>0} fp_{js}$$
$$+\sum_{i} US_{is} coc_i$$

The expression $\mathbb{1}_{Missed_{jzs}>0} fp_{js}$ is modeled by means of a big-M approach. The supply chain cost estimate is given by the objective of this stochastic optimization problem formulation.

### C. Robust optimization model

A supply chain disruption can cause an unmet demand, which decreases the production, transportation and inventory costs (costs in the narrow sense), since fewer items are produced, transported and stored but increases the sum of the costs in the narrow sense and non-delivery penalties comprising of lost revenues and a potential contractually agreed payment (costs in the broad sense). We differentiate between a variable per-item penalty and a fixed non-delivery penalty that is imposed as soon as a certain number (here 1) of items could not be delivered. The aggregated variable non-delivery penalties and the decrease in costs in the narrow sense are considerably correlated with each other. Therefore, unmet demand causes a non-negative costs variance for both the costs in the narrow and in the broad sense. Furthermore, a supply chain setting that minimizes the variance of the costs in the narrow sense would also have a comparatively small variance of the costs in the broad sense. A high variance of costs means a high unsureness about the actual costs and therefore a high risk. Thus, it is an important aim for a risk-averse decision maker to reduce the unsureness and therefore also the costs variance. We decided aiming to minimize the variance of the costs in the broad sense, since otherwise, the imposition of a fixed (item-independent) non-delivery penalty would not have any influence on the costs variance since the optimization objective already contains the variable non-delivery penalty.

The robust model introduces an additional constant $\sigma$ that specifies the risk affinity of the decision-maker [10] [13]. Large values of $\sigma$ cause a considerable increase in the costs accounting for the unsureness about the actual costs. Thus, a risk-averse decision-maker would select a rather high $\sigma$, whereas a risk-tolerant decision-maker would select a small value or drop this term altogether. Thus, the objective function changes to:

$$\text{Min. } \mathbb{E}(C) + \sigma \mathbb{V}(C) \tag{5}$$

where $\mathbb{E}(C)$ is defined in Equation 4. Since the computation of the variance requires quadratic programming, we decided to approximate it by the absolute variance [10] [14]:

$$\mathbb{V}_{abs}(C) := \sum_{s} p_s |C_s - \mathbb{E}(C)| \tag{6}$$

The absolute variance can be modeled by linear programming as follows. First, we introduce additional non-negative decision variables : $\phi(s)^+$ und $\phi(s)^-$ with the following two constraints:

$$\begin{aligned} \phi_s^+ &\geq p_s(C_s - \mathbb{E}(C)) \\ \phi_s^- &\geq p_s(\mathbb{E}(C) - C_s) \end{aligned} \tag{7}$$

The objective function is then given by:

$$\text{Min. } \mathbb{E}(C) + \sum_{s} \sigma(\phi_s^+ + \phi_s^-) \tag{8}$$

$\phi_s^+$ captures the part of the variance, where the costs exceed their expected value, whereas $\phi_s^+$ captures the remaining part, where the costs fall below their expected value. It can be shown that for the absolute variance, both parts must coincide. Thus:

$$\phi_s := \phi_s^+ = \phi_s^- \tag{9}$$

With this, the constraints in (7) simplify to [14]:

$$\phi_s \geq p_s(C_s - \mathbb{E}(C)) \tag{10}$$

and the objective function changes to

$$Min. \ \mathbb{E}(C) + \sum_{s} \sigma \cdot 2\phi_s \tag{11}$$

We call the objective value of this optimization problem the *risk costs* of the associated supply chain in the remainder of the paper.

## IV. Assessing node criticality

Thus far, we have explained our robust optimization model, which is the basis for our proposed node criticality assessment. In particular, the robust optimization method as described above estimates the supply chain‘s risk costs that are composed of the expected total supply chain costs considering several disruption risk scenarios and their variance. A large variance implies that the supply chain costs can vary strongly depending on the occurred risk scenarios. In this case, there is high uncertainty about the incurring costs and therefore the overall supply chain risk is quite high. In contrast, low variance means that the supply chain costs do not deviate much across the scenarios. In this case, the overall supply chain risk remains small. The risk costs are leveraged in our approach for identifying the critical nodes of the supply chain.

