Supply Chain Risk Management: A Neural Network Approach

Frank Teuteberg
E-Business and Information Systems &
Research Center for Information Systems in Project and Innovation Networks (ISPRI), Katharinenstraße 1, 49074 Osnabrück, Germany

Introduction

Effective supply chain risk management (Hallikas et al. 2002; Harland et al. 2003; Henke et al. 2006) requires the identification, assessment and monetization of risks and disruptions, as well as the determination of the probability of their occurrence and the development of alternative action plans in case of disruptions (cf. Zsidisin 2003; Zsidisin et al. 2004; Zsidisin et al. 2000; Vidal a. Goetschalckx, 2000). Companies traditionally use multiple sources for material procurement and/or hold safety stocks to avoid vulnerability. However, these strategies can negatively impact the supply chain performance, leading to higher purchase and logistics costs. The aim of this chapter is to illustrate how the implementation of the supply chain risk management concept can be improved by using a neural network approach.

The chapter is organized as follows: in the next section basic and theoretical concepts of supply chain risk management are presented. Section 3 outlines a framework for categorizing and analyzing risks in supply chains. In section 4, we present a neural network approach that can be applied to assess various risks in supply chains. In section 5 preliminary results of our neural network experiments are presented and discussed. In the final section some conclusions are drawn. We also provide recommendations for future research.

Supply Chain Risk Management – Theoretical Background

Since the mid-eighties the supply chain management concept has been discussed intensively in practice and within the scientific community.

However, besides enjoying successes, the supply chain management approach also faces new challenges (Barry 2004; Jung et al. 2004). The occurrence of new risks such as uncertain demand, the increasing vulnerability of supply chains due to trends such as globalization, saturation of markets or terrorist attacks have forced companies to establish new concepts for risk assessment. It is therefore necessary to define a "manageable" security/risk level which is ultimately a so-called trade-off between supply chain costs, security and performance (e.g. taking on responsibility in the case of disruptions in supply chains). Thus the supply chain management concept has to be enhanced by methods of complexity and risk management. Figure 1 illustrates the trade-off between supply chain costs and supply chain security.

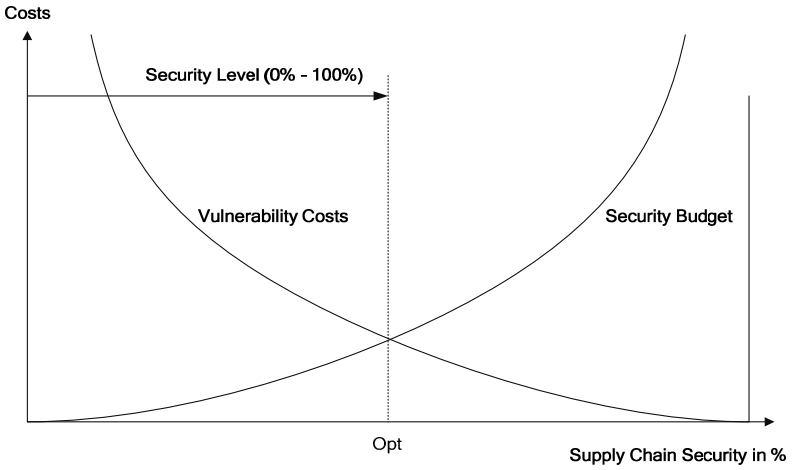

Fig. 1. The trade-off between supply chain security, vulnerability and costs (adapted from Teufel a. Erat 2001, p. 216)

In recent years, the notion of the term “risk” has been given greater attention in research on supply chain management both by academics and practitioners.
It is worth mentioning that 100% security or a 0% probability of risk occurrence is not possible in real-life supply chain scenarios. The goal is to determine a "manageable" security/risk level (denoted point *Opt* in Fig. 1).

The definition of the term "risk" strongly depends on the context and field of research involved (Spekman a. Davis 2004). An operational definition in the context of supply chain risk management is as follows: *"Risk is the product of the probability of occurrence of a (negative) event and the resulting amount of damage*". (Kersten et al. 2006, p. 5; March a. Shapira, 1987).

Risks within supply chains can be categorized into supply, process, demand, control and environmental risks in accordance with the SCOR (= Supply Chain Operation Reference) model processes *plan, source, make* and *deliver* developed by the non-profit organization SCC (Supply Chain Council) (cf. Fig. 2).

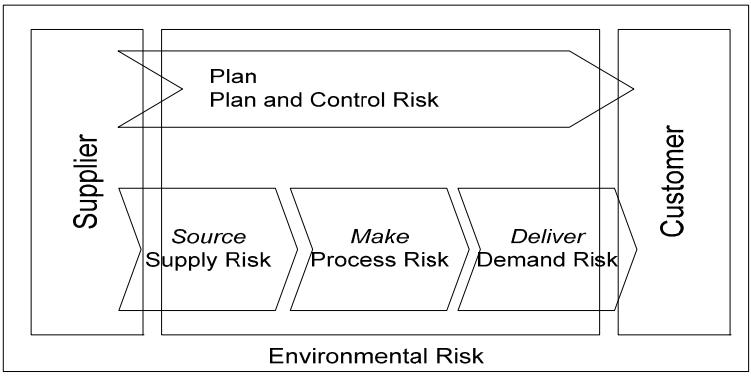

Fig. 2. Categories of risks in supply chains (cf. Kersten et al. 2006, p. 6)

The above-mentioned types of risks, risk drivers and their impacts are categorized in Table 1 (Chopra a. Sodhi 2004; van Wyk a. Baerwaldt 2005; Jahns et al. 2006. pp. 201-203).

