1. Introduction
Throughout the 1990s, the lean attitude assumed a relevant role within both academics and practitioners. Stripping every process down to its core, the streamlined manufacturing, low inventory and just-in-time movement of goods became standard practice. As substantial advantages, costs were more predictable, efficiencies increased, profits grew and important innovations in supply chain management led to new ways of doing business.
Growing competition and emphasis on efficiency and cost reduction, as well as the satisfaction of consumer demands, have brought new challenges for businesses in the global marketplace. Every day, companies face complex situations and even harsh business shocks much more often than they had to manage years ago. At the same time that businesses and, in particular, supply chains have become increasingly global, the industrial environment has become filled with uncertainty. Disruptions in Supply, in Internal Operations and in Demand are now becoming top agenda issues of managers,
reaching in importance all the typical business concerns such as revenues, costs and market-shares. Conversely, innovations in technology and especially the availability of electronic commerce in which the physical ordering of goods (and, in some cases, even delivery) is replaced by electronic orders, offer the potential for reducing risks associated with physical transportation due to potential threats and disruptions in supply chains. The combined effect of business globalization and the recent catastrophic events (e.g. terrorist attacks and devastating natural phenomena) are now bringing to light a new challenging field of research related to corporate security and resilience. Risk in a supply chain often originates from the lack of knowledge about the events that may affect operations and the ability of the network to endure them. Risk considerations should influence the supply chain design and structure and should be based on clear performance requirements and lines of communication between all entities. Businessmen often rely on their experience and intuition to manage risks. However, the more complex the business, the more important it is to identify risks that may prevent a business from realizing its potential, and to manage them in order to minimize adverse outcomes and maximize positive outcomes. Due to these changes in the whole context where industrial companies are engaged, the aim of this paper is to clearly define the main concepts related to the operational risk management world (such as hazard, risk and vulnerability) in order to highlight different approaches and techniques that could be used to manage supply chain disruptions. Under the persuasion that a business that is not able to manage its related risks effectively will probably disappear, this paper would be the basis for further research actions devoted to the analysis of risks management models and frameworks both new and inherited from other sectors, such as the credit sector or the environmental sector (where generally the concept of risk management is already well-stated). The final aim of our research is to bring all these topics and issues together in a single, comprehensive reference framework.

The paper will be organized as follows: in section 2 the basic concepts are identified and clearly defined. Particular emphasis will be given to the concept of risk and to the ways it is connected to other concepts. Section 3 is devoted to the definition of the dimensions that are relevant for the analysis of risk, while section 4 presents different approaches to the disruption management within a supply chain. Section 5 reports some general framework for risk management while section 6 draw some conclusion remarks.

2. Risk, Hazard, and Vulnerability: defining the main concepts.
In a rational decision making process, at least three components should be clearly stated (Stewart et al., 1997):
- What requirements should be met
- Which is the probability of achieving such requirements
- What are the consequences if the requirements are not met

The concept of risk could be related to the second component, since the aim of assessing the probability of achievement of a requirement is a measure of the risk involved in the activity. The procedures for determining these probabilities have a degree of commonality across many industries and disciplines. Modern approaches have attempted to make the risk aspects more explicit and manageable but, though the original concept of risk has been acknowledged since the earliest times (at least, in an intuitive way), it is too general and faint for the adoption in
a structured risk management approach. At a first glance, risk appears as a multi-dimensional concept, that cannot be felt and is not precisely measurable, although it can be estimated with reference to a specific unit of measure, albeit imperfectly. The term risk embeds more semantics according to the different perspectives: for engineers it is a synonym of probability of occurrence of a specified (generally undesirable or adverse) event, while in insurance industry (where the concept of risk has been primarily addressed) the focus is on the value of the items or money “at risk”. However, a commonly accepted definition of risk encompasses both aspects: in many cases, risk can be expressed as the probability multiplied by the value of consequences (for example, Stewart et al., 1997; Ward, 1999, Haywood et al., 2004). Given this definition, the problem shifts from the definition of risk to the definition (and quantification) of consequences. Often the estimation of consequences is industry or context specific, not always quantifiable in terms of monetary value. As a conclusion, we can state that, in general term, risk can be defined as the probability that an event occurs during a stated period of time, leading changes in the company’s performances. Here, the concept of event is considered well known.

2.1. Hazards

Another generally used term related to risk is hazard. According to what safety professionals usually consider hazard, it is possible to refer to it as everything which is inherent to an activity, a workplace or a task and with a potential for loss of business opportunity, damages, injuries, or some combination of these (Allen et al., 1992, Stewart et al., 1997; Ayyub, 2003; NSW, 2005). Smith (2002) refers in general sense the term hazard to any work design factor that elevates the risk of detrimental performance by a worker (employee or manager) or an organizational system. This means that anything a company needs to achieve a defined goal brings a hazard. Thus, hazard is an objective and intrinsic state connected to any business decision, which increases the risk of poor performance. Hazards come from the decisions and choices adopted by companies: for example, moving the production plants far from the markets (due to low labour costs of some regions) introduces more hazards, since the transportation times are relevant. Moreover, there are countries with low labour costs combined with unstable political situations that could lead to business interruption or delay. The hazards should be clearly identified and assessed before taking a specific decision, since they might increase the risk up to an unacceptable level. In order to relate the concept of risk to that of hazard, we can better supplement the definition of risk as the probability that a particular (generally adverse) event occurs during a stated period of time, or results from a particular challenge, in circumstances arising from the realisation of a specified hazard.

