



A framework for designing robust food supply chains[☆]

Jelena V. Vlajic^{*}, Jack G.A.J. van der Vorst, René Haijema

Operations Research and Logistics Group, Wageningen University, Hollandseweg 1, 6706 KN Wageningen, The Netherlands

ARTICLE INFO

Available online 1 December 2011

Keywords:

Disturbances
Vulnerability sources
Preventive redesign strategies
Reductive redesign strategies
Supply chain performances
Supply chain vulnerability

ABSTRACT

After years of emphasis on leanness and responsiveness businesses are now experiencing their vulnerability to supply chain disturbances. Although more literature is appearing on this subject, there is a need for an integrated framework to support the analysis and design of robust food supply chains. In this paper we present such a framework. We define the concept of robustness and classify supply chain disturbances, sources of food supply chain vulnerability, and adequate redesign principles and strategies to achieve robust supply chain performances. To test and illustrate its applicability, the research framework is applied to a meat supply chain.

© 2011 Elsevier B.V. All rights reserved.

1. Introduction

Today's business environment has become an international playing field in which companies have to excel in logistics performance, i.e. markets require full responsiveness, high quality products and high reliability of supply in small time windows at the lowest cost. As a consequence, supply chains have eliminated most non-value adding activities and have become leaner. However, lean supply chains without much inventory are more vulnerable to disturbances in logistic processes, which mean that they might be less consistent in their performance, i.e. are less *robust* (cf. Kleindorfer and Saad, 2005; Dong, 2006). Consequently, the competitive power of vulnerable supply chains in the market may diminish. In practice, in recent years there have been reported many events that have led to disturbances in supply chains processes (e.g. supplier failures caused by natural disasters or fires in the warehouses, delivery delays due to traffic accidents, product recalls due to lack of fulfilment of quality or safety requirements, etc.). Because of that, there is increasing interest by practitioners and academics to reduce supply chain vulnerability and design robust supply chains. This holds especially for food supply chains as these chains have specific characteristics that increase its vulnerability, such as seasonality in supply and demand and a limited shelf-life of products.

[☆] Paper selected from presentations at the 14th International Symposium on Logistics 'Global Supply Chains and Inter-Firm Networks', Istanbul, Turkey, July 5–8, 2009. The selection process has been managed by Dr Robert J. Mason, Cardiff University Business School, Cardiff CF10 3EU, United Kingdom, masonrj@cf.ac.uk.

^{*} Corresponding author. Tel.: +31 317 485644; fax: +31 317 485646.

E-mail addresses: jelena.vlajic@wur.nl (J.V. Vlajic), Jack.vanderVorst@wur.nl (J.G.A.J. van der Vorst), Rene.Haijema@wur.nl (R. Haijema).

In supply chain management theory, robustness and vulnerability are perceived as opposite though not mature concepts (Asbjørnslett and Rausand, 1999; Wagner and Bode, 2006). As a term, *robustness* has a broad meaning and it is often couched in different settings (Qiang et al., 2009). However, despite its frequent use, there is no general, widely accepted definition (Vlajic et al., 2010).

In a supply chain literature robustness is mainly considered as the ability of the system to continue to function well in the event of a disruption (Dong, 2006; Tang, 2006a; Waters, 2007) i.e. an unexpected event that severely impacts performance. Here, three points get attention. First, if the system functions well depends on what is measured and how it is measured and it varies from application to application (Snyder, 2003). Second, robustness of the supply chain could be jeopardized by various kinds of unexpected events: accidental events (e.g. a fire in the facility, a machine failure, flood or a traffic accident), and events that result from or belong to the systems characteristics (e.g. poor communication or decision making processes). Third, consequences of unexpected events could be measured at process or at system's (company or supply chain) level and the severity depends on system's design. The severity of the consequences determine the level of supply chain robustness, or it is opposite—supply chain vulnerability. In this paper we focus on (process) disturbances, i.e. any consequences of unexpected events at the process level and their impact to the robustness of the supply chain performance.

A literature review on supply chain robustness (Vlajic et al., 2010) shows that there is a lack of an integral framework that guides companies in managing disturbances and designing robust supply chains. With this paper, we aim to contribute to supply chain management theory by developing such an integrated framework for the design of robust (food) supply chains. To develop this framework we have conducted an extended literature review, participated in a number of workshops and conducted several interviews with field experts to get insight into practical issues in

food industry relevant for the framework. To test it, we applied it to a case in the meat supply chain, as one of the main chains in food industry. The data collection is based on observations, historical data and semi-structured interviews.

This paper is organized as follows. Section 2 discusses what supply chain robustness is. Section 3 presents the framework for designing robust food supply chains, and here we focus on the following elements: supply chain disturbances, sources of vulnerability and redesign strategies. Section 4 presents the application of the research framework in the case study. We conclude the paper with a discussion and issues for further research.

2. What is supply chain robustness?

The term robustness can be defined in many ways, depending on the specific context and research area (see Jen, 2005; Bundschuh et al., 2006; Qiang et al., 2009). In the supply chain management literature, robustness is considered both at a qualitative conceptual level and at a quantitative modeling level (Vlajic et al., 2010).

At *qualitative conceptual level*, robustness is considered as an important property of supply chains or as a strategy that can be used to improve supply chain resilience. In both cases, robustness is related mainly to supply chain vulnerability and uncertainty in general, and vulnerability is seen as consequence of various disruptions (Tang, 2006a). One of the first papers that considered robustness, resilience and vulnerability is the paper of Asbjørnslett and Rausand (1999). They introduced robustness and resilience as concepts that are opposite of the vulnerability concept. They define different kinds of disruptions that affect the business performances of a production system. Asbjørnslett (2009) continued this work in the context of supply chains. According to him, a *robust* system (supply chain) has the ability to resist disruptions, retaining its system structure intact, whilst a *resilient* system is adaptable, i.e. it will adapt to regain a new stable position. This approach to robustness is used also by Ferdows (1997) in the context of network robustness. Considering uncertainty in the global business environment, Ferdows (1997) made a relation between robustness and security and introduced the term “robust network” (Table 1). In this definition, extreme measures imply a change in supply chain structure. Following the same line of thoughts, some authors associated supply chain robustness with its ability to keep its

structure fixed (intact) in all situations including disruptions (e.g. see work of Kleijnen, 2005; Dong, 2006; Bundschuh et al., 2006; Chandra and Grabis, 2007; Dong and Chen, 2007; Viswanadham and Gaonkar, 2008). In these papers, the definitions of robustness imply that supply chains are robust if their structure is not changed and that supply chain robustness could be jeopardized only by disruptions. Moreover, dependent on the specific supply chain design various kinds of unexpected events could jeopardize the supply chain robustness, i.e. make supply chain vulnerable. Examples of various definitions on supply chain robustness are presented in Table 1.

At *quantitative modeling level*, robustness is mainly used in a context of modeling solutions or models for various problems in supply chains – such as planning (e.g. Zapfel, 1998; Van Landeghem and Vanmaele, 2002; Goetschalckx and Fleischmann, 2005; Leung et al., 2007), scheduling (e.g. Kutanoglu and Wu, 2004; Adhitya et al., 2007), network design (e.g. Snyder, 2003; Bundschuh et al., 2006; Mo and Harrison, 2005; Meepetchdee and Shah, 2007), inventory management (e.g. Tee and Rossetti, 2002; Ouyang, 2007), etc. Today, the term robustness as a measure is used a lot in Operations Research literature – especially in stochastic programming (e.g. see work of Goetschalckx and Fleischmann, 2005; Mo and Harrison, 2005) and robust optimization (e.g. see work of Mulvey et al., 1995; Snyder, 2003; Wu, 2006; Leung et al., 2007). The precise formulation of robustness depends on the particular technique used or type of the problem that is modeled. For instance, in robust optimization the modeling solution is defined as robust if it performs well for all scenarios of input data (Snyder, 2003), and a model is defined as robust if it remains “almost feasible” for all data scenarios (Mulvey et al., 1995). The definition of “performing well” varies from application to application and choosing an appropriate measure of robustness is part of the modeling process (Snyder, 2003). Despite an abundance of literature in the context of model and solution robustness, little work has focused on measuring supply chain's robustness, i.e. the ability of a supply chain to cope with unexpected events (Dong and Chen, 2007; Qiang et al., 2009).

2.1. Definition of robustness

In our view, supply chain robustness is a *desired property of a supply chain that is reflected in supply chain performances*. That is extremely important because today's business environment is characterized by increasing requirements toward robust performances (e.g. demands for reliable supply and higher product quality levels within smaller delivery time windows). According to Waters (2007, p. 159), a traditional way in business specifies an acceptable range for specifications, and the performance is considered acceptable if it stays within this range. We define supply chain robustness as *the degree to which a supply chain shows an acceptable performance in (each of) its Key Performance Indicators (KPIs) during and after an unexpected event that caused disturbances in one or more logistics processes*. To operationalize this definition, a supply chain is robust with respect to a KPI if the value of that KPI, adequately measured over an observation period, is sustained in a predefined desired range, even in the presence of disturbances. We call this predefined desired range the *Robustness Range*, and it is characterized by a lower and/or upper level. If a KPI performs above or below the robustness range, the supply chain is considered vulnerable. The stronger and longer the negative impact to performances is, the more vulnerable supply chain is to that disturbance.