Table 1. Categories of supply risks from the literature

Risk category	**Risk driver**	**Risk impact**
Plan and control risk	▪ Applied methods, concepts and tools ▪ IT systems (breakdown, introduction or change of IT systems, virus damage, change of interfaces, data loss)	▪ Opportunity costs ▪ Cost of capital ▪ Logistics costs
Supply risk	▪ Quality of material ▪ Suppliers (failure, single sourcing, adherence to delivery dates) ▪ Supplier dependence ▪ Global sourcing ▪ Supplier concentration ▪ Supply market ▪ Damage to cargo ▪ Monopoly situations (single sourcing) ▪ New strategic alignment of suppliers ▪ Illiquidity and insolvency of suppliers	▪ Production stop ▪ Replacement purchase costs ▪ Supply interruptions
Process risk	▪ Lead times ▪ Capacity bottleneck ▪ Output ▪ Quality ▪ Machine damage ▪ Human error ▪ Faulty planning ▪ Trouble with third-party logistics provider ▪ Major technological change	▪ Supply difficulties ▪ Repair costs
Demand risk	▪ Demand fluctuations ▪ Changes in preferences ▪ Cancellations ▪ Planning and communication flaws in sales	▪ Supply difficulties ▪ Safety stock (Bullwhip effect)

	department ▪ Inflexibility	
Environmental risk	▪ Natural disasters (fire, earthquake, flood, rock fall, landslide, avalanche, etc.) ▪ Weather (iciness, storm, heat) ▪ Political instability (strike, taxes, war, terrorist attacks, embargo, political labor conflicts, industrial disputes) ▪ Import or export controls ▪ Social and cultural grievances ▪ Crime ▪ Price and currency risks/inflation	▪ Opportunity costs ▪ Replacement costs

In 2004, the COSO (Committee of Sponsoring Organizations of the Treadway Commission) developed the so-called Enterprise Risk Management (ERM) Framework (cf. Fig. 3). ERM offers new methods to improve the risk management system in organizations (Henke et al. 2006, p. 97). Furthermore, it has become an important tool in the context of compliance, e.g. implementing directives in the context of the Sarbanes-Oxley Act of 2002. We will take the ERM Framework of COSO as a starting point for the proposed comprehensive Supply Chain Risk Management framework developed in this chapter.

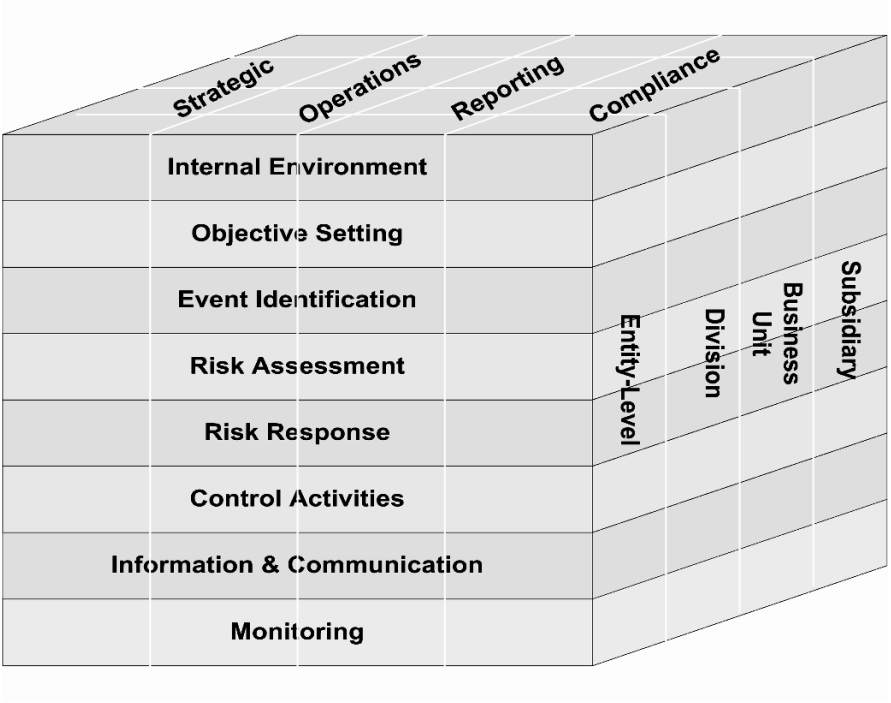

Fig. 3. Enterprise Risk Management (ERM) framework of COSO (COSO 2004)

Kersten et al. (2006) define supply chain risk management as *"a concept of Supply Chain Management, which contains all strategies and measures, all knowledge, all institutions, all processes and all technologies, which can be used on the technical, personal and organizational level to reduce supply chain risk"* (Kersten et al. 2006, p. 8).

As illustrated in Figure 4, rigorous supply chain risk management is a cyclic process encompassing the following six phases (Engelhardt-Nowitzki a. Zsifkovits, 2006, pp. 49-50; Jüttner 2006; Ritchie a. Brindley, 2007; Jahns a. Henke, 2004, pp. 38-44; Henke et al. 2006; Jahns et al. 2006, p. 197):

1) ***Formulation/Revision of Risk Strategy*:** In this phase a risk strategy is defined that needs to be aligned with companies' corporate strategy. The risk strategy determines the risk management processes as well as the organizational structure and technological infrastructure. The risk strategy profile is based on past experiences and the estimation of future risks that may occur.
2) ***Risk Identification & Monitoring:*** This phase includes the identification of stakeholders and objectives to create initial awareness of potential supply chain risks as well as the continuous monitoring of supply chain processes to anticipate disruptions before they occur (cf. Smeltzer a. Siferd, 1998).
3) ***Risk Analysis, Prioritization and Assessment:*** This phase requires the assessment, prioritization and monetization of risks in order to make them more operational for basing decisions on. Risk analysis and prioritization by risk impact, probability, risk level and other criteria, as indicated in Table 2, help us focus on the most critical supply chain risks.
4) ***Risk Response and Action Planning & Scheduling*:** This phase includes risk action planning and scheduling in order to react adequately to disruptions. The risks to be monitored will be assigned with the appropriate handling options (e.g. avoidance, transfer, prevention, acceptance or mitigation) (cf. Müssigmann 2006, p. 215).
5) ***Risk Controlling:*** This phase includes status reporting on the execution of risk action plans as well as risk tracking and tracing in terms of probability, impact and other risk metrics. The progress of the risk situation in their respective risk action plans is analyzed.
6) ***Comparison of Risk Situation and Risk Strategy*:** Learning from previous disruptions plays an important role in this phase. The knowledge gained in previous phases is used to draw up risk reports and compare the current risk situation with the risk strategy in order to adopt it. In future, certain risks may be managed in a more appropriate manner.

It is worth mentioning that the above-described phases do not necessarily have to be conducted in a sequential order; phases are often performed iteratively or even simultaneously.