2.2. Vulnerability

According to Christopher (2002) it is possible to argue that the complexity of modern supply chains tends to increase, bringing with it higher levels of risk and, hence, vulnerability. Supply chain vulnerability can be defined as an exposure to serious disturbances, arising from risks within the supply chain as well as risks external to the supply chain (Christopher, 2002). In other words, vulnerability is a result of any weakness in the system that can be exploited to damage the system itself (Ayyub, 2003). Vulnerability relates to risk management, or business continuity planning. In recent years, vulnerability has become a hot topic for many companies. In the past, disruptive events occurring in one part of the world were somewhat isolated, at least
geographically. Now, with complex supply chains interlinked around the globe, a crisis in Asia becomes a problem for a technology manufacturer in the Middle East. According to Sheffi (2005), a useful way to assess the level of vulnerability of a company is represented by this approach:

1. Define a disruptive event that reasonably the company could face. Given this disruption:
2. Define its likelihood.
3. Define the magnitude of the consequences the disruption could generate.
A typical vulnerability map is represented in Figure 1 where each point represents a disruptive event.

![Vulnerability map](image)

*Figure 1 – Vulnerability map (Adapted from Ward, 1999)*

### 2.3. Types and categories of risk

There are several more types of risk that could be found in literature and in current risk management implementations. According to different sources (as NSW, 2005), we can define at least three main types:

- **Opportunity-based risk**: risk associated with the choice about taking or not taking an opportunity. This type of risk is often financial and can have a positive or negative outcome, referring to both short-term and longer-term horizons. Opportunity-based risks related to operating a business include moving a business to a new location, acquiring new property, expanding a business, and diversifying a product line. Comparing risks and opportunities, the business owner should assess if the latter outweighs the first.

- **Uncertainty-based risk**: this type refers to risks associated with unknown and unexpected events. These risks are often unknown or extremely difficult to highlight and quantify and not possible to control or influence (such as, for example, catastrophic or disastrous in nature).

- **Hazard-based risk**: is the type of risk associated with a source of potential harm or a situation with the potential to cause harm. This comprises, among others, physical, ergonomic, and psychological hazards on the faced by the workforce.

Besides these types of risks, in order to have a structured approach to risk identification, it is helpful to consider the following *categories* of risk (see table 1). Considering risk related to a supply chain, it is possible to assume an *internal* or *external* perspective: internal risks arise from the interaction between the elements that
compose the supply chain, while external risks arise from the interaction between the supply chain and the environment.

<table>
<thead>
<tr>
<th>Risk category</th>
<th>Relates to</th>
</tr>
</thead>
<tbody>
<tr>
<td>FINANCIAL</td>
<td>Cash flow, budget, tax obligations, credit management, remuneration…</td>
</tr>
<tr>
<td>EQUIPMENT</td>
<td>Operation of the equipments, maintenance, safety…</td>
</tr>
<tr>
<td>ORGANISATIONAL</td>
<td>Cultural, structural and people issues associated with the effective operation of the business.</td>
</tr>
<tr>
<td>SECURITY</td>
<td>Security of premises, assets and people</td>
</tr>
<tr>
<td>LEGAL &amp; REGULATORY COMPLIANCE</td>
<td>Compliance with legal requirements such as legislation, regulations, standards and contractual requirements.</td>
</tr>
<tr>
<td>REPUTATION</td>
<td>Threat to the reputation of the business.</td>
</tr>
<tr>
<td>OPERATIONAL</td>
<td>Planning, operational activities, resources and support required within the operations of a business</td>
</tr>
<tr>
<td>SERVICE DELIVERY</td>
<td>Quality and appropriateness of the service provided, including customer interaction and after sales service</td>
</tr>
<tr>
<td>COMMERCIAL</td>
<td>Risk associated with market dynamics, business growth, diversification and commercial success.</td>
</tr>
<tr>
<td>PROJECT</td>
<td>Management of equipments, finances, resources, technologies, timeframes, and people associated with the management of projects</td>
</tr>
<tr>
<td>SAFETY</td>
<td>Safety of everyone associated with the business, from individual to social safety.</td>
</tr>
<tr>
<td>STAKEHOLDER MANAGEMENT</td>
<td>Relationship with stakeholders</td>
</tr>
<tr>
<td>STRATEGIC</td>
<td>Planning and sourcing requirements for the establishment and growth of the business.</td>
</tr>
<tr>
<td>TECHNOLOGY</td>
<td>Implementation, management, maintenance and upgrades associated with technologies.</td>
</tr>
</tbody>
</table>

Table 1 – Categories of risk (source NSW, 2005)

All these elements can be summarised as in Figure 2, which represents the four risk areas inside and outside the company.