3. Research framework

Now that we have defined supply chain robustness, this section discusses our research framework for designing robust

Table 1
Some definitions of robustness in the supply chain context.

Definitions of robustness:	Authors
The ability of a network to cope with changes in the competitive environment without resorting to changes in the network structure.	Ferdows (1997)
The system's ability to resist an accidental event and return to do its intended mission and retain the same stable situation as it had before the accidental event.	Asbjørnslett and Rausand (1999)
The ability of a supply chain design to find a supply chain configuration that provides robust and attractive performance while considering many sources of uncertainty.	Mo and Harrison (2005)
The ability of supply chain to maintain a given level of output after a failure.	Bundschuh et al. (2006)
The supply chains ability to withstand external and internal shocks.	Chandra and Grabis (2007)
The ability of a supply chain network to carry out its functions despite some damage done to it, such as the removal of some of the nodes and/or links in a network.	Dong (2006) Dong and Chen (2007)

(food) supply chains. We start with a definition of the supply chain and supply chain scenario as the study of the scenario in a specific case may identify elements that could cause supply chain vulnerability as well as elements that could mitigate it.

The literature provides many definitions of supply chains, but in general it can be said that a supply chain is a group of actors that perform specific roles and processes linked to each other via goods, information and money flows, using specific infrastructures aiming to fulfill consumer wishes at lowest cost (van der Vorst, 2000). Based on this definition we use the term supply chain scenario to describe the supply chain instance at hand. A *supply chain scenario* is an internally consistent view of a possible instance of the logistics supply chain concept, i.e. the managed, managing, and information systems and organization structure (van der Vorst, 2000). It considers relevant *contextual factors* (i.e. specific characteristics of food supply chains such as product quality requirements, as well as requirements that come from specific product – market combinations). The *managed* system refers to the physical design of the network and a facility and all other elements that perform logistic activities (such as equipment, vehicles and people), as well as product characteristics. The *managing* system refers to planning, control and co-ordination of logistic processes in the supply chain while aiming at realizing strategic supply chain objectives and logistical objectives within the restrictions set by the supply chain configuration. The *information* system refers to information and decision support systems within each of the decision layers of the managing system (from annual to daily planning), as well as the IT infrastructure needed. The *organization* structure refers to tasks, authorities and responsibilities of the departments and executives within the organization and supply chain as well as the coordination of tasks in order to realize defined objectives.

The main objective of the framework is that it helps in determining the best supply chain scenario that will enable robust supply chain performances for given circumstances. When we overview and integrate the literature on supply chain robustness and combine it with the findings of workshops and interviews (presented in Wognum et al., 2009), we find the following common steps that are relevant in this (re)design process:

1. The description and analysis of the supply chain scenario for a particular case and the identification of KPIs;
2. The identification of unexpected events and disturbances that affect performances;
3. The assessment of performances, i.e. how much and how long can the supply chain withstand disturbances?
4. The identification of sources of vulnerability that explain process disturbances, and as such, which may (strongly) affect the robustness of performance and eventually increase the vulnerability of the supply chain.
5. The identification of appropriate redesign strategies that eliminate disturbance by acting on sources of vulnerability or that

reduce the impact of the disturbance by disabling the domino effect to other processes and supply chain performances.

Let us give an example to clarify. Several hours delay of a delivery (i.e. a disturbance in the transport process) is caused by a traffic accident on the road (unexpected event), and this traffic accident could happen due to a poor traffic signalization, bad infrastructure or an inexperienced driver (which are vulnerability sources). Consequences of delays can be measured in potential inventory shortages and due to a domino effect as well in underachievement of production output, inventory shortage of final products or low delivery reliability to customers. In this case, the delivery performance is not robust as well and the entire supply chain can be signaled “vulnerable”. Appropriate redesign strategies should be selected and applied to improve this vulnerability.

Fig. 1 presents the research framework in which all elements are brought together. According to Viswanadham and Gaonkar (2008), an increased awareness of the existence of supply chain disturbances and their causes may enable better preparedness for handling or preventing them. In other words, the sources of vulnerability and related disturbances are the base for determining appropriate redesign strategies, i.e. strategic as well as tactical plans and operational actions that should increase the robustness level. The implementation of an appropriate redesign strategy implies a change in one or more elements of the supply chain scenario. As a result either the vulnerability source is eliminated (and therefore the frequency of disturbance is reduced) or the system becomes less vulnerable as the domino effect is disabled (and therefore the impact of disturbances in the supply chain is reduced). For example, the impact of a disturbances in the delivery of raw materials is reduced either by having buffer stocks or one eliminates or reduces the occurrence of such an disturbance by sourcing from multiple suppliers and having timely information that could trigger emergency actions. Alternatively the impact of a raw material delivery disturbance to a shortage of final products can be reduced by keeping a higher inventory level of final products.

The following sections will classify respectively disturbances, sources of supply chain vulnerability and supply chain redesign strategies.

3.1. Supply chain disturbances

In the supply chain management literature, there are only a few papers that focus on a definition and characterization of disturbances. Svensson (2000) introduced a conceptual definition of disturbance. He defined disturbance as “a deviation that causes negative consequences for the firm involved in the supply chain”. Melnyk et al. (2009) on the other hand defined supply chain disturbance from an operational viewpoint as the output of a

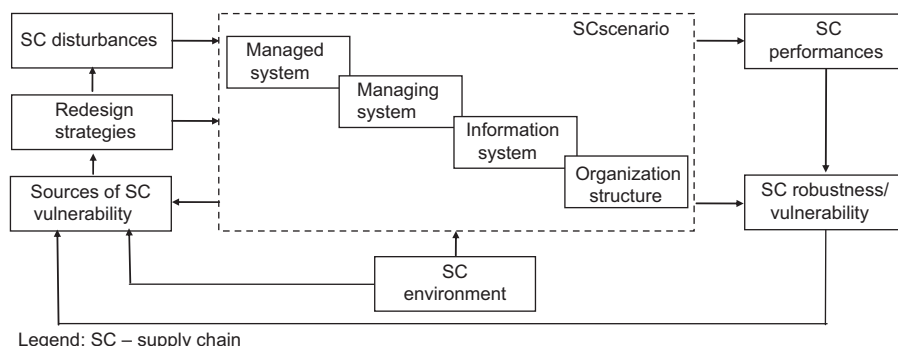


Fig. 1. Research framework for designing robust (food) supply chains.

chain of events triggered by an unexpected event at one point in the supply chain that adversely affect the performance of one or more components located elsewhere in the supply chain. In line with Melnyk et al. (2009) we define *supply chain disturbance as a minor or major deviation, or failure of one or more logistics processes triggered by unexpected events in the supply chain or its environment resulting in poor performance of the process itself, company and potentially along the supply chain in a given time period.*

In line with work of Scipioni et al. (2002), disturbances can be characterized by a number of elements, i.e. the *frequency of occurrence, the possibility of detection and the impact on supply chain performance.* In our work, we also consider disturbance *cause and size.* According to Svensson (2000) *causes of disturbances are related to volume and quality.* Causes of disturbances in volumes are related to a lack of materials for downstream activities in the chain, and we refer to it as the *quantitative dimension* of disturbances as it considers unexpected changes in quantity of materials. Causes of disturbances in product quality are related to deficiencies in materials in the supply chain, and we refer to it as the *qualitative dimension* of disturbances as it considers unexpected changes in quality of materials. We extend the disturbance classification of Svensson (2000) by adding the *time dimension* of disturbances that is related to unexpected changes in beginning or ending of process realization, or process duration (i.e. delays or idle times).

In line with the thoughts of van der Vorst and Beulens (2002), we express the *size* of the disturbance in the loss of value of relevant KPIs of the related logistics process that is directly affected by the unexpected event. A minor deviation of a KPI from the norm represents a small disturbance. At the process level it usually represents an acceptable variation in the process outcome and it is considered as part of “business as usual”. A major deviation of a KPI from the norm represents a large disturbance, i.e. the process is only partially realized. Extreme values of process KPIs represent a failure of the process execution. Note that the choice of relevant KPIs, their norms and deviation level is case dependent (determined by the supply chain scenario). An example of various sizes of disturbances and dimensions for one KPI is presented in Table 2.

The possibilities for disturbances *detection* also affect the selection of redesign strategies. Disturbance detection depends on the characteristics of the process, as well as on the decision of the management to monitor and trace disturbances in the supply chain. For that purpose, various techniques could be used, such as Data mining and Statistical Process Control (Shukla and Naim, 2007). The number of disturbances in an observation period represents its *frequency*.

In the end, the *impact* of disturbances on robustness of supply chain performances is crucial. In principle, the impact of a disturbance depends on the flexibility and responsiveness of the supply chain to adapt to the new situation caused by an unexpected event. Therefore, the impact of a disturbance can be local (e.g. delivery failure can have local impact on transport performance, but it will not jeopardize the production process if there is enough inventory or if a backup delivery option exists) or system wide (e.g. harvest failure or animal diseases outbreak can

cause lack of raw material, which effects will be transmitted through the whole chain). In both cases, the causality of events has to be considered because a disturbance in one process can cause a domino effect and affect other processes (Waters, 2007) and cause amplification of the impact (Wu et al., 2007). The Bullwhip effect can be also seen as a system wide impact of disturbances in demand along the chain (Wagner and Bode, 2006).