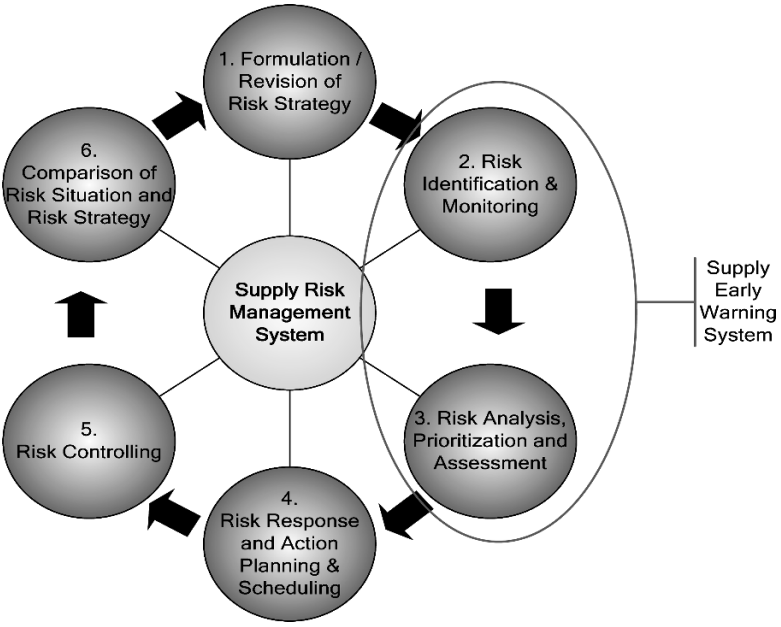

Fig. 4. Supply Chain Risk Management System (adapted from Jahns a. Henke 2004, pp. 38-44; Henke et al. 2006; Jahns et al. 2006, p. 197)

In Figure 4 the position of the subsystem “supply early warning system” is highlighted. This subsystem in the overall supply risk management system includes all methods and techniques that are applied to identify, analyze, control and assess supply chain risks (Jahns et al. 2006, p. 199).

A Framework for Analyzing and Assessing Risks in Supply Chains

Identification of disruptions plays an important role in the assessment of supply chain risks (Teuteberg a. Ickerott 2007). In Table 2, we classify disruptions by means of several criteria in a morphological box. Morphological analysis was developed by Fritz Zwicky in the late sixties (Zwicky 1969) for multi-dimensional, non-quantifiable socio-technical systems and problems.

For example, a differentiation can be made between unplanned and standard disruptions (e.g. order change), unplanned and non-standard disruptions (e.g. lost shipment, natural disaster), planned and standard disruptions (e.g. change of production machines) and planned and non-standard disruptions (e.g. transport strike). In 2000, for example, a fire damaged the plant of Nokia’s and Ericsson’s main supplier, which delivers mobile phone components. For illustration, we classify this specific event "Plant fire" by means of our morphological box for disruption classification (see Table 2).

Table 2. Disruption classification & assessment (adapted from Teuteberg a. Ickerott 2007, p. 96)

Criteria	**Attributes**											
Category	planned						unplanned					
Type	standard						non-standard					
Frequency of disruption	minutely		hourly		daily		weekly		monthly		yearly	
Duration of disruption	short				medium				long			
Severity of disruption	negligible	minor	routine		serious		critical		catastrophe			
Probability of occurrence	unlikely				seldom		occasional		likely		frequent	
Cost/Disruption	low				medium				high			
Time/Disruption	low				medium				high			
Resources/ Disruption	low				medium				high			
Disruption producer	unknown						known					
Appropriate response personnel/experts	Internal						External					
Disruption Process Level (SCOR)	Operations Strategy (SCOR Level 1)			Intra- and Inter-Company Configuration (SCOR Level 2)			Intra- and Inter-Company Process, Practise and System Configuration Elements (SCOR Level 3)		Intra- and Inter-Company Supply Chain Improvements (SCOR Level 4)			
Location of disruption	Near to suppliers			Internal focus			Near to customers		Dual focus (pooling of responsibilities)			
SC Planning Influence	Short-term plans		Master plans	Aggregate plans			Logistics strategy plans		Business strategy plans		Corporate strategy plans	
SC Flow Level	Information flow			Goods flow					Cash flow			
Recommended actions	Acceptance		Avoidance	Assurance					Make or buy		Activity	

In recent years, the so-called risk map (risk portfolio) is often used to assess risks in supply chains. Figure 5 illustrates such a risk map, containing four types of risk responses (action steps) with regard to the likelihood of risk occurrence and the risk impact:

1) *Risk acceptance*: Risks that occur very seldom and that have a small impact can be accepted.
2) *Risk assurance* (transfer): Certain risks can be transferred to assurance companies.
3) *Make or buy (outsourcing):* Risk management activities can be conducted by the company itself or can be outsourced to third-party logistics providers.
4) *Activity:* Risk can be mitigated by avoiding or reducing risky activities as well as by reducing and preventing risks (e.g. training and education of employees).

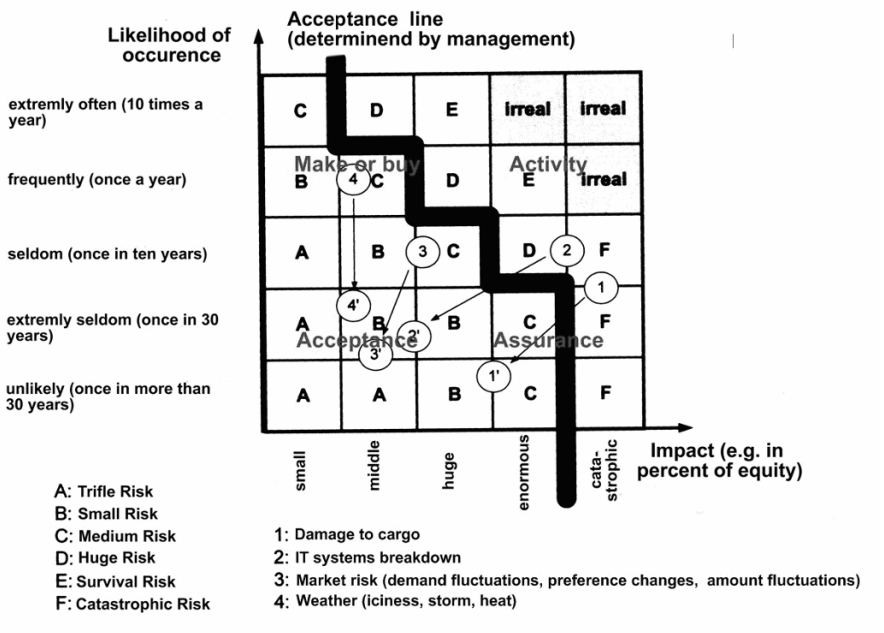

Fig. 5. Risk map (adapted from Königs 2006, p. 17)

The overall process of managing risks in supply chains is illustrated in Figure 6. The risk strategy (1), the development of security guidelines and risk metrics (2) as well as the following factors strongly influence the supply chain risk management system (3) and the implementation, planning and scheduling of action steps (4):

- *Political factors:* Political risks may originate from unstable political systems, a lack of political transparency, governmental business regulations and political conflicts.
- *Economic factors:* Economic risks may include globalization issues and growing markets (e.g. in China or Russia).
- *Social factors:* Social risks may originate from social disasters such as health pandemics (e.g. SARS) and terrorist attacks.

