Supply Chain Risks Management (SCRM). Case study: Steel Industry - OTELINOX

Daria VISSARION
Virgil POPA
"Valahia” University of Targoviste
virgilp51@yahoo.com

Abstract

Supply Chain Management includes planning and management of all activities involved in sourcing and procurement, conversion, and of all logistics management activities.

The extent that there is significant uncertainty about potential outcomes and / or disappointing of decisions to be taken.

A fundamental precondition for improving the resilience of supply chain is understanding the network that connects business with its suppliers and suppliers with customers from upstream.

Business continuity management (BCM) can be defined, according to Morris, as: "A holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities."

OTELINOX was established on June 01 1974, following an international auction won by Japanese companies NISSHIN STEEL CO Ltd. For manufacturing of cold rolled stainless steel strips and sheets and DAIIDO STEEL Co for manufacturing of hot rolled small profiles and wire rod.

The company has developed a risk management system which is still not based on ISO 31000, but it is a good start in terms of internal good practices, taking into consideration all the risk sources, for example an action plan, reaction plan and the analysis of the Failure Mode and Effects Analysis.

Keywords: Supply Chain Management, Supply Chain Risk Management (SCRM), risk management, vulnerability, response to risk, Supply Chain Security Management (SCSM), security management systems, ISO 28000, Business Continuity Management (BCM).

1.1. Supply Chain Management

The fierce competition in the global business environment and the increased demand led to the development and continuous evolution of a number of complex subjects, including Supply Chain Management (SCM). SCM can be defined as a perfect combination between design and management, value added to the process, beyond the organizational boundaries to meet the real needs of the end customer. Generally, SCM involves networking and managing of inputs and outputs of goods, services and information between producers, manufacturers and customers. A supply chain includes all activities and facilities in the operation flow, and transformation of goods and services from materials stage to the end user. It consists of a supply network, upstream, and downstream a channel. Nowadays, many organizations have become a part of at least one supply chain. A supply chain commonly includes supply, manufacturers, distributors, retailers and customers.
Supply Chain Management includes strategies and activities associated with the supply chain. Supply Chain Management includes planning and management of all activities involved in sourcing and procurement, conversion, and of all logistics management activities. Importantly, it also includes management coordination and collaboration with channel partners, which can be suppliers, intermediaries, service providers and customers. In essence, supply chain management integrates supply and demand management within and between enterprises. Supply Chain Management is an integrating function with primary responsibility for linking major business functions and processes within and across companies into a unified and efficient business model. Includes all logistics management activities noted above, as well as manufacturing operations and coordination of processes and activities with and across marketing, sales, product design, and finance and information technology.

It is now increasingly accepted that “one size does not fit all” when it comes to designing supply chain strategies to support a wide range of products with different characteristics. Supply chain strategy differs from traditionally accepted company strategies, in that it requires the coordination and commitment of many different firms to implement company strategic objectives.

There are three basic principles in developing supply strategy that will suit customer requirements. These include: understanding customers and uncertainty; understanding of supply chain capacity; as well as evaluating and selecting design options. Fisher (1997) developed a framework to help managers understand the nature of the product and the concept of each supply chain to meet demand. Each category of this framework requires distinct supply chains types leading to the main cause of that chain. Strategies discussed include: efficient supply chain, chain protection against risks, supply responsive and agile supply chains, the chain efficiency is high.

2. Supply Chain Risks Management

Sitkin and Pablo (1992) provides a general definition of risk “the extent that there is significant uncertainty about potential outcomes and / or disappointing of decisions to be taken. Zsidisin (2003) addresses in detail the context of supply chain and defines the risk as “a possible occurrence of an incident or failure to use the opportunities of supply where the results are to economic losses for the acquiring company”.

Risk management in supply chain

Perhaps there is still no common definition of risk management in the supply chain (SCRM), but there is an understanding of the main components of SCRM, although they may be approached differently. After a thorough research showed that many definitions include the following groups of activities, according to Teresa Wu and Jennifer Blackhurst:

- **Risk identification and modeling** - includes the sources and characteristics of risks, which can be triggered by the relationship with the performance of the supply chain in terms of efficiency and effectiveness;
- **Risk analysis, evaluation and impact measurement** - assessment of the likelihood of occurrence of the possible consequences;
- **Risk management** - generating and considering alternative scenarios and solutions, judging their quality, selecting solutions and initiating implementation;
- **Risk monitoring and evaluation** - monitoring, control and management solutions and evaluating their impact on business performance;
- **Personal and organizational learning including knowledge transfer** - trying to capture, to extract, to distill and disseminate lessons and experiences of others in the organization and associate members of the supply chain.

Current trends in business that increase vulnerability to the risks of the supply chain are (according to Christopher
and Lee, 2004; Harland et al., 2003; Norman and Jansson, 2004; Cucchiella and Gastaldi, 2006):

- The increased use of outsourcing production and R & D by suppliers;
- Globalization of supply chain;
- More interconnected and integrated processes between companies;
- Requirements for lower delivery times;
- Shorter life cycles of products and marketing for film;
- Highly complex products/services;
- Limiting the capacity of key components.

Figure 1: Risk Management in Supply Chain Framework – Overview

2.1. Vulnerability in Supply Chain

The vulnerability of a supply chain is determined largely by the complexity of the network. Lately complexity has often increased because of the company focus on core competencies and increased reliance on outsourcing. Risk management in supply chain cannot be equated with response to disasters. Rather, it means maintaining a complex process moving efficiently with a lower total cost without compromising product quality or customer satisfaction. Risk management in supply chain is defined as “the process of risk mitigation achieved through collaboration, coordination and implementation of risk management tools among partners to ensure continuity and long-term profit of supply chain”.

