Operational Risk Quantification – A Risk Flow Approach

Gandolf R. Finke

BWI Center for Industrial Management
ETH Zurich
8032 Zurich, Switzerland

Mahender Singh

Center for Transportation and Logistics
Massachusetts Institute of Technology
Cambridge, MA 02142, USA

Svetlozar T. Rachev

Chair of Statistics, Econometrics and Mathematical Finance
University of Karlsruhe and KIT, 76128 Karlsruhe, Germany
Department of Statistics and Applied Probability
University of California, Santa Barbara
Santa Barbara, CA 93106-3110, USA

Abstract

The topic of operational risk has gained increasing attention in both academic research and in practice. We discuss means to quantify operational risk with specific focus on manufacturing companies. In line with the view of depicting operations of a company using material, financial and information flows, we extend the idea of overlaying the three flows with risk flow to assess operational risk. We demonstrate the application of the risk flow concept by discussing a case study with a consumer goods company. We implemented the model using discrete-event and Monte Carlo simulation techniques. Results from the simulation are evaluated to show how specific parameter changes affect the level of operational risk exposure for this company.

Introduction

The number of major incidences and catastrophic events affecting global business operations is on the rise. The impact of recent volcano eruption in Iceland, earthquakes around the world, the BP oil spill and financial crisis is making headlines but companies may never know the true extent of the loss. These events reinforce the need for companies to consider operational risk in a more formal manner and act strategically to minimize the negative impact of these and other types of disruptions. Having a better view of operational risks can allow a company to act proactively in many cases to come out unscathed in fact such a capability can be converted into a competitive advantage.

Quantification and measurement is an integral part of managing operational risk. The topic of operational risk is very central to the financial industry due to the immediate and very direct impact of the bankruptcy of a financial institution on the economy and businesses. Not surprisingly, therefore, it has attracted a lot of attention from regulators, academics and practitioners alike. Targeted efforts have been made in researching operational risk especially since the Basel II guidelines on its assessment and the building of capital reserves came out in 2001 [1]. But the breadth of the catastrophic disasters mentioned above raises an important question: Is the domain of operational risk measurement too narrowly focused on financial institutions and their risk exposures? Clearly, assessing operational risk exposure is necessary in non-financial companies as well. To this end, we propose a method to quantify operational risk for any organization including non-financial companies. From this point forward, we will use risk and operational risk interchangeably and discuss it in the context of a manufacturing environment.

A fundamental issue in studying operational risk is a lack of uniform understanding of its meaning among academics and practitioners. Operational risk has been defined in a variety of ways in the literature so for the purpose of this research, we will adopt the definition proposed by the Basel Committee to define operational risk "as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." [1]. It should be noted that although developed for financial institutions and referring to specific risk elements, this definition is suitable for other industries as well. For more definitions and the historical development of operational risk perception we refer to Cruz [2] and Moosa [3] for extended background information to the topic.

In this paper, we will discuss the findings of a project that was completed in 2008/2009 in collaboration between the authors[1] and a Fortune 100 Consumer Packaged Goods company with global footprint, referred to as Company X, the sponsors of the research. Since there are no legislative instruments in place to guide non-financial institutions to build capital reserves for operational risk, Company X, like most other businesses, was focused on understanding the impact of various risks on its overall performance. Indeed, the negative impact on business performance can be directly or indirectly converted into financial terms to gauge the level of risk exposure. We modeled the supply network of Company X using a simulation software package and studied its behavior under different risk scenarios.

The rest of the paper is organized as follows. First, we discuss the state of the art with regard to operational risk and its quantification. We then compare and analyze different approaches to operational risk. Next, we propose our model for assessing operational risk, including the introduction to the concept of risk flows and the risk assessment process. A case study is presented to demonstrate the application of the model, followed by a discussion of the results, along with the strategic implications. Conclusions are presented to discuss limitations and potential future research directions.

[1] The first two authors were key members of the extended team that worked on this project.

Literature Review

Many researchers have addressed the topic of operational risk in their work. Different quantification approaches have been proposed and applied. In this section, we will discuss some of the quantification methods available for operational risk and position this paper among the current literature.

A majority of the existing literature addresses operational risk of financial institutions with a strong focus on banks. Indeed, insurance companies have also been discussed [4]. Literature not only covers different quantification approaches outlined here [5-10], but also provides background to operational risk such as definitions, categorization and cyclicality [3, 6, 11-15].

The different quantification approaches can be divided into top-down and bottom-up approaches [16]. Top-down approaches use aggregated figures, often derived from financial statements or publicly available information. Little attention is given to the actual sources of risk, limiting the use of these approaches in operational risk management [6, 17]. But the simplicity of implementation has attributed to its popularity. Key among the top-down approaches are the single- and multi-indicator models which assume a correlation between an indicator such as profit and the operational risk exposure. The Basel Committee has also included indicator based quantification methods in their guidelines [1]. Multi-factor regression models use publicly available figures to measure company performance and relate this to input factors of the performance. The residual term is believed to describe operational risk. The CAPM approach is mentioned here only for completeness but its practical relevance and the underlying assumptions limit its validity. Scenario analysis and stress testing are also classified as a quantification approach, but their limitations with regards to expressing risk exposure are obvious.

Bottom-up models assess the risk exposure by identifying risk factors at a lower level and aggregating risk to derive the overall level of operational risk. This can be further divided into process-based models and statistical models. Process-based models portray the chain of reaction from event to actual loss. These include Causal models [16, 18, 19], Bayesian models [8, 20], Reliability theory [3, 21] and System Dynamics approach [11]. Statistical models include the value-at-risk approach and the extreme value theory. These are based on the historical loss distribution data. Lambrigger et al. [7] have combined internal and external data with expert opinions using a Bayesian inference method to estimate parameters of frequency and the severity distribution for a Loss Distribution Approach.