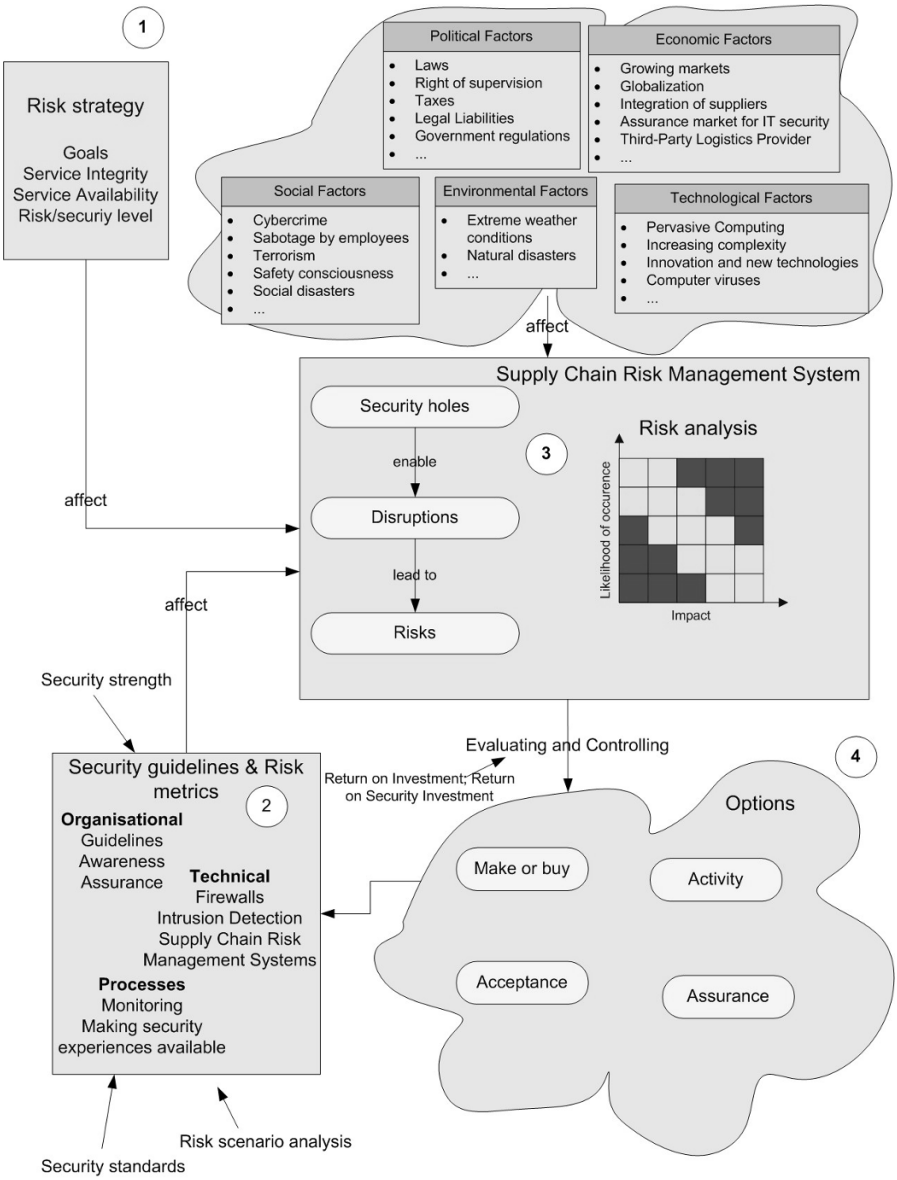

Fig. 6. Supply Chain Risk Management Framework (adapted from Müßig 2006, p. 42)

- *Environmental factors:* Environmental risks may arise from natural disasters such as earthquakes and extreme weather conditions (e.g. iciness).
- *Technological factors:* Technological risks may originate from IT failures, IT breakdowns or power cuts.

Supply Chain Monitoring – Risk Assessment Metrics

In order to monitor processes and disruptions in the supply chain to identify risks with regard to risk anticipation and avoidance, a risk measurement system needs to be implemented (Kleijnen a. Smits 2003; Svensson 2000). Metrics as quantitative risk indicators can be used to ensure an acceptable level of risk.
The key questions are:

- Which risk assessment metrics should be considered?
- How should they be used as guidelines for the formulation/revision of risk strategy?

Various metrics (risk indicators) that help quantify possible risk factors can be established in supply chain risk management (cf. Wisner et al. 2005, p. 66; Brewer a. Speh, 2000; Chan a. Qi 2003). Table 3 gives an overview of metrics that can be applied. In our neural network approach we use the metrics in Table 3 as input values for our neural networks.