Bjorn Egil and Marvin Rausand (1997) define the concept of vulnerability as applied to production systems: “A strong and resilient system is able to support without disruption or absorb a catastrophic failure and persist”. Powerful means being able to withstand an unforeseen event and return to the initial state.

A resilient company is better able to cope with the unpredictable world trade, gaining a competitive advantage, and to recover more quickly than its competitors in the event of a disaster.
According to Yossi Sheffi conception when supply chain suffering an accident, companies may - or may not - be able to return to the initial situation. Company’s survival depends only on the resilience of the company regarding this event.

2.2. Risk sources

Specialists have identified “sources” of risk as they saw and understood them, not by specific network location, or a risk of fire, flood, protests or terrorism as:

- Decisions based on cost;
- Requirements / performance;
- Delivery schedule adherence;
- Customer - supplier.

Figure 3 shows how the three relate, overlap and combine:

- Supply chain planning. Extreme left of the spectrum is occupied by supply chain planning, which, in a “perfect world” would be unloaded with legacy commitments or contracts existing plants suppliers;

- Supply chain operations management. On the right side are the operations management activities of the supply chain. This portion represents the daily activities undertaken by the management of a supply chain. It is the stage where volumes have evolved from development prototypes, by changing the full-scale production where demand

Source: Sheffi, 2005

Source: Haywood, 2002
patterns are meant to follow a predictable pattern. Properly managed supply chain is allegedly operating in a “steady state” in which supply and demand are perfectly balanced. In this state, the processes are not affected by sources of risk from the planned process changes or new product introductions;
– Change management in the supply chain. Center of the spectrum is occupied by activities of supply chain change management. Represents the times when planned changes to existing processes of the supply chain are implemented.

2.3. Response to risk solutions

"World Economic Forum" Concerns on the resilience and dynamism

Resilience is crucial because, in a hyperconnected and interdependent world, no one country or organization can manage global challenges on its own. To be resilient is to be able to adapt to changing political and economic contexts and pursue critical goals while also being able to withstand and recover from sudden shocks. Today's biggest challenges, meanwhile, also demand dynamism -- overcoming the ongoing global economic malaise, for example, requires the capacity for bold vision and even bolder action.

The Global Risks 2013 report is based on an in-depth survey of more than 1,000 experts across the world. It measures their perceptions of the potential impact of 50 global risks over the next ten years and, most important, how interconnected those risks are.

Those surveyed selected "severe income disparity" followed by "chronic fiscal imbalances" as the two most prevalent global risks. These results reflect ongoing concerns about high levels of government debt and a somewhat pessimistic overall economic outlook. After a year scarred by extreme weather, experts rated "rising greenhouse gas emissions" third.

2.4. Risk categories

Based on an original framework proposed by Mason-Jones & Towill (1998), we suggest that there are five categories of risk that can be subsequently devised in three categories:
– Inside the enterprise there are a "process" and a "control" risk;
– Outside the enterprise but inside the supply chain there can be identified a network risk, divided in "demand" and "supply".
– Outside the network, there is an "environmental" risk.

Environmental – These events could have a direct impact on the main company or on the ones from upstream or downstream, or even on the market itself. Could affect the value of a particular course (e.g.: product contamination) or
any node or link in the supply chain (e.g.: as a result of an accident, a direct action, extreme weather or natural disasters). May be the result of socio-cultural events, economic or technological or organizations removed from their own supply chain of the main company, but their effects can extend to links to other industrial networks. The type of timing of these events may be predictable (e.g. those arising from regulatory changes), but not many, although the impact of these types of events could still be assessed. (Appendix 1: Risk Categories)

3. Supply Chain reengineering

Conventional supply chains were often designed to optimize costs and/or for customer service, rarely the resilience was an “objective function” for the optimization process.

Given the risks faced by modern supply chains, this should change. Several recommendations are offered to provide the basis for designing risk mitigation supply chain.

i) Understanding supply chain

A fundamental precondition for improving the resilience of supply chain is understanding the network that connects business with its suppliers and suppliers with customers from upstream. Mapping tools can help identify “key points” and “critical paths”.

The key points are often characterized as bottlenecks where there is a capacity limit, and where alternatives may not be available e.g. ports capable of maintaining ships - large containers or central distribution plant if it becomes inoperable would put strong pressure on the rest of the system.

ii) Supplier based strategy

While there has been a tendency to reduce the supplier base in many companies, it may be limits to the process should be pursued. Sole supply, where one supplier is responsible for the supply of a particular item or service may have cost advantage and quality management perspective, but it is dangerous in terms of resilience.

iii) Design principles for supply chain resilience

A number of emerging principles should be taken into account in reengineering supply chain to improve resilience: the choice of supply chain strategy that keeps a few options open; and review of the exchange “efficiency vs. redundancy”. Supply chain resilient practices vs. attributes

The main activities to be undertaken to obtain a supply chain resilient are:

- The “inventory level” is affected positively by the strategic stock policies (the constitution of strategic inventory buffers in supply chain increases the inventory levels).
- The “information frequency” is improved by the increasing in the demand visibility.
- The “integration level” is positively related to the risk sharing strategies in the resilient supply chains. A higher level of responsiveness increases the “replenishment frequency”;
- The resilience practices prescribe the existence of supply chain capacity buffers provoking an increasing in “capacity surplus”.