It should be noted that the above mentioned approaches primarily focus on financial institutions and do not address the specific challenges of risk quantification for manufacturing companies. As mentioned previously, our objective is to propose a general approach to risk quantification that can be applied to non-financial companies as well.

Proposed Model

Concept of Flows

There are various ways to represent and study a business system. We can slice the business vertically along its functions to learn how various functions operate and contribute to the business success. A process driven approach will advocate breaking the business down to its sub-processes and review them individually for understanding and improving the system. As expected, each view has its strengths and weaknesses, so the choice of approach depends on the goal of the effort.

Another approach to study a system involves the identification and analysis of three different types of flows, namely product (or service), information and money. Mapping and evaluating these flows help capture the complex nature of internal and external interactions effectively. It is clear that for any business to exist, the presence of these three flows is essential. Furthermore, the flows are highly interdependent and must be understood individually and severally at a system level for a business to operate effectively. A flow view of operations provides an end-to-end perspective of the interconnectivity of various sub-processes and functions in terms of key aspect of the business, i.e., product, information and money.

The duality of risk and reward is at the heart of every business enterprise. Managing this couple is at the crux of all key management decisions. But risk is an all encompassing term that doesn’t have boundaries. Business risk can be triggered by events and forces that may or may not have anything to do with the business directly. It is all too common to learn of issues such as product contamination, counterfeiting, cyber attack, supplier insolvency, regulatory changes, network failure etc in global operations leading to loss of sales, reputational damage, loss of market share and even bankruptcy. Obviously organizations are faced with unknown risks each day despite trying hard to be in control of all possible problems.

Due to the complexity involved in managing risk in a modern enterprise, organizations focus on risk in a very local manner. The typical approach to risk management encourages the decision makers to create silos and ensure that local measures are in place to mitigate risk locally. Although this approach simplifies the problem, it leaves the system highly vulnerable. A local view underestimates the impact of risk on the system and therefore a new ways to deal with risk is much needed.

Risk Flow

Motivated by the flow view discussed above, we propose that risk should be studied in a holistic and an integrated manner as well. We propose to construct *risk flow* to sit atop the product, money, and information flows in a system. Although risk originates locally, it has the potential to travel upstream or downstream in unexpected manner due to interconnectivity of the system. A holistic view will show how a single disruption can potentially have disastrous implications for rest of the network in today’s fast moving global and complex business environment.

Conceptually, we treat risk flows to be a function of the disruptions of one or more of the three flows (product, money, information) that will cause delays in the system.

For the purpose of implementing the flow concept to our case study discussed in this research, we will limit our attention only to the delays triggered by the disruptions of product or service flow only. Focusing on product flow is especially meaningful given our context of manufacturing companies. Observing risk from the point of view of the physical flow of products contributes to a better understanding of the interdependence in manufacturing networks. Key reasons for this qualification are as follow:

1. The flow of product or service is central to the value proposition of a manufacturing company and account for a significant portion of its risk exposure. Additionally, data on physical flow disruptions is mostly available.
2. The monetary flow disruptions are limited to cases of disruption of actual transaction of money. Such disruptions are fairly infrequent and can be addressed quickly. In case there is a serious disruption in the flow of money, the effect will be felt directly on the product flow. In other words, the effect of money disruption will resemble a supply disruption. Credit default or lack of liquidity is not part of operational risk and as such not analyzed here.
3. Disruptions of the information flow poses a significant risk to the overall value proposition of a company and can directly affect the flow of products. In such cases too, however, the effect of the disruption resembles a physical supply disruption, so it can be studied as such instead of treating. It represents another cause of supply disruption.

Risk Assessment

Operational risk in our view is twofold: First, there are direct costs that can occur and have an impact purely in financial terms. An example would be damage to a machine that is not in use. This damage will not affect any flow directly, but its repair will cost money. Risk exposure from direct costs can be summed up easily since there is no network effect to be considered and the modeling of such issues using probability distributions has been carried out many times in research before.

Secondly, we consider operational risk at the system level as the risk of disruptions of flows. For example, a machine break-down that is used does not necessarily have a substantial impact in terms of cost for repair. However, during its downtime production would in this example be down for the whole plant causing a potentially severe loss in revenue for that period.

Indeed, risk mitigation is an important aspect of risk management efforts. These actions can change the risk exposure on two key dimensions: impact and/or probability. Mitigation efforts can be regarded as a means to limit consequences.

In principle, risk assessment of the exposure is a function of pure disruption risk and mitigation efforts made by the company. To this end, we propose to collect and analyze data on risk drivers that affect flows within the network and different mitigation efforts such as positioning of inventory or additional capacity. The actual location of drivers within the network is also crucial to the analysis as each location exerts influence on the whole network differently. In other words, risk exposure is not simply additive; only direct costs are.

The risk exposure of a company is governed by the severity of flow disruptions. Since risk drivers affect these flows, each flow has a potential risk exposure associated with it. These individual exposures travel downstream after getting compounded by other exposures along the way to the point where the system interfaces with customers. *Any disruption that limits the product flow to the customer and affects the service level is a critical disruption and a true risk exposure for the company.*

Model development approach

The proposed quantification approach has multiple advantages over approaches that assess risk exposure only based on historical data. Firstly, mapping risk flow and related parameters enables us to incorporate any changes related to the company's risk environment as for example the network structure, mitigation efforts or organizational changes into the analysis rather easily. Secondly, risk assessment can be undertaken by combining different sources such as expert opinions and internal and external historical data to best describe the current risk environment. Thirdly, it enables the analysis of complex production networks with regards to their real risk exposure, not only accounting for drivers of operational risk but also for the mitigation efforts in place.

