RESEARCH PAPERS OF THE WROCŁAW UNIVERSITY OF ECONOMICS
No. 35 — 2008
Advanced Information Technologies for Management – AITM 2008

**Paolo Ceravolo, Stelvio Cimato, Ernesto Damiani,
Fulvio Frati, Gabriele Gianini, Cristiano Fugazza,
Stefania Marrara, Olga Scotti**

University of Milan, Milano, Italy
{ceravolo,cimato,damiani,frati,fugazza,gianini,marrara,oscotti}@dti.unimi.it

HAZARDS IN FULL-DISCLOSURE SUPPLY CHAINS

Abstract: Supply chain optimization is based on information shared with other partners or with a trusted external decision maker. Some works in the literature assume the full-disclosure paradigm, thinking that a peer increases the confidence in the alliance. In contrast to this claim, we underline that each participant to the coalition has its own objectives which need to be re-conciliated with the achievement of the common good. If achieving such common good requires completely missing their objectives, participants may be tempted to adopt a non-cooperative behavior. For this reason, supporting the representation and evaluation of information sharing risks is an important requirement for implementing advanced supply chain management procedures. In particular in this work we discuss a methodology for analyzing information flow and identifying the data items that, if shared, can increase the risk of non-cooperative behavior. Also we demonstrate that, under given conditions, obfuscating this information can be a sufficient requirement for making cooperative behavior the best strategy to be adopted by participants.

1. Introduction

Risk Assessment is a relevant problem in supply chain configuration. It is widely recognized [Juttner 2005] that supply chain models need to be enhanced to include means by which risks can be represented and addressed, increasing the supply chain's resilience. Several publications mention how certain characteristics of a supply chain might increase or decrease the risk of negative outcomes [Helferich, Cook 2002; Norrman, Lindroth 2004]. On the other hand, analyzing methodologies and tools available for supply chain management (e.g., those in the surveys [Brun et al. 2005] and [Gunasekaran et al. 2004]) a scarce development of risk assessment procedures can be noted; in particular, they do not address risks related to information disclosure.

Traditionally, the notion of Supply Chain Risk has been used to designate various types of unfavorable events (see [Gaonkar, Viswanadham 2004] for a classification), such as for instance volatility of the demand [Juttner et al. 2003], technological or market dependencies [Hallikas et al. 2004], supplier concentration [Tang 2006], scarce sources [Park, Ungson 2001], or social and natural environment [Peck 2005]. Also, as any collaborative alliance, supply chains need to be founded on trust among parties, and the perception of a risk can even cause the abandonment of the supply chain. Note that the risk assessment procedure, in case of information disclosure, requires an analysis that radically differs from the methodologies usually proposed in the literature. This is because much attention was paid to external factors [Juttner et al. 2003; Peck 2005], undertaking risk assessment as qualitative evaluation of the contingencies.

On the contrary, when focusing on information disclosure the risks to be identified are internal to the supply chain and relate to the actions one actor can undertake for damaging the other partners, using the information shared in the supply chain. Typical actions to be monitored consist in the introduction of fake information to orient the distribution of orders in favor of itself. For this reason, a methodology for assessing disclosure risk requires a representation of information flow, the data items exchanged, and the identification of configurations that can lead to opportunistic behaviors.

Collaborative supply chain management largely consists of the combined optimization of supply and delivery within the virtual organization defined by the supply chain boundaries. Optimization is carried out to sustain competition with other supply chains working in the same business area. Supply chain optimization is based on data provided by each partner in the supply chain. In other words, each actor needs to share information with other partners or with a trusted external decision maker. Some works in the literature assume that increasing information sharing is automatically a factor of quality, because it increases the confidence in the alliance [Christopher, Lee Hau 2004; Lee Hau, Whang 2000]. This gives rise to full-disclosure supply chains, i. e. supply chains where all information is made available to all actors, e. g. via a shared white-board mechanism.

In contrast to this claim we underline that managing a supply chain implies the resolution of a social dilemma [McCarter, Northcraft 2007]. Actually, each actor participates to the coalition with its own objectives, which need to be re-conciliated with the achievement of the common good. We can assume that individual actors will be willing to co-operate toward global optimization, seen as the coalition's common good; but if achieving such common good requires completely missing their objectives, actors may be tempted to adopt a non-cooperative behavior, e.g. by altering the information used for the global optimization in order to push the coalition back to a situation fairer to them.