4. Supply Chain Security Management

Supply Chain Security Management (SCSM) is a relatively new discipline in the field of Operations Management Research, thus lacking introductory and tutorial papers. The recent concerns on security in global supply chains are driving the introduction of new security initiatives, standards and measures to such an extent that they are becoming an integral part of supply chain management.

Security, its demands and constraints, constitute obstacles (logical and physical barriers) in the flow of supply and distribution. These “barriers” created by a perceived increased need for security, or political reasons, reduce the reaction capacity and the physical and economical performance of the company. Integrating the security dimension into the logistics strategy, organization and
operations has become a new challenge for supply chain management.

The recent security concerns have led to the development of multiple initiatives and potential solutions to enhance security in international supply chains without affecting efficiency. Businesses, governments and researchers are tackling the problem from different perspectives and by using several methodologies. However, inherent complexities such as the large quantity and diversity of the actors involved in international supply chain processes, and the need to identify cost-effective security measures, have generated multiple academic research questions in the domain of SCSM.

The first pure SCSM paper was published at MIT (Sheffi, 2001), a few months after the infamous terrorist attacks in September 2001. Since then, researchers and industrial practitioners have organized and published SCSM conference and journal papers, primarily in the US but also in Europe and other continents.

The existing literature on SCSM, is somehow adding a layer of security to each researcher’s own expertise domain. Some of the discussed principles are presented in the following paragraphs.

4.1. Global and governmental concerns for risk management and supply chain security

Through the National Strategy for Global Supply Chain Security (the Strategy), we articulate the United States Government’s policy to strengthen the global supply chain in order to protect the welfare and interests of the American people and secure our Nation’s economic prosperity. Our focus in this Strategy is the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructures by which goods are moved from the point of manufacture until they reach an end consumer, as well as supporting communications infrastructure and systems. The Strategy includes two goals:

**Goal 1: Promote the Efficient and Secure Movement of Goods** – The first goal of the Strategy is to promote the timely, efficient flow of legitimate commerce while protecting and securing the supply chain from exploitation, and reducing its vulnerability to disruption.

**Goal 2: Foster a Resilient Supply Chain** – The second goal of the Strategy is to foster a global supply chain system that is prepared for, and can withstand, evolving threats and hazards and can recover rapidly from disruptions. To achieve this we will prioritize efforts to mitigate systemic vulnerabilities and refine plans to reconstitute the flow of commerce after disruptions.

**Manage Supply Chain Risks**

The global supply chain is subject to an ever-evolving array of risks. Our competitiveness as a Nation depends on managing risks to supply chain-related physical infrastructures to enable the movement of goods, energy, people, and information from one place to another. To manage risks, we will work to:

- **Understand and address vulnerabilities** to the supply chain that stem from both exploitation of the system by those seeking to introduce harmful products or materials and disruptions from intentional attacks, accidents, or natural disasters. We will focus our efforts on those risks that can bring the most harm to American citizens or threaten the functionality of the supply chain system.
- **Utilize layers of defense** to protect against a diverse range of traditional and asymmetric threats. These layers include: intelligence and information analysis; appropriate use of technology; our laws, regulations, and policies; properly trained and equipped personnel; and effective partnerships.
- **Adapt our security posture** to meet evolving threats. We will work to promote a dynamic and flexible risk management approach that prioritizes actions to address risks with the greatest potential impact. We must also establish an environment in which we assess...
emerging threats and reprioritize our actions accordingly.


The main external risk factors of the supply chain are: natural disasters, political conflict situations, sudden demand shocks, restrictions on import/export, terrorism.

Systemic risks within supply chain and transport networks are characterized by an unexpected trigger event and a network setup that cannot absorb the shock and knock-on effects. The initial event results in a cascading disruption or failure across regions or industries.

However, prediction of specific disruptions is felt to be less important than having the resiliency in place for effective response, no matter what the cause. While highlighting industry robustness in the face of recent shocks, experts identified the vulnerabilities of most concern that limit the resilience of supply chain and transport networks.

Implementing Improved Systemic Risk Management

The expert group assessed the difference between the risk management methods available today and those most important in the future to identify risk management methods most in need of development.

4.3. Security management systems for the supply chain

This Publicly Available Specification specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. Security management is linked to many other aspects of business management. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

Management review and continual improvement

Top management shall review the organization's security management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. Reviews shall include assessing opportunities for improvement and the need for changes to the security management system, including the security policy and security objectives and threats and risks.

Figure 5: Elements of the security management system

Records of the management reviews shall be retained. Input to management reviews shall include: results of audits and evaluations of compliance with legal requirements and with other requirements to; which the organization subscribes; communication(s) from external interested parties, including complaints; the security performance of the organization; the extent to which objectives and targets have been met; status of corrective and preventive actions; follow-up actions from previous management reviews; changing circumstances, including developments in legal and other requirements related to its security aspects, and; recommendations for improvement.

5. Business Continuity Management

Business Continuity Management Strategy

This Business Continuity Strategy provides the framework within which Thanet District Council can comply with best practice guidelines, produced by the British Standards Institute (BS 25999), and which is consistent with corporate governance best practice. Business continuity plans will ensure that the organization can continue to deliver a minimum level of service in its critical functions in the event of any disruption.

The Strategy requires senior managers to demonstrate that they have considered the need for business continuity planning to cover each functional process within their area of responsibility. The focal point for the production, coordination, validation and review of the council’s business continuity activity strategy will be the Corporate Governance and Risk Officer.

Corporate business continuity is closely linked to corporate risk management and this strategy should be read in conjunction with the council’s Risk Management Strategy. The basic principles of the Business Continuity Strategy have been accepted by the Corporate Management Team, Governance and Audit Committee and Cabinet.