Risk Profiles: Creating risk profile of each node in the production network is the first step in this process. Risk profiles are created by combining all sources of operational risk that can affect the same location and provide a basis for comparative assessment of these locations. The term location in this context is not necessarily used in a geographical way since the principle of flows is applicable at any level of aggregation. Theoretically, even a single business process could have a risk exposure associated with it and hence be treated as a location.

At each location two separate tasks are performed: computation of the risk inherent to that location due only to its own risks; and compounding it with the risk exposure of all incoming flows into that location. The compounded risk exposure also takes into the mitigation efforts in place at that location to lower the risk exposure. This compounded risk exposure is then associated with the outgoing flow from that location. This idea is illustrated in Figure 1. As mentioned before, in this sense, critical risks are those that cause true risk exposure at the customer interface.

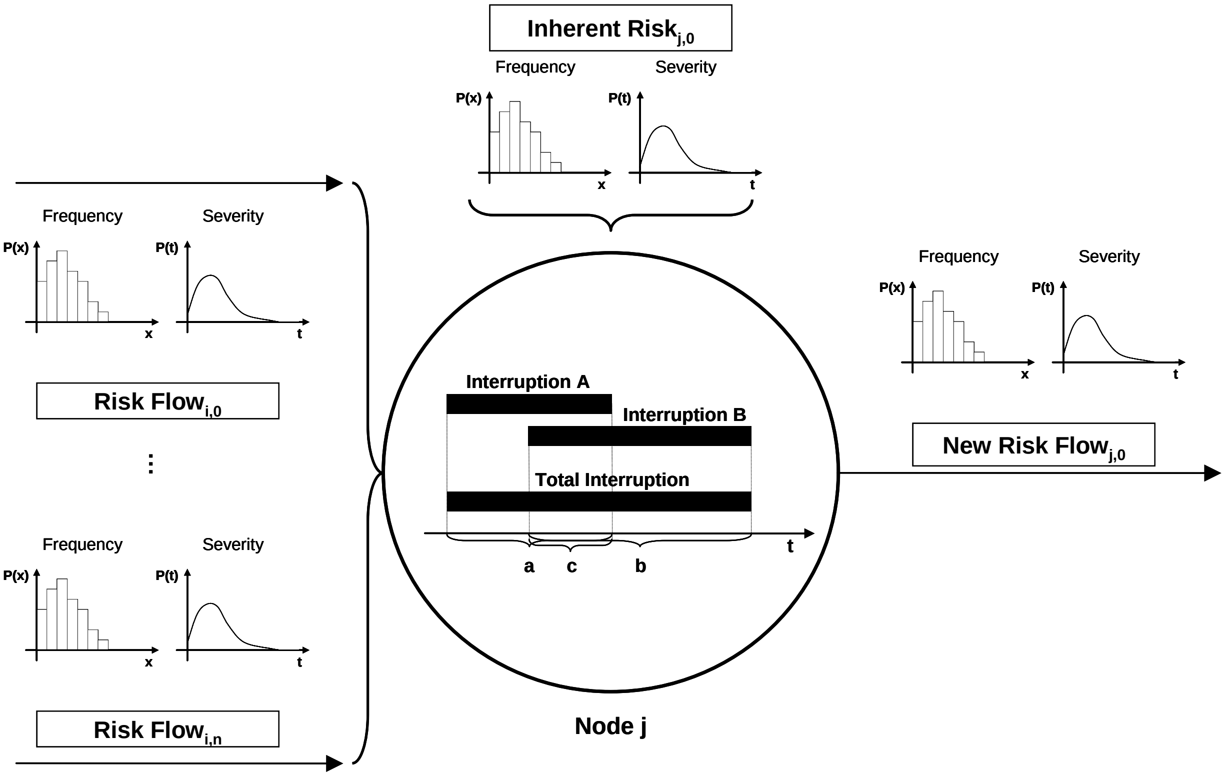

Figure 1: Inherent and preceding risk flows combine to form a new risk level at each node

For it to be useful for decision making, it is important that risk exposure is measured in financial terms. We use elapsed time to measure risk for several reasons in our model. Indeed, the resulting output of the model can be converted into financial value using some sort of transformation function based on historical data. The reasons for using time as a measurement in the model are discussed below:

1. Risk exposures are easily viewed in terms of elapsed time, i.e. system downtime.
2. Risk event occurrence is measured in terms of instance per unit of time.
3. Time can be easily converted into other types of measures. For example, the time that a company cannot serve its customers may be convertible into financial figures to describe the risk exposure.
4. Overlap of two simultaneous disruption events at one location, for example, the situation in which both an inherent event and an already disrupted inflow occur at the same time, can be accounted for easily in terms of time and avoid double counting.
5. Reliability of machines and lifetime of equipment is measured in terms of time.
6. It is very difficult to measure the precise financial impact of a disruption event inside the network.
7. Both frequency and severity can be measured in terms of time. Frequency as 1/time and the severity as the duration of downtime. Thus, also the distributions of frequency and severity are defined using time.

In the following section we will show how this model was implemented using discrete-event and Monte Carlo simulation. We will also present and discuss the results of the simulation.

Case Study

We applied our modeling approach to Company X to study the flow of risk in their network. We selected a popular product line of Company X to develop the model. The modeled network included multiple production sites and supplier locations worldwide. All data including the network details have been masked to protect the identity of the company. The risk assessment process consists of six phases as described below.

Phase 1: Network Structure

As a first phase, the structural outline of the production network or the scope of analysis is mapped. We have mentioned before that the level of aggregation for this step is not fixed and the outline could also include only company-internal parts of the network.

A simplified version of the modeled network is presented in Figure 2. The network shown here consists of five suppliers, three retail stores and three production plants.