Table 3. Risk Metrics (Indicators)

Metric	**Example (Risk Indicator)**
Cost/Price/ Financial	• Mean costs of production logistics per production order
	• Mean costs of transport per production order
	• Cost breakdowns
	• Willingness to negotiate price
	• Inventory cost, Transportation cost
	• Total cash flow, Rate of return on investment
	• Costs of defects, rework and problem-solving associated with purchases
Quality	• Degree of service, Complaint rate
	• Proportion of defects, Proportion of statistical process controls
	• Actual quality compared to: historical quality, specification quality, target quality
Delivery	• Delivery reliability/on-time delivery, Delivery quantity reliability
	• Delivery quality reliability/defect-free deliveries
	• Confirmation rate of customer's desired delivery date
	• Actual delivery compared to: promised delivery
	• Extent of co-operation leading to improved delivery, Changes in delivery schedules
	• Request, filled, prepared, delivered time, Transit type (airway, seaway, etc.)
Responsiveness and Flexibility	• Mean throughput time at goods exit
	• Order picking items per employee hour
	• Market reaction elasticity
	• Outstanding days payable
	• Average lead time
	• Ability to solve emergency problems in time

Environment	• Responsiveness to customers/Responsiveness to changing situations • Degree of participation in new product development • Degree of environmental responsibility • Environmental management system such as ISO 14000 • Extent of co-operation leading to improved environmental issues
Structure/ Organization	• Number of externally sourced articles, Number of customers, Number of suppliers • Proportion of quality inspections at goods arrival • Ratio of personnel costs/materials costs in logistics • Mean planned replacement time, Storage quota for raw materials • Turnover rate of the total inventory, Turnover rate for circulating material • Number of source material per product, Number of products • Proportion of logistics area, Proportion of external transport • Employee fluctuations • Reliability of supply network partner

A Neural Network Approach for Supply Chain Risk Management

By means of the proposed neural network approach, critical paths within a supply network can be anticipated (see Fig. 7). To determine the critical paths for each node and for each link in a supply network, a vector of risk metrics (see Table 3) has to be calculated. Nodes or edges (transport paths) are critical if their risk level is higher than a threshold value (e.g. risk level > 0.75), predefined in the risk strategy phase.

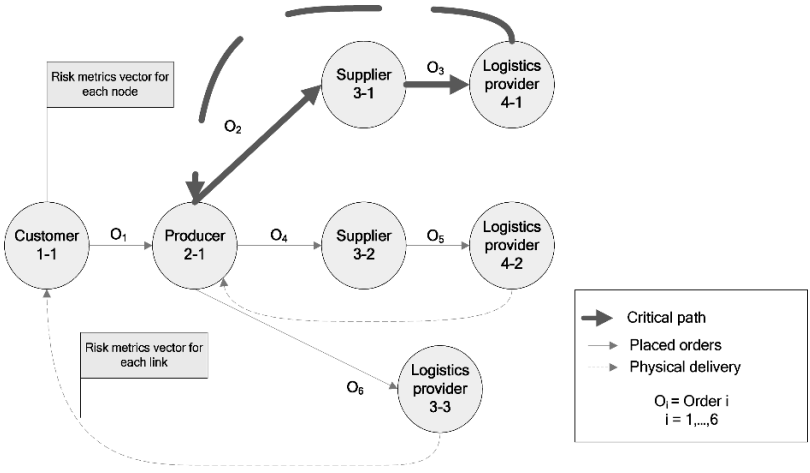

Fig. 7. Supply Network with critical path

For example, neural networks can be applied to calculate the probability of risk occurrence between the nodes of the supply network or at a specific node, as illustrated in Table 4, taking various risk metrics as input vectors. In Table 4, values with a risk level (probability of disruption occurrence) > 0.5 are highlighted in bold. In our example in Figure 7 and Table 4, a critical path can be determined between Producer 2-1, Supplier 3-1 and Logistics provider 4-1, because the risk level for each node and link is > 0.5.

Table 4. Risk Assessment Matrix

	Probability of disruptions at a specific link							**…at a specific node**
	1-1	2-1	3-1	3-2	3-3	4-1	4-2	
1-1	0	0.465	0.413	0.357	0.345	0.005	0.467	0.478
2-1	0.345	0	**0.976**	0.471	0.453	0.456	0.436	**0.599**
3-1	0.435	0.368	0	0.481	0.334	**0.911**	0.412	**0.612**
3-2	0.123	0.231	0.462	0	0.442	0.432	0.239	0.399
3-3	0.478	0.490	0.390	0.444	0	0.333	0.267	0.346
4-1	0.345	**0.957**	0.456	0.327	0.429	0	0.331	**0.685**
4-2	0.045	0.127	0.235	0.455	0.342	0.124	0	0.345

After identifying and visualizing critical nodes and edges in supply networks, appropriate action steps have to be considered (e.g. acceptance, avoidance, reduction, prevention, transfer (assurance), make or buy). For this purpose, nodes and edges can be transformed and visualized into the risk map (cf. section 3) using the probability of risk (disruption) occurrence and the risk impact (both values estimated by means of neural networks (cf. next section) as the x- and y-axis.

Neural Networks

Neural networks (for an introduction see Lippman 1987) are useful for solving classification problems and are well suited for complex information processing problems, since they are capable of learning from noisy data and generalizing (Bishop 1995). The first neural network model (perceptron) was developed by Rosenblatt in the late 1950s (Wassermann 1989). Since then, neural networks have been applied to various classification and prediction problems, for example in time series forecasting, stock market prediction, supply chain planning and pattern recognition (Bishop 1995; Bansal et al. 1998; Chiu a. Lin 2004; Vellidoa et al. 1999). Neural networks that are inspired by biological nervous systems can be described as a directed, weighted graph consisting of three or more layers: one input layer, one or more hidden layers and an output layer (see Fig. 8). The arcs represent the weighted connections between the processing elements (nodes). The nodes of the neural network are called neurons, which operate in parallel. w_{ij} is the weight of the connection between neuron *i* and neuron *j*.

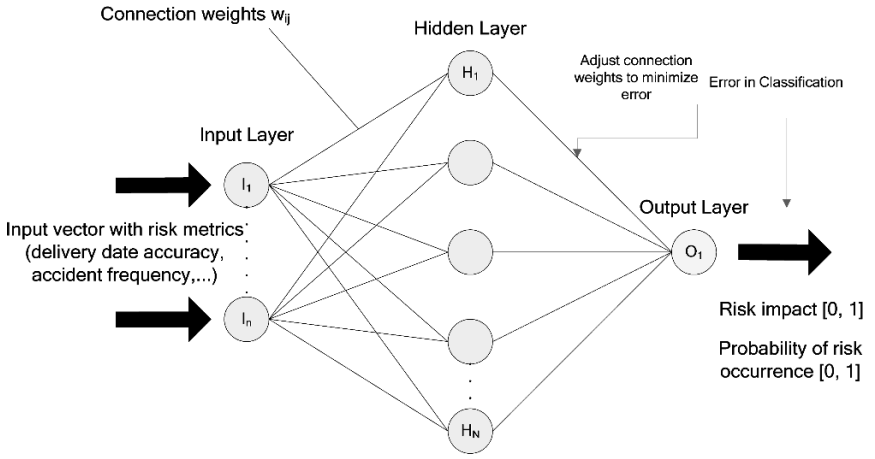

Fig. 8. Neural Network with one hidden layer

Figure 9 illustrates the three-step information processing sequence inside a neuron.

