International Journal of Computer Science and Applications,
©Technomathematics Research Foundation
Vol. 10, No. 2, pp. 33 – 52, 2013

A MULTI AGENT FRAMEWORK FOR RISK MANAGEMENT IN CONTAINER TERMINAL: SUSPECT CONTAINERS TARGETING

MEHDI NAJIB

University of Le Havre, Cadi Ayyad University
Le Havre, France - Marrakesh, Morocco
mehdi.najib@univ-lehavre.fr

JAOUAD BOUKACHOUR

University of Le Havre
Le Havre, France
jaouad.boukachour@univ-lehavre.fr

ABDELAZIZ EL FAZZIKI

Cadi Ayyad University
Marrakesh, Morocco
elfazziki@uca.ma

Container Terminal (CT) plays a relevant role in the global supply chain. Thus, the occurrence of an accidental event causing the interruption of its functioning will affect a large scale of its collaborators. However, the rise of terroristic activities that exploits transportation systems for fraudulent activities makes the risk management process at the keen interest. For this purpose, the aim of this paper is to propose a multi agent framework for targeting high risk containers. The proposed system analyses information provided by several systems to prevent risks. In addition, it enables the assessment of the containers inspections impact on the CT performance. Thus, we integrate the risk management processes in the CT management policy and we simulate its functioning.

Keywords: Suspect Container Targeting, Risk Management, Multi Agent System, Rule Based System, Business Process, Container Terminal.

1. Introduction

Since the introduction of the container in 1960 containerization has become the most important mode of merchandise transportation [Bandeira *et al*. (2009)]. Furthermore, due to the globalization of markets and the relocation of industries in Asia the number of containers has emerged from 50 million TEU (Twenty feet Equivalent Unit) in 1985 to 350 million TEU in 2004 [Kim and Gunther (2004)]. In addition, the containers annual growth rate is projected at 10% until 2020. The stable evolution forecast of the container traffic has been impacted by the global economic crisis in 2008. However, recent studies show that in the beginning of 2010 the traffic has gradually evolved particularly in Europe [Nedyalkov and Andreeva-Nedyalkova (2011)]. Thus, seaports have to be regarded as the most important rings of the global supply chain proportionately to the

containers turnover [Longo (2010)]. Consequently, the efficiency of these maritime platforms is the basis for assuring the liability of the global supply chain.

Seaports are confronted with changing economic and logistics systems [Notteboom (2007)]. This challenging context brings into focus the competitiveness aspect and the global efficiency of CT. The CT attractiveness is based on its ability to meet client's demand by handling large amounts of containers in short delays and low costs. Therefore, control for efficiency and high degree of coordination are necessary [Vis and koster (2003)]. Nevertheless, since the 9/11 terrorist attacks in 2001, concern has increased about the goods transport safety [Milazzo *et al*. (2009)]. In addition, seaports are threatened by different risk sources emerging from the heterogeneity of its collaborators, the complexity of its business process and the hazardous nature of the handled goods. Consequently, the international community proposed several initiatives and conventions to improve the maritime transportation security.

In effect, the CT vulnerability to a plethora of risks makes the enhancement of security and safety of its operations a critical activity. In addition, the proposed security initiatives do not directly deal with the real application of these recommendations and do not evaluate the impact of these activities on the CT performance [Longo (2010)]. We focus on the Risk Management (RM) at Le Havre seaport in France, particularly on the *Terminal De France* (TDF) CT. This seaport is the first French maritime platform for container traffic with over than 2.2 million TEU (Twenty foot Equivalent Unit). It is structured into six terminals and a multimodal terminal is under construction. The following picture gives an overview of Le Havre seaport:

Fig. 1. An overview of Le Havre Seaport (by Google Map)

The TDF is one of the principal CT in Le Havre seaport due to its ability to treat dangerous goods and to handle 500.000 container/year. The fierce competition with the other seaports existing in the same coastline imposes the adaptation of its handling process in order to improve its competitiveness. However, the international context imposes the application of new security measures to ensure its reliability. These measures may present an impediment for enhancing the CT performance. For this, we propose the integration of a risk management process into the CT management policy and to analyse its impact. Thus, the first step deals with the containers' inspections based on the integration of a process for targeting high risk ones. The second step aims to assess the

impact of this intervention on the CT functioning in order to reconcile the application of the risk management approach with the CT performance.