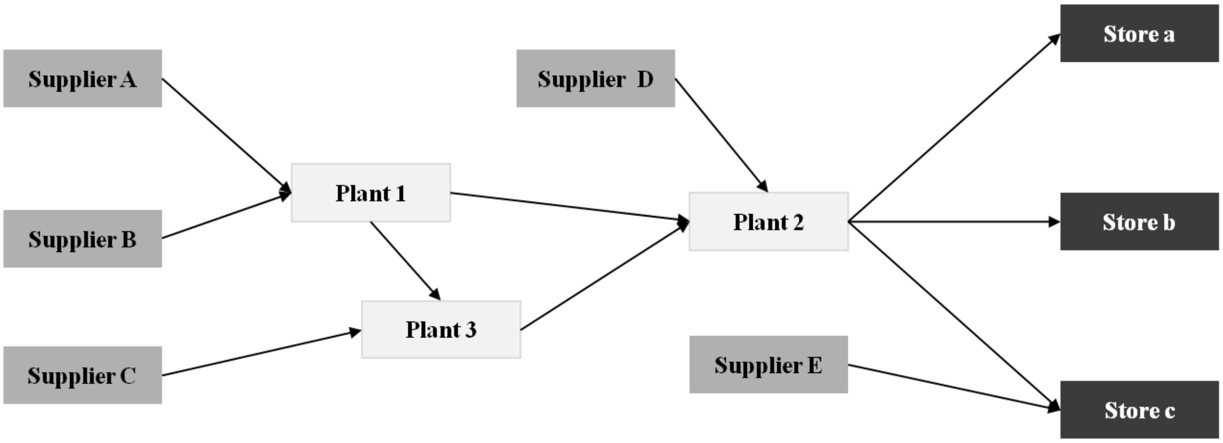

Figure 2: Network architecture of the modeled product line of Company X

Phase 2: Network Data Collection

Data collection is part of the risk quantification process. Phase 2 describes the data collection on the network as such. Detailed data on company's operations such as demand distributions, transportation times, order policies and production and shipping batch sizes are used in the assessment.

Before starting data collection and model development, the team must decide the level of aggregation. For Company X, the level of aggregation was site i.e., all product flows between sites are taken into account and related quantitative information is to be collected.

Phase 3: Risk Data Collection

The level of aggregation drives the granularity and source of various types of data needed to assess risk. Risk drivers and their parameters in terms of frequency and severity are collected for each flow. The data collection process is two-folded combining qualitative and quantitative aspects.

The qualitative data is extracted from multiple interviews with local plant managers. In each interview, open-ended questions with the aim of collecting information on why, where, when, what disruption occurred and with which recovery process and speed, impact on market and estimated cost that disruption was associated. At each site business continuity and operations staff discussed the different categories of disruptions and their parameters, resulting in one spreadsheet per site. This can of course only reflect those years that people have worked at the specific site which could be as much as 15 years. Government databases, on the other hand, provided quantitative data that covers 50 years.

All risks affecting one site were aggregated to compile the site's risk profile. Depending on the type of risk, the appropriate approach is adopted to collect the data. For instance, in our case, most disruption occurrences were modeled using a Poisson distribution. This reflects the assumption that such events are memoryless.

The severity was captured using a triangular distribution. In contrast to a normal distribution, the parameters needed for a triangular distribution, namely minimum, maximum and most likely value are easily understood and intuitive, and can thus be estimated more accurately than the standard deviation of a normal distribution. We have also included variation in transportation times as a source of risk for Company X.

As a next step, information on risk mitigation efforts and strategies already in place at Company X were collected. This essential meant gathering information about inventories and related policies. However, since time was defined as the main measurement unit, the inventory levels had to be expressed in weeks instead of number of unfinished or finished products in stock.

Phase 4: Simulation

The master simulation model was built using discrete-event simulation software. We used Arena by Rockwell Automation Technologies Inc. This phase was further split into two separate steps. In the first step, a simulation model was used to compile all risks at a specific location into one risk profile.

This was done also using discrete-event simulation; however simulation took place separately for each node. In this first simulation model entities that each represent a disruption were created according to the gathered data and categories of risk sources. The parameters used are the results of the data collection process. The model comes with the ability to have the different risk categories' entities to be created independently. At the same time, the model could also account for overlapping of two or more disruptions in order for them to not be counted twice. The result of the first step were thus empirical distribution functions for each node that were then parameterized using distribution fitting techniques in order to serve as input for the master simulation model.

The second step, the master simulation model, combined all individual risk flows in the global network. The complete simulation model is shown in Figure 3 below. The model possesses an interface to read in and write out data to Excel files for enhanced user friendliness. The ability to read in allows even users unfamiliar with the software to manipulate input parameters of the model and run different scenarios. Writing out the time and duration of every disruption enables the user to comprehend the whole simulation run and to use the data for further processing.

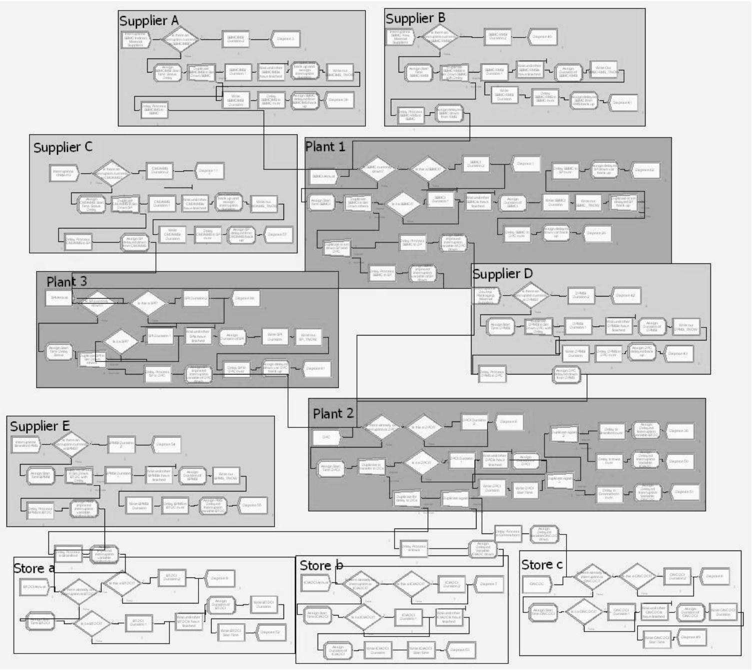

Figure 3: Layout of the overall simulation model combining all nodes in the global network