3.2. Sources of supply chain vulnerability

In line with Juttner et al. (2003) define risk sources as environmental, organizational or supply chain-related variables that cannot be predicted with certainty and that have impact on the supply chain performance. In a similar manner, we define *vulnerability sources as characteristics of the supply chain or its environment that lead to the occurrence of unexpected events and as such, they are direct or indirect causes of disturbances.*

In literature, there are several approaches to classify vulnerability sources. Based on the reviewed literature (e.g. Albino and Garavelli, 1995; Mason-Jones and Towill, 1998; Asbjørnslett and Rausand, 1999; Svensson, 2000; Scipioni et al., 2002; van der Vorst and Beulens, 2002; Waters, 2007; Simchi-Levi et al., 2008; Asbjørnslett, 2009) we distinguish two basic groups of vulnerability sources: internal and external sources. Within these two groups, we found a number of generic sources that could be found in almost any supply chain, as well as specific sources for food supply chains. These specific sources result from the specific characteristics of food chains, such as the perishability of goods, the importance of food safety and quality management, the valorization of by-products, the variability in process yield and the rigid time constraints (van der Vorst, 2000).

The roots of *external sources* of supply chain vulnerability are in the supply chain environment; some of them are controllable to some extent (e.g. societal or financial sources), others are not (some market sources as well most of environmental sources), see Simchi-Levi et al. (2008, p. 316). We have extracted a list of external sources from the reviewed literature, and classified them to 21 main sources using the classification criteria of Asbjørnslett and Rausand (1999) and Wu et al. (2006) and assigned them codes (see Fig. 2, e.g. MX—Market source, External factor).

Roots of *internal sources of supply chain vulnerability* are within the supply chain, i.e. within the elements of the supply chain scenario (the managing, managed and information systems or in the organizational structure). From a company perspective, these internal sources are controllable to some extent (Simchi-Levi et al., 2008, p. 316), depending on their origin: within the company or within the supply chain. Sources of vulnerability at the company level are mostly controllable (Wu et al., 2006) and can be resolved when they result directly from choices and actions of the company's management (Ritchie and Brindley, 2009). Internal sources related to product characteristics, such as the quality decay of fresh food can be controlled only partly. The sources of vulnerability at the supply chain level are partially to fully controllable (Wu et al., 2006). They come from the supply and demand side of the focal company and the controllability level depends on the level of supply chain integration

Table 2
Example of classification of disturbances in delivery process.

Dimension: KPI:	Quantity dimension Loss of material during transport	Quality dimension Number of products damaged in transport	Time dimension Transport time
Size			
Minor deviation	A few products are lost	A few product are damaged	A small delay
Major deviation	A shipment is partially received	A significant part of the shipment is damaged	A significant delay
Failure	Loss of an entire shipment	All products of a shipment are damaged	Inability to perform delivery in required time window

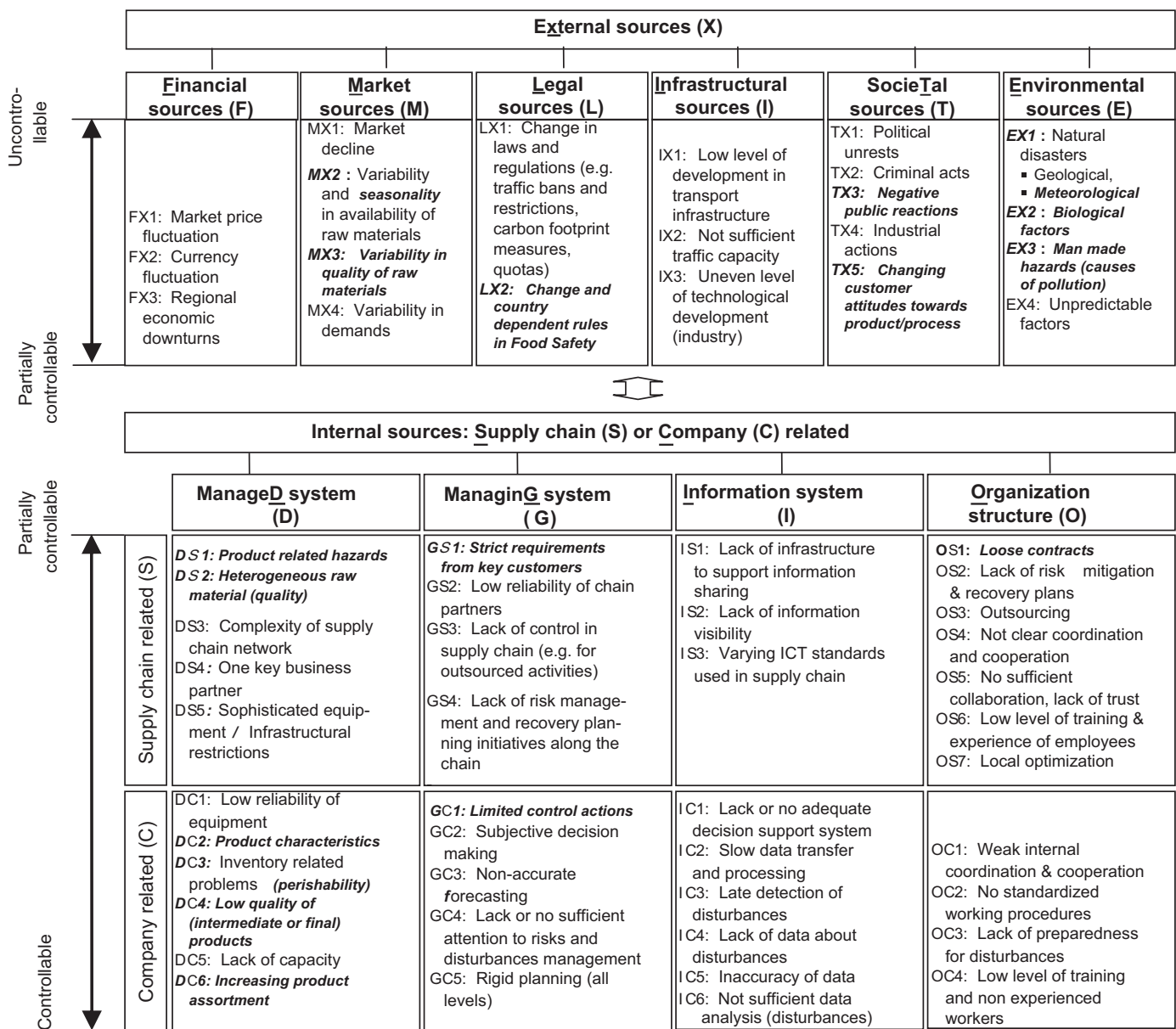


Fig. 2. List of sources of supply chain vulnerability (**bold-italic** letters denote specific sources related to food supply chains) and controllability level (from company's management perspective).

and collaboration. According to Qiang et al. (2009), till now research has been mainly focused to vulnerability sources that come from the demand-side of the focal company, such as fluctuations in the demand for products, as opposed to the supply-side sources, which are related to uncertain conditions that affect the production and transportation processes of the supply chain. From the literature we have extracted a list of internal vulnerability sources, classified them in 41 main sources according to the controllability level and the elements of the supply chain scenario and we have assigned codes: e.g. G—managing system, C—Company level (Fig. 2). Each of these main sources can have multiple forms (e.g. low quality of raw material can manifest as damaged or spoiled products, or as products with a bad organoleptic characteristics, etc.).

Additionally, it has to be taken into account that sources of vulnerability are interconnected with each other, both within each level and across the levels (Asbjørnslett and Rausand, 1999; Peck, 2005). In that way, they make a chain of causes and consequences, which effects are observable as disturbances in the realization of logistics processes.

In this paper we focus mainly on internal sources of vulnerability (company and supply chain level sources).

3.3. Categorization of redesign strategies

In supply chain management literature many redesign principles are given (also referred as risk responses, risk protection strategies, mitigation strategies and mitigation tactics), and in essence all of them represent possible approaches to define the most appropriate way of dealing with risks and disturbances in the supply chain. The principles are either related to the concept of uncertainty (van der Vorst, 2000; Lee, 2002; Simchi-Levi et al., 2008; van der Vorst and Beulens, 2002; Simangunsong et al., 2008), and more recently, to disturbance and risk (e.g. Zsidisin et al., 2000; Tang, 2006a, 2006b; Tomlin, 2006; Waters, 2007; Hopp, 2008; Macdonald, 2008; Simchi-Levi et al., 2008; Dani, 2009). van der Vorst and Beulens (2002) presents an overview of supply chain redesign principles to deal with uncertainties, such as changing the roles and processes in the supply chain, reducing

Table 3
Overview of redesign principles aimed at disturbance prevention.