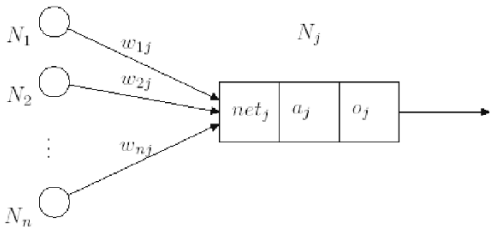

Fig. 9. Information processing in neurons (Wilbert 1996, p. 52)

All inputs, which themselves are also outputs of previous neurons, are multiplied with the associated weights and aggregated to a single value net_j, as shown in equation (1.1). This value net_j is passed on to the activation function, as shown in equation (1.2). Commonly used types of activation and output functions, respectively, include linear, quadratic or sigmoid functions. The new activation state of a neuron is a result based on the previous state and the net input. In the last step, the newly calculated activation state is used to compute the final output o_j, as shown in equation (1.3).

$$\mathrm{net}_j = \sum_i o_j \times w_{ij} \qquad (1.1)$$

$$a_j(t+1) = F_j(a_j(t), \mathrm{net}_j(t)) \qquad (1.2)$$

$$o_j = f_j(a_j) \qquad (1.3)$$

The input layer contains a number of elements that pass weighted inputs to the neurons of the hidden layer, according to the connection weights. Inputs to the neurons in our problem are risk metrics, as listed in Table 3. The neurons in the hidden layer process their inputs and propagate their outputs to the output layer, which produces the network's response. Outputs in our case are the probability of risk occurrence or the risk impact calculated in the intervals [0, 1]. Commonly, neural networks are trained so that a particular input leads to a specific target output. This adjusting (training) process is called *supervised learning*. Training means adjusting the values of the connections (weights) between the neurons.

Preliminary Experimental Results

The multi-layer perceptron (MLP) is the basic model of the work reported here. A simple MLP consists of three layers: an input layer, a hidden layer and an output layer. A commercial neural network simulation tool called *NeuroSolutions* (www.nd.com) was applied to implement the networks. NeuroSolutions provides several options with regard to learning algorithms, the number of neurons, the number of hidden layers, and other network parameters, which can be set by the user via a graphical editor. The software can be run within Excel, exploiting Excel's power and facilities for importing risk profiles as well as exporting and interpreting neural network results.

For our experiments we use a demonstration model of a supply network, delivered by the commercial simulation software called *Flexsim* (www.flexsim.com). The Flexsim supply network consists of three locations in Vancouver, Florida and California which order various helicopter parts. These parts were delivered by two distribution centers, two local trans-shipment centers and an original equipment manufacturer. The selection of suppliers depends on their availability. Transport of helicopter parts is possible both by air and via seaway.
Figure 10 illustrates the above-described supply network. In our experiments we anticipate the risk of orders by one node of the supply network via a specific transport way (airway, seaway). Based on several risk metrics, orders were considered "risky" (output value 1) or "not risky" (output value 0).

During simulation the Flexsim supply network demo generates data that can be exported in Excel spreadsheets as input vectors for our neural network simulator NeuroSolutions. In the training phase, a set of data, as illustrated in the Excel spreadsheet in Figure 11, is given as input to the neural network. The weights of the neural connections are adjusted such that the output of the network approximates the desired output (e.g. 0 or 1). To set the weights, the mean squared error (MSE) is computed. The MSE is the sum of the squared differences between the desired output and the actual output of the output neurons averaged over all training exemplars. A small value (e.g. close to zero) indicates that the network has learned well and is suited to the classification problem.

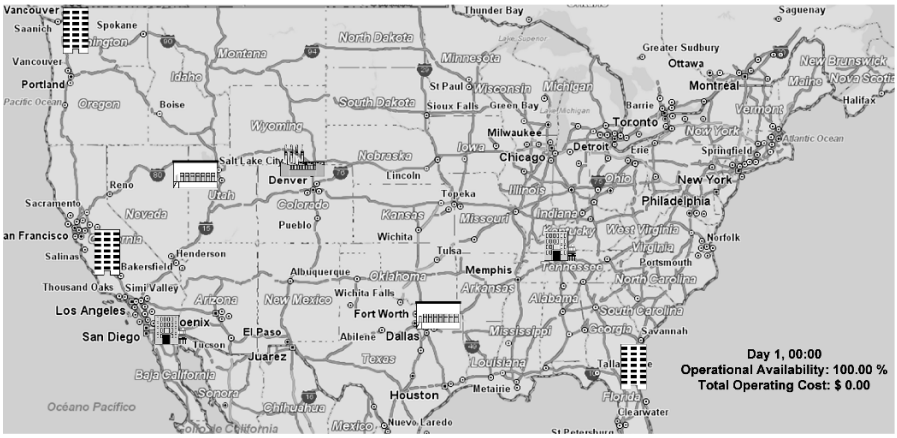

Fig. 10. Supply network demonstration of Flexsim

Risk metrics as outlined in Table 3 are coded and represented in Excel spreadsheets. Figure 11 shows an excerpt from such an Excel spreadsheet. Each row describes one input vector (risk profile). The columns contain the risk metrics. In real-life application scenarios such risk profile data can be automatically generated via sensor networks, data warehouses, ERP systems, global positioning systems and Auto-ID/RFID systems.

For our experiments we use the data of 20 simulation days in Flexsim. The first 15 simulation days are used as training data and the next five days are used as test data for our neural networks. Thus we can train and test our neural networks with 424 input vectors (106 for testing and 318 for training the networks).