This Strategy applies to all parts of the council as all areas play a key role in maintaining service delivery. The requirement to plan applies to activities identified as critical through the council’s business continuity methodology and agreed by the Corporate Management Team, Governance and Audit Committee and Cabinet.

Business continuity management (BCM) can be defined, according to Morris, as: “A holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.”

The aim being that at all times key elements of service are maintained at an emergency level and brought back up to an acceptable level as soon as possible.

Delivering the Strategy – Methodology

The process being used within the council is based on the BCM model outlined in BS 25999 Business continuity management – Part 1: Code of Practice published by the British Standards Institute – see below.
This process involves the following activities:

**a. BCM programme management:**
- assigning responsibilities for implementing and maintaining the BCM programme within the council
- implementing business continuity in the council – including the design, build and implementation of the programme
- the ongoing management of business continuity – including regular review and updates of business continuity arrangements and plans.

**b. Understanding the organisation**

The use of business impact and risk assessments (see below) to identify critical deliverables, evaluate priorities and assess risks to service delivery.

- Business Impact Analysis (BIA) – identifying the critical processes and functions and assessing the impacts on the council if these were disrupted or lost. BIA is the crucial first stage in implementing BCM, and helps measure the impact disruptions on the organisation
- Risk assessment – once those critical processes and functions have been identified, a risk assessment can be conducted to identify the potential threats to these processes.

**c. Determining BCM Strategy**

The identification of alternative strategies to mitigate loss, and assessment of their potential effectiveness in maintaining the council’s ability to deliver critical service functions.

**d. Developing and implementing a BCM Response**

This Business Continuity Plan ensures that actions are considered for:
- the immediate response to the incident
- interim solutions or maintaining an emergency level of service, leading on to
- reinstating full services.

**e. Exercising, maintaining and reviewing**

Ensuring that the business continuity plan is fit for purpose, kept up to date and quality assured. An exercise programme will enable the council to:
- demonstrate the extent to which strategies and plans are complete, current and accurate and
- identify opportunities for involvement.

**f. Embedding BCM in the council’s culture**
The embedding of a continuity culture by raising awareness throughout the council and offering training to key staff on BCM issues.

Ensuring that the plan reflects ongoing changes within the business is crucial. This task includes updating the plan and revising this document to reflect updates; testing the updated plan; and training personnel. The Corporate Governance and Risk Officer is responsible for this comprehensive maintenance task.

6. Good practices and International standards
6.1. BSI – Standard 100-4 Business Continuity Management

Business Continuity Management is a discipline that prepares an organization for the unexpected. It is a management process that provides the framework for building resilience to business and service interruption risks, responding in a timely and effective manner to ensure continuity of critical business activities, and ensuring the long term viability of the organization following a disruptive event.

The purpose of business continuity management is to ensure that critical business processes are interrupted only temporarily, even in critical situations, and the organization will exist after the appearance of serious damage.

Ruptures of business processes can have different causes, namely, effects. To illustrate the events described in the Business Continuity Management framework we provide a brief explanation of the terms: “emergency”, “crisis” and “disaster” as they were understood and used in this standard.

“Emergency” is an event in which an organization’s processes and resources do not work properly. These processes and resource availability cannot be restored in the time established by the framework.

“Crisis” is understood as a situation deviated from the normal state, which can occur at any time, regardless of protective measures implemented in the company or government organization in question and cannot be solved by normal operational and organizational structures. Emergency situations that may affect the continuity of business processes can develop and turn into crises.

Figure 7: Business Continuity Management process

<table>
<thead>
<tr>
<th>Initiation of business continuity management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contingency planning</td>
</tr>
<tr>
<td>Implementing the concept of contingency planning</td>
</tr>
<tr>
<td>Business continuity response</td>
</tr>
<tr>
<td>Tests and exercises</td>
</tr>
<tr>
<td>Maintenance and continuous improvement of business continuity management process</td>
</tr>
</tbody>
</table>

Source: Western Australian Government, 2009
management, contingency planning, implementing the concept of contingency planning, business continuity response, tests and exercises, as well as maintenance and continuous improvement of business continuity management.

The relationship between risk management and business continuity management

Figure 8: Risk Management and Business Continuity Management interface

Risk Management represents the practice of systematically identifying, understanding, and managing the risks encountered by an organization.

6.2. ISO 22313

This International Standard for business continuity provides guidance based on best international practice for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a documented management system that enables organizations to prepare for, respond to and recover from disruption.

It is not the intent of this International Standard to imply uniformity in the structure of a BCMS but for an organization to design a BCMS that is appropriate to its needs and that meets the requirements of its interested parties.

Business continuity management system (BCMS) is that part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

7. CASE STUDY S.C. OTELINOX S.A.

OTELINOX was established on June 01 1974, following an international auction won by Japanese companies NISSHIN STEEL CO Ltd. For manufacturing of cold rolled stainless steel strips and sheets and DAIDO STEEL Co for manufacturing of hot rolled small profiles and wire rod.

The company has developed a risk management system which is still not based on ISO 31000, but it is a good start in terms of internal good practices, taking into consideration all the risk sources, for example an action plan, reaction plan
and the analysis of the Failure Mode and Effects Analysis.