By using risk costs instead of ordinary deterministic costs, we obtain more accurate criticality assessments of the nodes. Consider for example the case, that an important supplier $S$ is backed up by a second supplier, which is threatened by probable bankruptcy. In a deterministic setup, the supplier $S$ would be assigned a low criticality because of the provided backup supplier. However, in case supply chain risks are considered, the criticality of supplier $S$ remains high due to the foreseeable default of the backup supplier.

In our approach, a supplier node is considered critical, if its complete breakdown causes a high increase in risk costs of the supply chain, which can be estimated by our robust optimization approach. In contrast, a node is considered uncritical, if the total risk costs of the supply chain do not change in case the associated supplier breaks down and can no

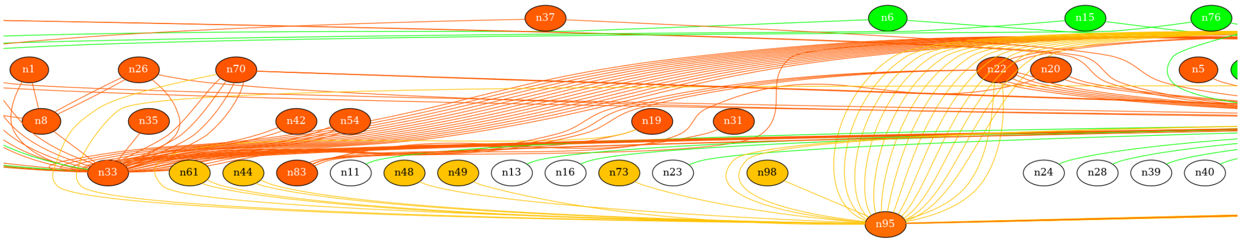


Fig. 4. Part of our example supply chain, where supplier nodes and transportation links are colored according to their criticality.