Element of SC scenario	Redesign principles—disturbance prevention
Managed system	DP1: Adjust the structure of the supply chain (van der Vorst, 2000; Waters, 2007) • Reduce the length of the supply chain DP2: Use product management (Waters, 2007; Melnyk et al., 2009) • Avoid risky products • Plan component/material substitution DP3: Use technical solutions for performance monitoring (e.g. temperature, humidity, etc) • Change the location of facilities • Rationalize the product range
Managing system	GP1: Invest to avoid or reduce exposure to vulnerability sources (Tang, 2006) • Regular replenishment of equipment, vehicles • Economic supply incentives to cultivate additional suppliers GP2: Control variability (Zsidisin et al., 2000; Tang, 2006a; Waters, 2007; Hopp, 2008; Simangunsong et al., 2008; Simchi-Levi et al., 2008; Dani, 2009) • Careful supplier selection process using vendor rating techniques; supplier audits and quality certification programs • Use (virtual) pooling: centralization of decisions • Increase price stability • Sell products to various markets GP3: Use revenue management strategies (Tang, 2006; Simchi-Levi et al., 2008) • Use dynamic pricing (convenient for perishable products) • Use promotion GP4: Decrease lead time (Waters, 2007) GP5: Use short term forecasts or aggregate forecasts (Waters, 2007) • Innovations (e.g. to packaging, information system, etc.) • Increase capacity • Use standardized work (procedures) • Use procedures and techniques to improve quality control, as well as industry standards • Develop proactive maintenance • Use demand postponement strategy
Information system	IP1: Use IT to increase data accuracy and speed and support decision making (van der Vorst, 2000; Shukla and Naim, 2007; Hopp, 2008; Simchi-Levi et al., 2008; Simangunsong et al., 2008) • Implement real-time information systems • Use the same information standards • Use techniques for automatic disturbance detection IP2: Create support for information transparency in the supply chain (van der Vorst, 2000; Zsidisin et al., 2000; Waters, 2007; Hopp, 2008) • Insure infrastructure to enable information exchange and sharing IP3: Collect relevant data about disturbances (e.g. Hopp, 2008) • MTTF (mean time to failure), MTTR (mean time to repair), variances in lead times • Use Tracking and Tracing system • Use DSS for production planning and scheduling, inventory management, demand management, etc
Organization	OP1: Increase collaboration in supply chain (Zsidisin et al., 2000; Tang, 2006; Waters, 2007; Simchi-Levi et al., 2008; Hopp, 2008; Ritchie and Brindley 2009) • Use information sharing • Joint forecasts and planning • Develop Supply Chain Risk Management OP2: Increase cooperation and coordination between departments (Waters, 2007) • Closer cooperation between people who are doing planning and people who execute plans OP3: Create an adaptive supply chain community (van der Vorst, 2000; Zsidisin et al., 2000; Waters, 2007; Simchi-Levi et al., 2008) • Establishment of risk mitigation plans together with suppliers • Align objectives and define KPIs OP4: Improve human resource management • Select experienced workers • Ensure proper training of employees • Establishment of strategic alliances, such as transport alliances, VMI, etc

Table 4

Overview of redesign principles aimed at reducing the impact of the disturbance to robustness of performances.

Element of SC scenario	Redesign principles—disturbance impact reduction
Managed system	DR1: Adjust the structure of the supply chain (Zsidisin et al., 2000; Snyder et al., 2006; Tang, 2006; Tomlin, 2006; Waters, 2007; Melnyk et al., 2009) ● Increase the width of the supply chain ● Use multiple modes of transportation DR2: Buffering in capacity and inventory (Zsidisin et al., 2000; Snyder et al., 2006; Tomlin, 2006; Waters, 2007; Hopp, 2008; Simangunsong et al., 2008; Simchi-Levi et al., 2008; Melnyk et al., 2009) ● Increase number of equipment, vehicles or workers ● Make strategic (safety) stocks ● Increase capacity of equipment, vehicles or space ● Make well stocked supply pipeline DR3: Increase flexibility of the supply chain (Tang, 2006; Tomlin, 2006; Waters, 2007; Hopp, 2008; Simangunsong et al., 2008) ● Use multiple modes of transportation ● Use flexible automation ● Use multiple purpose resources (e.g. standardized equipment, vehicles, cross-trained employees) ● Use temporary workers DR4: Use product management (Tang, 2006a; Waters, 2007; Hopp, 2008; Simangunsong et al., 2008) ● Use possibilities of product substitution, e.g. silent product rollover ● Use product postponement DR5: Use of technical solutions to deal with disturbances (alarms, fire distinguishers, etc)
Managing system	GR1: Hedging (Tang, 2006; Tomlin, 2006; Waters, 2007; Hopp, 2008) ● Produce certain products in-house and outsource other products ● Using business disruption insurance ● Diversifying operations across multiple markets GR2: Make back up options (Snyder et al., 2006; Tang, 2006; Tomlin, 2006; Waters, 2007; Hopp, 2008; Simchi-Levi et al., 2008) ● Use a flexible supply contracts for non-strategic components, such as: Long term contracts (forward or fixed commitments contracts), Flexible or Option contract, or Spot purchase ● Use alternative suppliers ● Prepare backup for emergency supply ● Make alternative transport routes GR3: Increase flexibility of planning and control (van der Vorst, 2000; Fleischmann et al., 2005; Tang, 2006, 2006a; Waters, 2007; Hopp, 2008; Melnyk et al., 2009) ● Increase manufacturing flexibility, e.g. use flexible receipts, coordinate and redesign policies ● Do tasks parallel instead sequential ● Allow time and capacity buffering in plans and operations ● Use postponement ● Use event driven planning (update after event) ● Use component/material substitution GR4: Use lead time management (van der Vorst, 2000; Tang, 2006; Waters, 2007; Simangunsong et al., 2008)
Information system	IR1: Use IT to increase speed of disturbance detection and support decision making (e.g. Zsidisin et al., 2000; Shukla and Naim, 2007; Melnyk et al., 2009) ● Statistical process control ● Data mining IR2: Create support for information transparency in the chain (e.g. van der Vorst, 2000; Zsidisin et al., 2000; Lee, 2002; Waters, 2007; Hopp, 2008; Simchi-Levi et al., 2008; Simangunsong et al., 2008) ● Enable continuous data exchange with partners in the supply chain ● Implement real-time information systems ● Insure infrastructure to enable information exchange and sharing IR3: Use feedback loops (e.g. Disney et al., 1997)
Organization	OR1: Increase preparedness to disturbances (e.g. Hopp, 2008) ● Enable empowerment (authorization of employees to make independent decisions) ● Build awareness for crises situations OR2: Increase collaboration in chain (e.g. Zsidisin et al., 2000; Tang, 2006; Simchi-Levi et al., 2008) ● Establish strategic alliances OR3: Create an adaptive supply chain community (e.g. Tang, 2006; Simchi-Levi et al., 2008) ● Establishment recovery planning systems along the chain OR4: Use risk sharing supply contracts for strategic components (e.g. Tang, 2006, 2006a; Simchi-Levi et al., 2008; Hopp, 2008), such as: ● Revenue sharing contracts ● Sales rebate contracts ● Back-up (advance purchase) contracts ● Capacity reservation contracts ● Quantity flexibility contracts ● Cost sharing contracts ● Wholesale price contracts ● Buy-back contracts

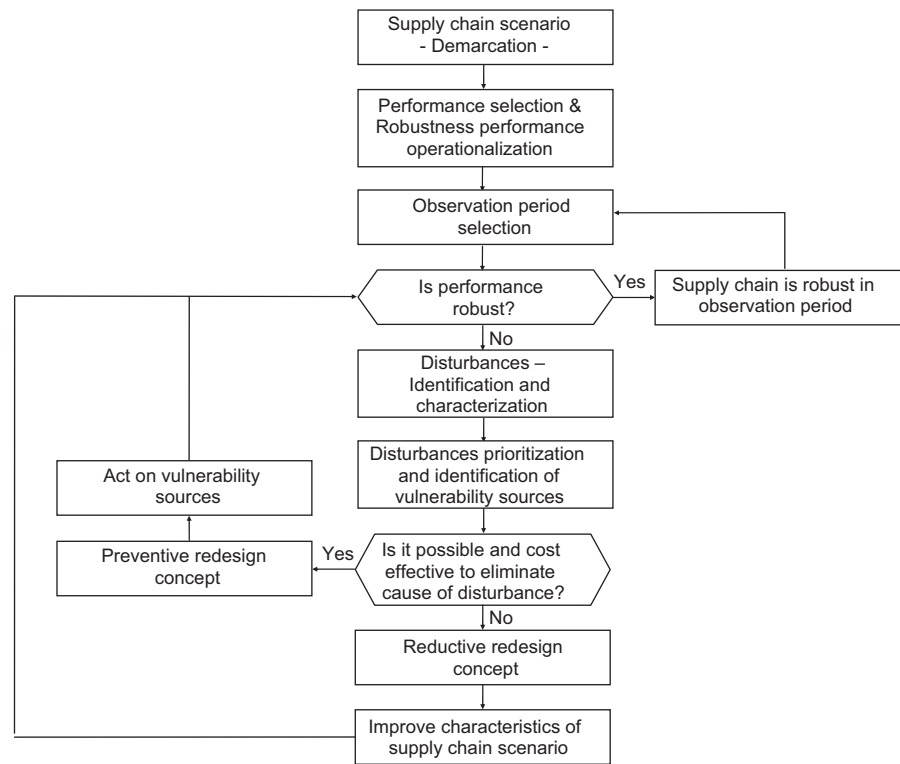


Fig. 3. Application of the research framework.

customer order lead times, coordinating logistical decisions and creating information transparency. Simchi-Levi et al. (2008) offer several approaches to deal with risks, depend on their controllability. Peck (2005) mentions strategies such as outsourcing and contract forms that should be used to mitigate supply chain risks and to achieve supply chain resilience. Tang, 2006a identifies nine strategies that can be implemented under normal business circumstances or after major disruptions, and he describes main challenges for selecting an appropriate (redesign) strategy. In another paper (Tang, 2006b), those strategies are typified according to four SCM areas: supply management, demand management, product management and information management. Based on our review, we define *redesign strategies as sets of strategic and tactical plans and operational actions that aim to reduce the vulnerability of supply chains based on one or more redesign principles that make changes in elements of the supply chain scenario*.