The action plan (Appendix 2) was developed to minimize the effects in case of emergency situations, like:
1. Destructive geological phenomena (earthquakes, landslides)
2. Extreme weather events (storms, torrential rains, floods, etc.)
3. Exceptional circumstances (war, embargo, revolution)
4. Situations considered as force majeure (strikes, violent conflicts, etc.)
5. Fires
6. Accidental pollution
7. Health Risks and Safety
8. Key Equipment Failure
9. Utilities disruptions
10. Labor issues. Lack of qualified staff
11. Disruptions in the supply of raw materials. Lack of capacity at suppliers
12. Lack of transportation. For a detailed description of the emergency plan, prevention actions and those responsible for them.

There is a reaction plan (Appendix 3) in which there are comprised potential and real situations that can arise to nonconformities in which these ones are enumerated and the actions that must be taken afterward, respectively the responsible persons for these. The potential situations that can arise in nonconformities:
1. Raw material defects
   Failure to comply with the quality requirements of raw materials identified in various stages of processing in the production flow with repercussions concerning fulfilling in time the orders.
2. Technological defects
   Technological defects may arise in any of the technological flows resulting from the three basic technological flows.
3. Electrical or mechanical malfunctions
   Malfunctions of production lines, of monitoring and measuring equipments
4. Failure to satisfy capability conditions, variations in product characteristics
   The analyzed distribution characteristics do not meet customer requirements/ standard values.

But the most important aspect of the risk management is the use of the specific quality tool: Failure Mode and Effects Analysis. The company has set up a Failure Mode and Effects Analysis process in order to eliminate or at least reducing the occurrence of potential failures in order to control the sources of risk and to meet customer requirements.

This process is carried out for the entire automotive production flow according to the reference manual published by AIAG FMEA (Automotive Industry Action Group).

The attached procedure and the conduct of business analysis include all steps of manufacturing process to finished goods storage warehouse. At each step of the process are identified potential and actual failures, the estimated impact of the worst possible effect that failure can have on the client and identify the causes and measures that can be taken.

Each such document receives an identification number and date of issue, very important for each review is the reference number and original date remains the issue one, along with those of subsequent revisions.

It starts with establishing a core team, which is added gradually specialists in the areas involved, setting rules, team leader and others responsible. The first meeting of the implementation of the analysis starts at the ground line for the observation of the trial, to form a common vision.

Within the company are developed system applied FMEAs. FMEA is an early step, but necessary and important in identifying risk.

Definitions:

FMEA is a tool to identify and evaluate: potential failures of process and product, failure effects and actions could eliminate or decrease the potential failures apparition.

Process steps. The main steps through the raw material passes in order to be obtained the final product (E.g.: rolling mill, heat treatment, tension levelling, slitting, packing).
Potential failure effect. It is the impact of non-compliance with customer demand.

Severity. The impact assessment of potential failure effect on customer, by giving marks from 1 to 10.

Function. It represents the role (purpose) has to be accomplished by an operation.

Potential failure mode. It represents the non accomplishment of function (nonconformity).

Special characteristic. It is any characteristic what if is not followed, gives serious prejudices for product utilisation or end user. This can be critical or significant according Severity rating (critical characteristic: 9 and 10 points, significant characteristic: 8 points).

Apparition. The frequency assessment which can appear nonconformity (potential failure mode) because of specific cause, by giving marks from 1 to 10.

Detection. The efficacy assessment of detection methods, by giving marks from 1 to 10.

Risk priority number. It is the result of multiplication of severity, apparition and detection marks.

RPN threshold of the customer. Maximum limit, required by customer, for establishing of improvement actions.

Responsibilities and description of activities required for the analysis and evaluation of failure modes and their effects are described in the following flow chart:

Starting from the Customer Support process is established the necessity to elaborate the FMEA for each new product, before its launching in manufacturing.

Establishing the Project Development Process Chief – Depending on the department were the FMEA will be applied is established the person with the necessary authority.

Setting up the team – The team is set up along with everyone’s responsibilities.

Initiating the FMEA opening meeting – The team is convened.

Establishing the scope of FMEA. Defining the limits of the process for which is realized the FMEA. The work rules are established.

Identifying all requests of the customer – The “requests” column is filled out by identifying the expressed or not expressed requests, for external customers and also for the internal ones.

Process development – Identifying the main phases of the correlation process with the identified requests.

Setting operations – Each phase of the process is decomposed in operations.

Verifying the correlation between operation and requests – Is verified the existence of at least one request for each operation. In case it has not been identified any request for an operation, it is added the corresponding request or the operation is excluded.

Identifying the effects – These result following the failure to meet the request (“not ok request”).

Severity – It sets the marking grid applying to all stages of the process analyzed in the FMEA system.

Functions – The functions for each operation are established, using the question “What role does he have?” For an operation there can be identified more functions. In this phases are ignored the requests and the effect.

The potential failure mode - Resulting from failure to meet the function (“function not ok”).

Special features (of product or process) – They can be identified by the client, by the manufacturer, even if they are not submitted to the customer.

Potential failure causes – The ones that generate the potential failure mode. It can be identified one or more causes for one failure mode, using the question: “Why the failure mode occurs?” If they are not easy to identify, there will be used specific tools.

Methods of prevention – There are identified documents which set out the right way to prevent the failure mode. It is used the question: “Why does that failure
mode appears from a certain failure cause?" (E.g.: technological instructions/ work, documentation).

**Apparition** - It sets the marking grid for each stage of the analyzed process.

**Detection methods** – There are identified ways through which it can be identified the failure mode occurred from a certain cause, using the question: "Why does the failure mode appears from a certain cause? (E.g.: control instructions, checklist, alarms, etc.).