Figure 3 only intends to provide a rough overview over the whole simulation model. Figure 4 however, can be used to explain the simulation mechanics exemplarily for one of the nodes. Every entity that represents a local disruption is created in the top left box and travels to the first decision box (diamond). Here, the model checks whether the node is currently functional or not in order to account for overlapping disruptions. In case of a normally operating site, the entity is assigned a start time of disruption and then duplicated. This duplication takes places, as the subsequent node in the network will also be disrupted, assuming no mitigation measures are in place.

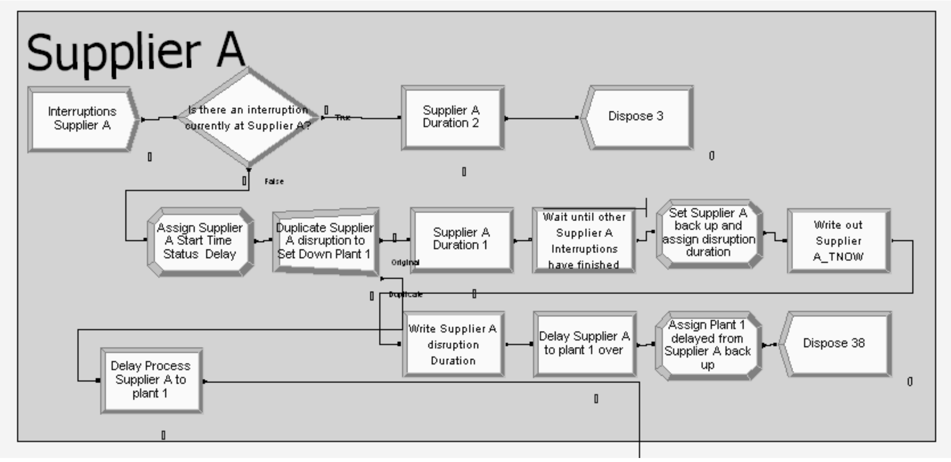
Supplier A
Interruptions Supplier A
Is there an interruption currently at Supplier A?
True
False
Supplier A Duration 2
Dispose 3
Assign Supplier A Start Time Status Delay
Duplicate Supplier A disruption to Set Down Plant 1
Original
Duplicate
Supplier A Duration 1
Wait until other Supplier A Interruptions have finished
Set Supplier A back up and assign disruption duration
Write out Supplier A_TNOW
Write Supplier A disruption Duration
Delay Supplier A to plant 1 over
Assign Plant 1 delayed from Supplier A back up
Dispose 38
Delay Process Supplier A to plant 1

Figure 4: Exemplary simulation mechanics at one node of the network

The original entity then goes on to travel to the box “Supplier A Duration 1” where it waits for the duration that is assigned according to the assigned distribution and its parameters. After this, the entity waits until all other simultaneously appearing disruption are over, before the time for the total disruption is assigned and written out into an Excel file. The delay for a disruption in a subsequent node that represents in this case the transportation time is also accounted for. The disruption from Supplier A then enters the decision box of Plant 1, the subsequent node. Due to difficulties in modeling, the treatment of inherent and non-inherent disruptions is slightly different but the working mechanism is essentially the same at all nodes of the network.

Phase 5: Verification and Validation

Different means were used to verify and validate the model. Verification, ensuring that the model works as intended, was performed by reviewing the simulation results manually for isolated portions of the model; for instance, seeing how the downtimes at one location travel to the next stage of the network. Further verification was performed by following the slow-motion of a simulation run visually. Ensuring that adjustment of parameters such as the frequency or severity of a disruption caused the predicted effects contributed to verification as well. Validation of the model ensures that the model accurately reflects reality and was performed through comparison with data from a different simulation model which was developed in close collaboration with Company X for a similar purpose.

Phase 6: Output Analysis

Data processing was the last step of quantification. Up until this step, we had collected one frequency distribution, defined by the inter-arrival times of disruptions, and one severity distribution, characterized through the durations, for each node in the network. Now, the two derived distributions for each and especially for the last node in the network i.e. the customer interface, were combined to one distribution. We call this distribution the aggregate loss distribution as it aggregates the losses and expresses the final node’s downtime in days per year. Combining the two distributions was carried out using Monte Carlo simulation technique. Figure

5 shows a sample aggregate loss distribution. It reflects the simulation data of how many days within a given year a specific node is disrupted. Several statistical measures such as mean, median, standard deviation and different percentiles allow for comparability with other nodes. The figure also indicates the shape of the related parameterized distribution function.