Similar to the classification of risk responses in Waters (2007) we consider two groups of redesign strategies: disturbance prevention and disturbance impact reduction. *Disturbance prevention* aims for the reduction of disturbance frequencies and its sizes i.e. acting in advance in order to eliminate, avoid or control any direct cause of disturbances (which can be any source of vulnerability). The *reduction of the impact of a disturbance to robustness of supply chain performances* implies a change of the characteristics of the supply chain scenario elements, such as using buffer stocks or increasing process flexibility. The use of the second group of strategies usually applies when disturbance prevention is impossible as one cannot act on the identified vulnerability source, or when prevention requires a large investment. This classification helps us to determine at the higher conceptual level what kind of response to use for a particular class of disturbances; however, the selection of particular redesign strategy depends on the *impact of disturbance to robustness, characteristics of the supply chain scenario and vulnerability sources*.

Within each group of redesign strategies, in line with the work of van der Vorst and Beulens (2002), we classified and coded the

redesign principles related to the element of the supply chain scenario that is influenced the most by its implementation. In Table 3 we present 14 redesign principles aimed at disturbance prevention and in Table 4 we present 16 redesign principles aimed at impact reduction and classify them according to the elements of supply chain scenario (e.g. GP—Managing system, Preventive redesign concept; DR—Managed System, Reductive redesign concept). In both tables, within each principle, we listed examples of redesign strategies. Here, we have to mention that some of these principles can be used for both purposes (especially in the part related to information system and organization).

3.4. Application of the research framework

Now that we have formulated the framework, it is important to describe the dynamic process of using it. Fig. 3 presents an overview (partly based upon the Process Failure Modes and Effects Analysis—PFMEA method (see Scipioni et al., 2002), which is applicable for our research framework).

For a selected case, it is necessary to describe the elements of the supply chain scenario and their characteristics, as well as boundaries of analysis. Here, the main element is the identification of the most important KPIs for the company and its supply chain and the operationalization of the robustness range. In the case study, for a specified length of the observation period, the performance on its KPIs can be assessed resulting in insight on the supply chain's or company's vulnerability. The existence of vulnerability periods indicates the presence of disturbances in logistic processes.

Possibilities for disturbances detection represent one of the major elements that drive the selection of redesign principle and strategies. Disturbance detection depends on the characteristics of the process, as well as on the decision of the management to monitor and trace disturbances in the supply chain. For that purpose, various techniques could be used, such as Data mining and Statistical Process Control (Shukla and Naim, 2007). In our work, based on the company's documentation and on interviews with

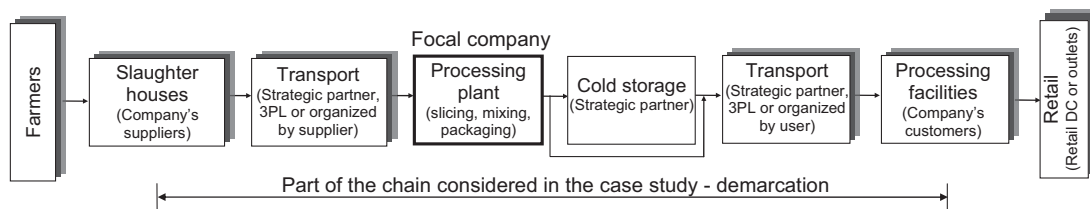


Fig. 4. Meat supply chain.

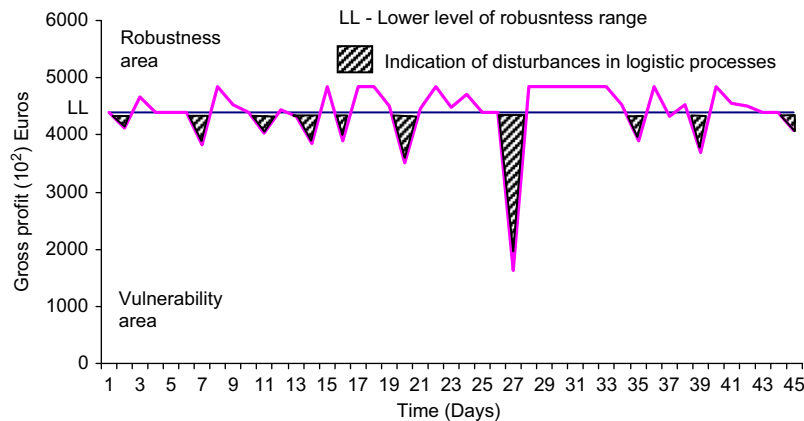


Fig. 5. Performance assessment—an example.

employees, for each vulnerability period disturbances in logistic processes are identified, characterized and their impact on supply chain performances is assessed (see Section 3.1).

That way it is possible to rank disturbances and roughly indicate the level of vulnerability of the supply chain or the company under consideration. For the disturbances with the highest frequency and impact it is necessary to identify the main causes that may lead to them (i.e. vulnerability sources) and to assess all possible redesign strategies. It is clear that first attention should be given to redesign principles aimed at disturbance prevention (as this removes the problem), and next to principles that reduce the impact of the disturbance. In the end, a cost-benefit analysis of the most interesting redesign strategies should result in the selection of the best strategy.

4. Case study

To test the research framework we applied it to a case in the meat processing industry in the Netherlands. We performed data collection in the period from September 2008 till September 2009. The data is collected through several visits and student internships at a focal company that processes the meat as well as at a cold storage and a transportation company that takes care of the delivery of raw materials and the storage and distribution of final products. Data sources used are available reports, observations, as well as semi-structured interviews with the company directors and the operations and logistics managers. The data obtained is validated and checked with insights obtained in an earlier broader case study of the European meat supply chain (in Wognum et al., 2009).

In this section, we first briefly present relevant characteristics of the supply chain scenario and define the performance robustness for one selected KPI. Further, in line with the framework, we present an approach to identify and to rank disturbances, their characteristics, as well as a way to choose redesign strategies that

may help to achieve performance robustness and reduce supply chain vulnerability.

4.1. Main elements of supply chain scenario and performance robustness assessment

The focal company is a company for meat slicing and processing. Upstream in the supply chain are slaughterhouses (suppliers) and farmers. Downstream are service providers (cold storage and transportation companies) and other meat processors (customers), retail distribution centers and outlets that buy packed meat products. The focal company works together with a logistics service provider (strategic partner) that manages transport and warehousing for the focal company (Fig. 4).

The *logistical objective* of the company is to maximize the company's gross profit while maintaining a high customer service level. According to the company's managers, the company shows a *robust performance in profit* if the *operational gross profit is equal or greater than the value of the fixed overhead costs*. For example consider Fig. 5, which shows that the values of the operational gross profit (as recorded once a day) is fluctuating over time and sometimes drops below a lower level (LL) of the robustness range. In periods in which the gross profit is below the lower level the company is vulnerable as the gross profit suffers from one or more disturbances in some logistic processes. Periods in which values of the operational gross profit are in the robustness range (that is above the lower level) are called robust periods (with respect to the KPI operational gross profit).

In Fig. 5 multiple robust periods and non-robust periods are observed over the given observation period. This implies that the company's vulnerability (with respect to the KPI operational gross profit) is caused by one or more unexpected events that affect the logistic processes. The impact of disturbances is displayed by the length and the depth of each non-robust period. The largest

Table 5
Disturbances and their characteristics.