**Detection** - It is set the marking grid for each stage of the analyzed process.

**Risk priority number (RPN)** – The product of the three awarded grades. (Severity x Apparition x Detection).

Its value is very important for establishing the Improvement Actions that are going to be taken, respecting the following rule: Are selected the effects with the severity scoring ≥7. For the first third of the biggest value of RPN are established improvement actions, mentioning in the FMEA table what is being followed: to reduce the Apparition and Detection.

Severity can be reduced only through modification of the process or in technology, implying bigger costs, so **Severity will never be proposed to be reduced, only if there are involved investments regarding the improvement of the technological processes or other similar situations**.

After implementation of the improvement actions is verified their efficiency (being treated as corrective actions) and the scores and RPN are evaluated again.

It resumes setting new actions for improvement from selection effects with notes on severity ≥7. If no further action can be set to improve, by this criterion, proceed to establish actions to effects that have the highest marks to appear.

But if the customer calls for a setting of improvement actions should be respected the RPN limit for customer request. For example may require improvement actions for all cases when RPN ≥ 200, even though the value is not found in the first third selected according to the rules manual FMEA / AIAG we are required to respect the customer’s requirement.

**Improvement actions** – For Severity ≥7 it ranks low for RPN values and determine actions needed only for the first third of them. The followings will be decided: - responsible persons, - deadlines, grades which we propose for Apparition and/ or Detection. If the client asks for a RPN threshold, his request will be respected.

**Efficiency assessment of improvement actions** – Apparition and/ or Detection are graded again using the corresponding tables, setting the new RPN. Is aimed the implementation of proposed actions and their efficiency.

**Design-Development.**

- Taking into consideration the confidentiality regulations, FMEA is not submitted to the client. He can only consult it during visits, audits, etc.

For the **Sustainable actions** upstream and downstream can be mentioned:

**Upstream:**
- Actions regarding elimination of risk generated actions by the raw materials suppliers: list of accepted suppliers (suppliers are being periodically assessed and even if the supply is not made from all of them, the capable ones are identified to deliver in the requested quality conditions normally used by Otelinox).

**Downstream:**
- Beside the situations mentioned in the Emergency Plan we may add: transporters’ strike, to which the product delivery of Otelinox is dependent on. For this situation has been developed a plan that insures in time delivery using railway transportation.

**8. Conclusions**

Even though the organization has already developed tools such as: Reaction Plan and Plan for Response to emergency situations, as an improvement opportunity
it is recommended drafting an integrated Plan on business continuity starting with the Balanced Score Card and the response to major risks plans which offer a systemic vision.

The existence of an infrastructure of the more advanced technological level, which ensures reduction level risk factors on product realization.

High qualification of the personnel and special attention for the continuous training of the personnel in order to ensure an immediate reaction in any situation that can generate risk or over the organization’s processes or product, from materials reception to final product delivery.

Suggestions
The establishment of a department or office in an existing department, to handle security risk management and business.

Creation of a post of Risk Officer.

The above mentioned department to integrate the problem of strategic management (planning, monitoring and performance control) with the problem of risk and security management in the Business Continuity Management.

Inclusion in the annual training specific courses related to risk management based on standards: ISO 31000 (Risk Management – Principles and guidelines), ISO 28000 (Management systems for supply chain security) and ISO 22313 (Business Continuity Management Standard).

Based on the Pareto principle (also known as 20/80 principle) to develop discussions with main suppliers and customers (Integrated in the Supply Chain).

Also, another improvement suggestion is to identify investments in growth initiatives that can help strengthen business sustainability; they can contribute to identifying the key characteristics and designing manufacturing technologies corresponding steel strips used in new applications.

References
Carvalho, H., Cruz-Machado, V., (2011), Integrating Lean, Agile, Resilience and Green Paragigms in Supply Chain Management (LARG_SCM), Portugal.
Popa V., (2009), Managementul lanțului de distribuție / aprovizionare pentru un răspuns eficient consumatorului, Valahia University Press, Târgoviște.