This conflict of interest and the resulting risk can be described as an information sharing problem. The data to be shared may include information usually kept con-

fidential within the company, like per-item production and transport costs, prices, stock levels, and other inventory. Their release or sharing can induce an assessment on the part of each actor of its own profitability. In other words, if revealed, this information can lead to non-cooperative behavior on the part of some actor [Von Lanzenauer, Pilz-Glombik 2002]. Therefore, supporting the representation of the information shared is an important requirement for evaluating risk of information disclosure in specific supply chain configurations.

In this work, we describe the framework for disclosure risk assessment we are developing in the context of the SecureSCM FP7 project [*Secure*… 2008]. In particular, our goal is to analyze information flow in order to detect the data items that, if shared, increase the risk of adoption of non-cooperative behaviors among participants. The paper is structured in the following way. Section 1 discusses the context and the motivation of this work. Section 2 provides an overview on the model adopted in order to configure the supply chain. Section 3 proposes a detailed example, where the elements of our methodology are depicted. In particular, Section 3.1 describes the full-disclosure scenario. Section 3.2 shows that this scenario is prone to attacks altering the information flow with fake declarations. Section 3.3 discusses the possible countermeasures that can be adopted to reduce risk of attack.

2. Modeling supply chain enactment

The main purpose of our current research is monitoring information flow; particularly, we are interested in the data items that can be exploited by an actor in order to augment its own profit at the expense of the common good. Such monitoring involves the assessment of the risk associated with an actor with respect to a given data item. It is clear that the topological features of the supply chain being established is of foremost importance for determining the probability of deviant behavior by an actor. Consequently, an important prerequisite to an effective coalition monitoring is a sound, expressive model for representing the coalition's value interchanges.

When selecting a feasible representation scheme for supply chains, we considered a broad range of formalisms. As an example, *Business Process Models* (BPM) (e.g. BPMN [*Business*… 2006], UML activity diagram [OMG 2003], etc.) provide very expressive means to describe the actions that are carried out by actors as well as the interaction between the distinct parties but the former are of little interest in our scenario. Among this category of formalisms, we selected a modeling technique which also allows for a graphical representation, the e^3value model [Gordijn, Akkermans 2003]. The formalism is grounding a tool for visual design of supply chains and envisages a logic-based representation. Moreover, the tool supports the generation of pre-formatted spreadsheets on the basis of the parameters defined in a value model; aside default parameters, we introduce the formulas that are used in the risk assessment analysis.

With this goal in mind, we extended the e^3value model with the parameters defined by a specific SCM model, expressing the actors involved in the supply chain and the information flow they generate when interacting with each other. For additional details, please refer to [Ceravolo et al. 2008a].

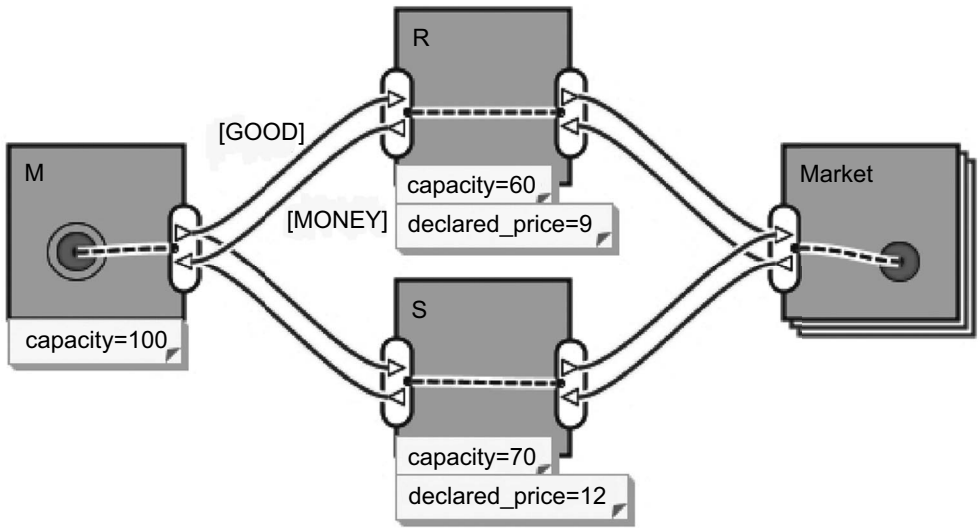

Figure 1. The e^3value view of our SCM model

Source: own elaboration.