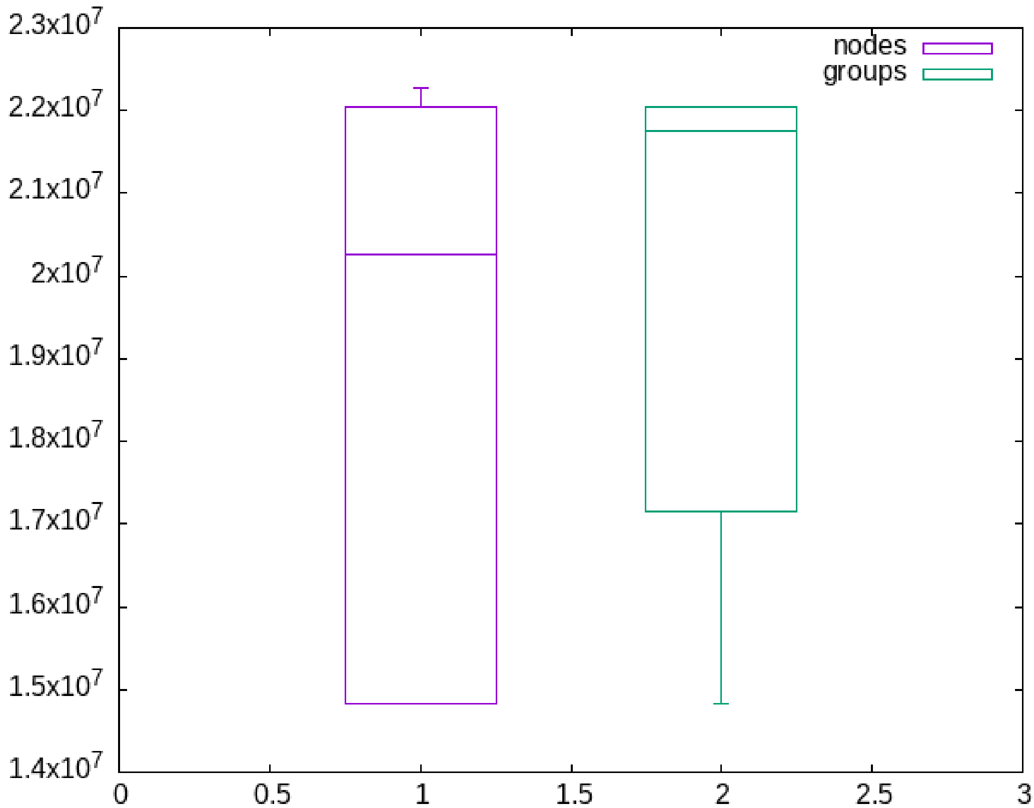


Fig. 5. Boxplot comparing the costs distribution of nodes and groups.

longer produce or deliver any goods. Therefore, we consider the criticality of a node being proportional to the overall risk costs increase of the supply chain when the node in question is removed. We will call in the remainder of the paper the risk costs of the supply chain, in which a certain supplier node $n$ is removed, the risk costs of this node $n$.

A node in the supply chain network can represent either a supplier or a customer, while the edges represent transportation links either between two suppliers or between a supplier and a customer. We consider in the following an example supply chain with 40 customers, 80 suppliers, 200 components and products, 200 transportation links, and 400 product demands. Due to its size, we only depict a part of the total supply chain in Figure 4, which has similar characteristics in terms of critical links and nodes as the total supply chain.

Each supplier node in this network is colorized according to its criticality. Suppliers are colored green if the risk costs of the supply chain are not increased by its potential breakdown, they are colored yellow if the supply chain risk costs are increased by a certain threshold factor $f_1$ (we use 30%), and red if the costs were increased by a second larger threshold factor $f_2$ (we use 60%) or more. Note that the exact values of factors $f_1$ and $f_2$ can vary depending on the corporate branch and the degree of competition. For costs increases between 0 and $f_1$, we interpolate the RGB color values linearly between green (red=0, green=255, blue=0) and yellow (red=255, green=255, blue=0), for costs increased between $f_1$ and $f_2$, we interpolate the color values between yellow and red (red=255, green=0, blue=0). Customers are not associated with any production risks and therefore their associated graph nodes are not colored and instead visualized by unfilled circles. The entire process is illustrated in the form of pseudocode in Figure 6.

Like critical nodes, we also visualize critical links in the supply chain. Analog to the node case, they are colored in green if uncritical, in yellow if somewhat critical, and in red if critical. Again, mixtures of the colors red and yellow as well as green and red are possible. In case there are several transportation modes available between two connected nodes, we consider only the most critical mode for the visualization. Note that a link originating from an uncritical supplier node must also be uncritical. However, the opposite does not hold. A link originating from a critical supplier node, can be considered uncritical, if alternative (backup) transportation modes are available.

The most critical node in our example supply chain would increase the risk costs by 50% in case of failure. Furthermore, by far the largest part of the suppliers is considered rather critical by our chosen definition of $f_2$, which is caused by the fact that backup suppliers are missing in most cases. The remaining suppliers are to the same part either non-critical (visualized in green) or somewhat critical (visualized in yellow). In contrast, the distribution of links is much more balanced. Almost 56% of the links are regarded as critical, the rest is either somewhat critical or uncritical. In particular, transportation links leading to a customer are all considered uncritical due to existing alternative transportation modes, while most of the inter-supplier links are critical. Optimally, the decision-maker should supply backup suppliers/transportation modes for all critical nodes and links so that all critical nodes / links become somewhat critical or uncritical.