### Appendix 1

#### Risk categories

<table>
<thead>
<tr>
<th>External risks to which it is subjected supply chain</th>
<th>Natural disasters</th>
<th>Accidents</th>
<th>Sabotage, Terrorism, Crime, War</th>
<th>Compliance with laws imposed by the government and political uncertainty</th>
<th>Unavailability of labor and lack of specialization</th>
<th>Constraints across industries (the relevant market)</th>
<th>Suppliers risks: external, contracts with producers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Natural disasters</td>
<td>Accidents</td>
<td>Sabotage, Terrorism, Crime, War</td>
<td>Compliance with laws imposed by the government and political uncertainty</td>
<td>Unavailability of labor and lack of specialization</td>
<td>Constraints across industries (the relevant market)</td>
<td>Suppliers risks: external, contracts with producers</td>
</tr>
<tr>
<td></td>
<td>Natural disasters</td>
<td>Accidents</td>
<td>Sabotage, Terrorism, Crime, War</td>
<td>Compliance with laws imposed by the government and political uncertainty</td>
<td>Unavailability of labor and lack of specialization</td>
<td>Constraints across industries (the relevant market)</td>
<td>Suppliers risks: external, contracts with producers</td>
</tr>
<tr>
<td></td>
<td>Natural disasters</td>
<td>Accidents</td>
<td>Sabotage, Terrorism, Crime, War</td>
<td>Compliance with laws imposed by the government and political uncertainty</td>
<td>Unavailability of labor and lack of specialization</td>
<td>Constraints across industries (the relevant market)</td>
<td>Suppliers risks: external, contracts with producers</td>
</tr>
<tr>
<td></td>
<td>Natural disasters</td>
<td>Accidents</td>
<td>Sabotage, Terrorism, Crime, War</td>
<td>Compliance with laws imposed by the government and political uncertainty</td>
<td>Unavailability of labor and lack of specialization</td>
<td>Constraints across industries (the relevant market)</td>
<td>Suppliers risks: external, contracts with producers</td>
</tr>
<tr>
<td></td>
<td>Natural disasters</td>
<td>Accidents</td>
<td>Sabotage, Terrorism, Crime, War</td>
<td>Compliance with laws imposed by the government and political uncertainty</td>
<td>Unavailability of labor and lack of specialization</td>
<td>Constraints across industries (the relevant market)</td>
<td>Suppliers risks: external, contracts with producers</td>
</tr>
<tr>
<td></td>
<td>Natural disasters</td>
<td>Accidents</td>
<td>Sabotage, Terrorism, Crime, War</td>
<td>Compliance with laws imposed by the government and political uncertainty</td>
<td>Unavailability of labor and lack of specialization</td>
<td>Constraints across industries (the relevant market)</td>
<td>Suppliers risks: external, contracts with producers</td>
</tr>
<tr>
<td></td>
<td>Natural disasters</td>
<td>Accidents</td>
<td>Sabotage, Terrorism, Crime, War</td>
<td>Compliance with laws imposed by the government and political uncertainty</td>
<td>Unavailability of labor and lack of specialization</td>
<td>Constraints across industries (the relevant market)</td>
<td>Suppliers risks: external, contracts with producers</td>
</tr>
<tr>
<td></td>
<td>Natural disasters</td>
<td>Accidents</td>
<td>Sabotage, Terrorism, Crime, War</td>
<td>Compliance with laws imposed by the government and political uncertainty</td>
<td>Unavailability of labor and lack of specialization</td>
<td>Constraints across industries (the relevant market)</td>
<td>Suppliers risks: external, contracts with producers</td>
</tr>
<tr>
<td></td>
<td>Natural disasters</td>
<td>Accidents</td>
<td>Sabotage, Terrorism, Crime, War</td>
<td>Compliance with laws imposed by the government and political uncertainty</td>
<td>Unavailability of labor and lack of specialization</td>
<td>Constraints across industries (the relevant market)</td>
<td>Suppliers risks: external, contracts with producers</td>
</tr>
</tbody>
</table>

#### Natural disasters
- Plagues
- Earthquakes
- Natural calamities
- Floods

#### Accidents
- Fires
- Explosions
- Crashes
- Discharge of hazardous substances

#### Sabotage, Terrorism, Crime, War
- Cyber attacks
- Products counterfeit
- Intellectual theft
- Physical theft

#### Compliance with laws imposed by the government and political uncertainty
- Fees, taxes and regulations
- Violation of the rules
- Logistics

#### Unavailability of labor and lack of specialization
- Quality
- Cost

#### Constraints across industries (the relevant market)
- Fluctuating prices
- Barriers to market penetration
- Brevets
- Supplier's profit margin too low
- Prices trends
- Recession / Inflation

#### Suppliers risks: external, contracts with producers

<table>
<thead>
<tr>
<th>Physical and regulatory risks</th>
<th>Production problems</th>
<th>Low quality</th>
<th>Financial losses and bonuses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main suppliers are in areas of high risk</td>
<td>Capacitate</td>
<td>Defects / contamination of manufactured products</td>
<td>The degree of competition /</td>
</tr>
<tr>
<td>Unavailability of materials / Planning faulty</td>
<td>Out of stock</td>
<td>Mergers &amp; Acquisitions</td>
<td></td>
</tr>
</tbody>
</table>

#### Production problems
- Capacitate
- Out of stock
- Repair cycle time required

#### Low quality
- Defects / contamination of manufactured products
- Mislabeling of products
- Lack of knowledge and specialized training

#### Financial losses and bonuses
- The degree of competition /
<table>
<thead>
<tr>
<th>Management risks</th>
<th>Profitability</th>
<th>Supply risks: Disruptions: entry or exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor planning risk management</td>
<td>Lack of business continuity plans</td>
<td>Lack of business continuity plan from suppliers</td>
</tr>
<tr>
<td>Lack of request a business continuity plan from suppliers</td>
<td>Failure to achieve continuous improvement</td>
<td>Escalating costs</td>
</tr>
<tr>
<td></td>
<td>Escalating costs</td>
<td>Purchase price inflation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lack of infrastructure</th>
<th>Roads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Railways</td>
<td></td>
</tr>
<tr>
<td>Harbors</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assets - insufficient capacity or accidents</th>
<th>Trucks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wagons</td>
<td></td>
</tr>
<tr>
<td>Ships</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The cargo's damage / theft / tampering</th>
<th>Physical injury</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Inappropriate deposits</th>
<th>Uncertainty</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Long pipeline, several operators</th>
<th>Longer delivery time</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Operational risks</th>
<th>Inventory losses (damages, moral purpose)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of equipment, mechanical capacity</td>
<td>Out of stock</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Planning mistakes</th>
<th>Data accuracy</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Financial</th>
<th>Knowing the cost suppliers</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Lack of factories / low reliability / capacity</th>
<th>Mechanical failures</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unsatisfactory development of the company / lack of added value</th>
<th>Customer satisfaction / loyalty</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Use of SRM standards (Supplier Relationship Management)</th>
<th>Lack of communication / coordination of internal / external effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication with suppliers (EDI web, real-time application, plans, projections, developments in technology)</td>
<td></td>
</tr>
</tbody>
</table>