The remainder of this paper is structured as follows: the second section gives an overview of related works dealing with risk management approaches and initiatives applied in the maritime transport, particularly in the CT case. The third section describes the context of this study and presents the principal steps of the adopted approach to integrate risk management in the CT operations. The application of this approach is presented in the fourth section with a focus on the decision process for targeting high risk containers. Finally, we conclude by presenting the limitations and perspectives of this work.

2. Related Work

This section presents an overview of research works dealing with risk management in seaports. In the first part we identify the risk sources in the CT. The second part presents the principal initiatives and rules applied to improve the security of container transport. Finally, the last part tackles the principal approaches used to analyse the occurrence of a risk event.

Nowadays, CT plays a relevant role within the global shipping network. In addition, it ensures the role of the principal node in the global Supply Chain (SC). However, the increasing SC dependency to these maritime platforms brings into focus the reliability aspect. Consequently, we focus on the ability of the CT to face unpredictable events that may interrupt its functioning and affect the global SC. Particularly, the rise of terrorism and possible misuse of containers to smuggle fraudulent products. In addition, the possible exploitation of containers as weapons to attack vital infrastructure. According to Orphan [Orphan *et al*. (2005)] the potential risk of a terrorist attack involving a container are enormous and may cause the total shutdown of the global SC. For this purpose, the improvements of the security and safety aspect in CT are necessary to improve its reliability.

In response to CT vulnerability to several risks and particularly to improve the security aspect against the terrorist attacks, international organizations and industry have instituted preventive measures to improve security in the shipping trade [Dahlman *et al*. (2005)]. The first one is the Container Security Initiative (CSI) proposed by the USA after the 9/11 terrorist attacks. It consists of bilateral information exchange between the US coast guards and the foreign port. The aim of this initiative is to identify high risk shipment and to use radiation detection technologies to identify containers that present a security threat [Roach (2004)]. The second preventive measure is the International Ship and Port facility Security code (ISPS). ISPS aims to apply a set of rules in order to enhance security of ships and port facilities (IMO International Maritime Organization). Furthermore, it proposes an international framework that allows involved governments and maritime transport actors to share information and to specify preventive measures against incidents affecting ships and port facilities [King (2005)]. The third preventive measure is the Customs Trade Partnership Against Terrorism (C-TPAT). It is a voluntary

self-certification program that allows companies satisfying security standards to gain the status of certified shipper [Wein *et al*. (2006)]. Thus, the certified company has the advantage enabling it to facilitate the USA customs procedures and consequently to speed up its trade.

There are other strategies for maritime transport security improvement. Papa [Papa (2012)] has presented an interesting comparative study between strategies adopted in the united states and the European union and gives a description of these initiatives such as:

- Megaports Intiative: deals with the identification of suspect cargo and the installation of radiation detection equipment to identify nuclear and radioactive materials
- 24-hour rule: aims to advance the container information transmission to US customs 24 hours before to load containers at the last foreign port
- Importer Security Filing: eliminates uncertainty of container description and shipment information by the collection of the required information from both of importer and carrier
- 100% Scanning: attempts to extend the scanning procedures to all the inbound container flow to USA. The feasibility of this initiative in higher volume ports seems impossible.