## V. IDENTIFICATION OF CRITICAL GROUPS

A high supply chain density is not critical per se but only if all suppliers located in a close proximity have a common risk trigger like a natural disaster (see Figure 7) or certain political or economic circumstances (cf. [15] for an overview of major supply chain disruption risks). We call a group of such suppliers critical if their common failure would have a strong impact on the total supply chain costs. A critical group is in principle an extension of the concept of a critical node. Members of the same critical group are oftentimes located in a geographical neighborhood, although this is not a strict requirement. The criticality of a group is determined analogous to the criticality for nodes or link as presented earlier by risk costs. In particular, the risk costs of a group are given by the risk costs of the supply chain (including lost revenue and potential contract penalties due to missed demand) in which all the individual group members are blocked and are not able to produce (and potentially also deliver) any goods. A group is considered critical if the failure of the entire group considerably increases the supply chain costs so that they exceed a certain predefined threshold value.

The identification of critical groups gives the decision maker another criteria to identify potential weaknesses and bottlenecks in the supply chain. After their identification, s(he) has the following options to mitigate potential repercussions of a complete group failure.

**procedure** GET_RISK_COSTS_COLOR($nodes$, $costs_{hf}$)
  Input $nodes$: list of total supply chain nodes
  Input $costs_{hf}$: “happy flow” costs
  $red := (255, 0, 0)$
  $green := (0, 255, 0)$
  $yellow := (255, 255, 0)$
  $hm := \{\}$ # associated risk costs of a node
  $hm\_color := \{\}$ # associated RGB values for a node
  **for** $n \in nodes$ **do**
    **if** type($n$)==Supplier **then**
      $costs := obj\_value(min_{costs}(nodes \setminus \{n\}))$
      $hm[n] := costs$
      **if** $costs < (1 + f_1)costs_{hf}$ **then**
        $w := (costs - costs_{hf})/(f_1 \cdot costs_{hf})$
        $hm\_color[n] := w \cdot yellow + (1-w) \cdot green$
      **else if** $costs < (1 + f_2)costs_{hf}$ **then**
        $df := f_2 - f_1$
        $dcosts := costs - (1 + f_1)costs_{hf}$
        $w := dcosts/(df \cdot costs_{hf})$
        $hm\_color[n] := w \cdot red + (1 - w) \cdot yellow$
      **else** $hm\_color[n] := red$
      **end if**
    **end if**
  **end for**
  return hm, hm_color
**end procedure**

Fig. 6. Identification of risk costs and node criticality for all suppliers.

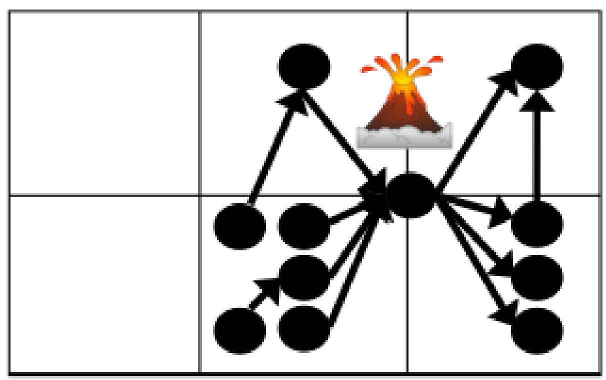

Fig. 7. Supplier group with a volcano as a common risk trigger.

- (S)he can reduce the impact of an occurred risk, usually by providing a backup supplier for each member of a critical group.
- (S)he can reduce the probability that the risk occurs. Note that this option might not always be available, since the decision maker can oftentimes not directly influence the underlying cause of the risk.
- (S)he can resolve the risk scenario altogether by replacing all group members with equivalent suppliers that are not affected by the risk in question. For instance, if a certain set of suppliers is located in the immediate neighborhood

TABLE II
RISK SCENARIO AND ASSOCIATED SUPPLIER GROUPS.

| Risk Scenario | Potential group members |
|---|---|
| Labour Strike | suppliers in the same country and of identical corporate branch |
| Natural Disaster | suppliers in the vicinity of where the natural disaster is expected to occur |
| Political Instability (e.g., danger of coups) in a certain country | all suppliers in this country |
| Vulnerability to cyber attacks | suppliers with a strong dependencies on IT infrastructure that is accessible from outside, e.g., companies conducting e-commerce and selling their goods and services directly to the end-cunsumer over the internet. |

of an active volcano, the decision maker can replace them with suppliers in a different geographical area.