A sample supply chain expressed in this formalism is shown in Figure 1 and depicts the example that will be considered in the following parts of this paper. It consists of a manufacturer M selling its product (indicated by value object GOOD) by means of resellers R and S. Each actor has a maximum capacity bounding the distribution of goods; moreover, resellers are required to declare the sale price for the value object to enable the supply chain enactment.

To evaluate the supply chain configuration we compare the indicators *Maximal Profitability*, the supply chain configuration where profit is maximal, with the *Shapley Value*, representing the fairness of the profit distribution. A description of the equations expressing these indicators can be found in [Damiani et al. 2008] (respectively equations 1 and 2).

For example, using the e^3value tools and assuming a white-board scenario, we will execute a simulation showing for which values of parameter declared_price R could move profit toward its Shapley by lying on the sale price (Figure 2), as better described in Section 3.2. If this action is possible, the simulation demonstrates that parameter declared_price cannot be shared among actors without increasing the risk of actor R to misbehave.

NAME	R	R
UID	4	4
profit	e^3	135
capcity	60.0000	60
revenue	e^3	270
declared_price	9.00000	9
shapley_value	e^3	180

(a)

NAME	R	R
UID	4	4
profit	e^3	150
capcity	60.0000	60
revenue	e^3	540
declared_price	9.00000	13
shapley_value	e^3	180

(b)

Figure 2. Tabular representation of SCM parameters of the example shown in Figure 1
Source: own elaboration.

We consider hereafter a specific example. In particular, in our example we will show that adopting a full-disclosure paradigm allows actors to compute between the revenue they get under Maximal Profitability conditions and their Shapley Value. Having such information, actors can evaluate the introduction of fake information to move the distribution of profits toward their Shapley Value. Several countermeasures can be taken in order to prevent opportunistic behaviors. In particular, we will discuss the adoption of a configuration paradigm limiting the disclosure of such information that are potentially risky for the overall supply chain.

3. An example of supply chain analysis

Our intent is to evaluate which actor, in the supply chain, is prone to adopt an opportunistic behavior abusing of the knowledge of certain information.

The structure of the chain

We consider here a Supply Chain consisting in three actors: a manufacturer M and two resellers R and S, subject to the following assumptions:

– the production capacity of the manufacturer is equal to 100 product units,
– the absorption capacity of the market is exactly equal to 100 product units,
– the reselling capacity of R is equal to $\theta_R = 60$ at the price of 9 €,
– the reselling capacity of S is equal to $\theta_S = 70$ at the price of 12 €.

Each reseller is aware of the other reseller's capacity.

The maximum revenue of the chain is obtained when M gives 70 product units to S and 30 to R: the maximum revenue amounts to 1110 €. The Chain as a whole is interested in setting its working point on the optimum (we can assume, for instance, that from the revenue a percentage – say 20% – is taken so as to be re-invested into common infrastructures, we will indicate this as the *infrastructure-tax*) for this reason a rule is stated (but not necessarily enforced as we will see) whereby the price, for each product unit, paid by the reseller to the manufacturer should be *half* of the price at which the product is resold (from now on this will be indicated as the

half-price rule). Consequently, M is prone to allocate products by first saturating the capacity of the reseller which is most profitable to him: the manufacturer will drive the chain towards the maximum, simply following an egoistic goal.

We will consider two main scenarios:

– in the first everyone behaves honestly, either by its own sake or due to the fact that there is a strong enforcement of the *half-price* rule;
– in the second scenario resellers are allowed to lie over the reselling price (only if they declare a reselling price higher than the actual one: it is strongly enforced only the rule whereby no reseller is allowed to declare a lower reselling price); the manufacturer M will give priority to the reseller which declares the highest price.

In the first scenario we assume that resellers know each other's reselling price. In the second scenario we will assume each reseller is not aware of the other reseller's reselling prices.

3.1. First scenario: Everybody tells the truth

If everyone tells the truth:

– R pays to M 4.5 € apiece, whereas
– S pays to M 6.0 € apiece, hence
– M delivers first to S 70 units (obtaining 6 € apiece, for a total of 420 €),
– M then delivers to R 30 units (obtaining 4.5 € apiece, for a total of 135 €, a grand total to M of 555 €).

The revenues and profit margins from the above mentioned product units are:

– S obtains a revenue of 70*12 = 840 € (a margin of 840 – 420 = 420 €),
– R obtains a revenue of 30*9 = 270 € (a margin of 270 – 135 = 135 €).