Category	Process/Disturbance (D)	Indicator	Disturbance characteristics			
				Size	Impact	Frequency
Quantity	Production D1: Low utilization of the raw materials	Percentage of production waste	D11	Minor deviation: Parts of items	Low	Very frequent (every day)
			D12	Major deviation: Complete items	Medium	Occasionally (once per two month)
	Inventory management D2: Lack of raw material (Stock-outs)	Number of periods out of stock	D21	Major deviation: Several hours	Medium	Rare (few times per year)
			D22	Failure: Several days	High	Very rare (once per few years)
Quality	Production D3: Low quality of the final product	Products returned	D31	Major deviation: Part of shipment	Medium	Frequently (several times/month)
			D32	Failure: Entire shipment	High	Very rare (once per few years)
	Inventory management D4: Obsolete and damaged products in stock	Number of obsolete and damaged products	D41	Major deviation: Item level	Medium	Occasionally (once per three months)
			D42	Failure: Entire batch	High	Very rare (once per few years)
Time	Production D5: Low line productivity	Duration of idle time	D51	Major deviation: Several hours	Medium	Rare (few times per year)
			D52	Failure: Several days	High	Very rare (once per few years)

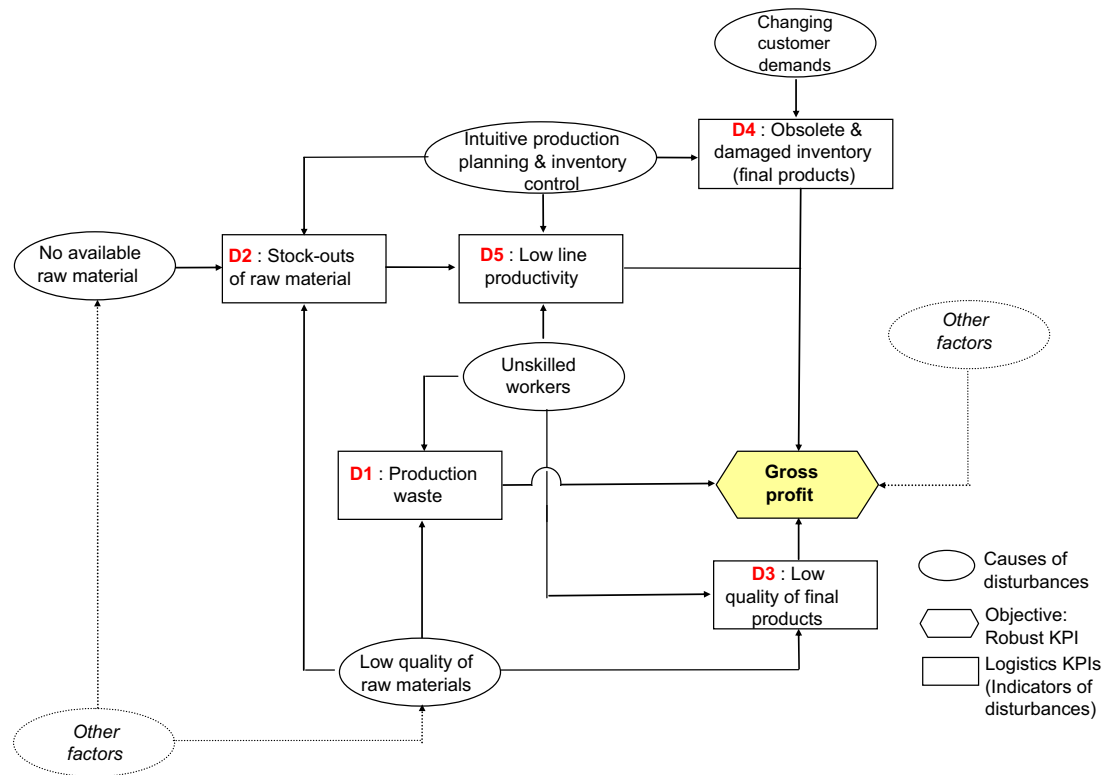


Fig. 6. Influence diagram of main logistic KPIs to gross profit.

shadowed part indicates a failure that was rapidly resolved (within 24 h).

4.2. Disturbances in processes and vulnerability sources

To find out what kind of disturbances are causing vulnerability, the research team conducted process mapping and logistic processes analysis. As a result, the main logistics processes were identified as well as the following disturbances: inventory shortage (raw materials), inventory obsolescence (final products), low utilization of raw material, low line productivity and low quality of final products. For each disturbance, we defined corresponding indicators and

diagnosed the characteristics of the disturbance (Table 5) based on company data and interviews with logistic managers.

We constructed an influence diagram (Fig. 6) to trace the vulnerability sources that caused the disturbances and to consider the interactions between processes.

For example, production planning and control, as well as inventory management decisions are mainly based on subjective judgment and experience. Prepare backup for emergency supply of the manager (classified as GC2, Fig. 2). This characteristic of the managing system results in sub-optimal decisions, which may cause disturbances such as: stock-outs of raw material, the piling of final products in stock and their obsolescence, as well as low a line productivity. The lack of an advanced decision support

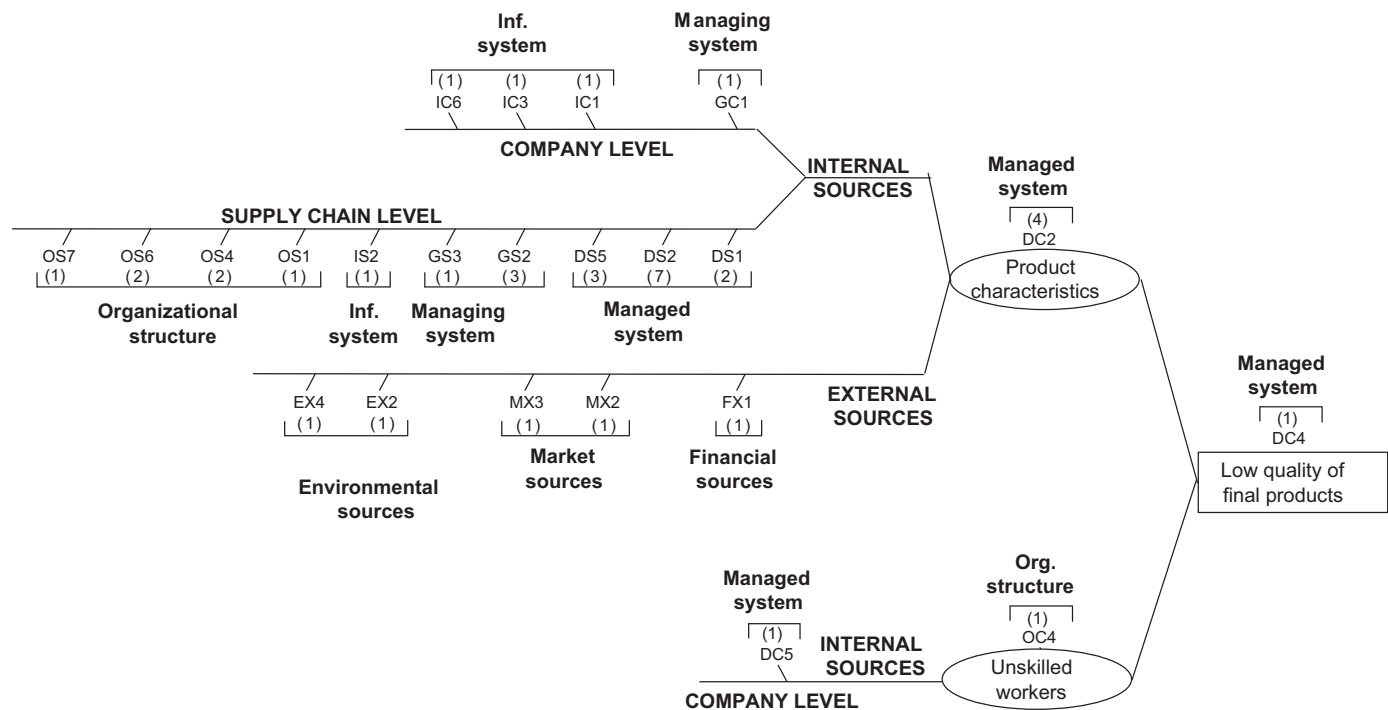


Fig. 7. Causal diagram: main sources of vulnerability that causes a low quality of final products (abbreviations according to classification scheme presented in Fig. 2; number represents number of relevant characteristic of each source).

system for production planning and inventory management (IC1) causes decentralized subjective decision making.

To structure the analysis we rank disturbances according to their impact on gross profit. The disturbances are characterized based on the manager's experience and judgment, supported by documentation and other data sources (where possible). Evaluation and ranking are done according to the principles of PFMEA. At a scale from 1 to 10, the highest value (10) is assigned to the greatest impact of disturbance and to the highest frequency, and the lowest value to the disturbance with the least impact and a very rare frequency.

The detection of some disturbances in this case, happens actually during the production process and they get a low rank (easily detectable disturbances: D1, D2, D5). Other disturbances (D3 and D4) are more difficult to detect—they are detected upon a customer complaint or by control procedures (e.g. periodic inventory control). The more difficult to detect disturbances are ranked higher. The multiplication of the rank values related to the impact, frequency and detection results in the, what we call, Disturbance Priority Number (DPN). The higher the value of DPN, the higher the vulnerability level is. For a disturbance with a high DPN value one should try to explain why the DPN value is that high by analyzing the (source of) vulnerability. This helps in identifying appropriate actions, i.e. redesign principles and particular strategies. Based on DPN, we categorized disturbances in three groups and redesign options:

- Disturbances that have a light impact on gross profit (D11, D21, D51) are acceptable by management;
- Disturbances that have a medium impact on gross profit require operational solutions and process improvements (D12, D41);
- Disturbances that have a high impact on gross profit require thorough analysis in order to prevent them or to reduce their impact (D22, D31, D32, D42, D52).

In order to test our framework, we focus on one of the disturbances that influences gross profit the most: a low quality of final

products (D31, D32) that result in product returns from customers. Based on interview data and analysis of database that contains data on customer complaints and other data as required by HACCP, we identified the main sources of vulnerability and classified them according to our classification scheme (presented in Fig. 2). We present our findings as a causal diagram in Fig. 7. It shows two main sources of vulnerability that cause a low quality of final products: low quality of raw material (belong to DC2 type of vulnerability source) and unskilled workers (belong to OC4 type of vulnerability source). Low quality of raw material is represented by four relevant characteristics: lack of product freshness, high bacterial level, bad organoleptic properties and undesirable structure (number of relevant characteristics is given presented as a number between brackets in Fig. 7).