![Figure 2 – Areas of risk inside and outside the company](image-url)
2.4. How risk does manifest itself in a supply chain

Each decision involves a risk. Within a modern supply chain, risks related to decisions can manifest themselves in several different ways, such as inventory risk, supply interruption risk, capacity risk, non-compliance risk.

- **Inventory risk**: no company wants to experience materials shortages that impact their ability to supply finished product to their customers. In highly dynamic markets this could lead to a stock upsurge. It is generally considered as one of the greatest risks for supply chains, since it could generate high capital immobilization and obsolescence or unexpected demand shifts. This is true especially in highly volatile demand sectors, such as electronics and IT.

- **Supply interruption risk**: by reducing inventory, outsourcing non-core activities, trimming the number of suppliers and sourcing globally, operations have become leaner and more efficient. But while the costs have come down, the risks have increased tremendously, due to the increased interdependency between companies. A failure in one element of the network (wherever located) could imply the serial interruption of the whole chain.

- **Capacity risk**: at a strategic level, managers should decide about the amount of resources (especially in terms of equipments) to be acquired, in order to cover future demands. Small capacity presents significant opportunity costs; conversely, excess capacity can curb the profits gained in the peak period.

- **Non-Compliance Risk**: due to the extension of the market all over the world, companies should pay greater attention to the different laws in force in the different countries.

- **Financial risk**: the economic climate and markets can be affected very quickly by changes in exchange rates, interest rates, and commodity prices. Financial risk arises through countless transactions of a financial nature, including sales and purchases, investments and loans, and various other business activities. Instantaneous availability of information means that changes, and subsequent market reactions, occur very quickly. As a result, it is important to ensure financial risks are identified and managed appropriately.

2.5. Risk acceptance and tolerability

Risks can be accepted either if they are not recognised as such or if they are recognised but perceived to be insignificant (Allen et al., 1992). If recognised, it is important to define the proper level of tolerance, that is related to the benefits that counterbalance the risk. It is then important to define the tolerable threshold under which the risk, considered know, is acceptable.

3. Characterising risk dimensions

According to the researches of Sitkin and Pablo (1992) the term risk could be considered as a concept composed by three dimensions: outcome uncertainty, outcome expectations and outcome potential.

The outcome uncertainty dimension is often defined in terms of the variability of outcomes, lack of knowledge of the distribution of potential outcomes and the uncontrollability of outcome attainment.

In the past, a relevant number of studies (see for example Kahneman and Tversky, 1979; Jackson and Dutton, 1988; Figenbaum and Thomas, 1988) suggested that positive expected returns cause completely different decision-making behaviours and attitudes than outcomes with negative expected values: when individuals deal with a risky alternative whose possible outcomes are good they appear to be risk adverse; but if they
are dealing with a risky alternative whose possible outcomes are poor they tend to be risk-seeking. Moreover, March and Shapira (1987) have noted that the term risk is quite always used to refer to negative expected outcomes. Contrarily, it is our belief that both positive and negative expected outcomes have to be considered as risks when a decision-maker has to face the issues related to outcome expectations. This position can be easily explained just considering that is not the type of outcome that defines a risk, but simply the gap between aspirations and the mean of the distribution of expected outcomes. Inherent in this formulation is that the outcome expectations dimension defines risk everything (positive or negative) that could be disappointing to the decision-maker or different from his aspirations.

The third dimension, outcome potential, is related to the potential consequences of decisions. This dimension describes an aspect of risk that is often not sufficiently taken under consideration: the overweight of extreme and unlikely outcomes (Kahneman and Tversky, 1979). This means that if a potential outcome is great, individuals often overweight the probability of the outcome itself. On the other hand high-impact/low-probability disruptions are not that rare if instead of considering just a company we consider the whole supply chain network. For instance, the 1995 Kobe earthquake in Japan caused the slow down of the production of PowerBook computers by Dell due to the interrupted production of display monitors of its supplier in Kobe; analogously, a small blaze shut down a Philips’s plant in Albuquerque, New Mexico causing tremendous impacts to the financial growth curve of Ericsson, a Philips’s customer (Sheffi, 2005).

To clarify the link between hazard and risk a three-dimensional framework is presented in Figure 2. The framework shows the three axes characterizing risk. The point (0,0,0) of the 3D space defined by the axes OU, OE and OP is the initial point before a new decision takes place (e.g. the selection of the supplier of a core component of a new product to release). When the decision is taken (e.g. the selection of the supplier) the point (0,0,0) moves from its original position to the point defined by the intersection of the three barriers. This means that the hazard associated to the decision taken defines three risk lower-bounds (or barriers), which the company, in the short-term and without taking strategic actions, is supposed not to trespass.