Note that different types of the same risk (e.g., political instabilities of two different countries) should be modeled as separate scenarios, since they usually have different repercussions and occurrence probabilities.

In Table II we give some examples of risk scenarios and associated potential supplier groups. The groups and supplier we used in our evaluation are specified in Table I. Note that all risk scenarios, affected supplier groups, and risk occurrence probability are currently manually specified. In principle, the affected supplier groups could be at least partially determined automatically by statistical analysis if enough background data is available.

The 8 groups in our supply chain are displayed in Figure 8. The nodes are colored from light to dark according to their criticality ranking ranging from 1 (most uncritical) to 8 (most critical) whereas darker color means a higher criticality. In case, a supplier belongs to several groups, the supplier is drawn in the color of its most critical group (associated colors: yellow, light orange, dark orange, green, blue, purple, brown, black). In this figure, the coloring only depends on the ranking from 1 to 8, while the costs are not directly reflected. In addition, all groups with a criticality level nearer to *critical* than to *somewhat critical* are displayed in an increased size. The figure shows that most groups in our example supply chain are critical, that the group size is rather moderate ranging from 1 to 4 suppliers and that several times a supplier belongs to different groups, thus the most uncritical group colored in yellow does not show up at all in the graph. In addition, it can be perceived that suppliers belonging to the same group show up in neighboring locations of the supply chain.

We also compared the risk costs distribution of critical nodes and critical groups. As can be seen in Figure 5, the risk costs of the groups usually exceed the ones of the nodes but not by a high margin. This might seem slightly surprising at first sight, since a group usually contains of several suppliers, thus a group failure should normally have a higher impact than a failure of a single supplier. Furthermore, the interquartile range (IQR) of the risk costs is considerably lower for the groups than for the nodes, i.e., for the former, the risk costs are more concentrated around the median of the distribution. This effect is mainly caused by the fact that there are some uncritical nodes, whose failure do not cause a considerable risk cost increase, while a group failure has almost always a large impact on the supply chain.

However, only our example scenarios 3 and 4 involve the failure of several suppliers and these suppliers are highly dependent of each other since a supplier as well as its direct upstream suppliers are affected by the risk scenario.

## VI. CONCLUSION

We described a method for identifying critical groups, nodes, and groups in a supply chain based on robust optimization. In contrast to other state-of-the-art methods, our method is very precise since it not only considers network topology but also network throughput as well as possible supply chain disruption risks. Furthermore, our method provides a concrete risk costs estimate for the breakdown of each supplier, group, and transportation link. In addition, we provided a representation as a risk graph that allows for easily pinpointing the supply chain vulnerabilities by a decision maker.

Furthermore, we applied our method on a real-world supply chain to analyze its vulnerbilities. The analysis revealed that most of the supplier nodes were considered critical with our employed threshold. Moreover, it could be shown that in average, the groups were only slightly more critical than node in terms of cost increase, which is caused by our specific risk scenario setup.

Currently, risk scenarios, supplier groups, and risk occurrence probabilities are all specified manually. A potential future work is to obtain the supplier groups affected by a certain risk by using statistical analysis of available background data.

## ACKNOWLEDGMENT

Hereby we thank all who supported us in this work, especially Gunter Krell for a lot of fruitful discussions and Uta Jüttner who provided us with fitting risk scenarios. Furthermore, we want to thank the Swiss Innovation Agency Innosuisse for funding the work leading to this publication.