	A	B	C	D	E	F	G	H	I	J	K	L
1	part ID	requesting station index	part priority	request time	filled time	prepared time	shipped time	providing station index	shipment number	transit type	delivered time	reason for starting travel
2	3	2	2	3,5388	3,5388	4,5388	4,5388	4	1	2	17,2804	2
3	3	4	2	3,5388	42,9476	43,9476	43,9476	7	32	2	56,3864	2
4	5	1	1	3,6012	3,6012	4,6012	4,6012	4	2	1	11,5394	1
5	5	4	3	3,6012	3,6012	4,6012	7,936	6	3	2	28,2822	2
6	5	6	3	3,6012	44,4784	45,4784	61,0473	8	33	2	69,7434	2
7	10	1	1	6,3352	7,3352	8,3352	8,3352	6	6	1	24,4989	1
8	11	1	2	6,936	6,936	7,936	7,936	4	4	2	21,9998	2
9	11	4	2	6,936	6,936	7,936	7,936	6	3	2	28,2822	2
10	11	6	2	6,936	17,1623	18,1623	18,1623	8	14	2	26,9595	2

Fig. 11. Excerpt of the Excel spreadsheet with input vectors

Table 5 shows the best training and testing results from our experiments with multi-layer perceptron networks. The MLP with four hidden layers and 75 neurons in each hidden layer turned out to be the winner. When this network was run to classify the training set, 94.2 of all risk profiles were classified correctly.

In our experiments, we applied MLP networks with one, two, three and four hidden layers and linear activation functions for the input and output layer. For the hidden layers we applied sigmoid activation functions (see the first three columns in Table 5). Additionally, we chose an indifferent window by means of the following rule to improve classification accuracy: *If output value > 0.75 then disruption will occur, else no disruption will occur at a supply network node/link.* Correct classification means a disruption has occurred at a specific link or node in our simulation and the neural network has anticipated this disruption correctly (e.g. output value > 0.75). Correct classification also means that no disruption has occurred and the neural network has also diagnosed this case correctly. The test data (last column of table 3) are unknown and have not been presented as input vectors for the neural networks before. Thus, the classification rate is not as good as with training data.

Table 5. Preliminary classification results from training and testing neural networks

Layers Activation function			**Correct classification Data sets (training)**	**Correct classification Data sets (test)**
In	**Hidden**	**Out**		
linear	1 sigmoid	linear	92.3%	83.8%
linear	2 sigmoid	linear	91.4%	82.7%
linear	3 sigmoid	linear	93.3%	84.7%
linear	4 sigmoid	linear	94.2%	86.6%

Our neural network training process was not as time-consuming as often claimed in the literature (in our experiments, it took less than ten minutes for 318 training data sets). Performance of the neural networks was also very good. Trained neural networks generate an output in less than 3 seconds when an unknown input vector with risk metrics is given as input for the input layer. Many other application scenarios of neural networks for supply chain risk management can also be considered. We are currently estimating suppliers' delivery times by means of neural networks and are ranking suppliers based on several supplier metrics (e.g. delivery costs, delivery time, etc.).

Neural Network Approach – Pros and Cons

Table 6 summarizes the pros and cons of our proposed neural network approach for supply chain risk management.

Table 6. Pros and cons of the neural network approach

Pros	Cons
▪ Neural networks learn from real-life cases (like a human brain) ▪ Anticipation of disruptions and risks is possible (even risk impact can be estimated) ▪ A "learning" supply network represented by a learning neural network can be established ▪ Neural networks determine coherences between risk metrics and the occurrence of disruptions ▪ Neural networks are flexible and can be adjusted to new risk scenarios ▪ They are capable of learning from noisy data and of generalizing ▪ Neural networks are very well suited for complex information processing	▪ Selection of appropriate training data is difficult ▪ Coding of training and test data sets ▪ Neural network is a “black box” (output results are not intuitive and sometimes difficult to interpret) ▪ The number of nodes in the hidden layer(s) and the number of hidden layers has to be determined via experimentation in a “trial-and-error” process (no criteria for the ”optimal” design of a neural network in a specific application domain) ▪ Too many nodes lead to overfitting. On the other hand, too few nodes reduce classification accuracy

Correlations (interdependencies) between risk metrics (indicators) are difficult to detect by supply chain decision-makers. For this reason, a rule-based approach in supply chain risk management is not the first choice. Instead, neural networks are capable of learning from past disruptions and are more flexible than static if-then rules (e.g. if delivery time is > 2 hours then…). By applying our neural network approach supply network members can

- understand the supply risk that exists,
- proactively assess the probability and impact of supply risk in advance,
- reactively learn from disruptions that occurred in the past and can thus improve their supply chain risk management system.

Conclusions and Future Research

In this chapter, a supply chain risk management approach based on neural networks was presented. Our first aim was to classify risk profiles of supply network nodes and links (transportation paths). For this purpose, several MLP networks were tried. All networks performed quite well. The winner, an MLP with three hidden layers and 75 neurons per hidden layer, exhibited reasonable generalization capability. When exposed to new data sets (unknown risk profiles), it classified 86.6% on average correctly. Today, the automatic observation and management of disruptions and other irregularities in supply networks is generally limited to single supply chain members. The neural network approach presented in this chapter is intended to integrate data from single members so that all members can assess and visualize risk profiles.

In this final section, we would like to discuss a number of problems and topics for further research in supply chain risk management based on neural networks. Challenges still to be solved include (Teuteberg a. Ickerott, 2007, p. 120):

- *Information overflow:* The mass of products, machine data and other resources that have to be scanned and transmitted in a supply network have to be managed in time-critical processes due to constraints in available bandwidth and computing power (Angeles 2005, p. 55).
- *Lack of co-operation:* Although our proposed approach provides a promising method of risk management in supply networks, supply network nodes can still refuse to share their information (risk profiles) with their partners.
- *Lack of honesty and hiding of information:* Supply chain partners could hide important information (e.g. data about disruptions) from each other in order to optimize individual utility, or they may be dishonest. Or else they may believe that they can solve problems before they start affecting other supply network members and may wait instead of alarming other members immediately. Thus, trust is an important prerequisite in our approach for transmitting risk metrics between supply network partners.

In future, it is intended to simulate typical business processes in supply networks and conduct neural network experiments based on real-world data (risk profiles) from business partners in order to see if our approach performs well in real-life, too.

Acknowledgements

This work is part of the research project “Mobile business processes and user interfaces based on Wireless Internet” (Mobile Internet Business) funded by the German Federal Ministry of Education and Research (http://mib.uni-ffo.de).

I would also like to thank Dipl.- Kfm. Jochen Friedemann for various discussions in the context of this work.