According to this structure, managing the risk in the short-term means then implementing actions for trying to be as closer as possible to the point identified by the intersection of the new axes OU’, OE’ and OP’. Talking about disruptions (e.g. reduced production capacity, shortage of critical parts and distribution networks shutdown) the first thing to point out is that disruptions do not result only from disasters and catastrophes, such as earthquakes, tornados, floods and a terrorist attacks. They can be even much more related to the economical situation, the market prospects, the technological changes and the business organization, strategies and activities.
To better understand this assumption we provide in Figure 4 a two-dimensional model. The horizontal axis represents the origin of the event, act or situation able to cause a disruption (i.e. from within or outside the company), while the vertical axis defines if the events, acts or situations causing disruptions are directly related to the business activities and/or to the way people work to achieve the defined objectives.

<table>
<thead>
<tr>
<th>Related to business activities</th>
<th>Not related to business activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidents, Visible quality problems, IT system failure, Ineffective planning,…</td>
<td>Vandalism, Thefts, Workplace violence,…</td>
</tr>
<tr>
<td>Random variations in demand, Technological changes, Interest rate fluctuation, Loss of key supplier,…</td>
<td>Natural disasters, Terrorism,…</td>
</tr>
</tbody>
</table>

Figure 4 – Classification model of events, acts or situations that can lead to disruptions
Such a map can help managers and senior executives to list and prioritize events, acts or situations that can lead to disruptions. Besides, using this model can help the whole organisation to better address the right policies since it defines both the origin of threats and the dependence with the business activities.

4. How to manage disruptions in operations and supply chain.
We can state that enterprise risk management deals with risks and opportunities affecting value creation or preservation. It is a process designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. However, things always happen and disruptions could occur in any time and in any place. In that case, it is important to have suitable management methods aiming at mitigating or preventing the impact on a business.

4.1. Reactive Approach
When a disruptive event occurs, the only reasonable approach is a reactive one. Briefly, this means selecting the appropriate actions to face a disruption that is deteriorating the company’s performance, or, in other words, the system reacts only when it receives some specific inputs (in this case when the disruptive event takes place). Sometimes this is interpreted as being unprepared and facing the situations just improvising. This is a wrong way to see the reactive process. Of course this process is sometimes the only approach used and often it collapses consequently in degenerated forms (e.g. many safety management systems are corrupted example of reactive process-based systems). Generally, the reactive approach needs “preparation” and a well-established management system.

According to the Sheffi’s profile of a disruption (2005), when the disruptive event takes place the only way to response for a company is to perform as better as possible the following actions:
1. First response: includes all the activities able to mitigate the impact of the disruptive event;
2. Recovery preparation: has to follow immediately the first response or better start in overlapping. If the full impact of the disruptive event can be felt by the company in a time-delayed manner (e.g. a huge inventory can protect a company by the loss of key suppliers for days or weeks) a good risk-management program should be able to start the recovery program before the disruptive event is fully felt.
3. Recovery program: if recovery preparation looks at the soft-side of recovery (i.e. planning, programming, checking, monitoring…) this phase is the hard-side. It usually takes a lot of time since it deals with physical assets (e.g. restarting production, rebuilding damaged or destroyed facilities…). The final goal of this phase remains obviously to restore the performance the company had before the disruption.

The reactive approach is not the only one a company can adopt to face disruptions. The reactive approach versus what is called the proactive approach is a crucial issue regarding different areas of research in the management sphere, such as safety management (Reason, 1997; Sutherland et al., 2001) and organization change and development management (Buchanan and Huczynski, 1997).
Both strategies obviously have to co-exist to increase both the level of resilience and security of a company, where the term resilience refers to the ability of a company to recover quickly after a disruption (Sheffi, 2005). That is different from the term security, which is related to the capability to reduce the likelihood of a disruptive event. Back to the vulnerability map in Figure 1, this means that to reduce the gravity of a possible disruptive event a company has to be resilient, respond rapidly to the disruptive event, in other words has to react as better as possible following, for instance, the three-steps path presented above. The probability axis deals with the ability of increasing security (reducing the likelihood of given disruptive events) by addressing the typical characteristics of the proactive approach process.

4.2. Flexibility

In the organizational theory area it is widely accepted that when internal or external factors make pressure on an organization, only prepared ones with appropriate characteristics and with suitable structures can react quickly and with good results (Burns and Stalker, 1961; Litterer, 1973; Eisenhardt and Bourgeois, 1988). In the operations management context being prepared means building in flexibility and, sometimes, in redundancy (see section 4.3.).