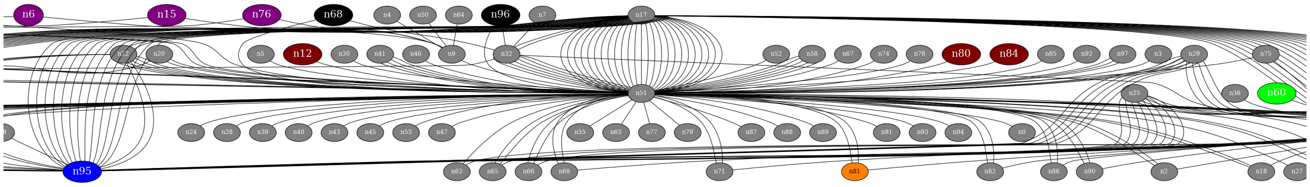


Fig. 8. Identified critical groups in our supply chain (selected part of the total supply chain contains all group nodes).

## REFERENCES


[1] T. vor der Brück and R. Meier, “Identification of critical nodes and links in a supply chain by robust optimization,” in *Sixteenth International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP)*, Valencia, Spain, 2023.

[2] M. Falasca and C. W. Zobel, “A decision support framework to assess supply chain resilience,” in *Proceedings of the 5th International ISCRAM Conference*, 2008, pp. 596–605.

[3] C. W. Craighead, J. Blackhurst, M. J. Runtusanatham, and R. B. Handfield, “The severity of supply chain disruptions: Design characteristics and mitigation capabilities,” *Decision Sciences*, vol. 38, no. 1, pp. 131–156, 2007.

[4] X. Zhang and J. Han, “Analysis of the importance of nodes in supply chain network,” in *Proceedings of the 2011 International Conference on Business Computing and Global informatization*, Shanghai, China, 2011, pp. 387–388.

[5] T. Yan, T. Y. Choi, Y. Kim, and Y. Yang, “A theory of the nexus supplier: A critical supplier from a network perspective,” *Journal of Supply Chain Management*, vol. 51, no. 1, 2015.

[6] V. Gaura, O. Yadavb, G. Sonia, and A. Rathorea, “Identification of critical nodes and edges in a network based on clustering,” in *Proceedings of the 30th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM2021)*, Athens, Greece, 2021, pp. 1298–1304.

[7] F. Sabouhi and M. S. Jabalameli, “A stochastic bi-objective multi-product programming model to supply chain network design under disruption risks,” *Journal of Industrial and Systems Engineering*, vol. 12, no. 3, pp. 196–209, 2019.

[8] D. M.Scotta, D. C. Nova, L. Aultman-Hall, and F. Guo, “Network robustness index: A new method for identifying critical links and evaluating the performance of transportation networks,” *Journal of Transportation Geography*, vol. 14, pp. 215–227, 2006.

[9] J. Kim, B. D. Chung, Y. Kang, and B. Jeong, “Robust optimization model for closed-loop supply chain planning under reverse logistics flow and demand uncertainty,” *Journal of Cleaner Production*, vol. 196, pp. 1314–1328, 2018.

[10] R. Babazadeh and J. Razmi, “A robust stochastic programming approach for agile and responsive logistics under operational and disruption risks,” *International Journal of Logistics Systems and Management*, vol. 13, no. 4, pp. 458–482, 2012.

[11] E. Khorshidi and V. R. Ghezavati, “Application of mathematical modeling value-at-risk (var) to optimize decision making in distribution networks,” *SN Applied Sciences*, vol. 12, no. 1, 2019.

[12] N. Azad, H. Davoudpour, G. K. D. Saharidis, and M. Shiripour, “A new model to mitigating random disruption risks of facility and transportation in supply chain network design,” *The International Journal of Advanced Manufacturing Technology*, vol. 70, no. 9-12, pp. 1757–1774, 2014.

[13] J. M. Mulvey, R. J. Vanderbei, and S. A. Zenios, *Operations Research*, vol. 43, no. 2, pp. 264–281,

[14] C.-S. Yu and H.-L. Li, “A robust optimization model for stochastic logistic problems,” *International Journal of Production Ecnonomics*, vol. 64, pp. 385–397, 2000.

[15] S. DuHadway, S. Carnovale, and B. Hazen, “Understanding risk management for intentional supply chain disruptions: Risk detection, risk mitigation, and risk recovery,” *Annuals of Operation Research*, vol. 283, pp. 179–198, 2019.