The involvement of several international actors in the maritime transport in addition to the intermodal transport of containers makes the international container movement vulnerable to terrorist attacks and theft acts. For this purpose, Chatterejje [Chatterejje (2003)] focused on the terrorist acts involving marine containers and investigated possible preventive measures, such as container inspection, to mitigate possible risks. Cariou [Cariou *et al*. (2009)] has proposed a study to define the criteria to select vessels that should be inspected by port authorities based on the results of the 26515 inspection intervention.

The establishment of a risk management process in CT is the basis for improving the liability of the global transport network. Great attention has been concentrated on the prevention of possible accidents during handling operations in CT, the identification of risk sources and their consequences. Rigas [Rigas and Sklavounos (2002)] had investigated the assessment of the consequences of hazardous materials accident scenario in seaport, such as toxic gas dispersion and fireball events using simulation models. Furthermore, the study carried out by Millazo [Millazo *et al*. (2009)] aims to simulate the occurrence of a terrorist attack in the hazardous materials transport in urban areas using a dynamic geoevent approach. This approach is a helpful tool for emergency management because it allows the representation of the incidental scenario evolution.

The construction of a risk scenario and the estimation of its frequency and consequences are the basis of the risk management. Thus, Ronza [Ronza *et al*. (2003)] had tackled the estimation of events frequency in an accident scenario based on the analysis of the historical accident scenarios in seaport and the use of event tree. Fabiano [Fabiano *et al*. (2010)] had proposed a statistical study about the impact of the human factor on the CT accidents and how the experience of workers may reduce the occurrence of accidents. The research work carried out by Darbra [Darbra and Casal (2004)] shows that the evolution of accidents number in port is related to the evolution of container

traffic. Moreover, they present that accidents occurrence is more concentrated in the loading and unloading operations of containers and the stacking operations in the storage area.

In effect, the responsibility for the safety of containers marine transport is not limited to the handling operations in seaports but it depends also on the reliability of the participants involved in the packaging and the consolidation of products in the container. On that account, to identify the main factors contributing to the occurrence of ship accidents particularly in the case of hazardous goods transport, Ellis [Ellis (2011)] had proposed an analysis of events reported during 11 years (1998-2008) in a national database. Therefore, the results prove that 66% of causes contributing to release of dangerous goods could be assigned to packaging deficiencies and 25% of the causes are related to the consolidation activities.

3. Proposed Approach

The establishment of a risk management process in a complex system such as CT needs a detailed description of its components and its actors. To this end, we propose a structured approach to deal with the complexity of the studied case. The proposed approach is structured into four main steps; the first one focuses on the presentation of the case study and presents a domain analysis based on the modelling of the CT business process using Business Process Modelling Notation (BPMN). The analysis of the CT business process and the identification of the potential risk scenarios that may affect its normal functioning are presented in the second step of this approach. The third step aims to specify countermeasures to prevent the occurrence of the identified risk scenarios. The last step deals with the integration of the risk preventive actions in the CT operations and to assess the impact of these control processes on the CT performance. The following figure gives an overview of the proposed approach:

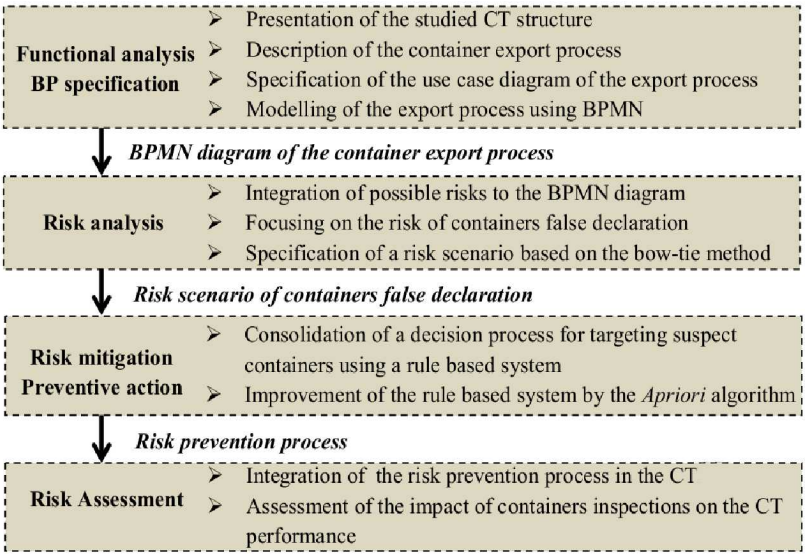

Fig. 2. The principal steps of the proposed approach

3.1. *Functional analysis: business process specification*

The business process specification represents the basis of this study because it allows us to understand the functioning of the CT and to identify its actors. According to Barjis [Barjis (2008)], business process modelling will become even more crucial as systems grow in scale and complexity. Particularly, the case of CT which is managed by distributed actors and operates in an evolving context. Thus, to overcome the complexity of this task and to achieve an accurate description of the studied system, this analysis phase is structured into two main steps; the first one is based on the use of a Use Case Diagram (UCD) to identify the principal actors and functions. The second one aims to model the sequence of tasks composing a business process using the BPMN.

- Use case diagram: is one of the simplest diagrams proposed by UML (Unified Modelling Language). However, it represents an efficient tool for the preliminary analysis to identify the main functions provided by a system and its interactions with external actors. In addition, it allows the identification of dependencies between system functions which facilitates the specification of the tasks sequence composing the business process. We use the UCD to identify the actors existing in the CT such as straddle carriers and the tasks they ensure (figure 5).
- Business process: is a structured set of activities executed by various actors and satisfy a set of constraints in order to achieve the goal set by its owner. Muehlen [Muehlen and Indulska (2009)] defined the business process as a collection of actions that address a set of input values to produce a result to the client. To model the case study, CT handling process, we use the BPMN. This modelling notation was proposed by the Object Management Group (OMG) as a standard for modelling BP. According to Vergidis [Vergidis (2008)], the BPMN allows a visual and intuitive description of business process. A comprehensive study about the BPMN standard, its specification and its relationship with other tools of business process modelling was proposed by Chinosi [Chinosi and Trombetta (2012)]. We use the BPMN to model the container export process inside the CT and to specify the execution sequence of tasks which it is composed (figure 6).

3.2. *Risk analysis*

The aim of this step is to analyse the functioning of a system and the interaction of its components in order to identify risk events. Thus, the business process models provided by the previous phase are used to specify the potential risks that threat the CT. Moreover, the identification of the causes and consequences of the identified risk events represents the basis for the specification of possible risk scenarios. Therefore, to achieve an accurate risk analysis and to generate realistic risk scenarios we propose the use of the bow-tie approach. This approach is founded on the combination of the Event Tree Analysis (ETA) and the Fault Tree Analysis (FTA). Consequently, it allows the construction of risk scenarios based on events analysis on the upstream and downstream of the risk event occurrence.

- Event tree analysis: is based on a decision tree that gives a logical view of the events sequence triggered by the occurrence of an initial event. According to Marhavilas [Marhavilas *et al*. (2011)], ETA allows to understand how external events and

countermeasures influence the evolution of an accident. In addition, it enables to associate probabilities to the resulting events based on the analysis of the previous scenarios. Consequently, the principal goal of adopting the ETA method is to identify the possible consequences of a risk event occurrence in CT. Furthermore, it allows prioritizing prevention measures proportionally to the magnitude of the damages generated by each risk scenario.

- Fault tree analysis: is a deductive method that aims to define the causes of an accident. This method allows to achieve a graphical representation of the logical relationships among human errors, hardware failures and external factors that has triggered a risk event [Marhavilas *et al.* (2011)]. In addition, it identify of the minimal sequence of events that leads to the occurrence of the risk event. Moreover, it enables the calculation of the risk probability based on the probability of its causes. Thus, the identification of the risk causes allows the establishment of countermeasures to impede the risk event triggering.