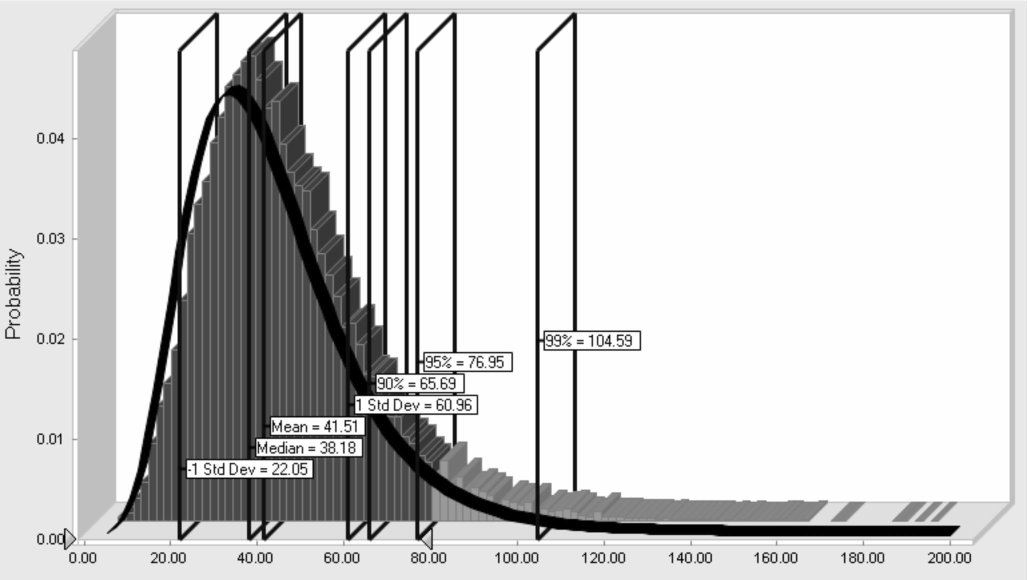

Figure 5: Aggregate loss distribution showing system down-times per year in days

In addition to the quantification process, different scenarios were created to assess the effect of parameter changes on the aggregate loss distribution. Resiliency towards specific events, different levels and locations of inventory were among the scenarios tested at this stage.

Results and Interpretation

Results of the project can be broadly categorized into three different sections: a) identification of risk drivers; b) local risk profiles of locations; and c) network effect of operational risk and related implications. As the focus of this paper is mainly to introduce the concept, we will only briefly discuss some of the insights and learnings with regard to the overall network effect.

Inventory buffers are a common means to mitigate operational risk. The inventory buffer size and its placement in the network directly affect the propagation of risk through the system and as such the final product flow to the customer. In the following example we show the effect of inventory buffer size and location on risk exposure. For this purpose, we illustrate the risk exposure of the final flow to one of the customers - Store b in Figure 2. Again, the aggregate loss distribution is used to measure and illustrate the risk exposure.

Figure 6 provides four different aggregate loss distributions: a) is the inherent risk profile of the node itself; b) shows the combined risk profile of inherent and preceding risk exposures arriving at the node without any inventory in the network; c) illustrates the node's risk profile with 1 week worth of inventory at each supplier and d) indicates the aggregate loss distribution for the node with one week worth of inventory at every preceding node.

Inventory at a preceding node essentially translates into protection from all types of disruptions lasting less than one week and from those longer one week is “deducted”. For this special case it does not matter whether this inventory is a finished goods inventory at the preceding node, incoming goods inventory at the node itself or goods in transit.

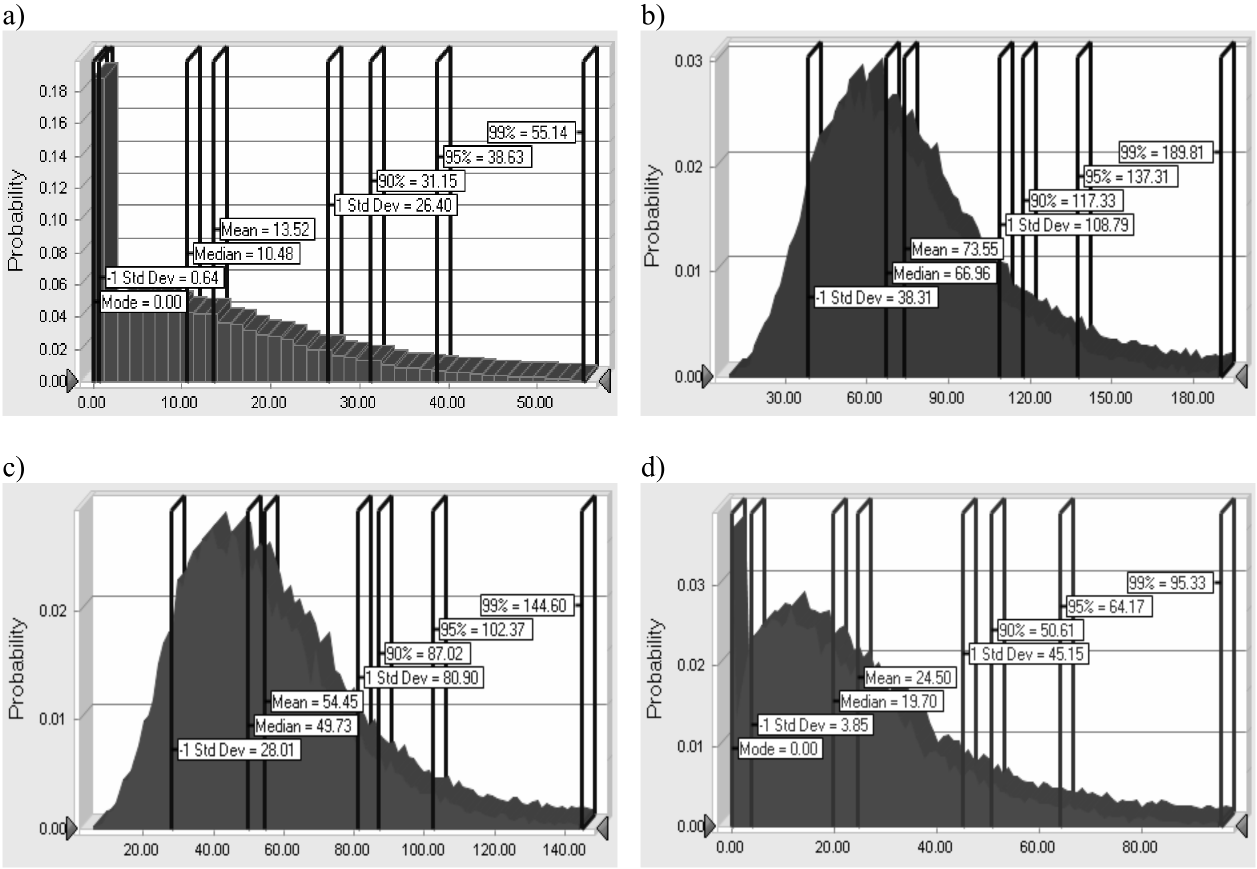

Figure 6: Aggregate loss distributions of Store b) describe risk exposure in days per year