According to the multidimensional flexibility concept of Gerwin (1993) it is possible to identify seven types of flexibility related to the types of uncertainties and the strategic objectives (summarised in Table 2). Moreover, according to Slack (1988), each flexibility dimension has two sub-dimensions: range and time. A production system is more flexible than another if it can manage, for example, a wider range of products. In the same way, a production system is more flexible than another if it can produce, for example, the same range of products in a shorter time.

1. **Mix**: represents the ability to handle a range of products or variants efficiently in order to cope with market requirements. The range sub-dimension represents the extent of product variety while the temporal aspect essentially reflects set-up time.

2. **Changeover**: represents the ability to rapidly introduce new products against those currently offered. The range sub-dimension represents the variety of introductions that can be performed while the temporal aspect reflects the manufacturing start-up time.

3. **Modification**: represent the ability to implement minor changes to given products to meet the customers’ desires. The range aspects reflects how many different minor changes are performable while the temporal sub-dimension indicates the lead time a minor change requires to be completed.

4. **Volume**: represents the ability to increase or decrease the aggregate production level. The amount of change reflects the range aspect; the timeframe to make a change represents the time sub-dimension.

5. **Rerouting**: this dimension deals with the machine downtime uncertainty. The machine downtime can be either long-term (i.e. to accommodate major product design changes) or short-term (i.e. due to equipment and/or quality problems). Rerouting is the ability to create alternative production paths. The range sub-dimension is related both to the variety of parts for which rerouting occurs and to the extent to which a part can be rerouted. The timeframe which is necessary to make the adjustment represents the time sub-dimension.

6. **Material**: as we pointed out above, a supplier represents for the downstream company a source of uncertainty in the way it provides input-materials. This dimension delineates the ability of the manufacturing department to manage
unexpected inputs variations. The range aspect deals with the number of different variations the production unit is able to handle as well as their magnitude. The time sub-dimension considers how long it takes to perform an adjustment.

7. **Flexibility responsiveness**: obviously the above uncertainties change uncontrollably over time generating new conditions. A company consequently should have a strong strategic adaptability in order to quickly adjust the objectives for the new context. This means in term of flexibility dimension having a manufacturing unit able to rapidly change the sub-dimensions range and time of all the six flexibility dimensions.

<table>
<thead>
<tr>
<th>Type of uncertainty</th>
<th>Strategic objective</th>
<th>Flexibility dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market acceptance of kinds of products</td>
<td>Diverse product line</td>
<td>Mix</td>
</tr>
<tr>
<td>Length of product lifecycles</td>
<td>Product innovation</td>
<td>Changeover</td>
</tr>
<tr>
<td>Specific product characteristics</td>
<td>Responsiveness to customers’ specs</td>
<td>Modification</td>
</tr>
<tr>
<td>Aggregate product demand</td>
<td>Market share</td>
<td>Volume</td>
</tr>
<tr>
<td>Machine downtime</td>
<td>Customers’ due dates</td>
<td>Rerouting</td>
</tr>
<tr>
<td>Characteristics of materials</td>
<td>Product quality</td>
<td>Material</td>
</tr>
<tr>
<td>Changes in the above uncertainties</td>
<td>Strategic adaptability</td>
<td>Flexibility responsiveness</td>
</tr>
</tbody>
</table>

Table 2 – Dimensions of flexibility (Gerwin, 1993)

The first four dimensions are generally referred to as market-oriented, since they deal with the uncertainties in the demand of products. The 5th and the 6th dimensions deal with the manufacturing process (i.e. machines and materials). The last dimension is “the uncertainty of the uncertainties”; it considers the unpredictable and uncontrollable changes in the types and intensities of the uncertainties which have to be managed.

To address flexibility, a company should then try to plan, introduce, apply and use any operations management technique which can be useful to increase range and time performance of each dimension (e.g. modular products, postponement and channel assembly techniques: 1st dimension; define cross-functional design teams: 3rd dimension; subcontracting: 4th dimension;…).

But a challenging point is: how to measure the level of flexibility? According to Pagell and Krause (1999) we believe that to understand its level of flexibility a company should focus on the shop-floor. Some works (e.g. Miller and Roth, 1994) outline the relationship between the manufacturing strategy (i.e. defining three main manufacturing strategic groups) and some dimensions of flexibility (e.g. design flexibility, volume flexibility and mix flexibility). As the importance of the strategic process is the implementation of the strategy itself, a flexibility performance framework should primarily focus on the manufacturing operations, designing, for instance, for each Gerwin’s flexibility dimension the appropriate plant-level indicators. The indicators should report the flexibility’s performance measuring each sub-dimension (i.e. range and time) for each Gerwin’s flexibility dimension.
Some of the benefits of doing in this way include the following:

1) define a continuous link between manufacturing strategy and operations;
2) control if the production system is following the manufacturing strategy as well as the business strategy;
3) reduce the possibility of formulating strategies which are difficult to achieve for the manufacturing department;
4) define the appropriate actions to support the manufacturing strategies.

Further studies will address this field of the industrial research.