References

Angeles R (2005) RFID Technologies: Supply-Chain Applications and Implementation Issues. Information Systems Management, 1:51-65

Bansal K, Vadhavkar S, Gupta A (1998) Brief Application Description. Neural Networks Based Forecasting Techniques for Inventory Control Applications; Data Mining and Knowledge Discovery. 2/1:97-102

Barry J (2004) Supply chain risk in an uncertain global supply chain environment. International Journal of Physical Distribution & Logistics Management. 34/9:695-697

Bishop CM (1995) Neural Networks for Pattern Recognition, Oxford

Brewer PC, Speh TW (2000) Using the balanced scorecard to measure supply chain performance. Journal of Business Logistics 21/1:75-93

Chan FTS, Qi HJ (2003) An innovative performance measurement method for supply chain management. Supply Chain Management: An International Journal 8/3:209-223

Chiu M, Lin G (2004) Collaborative supply chain planning using the artificial neural network approach. Journal of Manufacturing Technology Management 15/8:787-796

Chopra S, Sodhi M (2004) Managing Risk to Avoid Supply Chain Breakdown. MIT Sloan Management Review 46/1:53-61

Christoper M, Peck H (2004) Building the resilient Supply Chain. International Journal of Logistics Management 15/2:1-13

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004) Enterprise Risk Management – Integrated Framework. Executive Summary. http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.

Engelhardt-Nowitzki C, Zsifkovits H (2006) Complexity-Induced Supply Chain Risks – Interdependencies Between Supply Chain Risk and Complexity Management. In: Kersten W, Blecker T (eds) Managing Risks in Supply Chains: How to Build Reliable Collaboration in Logistics, pp. 37-56, Berlin

Hallikas J, Virolainen V, Tuominen M (2002) Risk analysis and assessment in network environments: a dyadic case study. International Journal of Production Economics 78/1:45-55

Harland C, Brenchley R, Walker H (2003) Risk in supply networks. Journal of Purchasing & Supply Management 9/1:51-62.

Henke M, Kurzhals R, Jahns C (2006) Enterprise and Supply Risk Management from the Perspective of Internat and External Auditors. In: Kersten W, Blecker T (eds) Managing Risks in Supply Chains: How to Build Reliable Collaboration in Logistics. pp. 97-109, Berlin

Jahns C, Henke M (2004) Supply Risk Management. Management- und Überwachungssystem nach KonTraG zur systematischen Risikobeherrschung, Beschaffung aktuell, 4:38-44

Jahns C, Hartmann E, Moder M (2006) Managing Supply Risks: A System Theory Approach to Supply Early Warning Systems. In: Kersten W, Blecker T (eds) Managing Risks in Supply Chains: How to Build Reliable Collaboration in Logistics. pp. 195-212, Berlin

Jung JY, Blau G, Pekny J, Reklaitis G, Eversdyk D (2004) A simulation based optimization approach to supply chain management under demand uncertainty; Computer and Chemical Engineering 28/10:2087-2106

Jüttner U (2005) Supply chain risk management: Understanding the business requirements from a practitioner perspective. The International Journal of Logistics Management 16/1:120-141

Kersten W, Böger M, Hohrath P, Späth H (2006) Supply Chain Risk Management: Development of a Theoretical and Empirical Framework. In: Kersten W, Blecker T (eds) Managing Risks in Supply Chains: How to Build Reliable Collaboration in Logistics, pp. 3-17, Berlin

Kleijnen JPC, Smits MT (2003) Performance metrics in supply chain management. Journal of the Operational Research Society 54/5:507-514.

Königs HP (2006) IT-Risiko-Management mit System, Wiesbaden

Lippman RP (1987) An introduction to computing with neural nets; IEEE ASSP Magazine, 2:4-22

March JP, Shapira Z (1987) Managerial Perspectives on Risk and Risk Taking, Management Science, 33:1404

Müßig S (2006) Haben Sicherheitsinvestitionen eine Rendite? HMD, 248, April 2006, pp. 35-43

Müssigmann N (2006) Mitigating Risk during Strategic Supply Network Modeling. In: Kersten W, Blecker T (eds) Managing Risks in Supply Chains: How to Build Reliable Collaboration in Logistics, pp. 213-226, Berlin

Ritchie B, Brindley C (2007) Supply chain risk management and performance: A guiding framework for future development. International Journal of Operations & Production Management 27/3:303-322

Smeltzer L, Siferd S (1998) Proactive supply management: the management of risk, Journal of Supply Chain Management 34/1:38-45

Spekman RE, Davis EW (2004) Risky business: expanding the discussion on risk and the extended enterprise. International Journal of Physical Distribution & Logistics Management 34/5:414-433

Svensson G (2000) A conceptual framework for the analysis of vulnerability in supply chains. International Journal of Physical Distribution & Logistics Management, 30/9:731-749

Teufel S, Erat A (2001) Sicherheitsmanagement im Electronic Business. In: Meier A (eds) Internet & Electronic Business, Zürich

Teuteberg F, Ickerott I (2007) Mobile Supply Chain Event Management Using Auto-ID and Sensor Technologies - A Simulation Approach. In: Jung H, Chen FF, Jeong B (eds) Trends in Supply Chain Design and Management: Technologies and Methodologies, Springer Series in Advanced Manufacturing, pp. 93-126

van Wyk J, Baerwaldt W (2005) External Risks and the Global Supply Chain in the Chemicals Industry. Supply Chain Forum: An International Journal 6/1:1-15

Vellidoa A, Lisboaa PJG, Vaughanb J (1999) Neural networks in business: a survey of applications (1992–1998); expert systems with applications, 17:51-70

Vidal CJ, Goetschalckx M (2000) Modeling the effect of uncertainties on global logistics systems. Journal of Business Logistics 21/1:95-120

Wasserman PD (1989) Neural Computation: Theory and Practice, New York

Wilbert R (1996) Interpretation und Anwendung Neuronaler Netze in den Wirtschaftswissenschaften, Frankfurt/Main

Zsidisin G (2003) Managerial perceptions of supply risk. Journal of Supply Chain Management 39/1:14-26

Zsidisin GA, Ellram LM, Carter JR, Cavinato JL (2004) An analysis of supply risk assessment techniques. International Journal of Physical Distribution & Logistics Management 34/5:397-413

Zsidisin GA, Panelli A, Upton R (2000) Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study; Supply Chain Management. An International Journal 5/4:187-198

Zwicky F (1969) Discovery, Invention, Research – Through the Morphological Approach. The Macmillian Company, Toronto