### Emergency Plan (Examples)

<table>
<thead>
<tr>
<th>No</th>
<th>Identified emergency situations</th>
<th>Preventive actions</th>
<th>Responsible Preventive actions</th>
<th>Emergency actions</th>
<th>Responsible Emergency actions</th>
</tr>
</thead>
</table>
| 1  | **Destructive phenomena of geological origin**  
   a). Earthquakes  
   b. Landslides  
   (Production of significant earthquakes are rare, and landslides probability is low.) | - Check the resistance of building structures on site  
   - Repair foundations or elements of masonry of buildings where necessary (with authorized companies);  
   - Proper storage of heavy objects;  
   - Repair of electrical installation and gas installation; | Administrative Team  
   Purchasing Dept.  
   Chiefs of workplaces  
   Chief of Maintenance (using authorized companies)  
   ES responsible/ Chiefs of workplaces | In case of force majeure:  
   - It is called the cell for Emergency situations, private service for the Emergency Situations, firemen team (if it imposes);  
   - ESI Dâmboviţa is informed tel. (0)112, about the situations created and about the need of support; | Duty Officer  
   President of Emergency Situation Cell  
   Chief of ES |
| 2  | **Extreme weather phenomena:**  
   a. Thunderstorms, heavy rain, tornadoes  
   b. Floods caused by extreme weather production (Events may cause damage to building roofs, rainwater pipes, clogged sewers, flooding of technological lines, basements of buildings or hydraulic cellars, electrical rooms, etc.) | - Personnel training in order to know the color codes for weather alerts and warnings and to take preventive measures;  
   - Preventive inspection of the condition of rainwater pipes and collection pipes;  
   - Check the condition of sewers and clean them  
   - Establish the areas / locations where the water infiltration may occur due to various cases, determine the drainage ways and set the "action plans in case of emergency";  
   - Provide sectors with submersible pumps and equipment for intervention (rubber boots, etc.) | SU responsible/ Chiefs of workplaces  
   Chief of Administrative Team/ Chiefs of workplaces  
   Chief of Energy team and utilities  
   Chiefs of plants / Chiefs of work places  
   Chiefs of work places | - Announce the chief of plant and the duty officer;  
   - Announce the management of the company;  
   - Personnel from the affected line in collaboration with the maintenance staff (under the command of the chief of the workplace) initiate measures to limit the consequences and to remove the event, according to the "Action plans in case of emergency";  
   - By case it is also requested the help of firemen team. | Chiefs of the workplaces (foremen / team chiefs)  
   Duty officer / Chief of plant  
   Chief of workplace  
   Chief of plant/ Chief of workplace |
| 3  | **Exceptional situations:**  
   a. War  
   b. Embargo  
   c. Revolution  
   (Probability of such events is very low.) | - Maintenance of the alarm sirens, of the ALD shelter in functioning state  
   - Ensuring safety lighting (in plants and buildings);  
   - Maintenance of telephone lines;  
   - Set working instructions in case of war;  
   - Train personnel regarding the usage of warning signals;  
   - Establishing evacuation assembly points and conducting evacuation exercises with the employees. | Chief of maintenance  
   Chief of Maintenance  
   Chief of Administrative General Director  
   ES Responsible/ Chiefs of workplaces | - Turn on the electric sirens (after receiving the notification and turn on agreement from local authorities );  
   - Taking the decision to evacuate the personnel on site;  
   - Telephone announcement about the evacuation of the employees at the site (following the decision of the General Director). | Duty officer / Chief of Administrative  
   General Director  
   HR Director/Chief of workplaces |
### Reaction Plan (Examples)

<table>
<thead>
<tr>
<th>Potential situations that may result to nonconformities</th>
<th>Emergency actions taken</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Raw material defects:</strong>&lt;br&gt;1.1. Failure to comply with the quality requirements of raw materials identified in various stages of processing in the production flow with repercussions concerning fulfilling in time the orders.</td>
<td>- It is blocked the nonconformity coil that presents defects from raw material;&lt;br&gt;- In case of blocking of at least 3 raw material coils in over 24 hours that comes from the same supplier and shows the same type of defect is prepared and sent an RNAC to the supplier;&lt;br&gt;- In the next 24 hours the stocks of raw materials from the supplier involved is analyzed by QC&amp;CS and Processes Programming &amp;Control teams and in consequential the coils that may have the same problem are blocked and isolated;&lt;br&gt;- Are requested informations from supplier about quality of raw material in stock;&lt;br&gt;- If the answer of the supplier imposes this, is requested the emergency replacement of raw materials affected.</td>
<td>QC inspector&lt;br&gt;QC engineer&lt;br&gt;Responsible for complaints of raw material&lt;br&gt;QC engineer &amp; Processes Programming &amp;Control&lt;br&gt;QC engineer responsible for complaints of raw material</td>
</tr>
<tr>
<td><strong>4. Failure to satisfy capability conditions, variations in product characteristics</strong>&lt;br&gt;4.1. Analyzed distribution characteristics does not meet customer requirements / standard values</td>
<td>- Products that do not meet customer requirements, or are not within the OTELINOX standard value are blocked;&lt;br&gt;- The nonconforming product are 100% inspected and it is decided the way it can be handled according to the “Nonconformities control” procedure, code ...;&lt;br&gt;- There are established corrective actions for all non-compliant products in order to eliminate the causes that generated nonconformities;&lt;br&gt;- All records of non-compliant products are kept within QC&amp;CS team;&lt;br&gt;- For all non-compliant products management staff of the department from where are generated is informed.</td>
<td>Operator&lt;br&gt;QC inspector&lt;br&gt;Plant chief&lt;br&gt;QC engineer</td>
</tr>
</tbody>
</table>