The four different graphs clearly show the network effect of risk and how inventory size at different locations affects this exposure. The inherent profile in a) depicts a low average of disruption days per year while the combined risk flows from all preceding nodes add up to form the much higher average in b). Placing one week worth of inventory in the network at the suppliers, i.e. between suppliers A, B, C and D and the respective nodes they supply, causes the average number of days yearly down to decrease from 73.55 days without inventory to 54.45 days with inventory. This mitigation effect is enhanced when placing one week worth of inventory on all arrows in Figure 2. The average then drops to 24.50 days.

The effect of inventory in the network aligns with our expectations. The more inventory in the network, the lower was the risk exposure at final flows. The network effect of risk as such, that is the transformation from Figure 5 a) to b) is also clear as all disruptions of preceding nodes affect the node additionally to the inherent profile.

Practical relevance of this analysis lies in its ability to help the company test different inventory buffer sizes and locations. For each size/location combination, the aggregate loss distribution can be generated to perform an objective cost-benefit analysis. Being able to quantify the value for a risk mitigation effort in terms of downtime or service level will enhance and facilitate the use of objective risk management practices.

The peculiarities of an individual network, driven by locations of nodes, risk sources and their parameters, inventory sizes etc., lead to the fact that each system behaves in an idiosyncratic manner. Due to the presence of a number of influencing factors and interactions, the impact of a disruption on the network, as well as benefits of investing in making the network resilient are as such not easily conceivable.

A number of factors including network architecture, the location where a disruption appears and its duration determine these interactions. As a result it is important to study how the risk flows in a particular network to set realistic targets for the system and to make investment effective to enhance network performance.

Simulating a network under various risk scenarios allows to understand the net impact of different disruptions to further characterize the disruption itself. For instance a 2 day disruption at Supplier A may not be as detrimental as at Supplier B in terms of the overall affecting the product availability to customers.

This knowledge will help decision makers to make judicious investment decisions and utilize the limited resources more effectively. Similarly, decisions about investment into recovery plans can also be tested with simulation to determine when and where to implement business continuity plans for better system-level performance. The choice of investment for mitigation depends on location, duration and frequency of disruption as well as the interactions in the network which is why a local examination is not sufficient and an analysis on systems level must be applied.

Limitations

The concept of *risk flow*, the outlined model and its implementation are subject to limitations and simplifications. First of all, both the theoretical model and the implementation at Company X only address the product flow. Neither financial nor information flows or even direct costs associated with the events are accounted for. We have, however, argued that this is not a serious limitation and can be rectified by including necessary data into the model.

The model does not address the issue of product quality as part of operational risk discussion. With additional effort, the simulation model can be enhanced to incorporate the aspect of quality but a differentiation between flow-affecting and quality-affecting risk drivers seems necessary.

Next, it remains unclear on how to define the right scope and level of aggregation of assessment. Although the case study provides an example, the analyses of more supply chain tiers whenever possible would greatly contribute to the results' accuracy. Furthermore, the different risk factors that need to be included are not clearly defined. Although the most important ones are mostly captured, the risk scope can never be covered entirely.

Another downside of the proposed method is availability of good quality data as well as company resources. Not all companies are equipped to provide loss data covering more than a few years. The occurrence of low frequency/high impact events are thus in many cases not captured and as a result risk managers and others responsible are not fully aware of their problems. The state of mind, experience and loss horizon of those interviewed strongly affect the results of the simulation. Additionally, the assumptions of all risk sources being memoryless and the use of triangular distributions for severity distributions are further limitations. However, these only affect the significance of the case study's results and not the approach and the model itself. Generally, the data collection process should always be adapted to simulation objectives and data availability. It is important to acknowledge that the simulation model is capable of including any type of distribution.

Regarding the case study, we made some assumptions that were not all mentioned in this paper. For example, we assumed that the inventory replenishment was immediate if used as a buffer, which is clearly not realistic. More assumptions and additional background to the project and simulation models can be found in the thesis that also resulted from the project [22]. Despite these limitations, we believe that by implementing the proposed approach to risk management, companies can develop a powerful tool for operational risk management.

Conclusion

Risk is a serious challenge that confronts all organizations. Due to its very nature, most risk management efforts are not objective and in most cases, the response is inadequate and reactive at best. Failing to make sound decisions ahead of time, the organization deals with risk after a disruption has occurred, with the responsibility falling on the shoulders of the middle and lower management team to recover from it.

Comparing risk exposures levels of various nodes in the network and learning how risk propagates through the network offers key insights to decision makers to understand the vulnerabilities of the network more objectively. The effect of various disruptions, in terms of frequency and duration helps the decision makers understand where and when to focus their attention ahead of time and make necessary investments to protect the network. Similarly, the cost-benefit analysis of different risk mitigation efforts can also be performed to decide which one will be most effective. The company can put a direct value in terms of service level gain or decrease in downtimes to compare mitigation efforts. All these steps will make operational risk management more objective.