The low quality of raw material is mainly a consequence of vulnerability sources at the supply chain level, which are partially controllable by management of the focal company. In total, we found 32 specific causes that may lead to this problem. Most of them (9) belong to product related hazards (DS1: metal or plastic residues in parts of meat) and heterogeneous quality of raw material (DS2: aspects such as lack of freshness, high bacterial level, frozen products, bad organoleptic characteristic, various size, structure and weight of items). These groups of vulnerability sources indicate a low level of quality control at suppliers, as well as equipment problems or an infrastructural problem at the supplier site (DS5: failure of cooling system, production line or mistakes of machine settings). These sources amongst other decrease the delivery reliability of suppliers (GS2), as well as of the logistics service provider. The last 6 causes are related to contractual issues (OS1), i.e. to a low level of cooperation and coordination in the supply chain (OS4), to low skills of workers at supplier (OS6) and to silo mentality (OS7).

At the company level, we identified four controllable sources of vulnerability: limited control actions (GC1) originating from technological constraints (such as: proper quality control directly at a production line), information system constraints: lack of an adequate information system to record and detect quality problems of input material (IC3, IC6) as well as a decision support system to assess the

Table 6

Redesign principles and strategies aimed at disturbance prevention for identified vulnerability sources (Bold areas indicates controllable sources of vulnerability).

Vulnerability source	Managed system (DP)		Managing system (GP)		Information system (IP)		Organizational structure (OP)	
	Principle		Principle		Principle		Principle	
DC2	DP3	Technical solutions	/	/	/	/	/	/
DC5	/	/	/	/	IP1	Advanced DSS	OP4	Training for employees; certificates
GC1	/	/	GP2	Advanced procedures (QC)	/	/	/	/
IC1	/	/	/	/	IP1	Advanced DSS	/	/
IC3	/	/	/	/	IP1	Advanced DSS	/	/
					IP3	Collect data	/	/
IC6	/	/	/	/	IP1	Advanced DSS	OP2	Increase cooperation
OC4	/	/	/	/	/	/	OP4	Training for employees; certificates
DS1	/	/	GP2	Supplier selection	/	/	OP3	Align objectives and KPIs
			GP2	Quality certification programs	/	/		
DS2	/	/	GP2	Supplier selection	/	/	OP3	Align objectives and KPIs
			GP2	Quality certification programs				
DS5	/	/	GP2	Supplier selection	/	/	OP3	Joint mitigation plans
GS2	/	/	GP2	Supplier selection	/	/	OP3	Align objectives and KPIs
GS3	/	/	/	/	/	/	OP1	Make strategic alliances
IS2	/	/	/	/	IP2	Information sharing	/	/
OS1	/	/	/	/	/	/	OP1	Make strategic alliances
OS4	/	/	/	/	/	/	OP3	Align objectives and KPIs
OS6	/	/	/	/	/	/	OP4	Training for employees; certificates
OS7	/	/	GP2	Supplier selection			OP1	Make strategic alliances
							OP3	Align objectives and KPIs
FX1	/	/	/	/	/	/	/	/
MX1	/	/	/	/	/	/	/	/
MX3	/	/	GP1	Multiple suppliers	/	/	/	/
EX2	/	/	GP1	Multiple suppliers	/	/	/	/

Table 7

Redesign principles and strategies within disturbance impact reduction concept.

Redesign strategies—to reduce impact of a disturbances	
Managed system	DR4: Use product management Use possibilities of product substitution (offer another product to customers)
Managing system	GR1: Hedging Using business disruption insurance Diversifying operations across multiple markets (find customers with higher level of tolerance) GR3: Increase flexibility of planning and control Increase manufacturing flexibility, e.g. use flexible receipts Use component/material substitution (if possible, reuse returned products in production)
Information system	IR1: Use IT to increase speed of disturbance detection and support decision making Statistical process control Data mining

influence of quality problems on operational gross profit (IC1). However, we also identified a number of non-controllable sources of vulnerability, such as market price fluctuation (FX1), variability in availability (MX2) and quality of raw materials (MX3), as well as biological factors (such as animal diseases – EX2) and accidental events (EX4) such as traffic accidents that cause long delays. In the meat industry and food industry in general, especially in processing phases, the quality of final products depends to a certain extent on the health and skills of workers involved. Sources of vulnerability related to this problem are mostly company related, and they result from a need for additional, temporary flex-workers (DC5) and their lack of experience and training (OC4).

4.3. Selection of redesign strategies

According to our framework, there are two possible approaches: Either use redesign principles that aim to prevent the disturbance to happen, i.e. to reduce the number and frequency of product returns

due to quality flaws, or those that aim to reduce the impact of the disturbance on operational gross profit.

The Preventive Concept requires analysis of vulnerability sources, where the goal is to eliminate them or reduce exposure of the company to them. Therefore, for each source of vulnerability described in the previous section, depending on their controllability level (Section 3.2) we identified corresponding redesign principles and strategies. The results of this analysis are presented in Table 6.

Trying to reduce exposure to vulnerability sources requires changes in the Managing System in order to increase the flexibility of the system. In the case that preventive strategies are too expensive or impossible to implement, the company could resort to the reductive strategies presented in Table 7. For example, using principles DR4 and GR1 result in an improved Demand Management, while GR3 results in possibilities to reduce the costs of product returns. In the end, use of IR1 principle could lead to the better disturbance management and improved decision making in critical situations.

The above analysis shows that each source of vulnerability can be related to multiple redesign principles, ranging from operational/tactical changes (such as training employees or diversifying operations) to strategic changes (such as alternative suppliers, acting on multiple markets or installing new decision support systems). When this analysis is done for all main disturbances, an overview is created of all vulnerability sources and possible redesign principles. By evaluating the impact of these principles on the vulnerability level as a whole (each principle has an effect on the occurrence and impact of multiple disturbances), management can decide upon those principles that together will result in the best effect; hence chose for specific redesign strategies. Mathematical and simulation modeling efforts can be used in this process to support the management in quantifying the expected impact of possible redesign strategies.

5. Discussion, conclusion and future work

In this paper an integrated framework is developed that guides food companies in managing disturbances and in designing robust supply chains. We defined supply chain robustness as the degree to

which a supply chain shows an acceptable performance in (each of) its KPIs at various levels of disturbances. More particular, a supply chain is robust with respect to a KPI if the value of that KPI, adequately measured over an observation period, is sustained in a predefined desired range, even in the presence of disturbances.

Our framework consists of the following elements: (1) the description of the supply chain scenario, and the identification of KPIs; (2) the identification and characterization of unexpected events and disturbances in processes that impact the performance robustness; (3) the assessment of performance robustness; (4) the identification of sources of vulnerability; and (5) the identification of appropriate redesign principles and strategies. We have discussed the relationship between the elements of the framework and we have applied and tested the framework in an explorative case study. The results confirm that by analyzing the performance robustness of specific scenarios we can detect and typify disturbances. For each disturbance found, we identified a set of vulnerability sources that can represent a direct or indirect cause of the disturbance. Then, per vulnerability source a set of redesign principles and strategies were identified to prevent the disturbance itself. Alternatively, if that is not possible or cost effective, a set of redesign principles and strategies can be used to reduce its impact of disturbance to other processes in the company or supply chain members (domino effect).

The paper contributes to a better understanding of the concepts of vulnerability and robustness and of related issues in food supply chains. Moreover, here we synthesize and integrate relevant papers on supply chain vulnerability and supply chain robustness. From a practical point of view, the involved managers of the company concluded that the research framework supports the analysis of supply chain's robustness and vulnerability, and helps in finding and categorizing disturbances, vulnerability sources and appropriate redesign principles and strategies. However, more research is needed to extend and validate our findings. On the one hand more case studies could be done within the food industry to be able to construct generic overviews of sources of vulnerability and redesign strategies. On the other hand, in order to select the most appropriate redesign strategies for sources of vulnerability and disturbances identified in the case, more research is needed that models and quantifies the impact on key supply chain performance indicators for alternative supply chain scenarios.

Acknowledgment

We acknowledge the EU KP6 project Q-porkchains for supporting this research, the company managers for participating in this research, and our research assistants Sander van Lokven and Astrid van Moerkerk for their valuable inputs.

References

Adhitya, A., Srinivasan, R., Karimi, I.A., 2007. A model-based rescheduling framework for managing abnormal supply chain events. *Computers and Chemical Engineering* 31, 496–518.

Albino, V., Garavelli, A.C., 1995. A methodology for the vulnerability analysis of just-in-time production systems. *International Journal of Production Economics* 41, 71–80.

Asbjørnslett, B.E., Rausand, M., 1999. Assess the vulnerability of your production system. *Production Planning & Control* 10 (3), 219–229.

Asbjørnslett, B.E., 2009. Assessing the vulnerability of supply chains. In: Zsidisin, G.A., Ritchie, B. (Eds.), *A Handbook of Assessment, Management, and Performance*, 124. Springer, USA, pp. 15–33.

Bundschuh, M., Klabjan, D., Thurston, D.L., 2006. Modeling Robust and Reliable Supply Chains. Working Paper, University of Illinois at Urbana-Champaign.