### 4.3. Redundancy

Redundancy is the other major way to increase company’s resilience (probably the most easy and obvious one). Redundancy deals with having multiple suppliers, extra inventory, spare capacity, added workers and low utilization. Therefore redundancy can be considered as a sort of shield which can help a company recover quickly from a disruption. The point is that redundancy contradicts all the operations management theories produced during the last thirty years. Lean manufacturing systems (also known as Toyota Production Systems or synchronous manufacturing systems) aim at eliminating all forms of waste and redundancy and to address the production objectives using minimal levels of resources. Just-in-time technique, for instance, is a substantial portion of the lean production system. The final goal of lean production is to produce a great variety of products in large volume minimizing the usage of resources. This requires the identification and then elimination of all non-value-added activities. From this perspective redundancies bring extra expenses and non-value-added activities. Besides this opportunity of “doing more saving resources”, there is enough consensus among researchers about other important benefits from the adoption of lean manufacturing, such as higher product quality and service to customer (Schonberger, 1982; White et al., 1999).

Redundancy should then be just a short-term remedy while working for flexibility should be considered a long-term strategy. Considering the risk framework in Figure 3, building in redundancy means: given a decision (e.g. procurement focused on a single supplier) a company has to try to be as closer as possible to the outcome potential barrier (e.g. extra inventory). While building in flexibility involves a strategic process aimed to reduce the hazard (i.e. trying to push down the outcome potential barrier). If the company believes in working with a single supplier, such a strategy works if accompanied by deep-partnership with that supplier, since it becomes crucial for the company’s manufacturing system. Sharing data, information and collaborating together involves obviously strategic choices that can help a company to recover quickly from disruptions. (e.g. The Toyota Group and the Aisin Fire reported in Nisihiguchi and Beaudet, 1998).

### 4.4. Near Misses

As we pointed out above, the concept of security deals with the ability to reduce the likelihood of a disruptive event. The necessary activities to address this kind of objective have to follow a proactive approach. According to Crant (2000) being proactive means challenging the status quo, taking actions before a specific stimulus or a set of specific stimuli do not force a generic entity to react. The question is: how can a company be proactive? Sutherland et al. (2001) stands that “To be proactive you need information before accidents occur.” This is the central point of the proactive approach: to reduce the likelihood of a disruptive event, a company needs information before the
disruptive event occurs. Since there are typically many signs that a disruption is about to take place, near-misses represent the information to resolutely aim at a proactive approach. According to the classification algorithm of Cavalieri and Ghislandi (2006) we can define near-miss:

- an event which could have been a disruptive event but did not (i.e. event-driven near-miss); and
- every act or situation which does not lead to an event (i.e. a specific event is not recognizable) but with a prominent risk to generate a disruptive event (i.e. not event-driven near-miss or hidden near-miss).

In this way, being proactive means using the information available from the analysis of near-misses in order to take the necessary actions to reduce the likelihood of disruptive events.

The core part of a so called Near-Miss Management System is to reduce the likelihood of major disruptions, since, according to the clarifying study on the common cause hypothesis performed by Wright and van der Schaaf (2004), near-misses and accidents (i.e. large-scale disruption) have the same relative causal patterns. Disruptive events rarely occur without any warning. A large number of small incidents (i.e. event-driven near-miss) or hazardous, insecure acts or situations (i.e. not-event driven near-miss) may foreshadow more relevant accidents. Learning from small occurrences can help companies to correct the conditions that lead to major disruptions, thereby reducing the likelihood of large disruptions. Obviously, to gain all the remarkable benefits of the near-miss analysis a company needs a specific and well designed management system. Worthy of remark is the Near-Miss Management System proposed by Phimister et al. (2003). This seven stages framework includes:

1. **Identification**: a near-miss is recognized to have occurred; naturally, different companies have different rules for deciding what events, acts or situations can be considered near-miss.

2. **Reporting**: the near-miss is reported and recorded; according to Jones et al. (1999) a company should stimulate near-miss reporting and learn lessons from them in order to reduce occurrences of accidents.

3. **Prioritization and Distribution**: assessment of near-misses to define priorities and distribution of the information to those who will define follow-up actions.

4. **Causal Analysis**: given a near-miss, this step involves the analysis process of the direct and root causes that could have led to the accident.

5. **Solution Identification**: identification of solutions to prevent large disruption and definition of corrective actions.

6. **Dissemination**: dissemination to implementers and to a wider audience to increase awareness.

7. **Resolution**: implementation and evaluation of the corrective actions.