In this paper, we have proposed a simple yet effective approach to model and assess operational risk. We view operational risk as the potential disruption of three fundamental flows, i.e., product, information and money in the context of manufacturing companies. We specifically focus on the product or service flow in this paper. In the same vein, we have proposed and shown how mapping the resulting *risk flow* will offer a powerful yet simple way to manage risk. The implementation of the concept is based on discrete-event simulation technique and demonstrated for a case study. Results of simulation runs and their implications are also interpreted.

The relatively young field of operational risk is expected to grow rapidly in the near future. In general, more standardized guidelines throughout the quantification process would be desirable. To this end, we have shared the results and insights based on one case study. Additional research effort is required to test, validate and extend the model, assumptions and insights to make the results more meaningful.

Bibliography

1. BCBS, *Operational risk - Supporting document to the new Basel Capital Accord*, B.C.o.B. Supervision, Editor. 2001. p. 26.

2. Cruz, M.G., *Modeling, measuring and hedging operational risk*. Wiley finance series. 2002: Wiley.

3. Moosa, I.A., *Operational risk management*. 2007, Basingstoke, Hampshire : New York: Palgrave Macmillan.

4. Tripp, M.H., et al., *Quantifying Operational Risk in General Insurance Companies.* British Actuarial Journal, 2004. **10**: p. 919-1012.

5. Leippold, M. and P. Vanini, *The Quantification of Operational Risk.* SSRN eLibrary, 2003.

6. Chernobai, A.S., S.T. Rachev, and F.J. Fabozzi, *Operational risk : a guide to Basel II capital requirements, models, and analysis*. Wiley Finance. 2007, Hoboken, N.J: Wiley. 300.

7. Lambrigger, D.D., P.V. Shevchenko, and M.V. Wüthrich, *The Quantification of Operational Risk using Internal Data, Relevant External Data and Expert Opinions.* Journal of Operational Risk, 2009. **2**(3): p. 24.

8. Alexander, C., *Bayesian Methods for Measuring Operational Risk.* Operational Risk: Regulation, Measurement and Analysis, 2000.

9. Ganegoda, A., *Methods to Measure Operational Risk in the Superannuation Industry*. 2008.

10. Bonsón, E., T. Escobar, and F. Flores, *Sub-Optimality of Income Statement-Based Methods for Measuring Operational Risk under Basel II: Empirical Evidence from Spanish Banks.* Financial Markets, Institutions & Instruments, 2007. **16**(4): p. 201-220.

11. Shah, S. *Operational Risk Management*. in *Casualty Actuarial Society 2001 Seminar on Understanding the Enterprise Risk Management Process*. 2001. San Francisco.

12. Allen, L. and T.G. Bali, *Cyclicality in catastrophic and operational risk measurements.* Journal of Banking & Finance, 2007. **31**(4): p. 1191-1235.

13. King, J.L., *Defining Operational Risk.* ALGO RESEARCH QUARTERLY, 1998. **1**(2): p. 37-42.

14. Lopez, J.A., *What is operational risk?* FRBSF Economic Letter, 2002. **2002**(2): p. 1-4.

15. Moosa, I.A., *Operational Risk: A Survey*. Financial Markets, Institutions & Instruments, 2007. **16**(4): p. 167-200.

16. Marshall, C.L., *Measuring and managing operational risks in financial institutions : tools, techniques, and other resources*. 2001, Singapore. 608.

17. Allen, L., J. Boudoukh, and A. Saunders, *Understanding market, credit, and operational risk: the value at risk a*. 2004: Wiley-Blackwell. 312.

18. Frost, C., et al., *Operational Risk and Resilience*. 2000, Oxford ; Boston: Butterworth-Heinemann.

19. Gowen, L.D., *Using fault trees and event trees as oracles for testing safety-critical software systems.* Professional Safety, 1996. **41**(4): p. 41-45.

20. Cowell, R.G., R.J. Verrall, and Y.K. Yoon, *Modeling Operational Risk With Bayesian Networks.* Journal of Risk & Insurance, 2007. **74**(4): p. 795-827.

21. Rausand, M. and A. Høyland, *System reliability theory: models, statistical methods, and applications*. Wiley series in probability and statistics. 2004, Hoboken, NJ: Wiley-Interscience.

22. Finke, G. and F. Nägele, *Designing an applicable framework to quantify operational risk*, in *CTL, Massachusetts Institute of Technology*. 2009, Karlsruhe Institute of Technology, KIT: Cambridge.

Acknowledgements

The authors would like to express their thanks to the sponsor company and the staff that was involved from their side for their commitment and efforts in the project. Furthermore, Dr. Amanda Schmitt was a key part of the project team and the success of it is owed to her for a large part. Our thanks also go to Florian Naegele and Santolina Savannet for their contribution in terms of data and model presented. Florian Naegele additionally contributed to framing the paper in an initial phase.

Author Biographies

GANDOLF R. FINKE is a Ph.D. student at the BWI Center for Industrial Management at ETH Zurich. His research focuses on quantitative aspects of risk management with a special interest in simulation. Prior to his current studies he received his Diploma in Industrial Engineering and Management from the University of Karlsruhe and gained experience in different industrial and academic institutions including a stay at MIT. His email address is <gfinke@ethz.ch>.

MAHENDER SINGH is a Research Director at the Center for Transportation and Logistics at MIT. His research focuses on operations and supply chain management, with particular interest in exploring the underlying structure of complex supply chains. He received his Ph.D. from the University of Tennessee, Knoxville, and has over fifteen years of experience in the field of supply chain management. His email address is <msingh@mit.edu>.

ZARI RACHEV was a co-founder and President of BRAVO Risk Management Group - originator of the Cognity methodology, which was acquired by FinAnalytica where he serves as Chief Scientist. Rachev holds Chair-Professorship in Statistics, Econometrics and Mathematical Finance at University of Karlsruhe, and is the author of 14 books and over 300 published articles on finance, econometrics, probability, statistics and actuarial science. His email address is <rachev@kit.edu>.