Table 1. Calculation of the Shapley Value at the optimum operation point of the supply chain

Contribution to the coalition			
Permutation	*M*	*R*	*S*
M,*R*,*S*	0	540	480
M,*S*,*R*	0	270	840
R,*M*,*S*	540	0	480
R,*S*,*M*	1110	0	0
S,*M*,*R*	840	270	0
S,*R*,*M*	1110	0	0
Σ	3600	1080	1800
Shapley Value	600	180	300

Source: own calculations.

The grand total revenue of the supply chain is 840+270 = 1110 €. Since we assumed the products where generated at zero cost, also the profit margin of the supply chain is 300+630+180 = 1110 € (if we still assume the chain apply an "infrastructure tax" of 20%, then the value reinvested in the chain is 222 €). Hence at the optimum working point the profit margins to M, R and S respectively are 555, 135 and 420 €.

Shapley Value and Delta computation

If we compute the Shapley Value (for details of the computation see [Ceravolo et al. 2008b]) of the individual actors M, R and S, however, we find out – as shown in Table 1 – that they are 600, 180 and 300 € respectively. Reseller R in a white-board situation can compute his own Shapley Value and find out that his own marginal profit is far below his Shapley Value. Here the difference for R is $\Delta = 180-135$ €, i.e. $\Delta = 55$ €. In percentage it is 55/135 = 0.41, i.e. 41%. Furthermore reseller R can notice that reseller's S marginal profit is far above her own Shapley Value. Hence a higher propensity of reseller R to deliver an attack. As we will see, reseller R can hope to gain from the attack 15/135 = 0.11, i.e. to recover 11% of the gap.

3.2. Second scenario: Reseller R lies over the retail price

Let us assume it is possible to lie over the retail price (in excess only), and that R lies unilaterally. If R lies over his retail price and declares that he will sell at 13 € (one euro more than the competitor, in place of the actual 9 €), he will pay to M an amount 6.5 € apiece and will obtain the priority over S. (Note that we could imagine also that there is no half-price rule, and assume simply that R offers to M 6.5 € apiece). If R declares (lying) that he will sell at 13 € while S states (telling the truth) that she will sell at 12 €, then

- R pays to M 6.5 € apiece, whereas
- S pays to M 6.0 € apiece, hence
- M delivers first to R 60 units, obtaining a margin of 6.5 € from each, for a total margin of 390 €,
- M then delivers to S 40 units, obtaining a margin of 6.0 € from each, for a total margin of 240 €, and a grand total profit margin of 630 €.

From the mentioned product quantities:

- R obtains a revenue of 60*9 = 540 € (a margin of 540−390 = 150 €),
- S obtains a revenue of 40*12 = 480 € (a margin of 480−240 = 240 €).

The overall revenue of the chain is 540+480 = 1020 €.

Impact

As a consequence of the attack:

- M, who has gained 630 €, has increased its own profit by 630−555 = 75 €;
- R, who has gained 150 €, has increased its own profit by 150−135 = 15 €, getting closer to his own Shapley value of 180 € (Figure 2 gives an example of automatic calculation of this Δ);
- S, who has gained only 240 €, has decreased its own profit by 420−240 = 160 €;

– the overall chain has lost an amount of 90 € in revenue (if the chain takes 20% "infrastructure tax" the value reinvested is 204 €: 18 € less than before).

3.3. Countermeasures against R's attack in white board regime

Individual countermeasures

In a white-board scenario S can predict the above mentioned attack and can prevent the attack by declaring that she will sell at 14 €: she will pay 7 € to M: her per-unit margin goes from 6 € to 5 €, however she keeps the priority over R and gets 70 units of products, corresponding to a marginal payoff of 350 € (against the 240 € left by R's attack): at this point R can no longer attack, because to beat S's bid he should bid more than 7 € apiece, however already at 7 € his margin drops to 2 € apiece, which at full capacity would get him 120 €, less than what he gets for telling the truth.

Countermeasures based on economical incentives

In a white-board scenario the chain should find 150−135 = 15 € to give to R as an incentive to dissuade him from attacking. Those 15 € could for instance be taken from the 222 € of infra-structural tax at the maximum, this would still leave 207 € to reinvest.

3.4. Countermeasures based on obfuscation

Let us assume there is no white-board and the resellers cannot know each other's prices. If R cannot see S declaration, he cannot know for sure what is the price at which S will resell the products, but has to rely on probabilistic estimates, or priors. It is reasonable to assume that his own prior about S price would be approximately centered around his own actual reselling price (his own market perception).

If we examine all the strategies available to R and for each one compute the expected marginal payoff on the basis of the prior probability distribution of the values at which S could sell, we will see that R's attack gets discouraged.