Chandra, C., Grabis, J., 2007. *Supply Chain Configuration Concepts, Solutions, and Applications*, 1 edition Springer.

Dani, S., 2009. Predicting and managing supply chain risks. In: Zsidisin, G.A., Ritchie, B. (Eds.), *A Handbook of Assessment, Management, and Performance*, 124. Springer, USA, pp. 53–66.

Disney, S.M., Naim, M.M., Towill, D.R., 1997. Dynamic simulation modelling for lean logistics. *International Journal of Physical Distribution and Logistics Management* 27 (3/4), 174–196.

Dong, M., 2006. Development of supply chain network robustness index. *International Journal of Services Operations and Informatics* 1 (1/2), 54–66.

Dong, M., Chen, F.F., 2007. Quantitative robustness index design for supply chain networks. In: Jung, et al. (Eds.), *Trends in Supply Chain Design and Management, Technologies and Methodologies*. Springer Series in Advanced Manufacturing, pp. 369–391.

Ferdows, K., 1997. Making the most of foreign factories. *Harvard Business Review* March/April, 73–88.

Fleischmann, B., Meyr, H., Wagner, M., 2005. Advanced planning. In: Stadtler, H., Kilger, C. (Eds.), *Supply Chain Management and Advanced Planning, Concepts, Models, Software and Case Studies*, III edition, Springer, pp. 81–106.

Goetschalckx, M., Fleischmann, B., 2005. Strategic network planning. In: Stadtler, H., Kilger, C. (Eds.), *Supply Chain Management and Advanced Planning, Concepts, Models, Software and Case Studies*, III edition, Springer, pp. 117–138.

Hopp, W.J., 2008. *Supply Chain Science*. McGraw-Hill, Irwin, New York.

Jen, E., 2005. Stable or robust? What's the difference? In: Jen, E. (Ed.), *Robust Design: A Repertoire of Biological, Ecological, and Engineering Case Studies*. Oxford University Press, USA, pp. 7–21.

Juttner, U., Peck, H., Christopher, M., 2003. Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics: Research and Applications* 6 (4), 197–210.

Lee, H.L., 2002. Aligning supply chain strategies with product uncertainties. *California Management Review* 44 (3), 105–119.

Leung, S.C.H., Tsang, S.O.S., Ng, W.L., Wu, Y., 2007. A robust optimization model for multi-site production planning problem in an uncertain environment. *European Journal of Operational Research* 181, 224–238.

Kleijnen, J.P.C., 2005. Supply chain simulation tools and techniques: a survey. *International Journal of Simulation & Process Modelling* 1 (1/2), 82–90.

Kleindorfer, P.R., Saad, G.H., 2005. Managing disruption risks in supply chains. *Production and Operations Management* 14 (1), 53–68.

Kutanoglu, E., Wu, S.D., 2004. Improving scheduling robustness via preprocessing and dynamic adaptation. *IIE Transactions* 36, 1107–1124.

Macdonald, J.R., 2008. *Supply Chain Disruption Management: A Conceptual Framework and Theoretical Model*. Dissertation, University of Maryland, USA.

Mason-Jones, R., Towill, D.R., 1998. Shrinking the supply chain uncertainty circle. *Control*, 17–22.

Meepechdee, Y., Shah, N., 2007. Logistical network design with robustness and complexity considerations. *International Journal of Physical Distribution & Logistics Management* 37 (3), 201–222.

Melnyk, S.A., Rodrigues, A., Ragatz, G.L., 2009. Using simulation to investigate supply chain disruptions. In: Zsidisin, G.A., Ritchie, B. (Eds.), *A Handbook of Assessment, Management, and Performance*, 124. Springer, US, pp. 103–122.

Mo, J., Harrison, T.P., 2005. A conceptual framework for robust supply chain design under demand uncertainty. In: Geunes, J., Pardalos, P.M. (Eds.), *Supply Chain Optimization*, 98. Springer Science+Business Media Inc, pp. 243–264.

Mulvey, J.M., Vanderbei, R.J., Zenios, S.A., 1995. Robust optimization of large-scale systems. *Operations Research* 43 (2), 264–281.

Ouyang, Y., 2007. The effect of information sharing on supply chain stability and the bullwhip effect. *European Journal of Operational Research* 182, 1107–1121.

Peck, H., 2005. The drivers of supply chain vulnerability: an integrated framework. *International Journal of Physical Distribution and Logistics Management* 35 (4), 210–232.

Qiang, Q., Nagurney, A., Dong, J., 2009. Modeling of supply chain risk under disruptions with performance measurement and robustness analysis. In: Wu, T., Blackhurst, J. (Eds.), *Managing Supply Chain Risk and Vulnerability, Tools and Methods for Supply Chain Decision Making*. Springer, pp. 91–112.

Ritchie, B., Brindley, C., 2009. Effective management of supply chains: risks and performance. In: Wu, T., Blackhurst, J. (Eds.), *Managing Supply Chain Risk and Vulnerability, Tools and Methods for Supply Chain Decision Makers*. Springer, pp. 9–28.

Scipioni, A., Saccarola, G., Centazzo, A., Arena, F., 2002. FMEA methodology design, implementation and integration with HACCP system in a food company. *Food Control* 13, 495–501.

Shukla, V., Naim, M., 2007. An operations management framework for disturbance detection in supply networks. In: *Proceedings of 14th International Annual EurOMA Conference*, Ankara, Turkey.

Simangunsong, E., Hendry, L., Stevenson, M., 2008. Supply chain uncertainty: a framework linking sources, management strategies and performance. In: *Proceedings of International Annual EurOMA Conference*, Groningen, pp. 1–9.

Simchi-Levi, D., Kaminsky, P., Simchi-Levi, E., 2008. *Designing and managing the Supply Chain, Concepts, Strategies, and Case Studies*, III edition McGraw-Hill, Irwin.

Snyder, L.V., 2003. *Supply Chain Robustness and Reliability: Models and Algorithms*. Dissertation, Northwestern University, USA.

Snyder, L.V., Scaparra, M.P., Daskin, M.S., Church, R.L., 2006. Planning for disruptions in supply chain networks. *Tutorials in Operations Research, Informatics* 2006, 234–257.

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

Tang, C.S., 2006a. Robust strategies for mitigating supply chain disruptions. *International Journal of Logistics: Research and Applications* 9 (1), 33–45.

- Tang, C.S., 2006b. Perspectives in supply chain risk management. *International Journal of Production Economics* 103, 451–488.
- Tee, Y.S., Rossetti, M.D., 2002. A robustness study of a multi-echelon inventory model via simulation. *International Journal of Production Economics* 80, 265–277.
- Tomlin, B., 2006. On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science* 52 (5), 639–657.
- van der Vorst, J.G.A.J., 2000. *Effective Food Supply Chains, Generating, Modelling and Evaluating Supply Chain Scenarios*. Dissertation, Wageningen University, The Netherlands.
- van der Vorst, J.G.A.J., Beulens, A.J.M., 2002. Identifying sources of uncertainty to generate supply chain redesign strategies. *International Journal of Physical Distribution & Logistic Management* 32 (6), 409–430.
- Van Landeghem, H., Vanmaele, H., 2002. Robust planning: a new paradigm for demand chain planning. *Journal of Operations Management* 20, 769–783.
- Viswanadham, N., Gaonkar, R.S., 2008. Risk management in global supply chain networks. In: Tang, et al. (Eds.), *Supply Chain Analysis: A Handbook on the Interaction of Information, System, and Optimization*. , Springer, pp. 201–222.
- Vlajic, J.V., van der Vorst, J.G.A.J., Hendrix, E.M.T., 2010. On robustness in food supply chain networks. In: Trienekens, et al. (Eds.), *Towards Effective Food Supply Chains*. , Wageningen Academic Publishers, The Netherlands, pp. 63–82.
- Wagner, S.M., Bode, C., 2006. An empirical investigation into supply chain vulnerability. *Journal of Purchasing & Supply Management* 12, 301–312.
- Waters, D., 2007. *Supply Chain Risk Management, Vulnerability and Resilience in Logistic*. Kogan Page Limited.
- Wognum, P.M., Trienekens, J.H., Wever, M., Vlajic, J.V., Vorst, J.G.A.J., van der Omta, S.W.F., Hermansen, J., Nguyen, T.L.T., 2009. Organisation, Logistics and Environmental Issues in the European Pork Chain, European Pork Chains. In: Trienekens, et al. (Eds.), , Wageningen Academic Publishers, Wageningen, pp. 41–72.
- Wu, T., Blackhurst, J., Chidambaram, V., 2006. A model for inbound supply risk analysis. *Computers in industry* 57, 350–365.
- Wu, Y., 2006. Robust optimization applied to uncertain production loading problems with import quota limits under the global supply chain management environment. *International Journal of Production Research* 44 (5), 849–882.
- Wu, T., Blackhurst, J., O'Grady, P., 2007. Methodology for supply chain disruption analysis. *International Journal of Production Research* 45 (7), 1665–1682.
- Zapfel, G., 1998. Customer-order-driven production: an economical concept for responding to demand uncertainty? *International Journal of Production Economics* 56/57, 699–709.
- Zsidisin, G.A., Panelli, A.P., 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), 187–197.