4.5. Layered Defence

Another important approach for increasing security is related to the concept of layered defence system. It is based on the idea of creating defensive layers with independent barriers installed in series. Consider, for instance, two barriers, \(B_1\) and \(B_2\), installed in series. Defining \(P(E)\) as the probability event \(E\) occurring over a given time period, \(P(B_1|E)\) as the probability barrier \(B_1\) fails if challenged given \(E\), and \(P(B_2|E[B_1])\) as the probability barrier \(B_2\) fails if challenged given \(E\) and \(B_1\) failing. Then, the probability \(P(D)\) of a disruption occurring is:
\[ P(D) = P(E) \cdot P(B_1|E) \cdot P(B_2|E[B_1]) \]

Consequently, the layered principle stands that if more barriers are installed in series, the probability of a disruption decreases drastically. For \( n \) barriers installed in series the general formula is:

\[ P(D) = P(E) \cdot \prod_{i=1}^{n} P(B_i \cap E[B_{i-1}]) \]

Besides being more effective, a layered defence is generally even less expensive than a single defensive mechanism. Remarkable is the difference between being layered and being redundant: a layered defensive measure uses different barriers to reduce the likelihood of a disruption; a redundant system uses extra quantities of the same barrier to mitigate the consequences of a disruptive event.

Considering Figure 3, working for security means reducing outcome uncertainty (Outcome Uncertainty dimension) and the gap between aspirations and the mean of the distribution of expected outcomes (Outcome Expectation dimension).

### 4.6. Section summary

There is no clear separation between security and resilience. The methods for increasing security increase the level of resilience and vice versa. Dealing with near-misses instead of full-disruptive events can provide important information to improve the flexibility and consequently the resilience of a company (i.e. proactive approach).

A resilient company can recover so quickly from a disruption (i.e. reactive approach) that it is felt just like a near-miss and not a full-disruptive event. In the same way many operations management techniques which increase the level of flexibility can even be considered as layered barriers which reduce the probability of a disruptive events.

Consequently, a layered system is able to stop a possible full-disruptive sequence and turn it into a near-miss situation. According to van der Schaaf (1995), near-misses represent a test for the company’s defence system by showing these defences in action. Table 3 sums up some of the main concepts highlighted in this section.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Vulnerability dimension</th>
<th>Performance dimension</th>
<th>Approach</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce the gravity of a disruptive event</td>
<td>Gravity</td>
<td>Resilience</td>
<td>Reactive approach</td>
<td>Building in redundancy and flexibility</td>
</tr>
<tr>
<td>Reduce the likelihood of a disruptive event</td>
<td>Probability</td>
<td>Security</td>
<td>Proactive approach</td>
<td>Layered defence, Identification and analysis of near-misses</td>
</tr>
</tbody>
</table>

Table 3 – Main concepts on how to manage disruptive event, act or situation in operations and supply chain

## 5. Risk management frameworks in operations and supply chain management

There are several approaches to risk management, generally depending on the characteristics of a specific sector, context or period. In Table 4 the evolution of the
concept of risk management is shown by introducing the focus of risk management applications in different decades (Artto and Hawk, 1999).

<table>
<thead>
<tr>
<th>Decade</th>
<th>Focus in applications</th>
<th>Focus in risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td>1950</td>
<td>Administration, Procurement, Planning</td>
<td>Schedule network models</td>
</tr>
<tr>
<td>1960</td>
<td>Scheduling</td>
<td>Probabilistic network models</td>
</tr>
<tr>
<td>1970</td>
<td>Organization, Leadership</td>
<td>Decision trees, Subjective probabilities</td>
</tr>
<tr>
<td>1980</td>
<td>Computerized applications, Quality</td>
<td>Probabilistic software, check lists, Response lists, Influence diagramming</td>
</tr>
<tr>
<td>1990</td>
<td>Processes, ICT, Networking</td>
<td>Team work, Organizational learning, Risk management processes, Risk management organization</td>
</tr>
<tr>
<td>2000</td>
<td>Cooperation models, Virtual organizations, Learning</td>
<td>Risk management knowledge bases, Cooperation, Response planning.</td>
</tr>
</tbody>
</table>

Table 4 – Evolution of the focus on risk management (Arrto and Hawk, 1999)

An interesting and general, cross-industry and cross-area model is the one proposed by the Australian Standards (AS/NZS, 2004) and represented in Figure 5.

![Figure 5 – The risk management process (AS/NZS, 2004)](image-url)
Since it has been demonstrated in different business contexts (e.g. industrial innovation, Rothwell, 1992) that the simple mono-directional approach is definitively ineffective, we believe in a coupling risk management process model which recognizes interaction between the different steps and the feedback loops between them. The model presented above addresses this aspect modelling the Monitor and review step as a phase along the entire process which interacts with each step bi-directionally. Since a very few risks will remain static, this Monitor and review phase should continuously interact with each step in order to identify the potential increasing trends of the recognized risk factor and new significant risk factors.

Going briefly through the steps of the model we have as follows:

- **Establish the context**: the aim of this phase is to define: (i) the internal context (e.g. goals and objective, projects and activities) to ensure that all significant risks are considered and to ensure that risk decisions always support the general objectives of the company; (ii) the external context (e.g. market, competitors, political regulations) to identify SWOT; (iii) the risk management context: this means establishing boundaries (e.g. the business object: introduction of a new product, the selection of a new supplier) and parameters (e.g. timeframe of the project, resources required, roles and responsibilities); (iv) risk criteria to specify the acceptable level of risk for a specific activity or event; (v) the structure for risk analysis: this means choosing the risk categories of the given project (e.g. finance, production, logistic).