The available strategies to R consist in paying respectively 4.5, 5.0, 5.5, 6.0 and 6.5 € apiece we have seen that paying 7.0 € is not profitable to R. Now we will compute the payoff of each strategy in case the strategy has success, then we will make some hypotheses about the prior distributions and see, for each prior, the probability of each strategy's success: putting the information together we will compute for any given prior the expected payoff of each strategy and see which is the strategy with the highest payoff.

3.4.1. Strategies' payoffs

Strategies consisting in paying less than 4.5 € to M are made impossible by the system policy, whereas strategies consisting in paying 7.0 or more, as we have seen above, are not profitable to R. The full range of viable strategies to R is the following:

STR-4.5 Paying 4.5 apiece to M. This is equivalent to telling the truth. It will win the priority (i.e. get to R the full capacity 60) only if S pays to M less than 4.5.

STR-5.0 Paying 5.0 apiece to M. Wins priority only if S pays M less than 5.0.

STR-5.5 Paying 5.5 apiece to M. Wins priority only if S pays M less than 5.5.

STR-6.0 Paying 6.0 apiece to M. Wins priority only if S pays M less than 6.0.

STR-6.5 Paying 6.5 apiece to M. Wins priority only if S pays M less than 6.5.

Let us look now at the marginal profit, i.e. the payoff of each strategy, considering that if it wins the priority will bring to R 60 product units otherwise only 30 product units:

STR-4.5 If successful, brings to R 4.5 * 60 = 270 € if not, the half 135.

STR-5.0 If successful, brings to R 4.0 * 60 = 240 € if not, the half 120.

STR-5.5 If successful, brings to R 3.5 * 60 = 210 € if not, the half 105.

STR-6.0 If successful, brings to R 3.0 * 60 = 180 € if not, the half 90.

STR-6.5 If successful, brings to R 2.5 * 60 = 150 € if not, the half 75.

3.4.2. Priors

From the point of view of R, when the other reseller's prices are obfuscate everything works as if Nature were setting the price S to M at an unknown value taken from a prior probability distribution of possibilities known to R.

An Example Prior

Let us assume for example that the prior known to R is the uniform density from 2.5 to 7.5: then the expected payoff of each strategy is:

STR_4.5: 4/10 * 270 + 6/10 * 135 = 189

STR_5.0: 5/10 * 240 + 5/10 * 20 = 180

STR_5.5: 6/10 * 210 + 4/10 * 105 = 168

STR_6.0: 7/10 * 180 + 3/10 * 90 = 153

STR_6.5: 8/10 * 150 + 2/10 * 75 = 135

It turns out that the strategy consisting in "telling the truth" is the winning strategy, i.e. the strategy with the highest expected payoff.

Other example priors

The same conclusions hold if we use as a prior several other likely distributions, such as the uniform density between 2.0 and 7.0 and the uniform density between 3.0 and 8.0. This holds also for the uniform located between 4.5 and 9.5:

STR_4.5: 0/10 * 270 +10/10 * 135 = 135

STR_5.0: 1/10 * 240 + 9/10 * 120 = 132

STR_5.5: 2/10 * 210 + 8/10 * 105 = 126

STR_6.0: 3/10 * 180 + 7/10 * 90 = 117

STR_6.5: 4/10 * 150 + 6/10 * 75 = 105

Telling the truth R knows with certainty he will obtain the minimum, i.e. 135, however, lying, in average gets only the things worse, in average: in all the above cases the cumulative of the density – which represents the probability that the strategy succeeds in gaining the priority – does not increases rapidly enough to compensate for the loss of marginal profit.

A special example prior

The case where R knows that the value paid by S is located uniformly between 4.5 and 5.5 is completely different. In this case:

STR_4.5: 0/10 * 270 + 10/10 * 135 = 135

STR_5.0: 5/10 * 240 + 5/10 * 120 = 180

STR_5.5: 10/10 * 210 + 0/10 * 105 = 210

Hence with this prior it is convenient to lie, adopting strategy STR-5.5, i.e. paying 5.5 € apiece. However this happens because the probability here is pretty localized: normally we can assume that after the obfuscation the knowledge of S's value with such a precision is not possible.

4. Conclusions

We discussed the adoption of a methodology for risk assessment of information disclosure in the enactment of supply chains. We showed that adopting a full-disclosure paradigm allows actors to computer a Δ between the revenue they get under Maximal Profitability conditions and their Shapley Value. Having such information actors can evaluate the introduction of fake information to move the distribution of profits toward their own Shapley Value. The possible counteractions may range from the introduction of economical incentives to the obfuscation of critical information. Countermeasure based on obfuscation were discussed, demonstrating that, under given conditions on the distribution of the prior probability, obfuscating can be a sufficient action for making cooperative behavior the best strategy to be adopted by participants.