- **Identify the risks**: when the context has been established, it is necessary to use all the information to identify as many risks as possible. The aim of this phase is to identify all the risks that can affect, either positively or negatively, the objectives of a company. Roughly, risk identification means answering the following questions: (i) what can happen? (ii) how can it happen? (iii) why could it happen? The classification model in Figure 4 can be used to classify what, in order to better identify how and why.

- **Analyse the risks**: this phase has essentially the aim to measure and prioritize the risks. This is needed to be able to choose suitable management actions for the identified risk factors. A possible further research activity could include how to use the risk’s dimensions framework presented above to implement a new risks measure strategy.

- **Evaluate the risks**: this step compares the level of risk measured during the last phase against the risk criteria established. The aim of this step is to decide if risks are acceptable or need treatment. Obviously, a risk may be acceptable for many reasons (e.g. cost of treatment exceeds the benefit, a low level of risk, no treatments available.)

- **Treat the risks**: this step is about considering options for treating risks, which were not considered acceptable at the previous stage. This phase should aim at identifying options to either reduce negative consequences, or to reduce the likelihood of adverse outcomes. The most common strategies for treating risks are risk transfer, risk taking, risk reduction and risk elimination.

Another important aspect which emerges from this model is the importance of the integration within the firm, upstream with suppliers and downstream with customers. Even the Communication and consult phase, like the Monitor and review phase, goes along the entire process and interacts with each step bi-directionally. There are two main aspects that make communication absolutely necessary for an effective and efficient risk management process:
- **information-based aspect**: it is rare that just a person or a company has all the information needed to identify and manage the risks. It is therefore crucial to identify the stakeholders who can make the information complete.

- **disruption-based aspect**: a disruption to a supplier’s supplier thousands of miles away may affect seriously the performance of a company. This is what is called the domino effect. Since disruptions not only negatively affect the performances of the company which has been hit but even the performances of the other participating players, it is anyone’s interest to be involved actively in the process and share information and expertise with the other partners.

Therefore, one of the main trends of today’s researches in the field of risk management in operations and supply chain management is how to define a risk management process in a networked environment. In this stream, one of the most interesting conceptual models is the one presented by Hallikas et al. (2004); to implement a network-based risk management process it is necessary that the partners of the network have assessed their own risks and implemented appropriate risk management activities. This is the core part of the model. The individual risk management process is a **conditio sine qua non** to define a collaborative risk management process. Such a risk management process is represented in Figure 6.

![Figure 6 – Risk management process in network environment (Hallikas et al., 2004)](image)

The most important aspects of the collaborative process are:
- the identification of risks that may be unimportant for a partner but could affect the whole network or partners’ operations;
- the identification and implementation of mutual means for risk reduction help to find out the best managerial actions. In addition, those actions could be too expensive to be implemented by a single partner but cheap if implemented by a network of partners;
- the mutual means for risk reduction may help companies to identify congruent and shared strategies. A good example is when a risk is transferred from a company to another. The total risk decreases if the company taking the risk can cope with it better than the company transferring it (e.g. a special-purpose investment for a company could be a common-investment for one of its suppliers, since it is able to
6. Conclusions and managerial implications
Risk management does not imply the formulation of business decisions; risk management can provide a particular perspective and support to a decision-maker. Moreover, it is important to understand that risk management does not guarantee protection from all kinds of risks. This is due to the fact that risk assessment is limited by the resources available, including information at hand, involvement of stakeholders, time and budget. From the evidences emerged, some interesting and challenging issues of research could be delineated. We agree with Hallikas et al. (2004) that an effective collaborative process is possible only if every company has its own risk management process. On the one hand this gives to the companies a starting-point to analyze together different scenarios, on the other hand it generates immediately a contradiction: the need to define a common risk management process which could be different from the individual risk management processes. This is due to the fact that the objectives of the collaborative process, the risks identification criteria and the actions for risks reduction, for example, are completely different. Since the overall objective is the maximization of the performances of the supply chain, the individual risk management processes seem to be just a preliminary condition to define a unique risk management process for the whole network. Consequently, this generates several practical problems: how can a collaborative risk management process be implemented? which companies are responsible for the definition, the implementation and the management of the process? which are the partners?

Another critical component of the overall business risk assessment is the IT risk assessment, which is the risk associated with the deployment and management of the various hardware, software and network technologies employed. Each technology element has associated risks that need to be identified and evaluated for significance. As a result, in our agenda of research, future studies will include some of those topics, as the definition of a systematic model to understand the relationship between individual risk management processes and the collaborative risk management process, and a reference model to understand how to implement a risk management process on the whole supply chain.

7. References