References

Business Process Modeling Notation (2006), Misc, OMG. http://www.bpmn.org/Documents/BPMN%20V1-0%20May%203%202004.pdf.

Brun A., Cagliano R., Caniato F., Fahmy Salama K., Sianesi A., Spina G.L. (2005), Supply chain performance measurement systems: How to evaluate their performance?, [in:] *Second European Forum on Market-Driven Supply Chains*, EIASM, Politecnico di Milano.

Ceravolo P., Cimato S., Damiani E., Fugazza C., Frati F., Gianini G., Marrara S. (2008a), Value models of collaborative chains. Technical report, [in:] *Secure Supply Chain Management* (SecureSCM) FP7-213531.

Ceravolo P., Cimato S., Damiani E., Fugazza C., Gianini G., Marrara S. (2008b), Risk management and information disclosure in supply chain analysis, [in:] *Proceedings of the 8th Conference on Advanced Information Technologies for Management (AITM'2008)*, 2008.

Christopher M., Lee Hau L. (2004), Mitigating supply chain risk through improved confidence, *International Journal of Physical Distribution & Logistics Management*, Vol. 34, pp. 388-396.

Damiani E., Ceravolo P., Cimato S., Gianini G. (2008), Obfuscation for the common good, [in:] *Proceedings of 3rd Conference on Security in Network Architectures and Information Systems (SAR-SSI 2008)*, Loctudy, France, October 13-17.

Gaonkar R., Viswanadham N. (2004), A conceptual and analytical framework for the management of risk in supply chains,[in:] *Robotics and Automation, 2004. Proceedings. ICRA '04. 2004 IEEE International Conference on*, Vol. 3, April-1 May, pp. 2699-2704.

Gordijn J., Akkermans J. (2003), Value-based requirements engineering: Exploring innovative e-commerce ideas, *Requirements Engineering*, Vol. 8, No. 2, pp. 114-134.

Gunasekaran A., Patel C., McGaughey R.E. (2004), A framework for supply chain performance measurement, *International Journal of Production Economics*, Vol. 87, No. 3, pp. 333-347.

Hallikas J., Karvonen I., Pulkkinen U., Virolainen V., Tuominen M. (2004), Risk management processes in supplier networks, *International Journal of Production Economics*, Vol. 90, pp. 47-58.

Helferich O.K., Cook R.L. (2002), *Securing the Supply Chain. Technical Report*, Council of Logistics Management.

Juttner U. (2005), Supply chain risk management: Understanding the business requirements from a practitioner perspective, *International Journal of Logistics Management*, Vol. 16, pp. 120-141.

Juttner U., Peck H., Christopher M. (2003), Supply chain risk management: outlining an agenda for future research, *International Journal of Logistics: Research and Applications*, Vol. 6, pp. 197-210.

Lee Hau L., Whang S., (2000), Information sharing in a supply chain, *International Journal of Technology Management*, Vol. 20, pp. 373-387.

McCarter M.W., Northcraft G.B. (2007), Happy together? Insights and implications of viewing managed supply chains as a social dilemma, *Journal of Operations Management*, Vol. 25, pp. 498-511.

Norrman A., Lindroth R. (2004), *Supply Chain Risk*, chapter Categorization of supply chain risk and risk management, Hampshire, pp. 14-27.

OMG (2003), *Unified Modeling Language* (UML), version 2.1.1, Technical report.

Park S.H., Ungson G.R. (2001), Inter-firm rivalry and managerial complexity: A conceptual framework of alliance failure, *Organization Science*, Vol. 12, pp. 37-53.

Peck H. (2005), Drivers of supply chain vulnerability: An integrated framework, *International Journal of Physical Distribution & Logistics Management*, Vol. 35, pp. 210-232.

Secure Supply Chain Management (2008), Research Project Funded under the 7th European Framework Programme, http://securescm.org.

Tang C.S. (2006), Robust strategies for mitigating supply chain disruptions, *International Journal of Logistics: Research and Applications*, Vol. 9, pp. 33-45.

Von Lanzenauer Ch.H., Pilz-Glombik K. (2002), Coordinating supply chain decisions: An optimization model, *OR Spectrum*, Vol. 24, pp. 59-78.