We used the bow-tie approach to specify realistic risk scenarios such as false declaration of containers and accident related to containers handling inside the CT. The generated risk scenarios help us to identify the causes and the possible consequences of a risk event. Thus, we can specify the suitable measures to prevent the risk occurrence and to mitigate the possible damages as seen in figure 7.

3.3. *Risk mitigation: preventive action*

Risk prevention is one primary security concept for managing risks and it is applied in several domains such as the installation safety. The aim of this step is to mitigate the occurrence of the risk event and to specify countermeasures that enable the elimination of its factors. In this study, we focus on the enhancement of the seaport safety and particularly the detection of containers false declaration. For this purpose, we deal with the prevention of smuggling products by targeting high risk containers that must be inspected by the customs officers.

We propose the adoption of a decision process based on rules. These rules represent the knowledge acquired by customs officers during their previous interventions. In addition, to go beyond the simple application of an expert system and to ensure the evolution of the decision process, we enrich our system by the integration of an association rule mining method. This method is applied to extract association rules from massive primary data. The following rule gives an example of an association rule to target high risk containers:

(Container destination is A) **and** (transporter is B) → High risk container

Finally, we propose the application of the Apriori algorithm to extract rules from the data describing the inspection interventions executed by the customs office. We apply the original Apriori algorithm proposed by Agrawal [Agrawal and Srikant (1994)] as described by the following algorithm:

```
1)  L1 = {large 1-itemsets} ;
2)  for ( k =2; Lk-1 ≠ ∅ ; k ++ ) do begin
3)      Ck = apriori-gen(Lk-1): // New candidates
4)      forall transactions t ∈ D do begin
5)          Ct = subset( Ck , t); // Candidates contained in t
6)          forall candidates c ∈ Ct do
7)              c.count++;
8)      end
9)      Lk ={ c ∈ Ck | c.count ≥ minsup }
10) end
11) Answer = Uk Lk ;
```

The Apriori algorithm uses an *apriori-gen* function that operates in two phases, union and pruning. The union phase generates all the k-itemsets candidates. The pruning phase remove the candidates with non frequent (k-1)-itemsets. Furthermore, This algorithm calculate the support of the generated association rules based on the percentage of its itemsets among all transactions and keep only the itemsets with the minimum support (Eq. 1.a). Thus, the support is used to eliminate uninteresting association rules. The selection of generated rules can be improved based on the calculation of the confidence of these rules. Consequently, the specification of a confidence threshold is useful to eliminate generated rules characterised by a weak occurrence probability (Eq. 1.b).

$$\text{Association rule R1: } X \rightarrow Y$$

$$(a) Support\,(R1) = \frac{Occurrence\ count\ of\ (X \cup Y)}{Transactions\ count} \qquad \text{(Eq. 1)}$$

$$(b)\ Confidence\,(R1) = \frac{Occurrence\ count\ of\ (X \cup Y)}{Occurrence\ count\ of\ (X)}$$

3.4. *Risk assessment*

As stated before, the risk management in CT is a tedious task due to the complexity of its process and the heterogeneity of its actors. Furthermore, beyond the effectiveness measurement of the applied risk management approach, the integration of these methods may affect the normal functioning of the studied system. Particularly the case of CT where the introduction of new security and safety measures may slow down its processes.

To deal with this problem, we adopt an integrated approach that combines the risk management approach provided by the previous phases and the applied management policy of the case study. This approach seeks to assess the impact of the risk management on the performance of the CT. Thereby; the decision process for targeting suspect containers is integrated into the functioning of the Container Terminal Management System (CTMS).

CTMS consists of a classified Multi Agent System (MAS) that represents the actors of the CT and integrates needed decision process to manage it [Najib *et al.* (2012)]. We

have developed this platform to simulate the CT operations in order to assess the effectiveness of the applied management policies. Our system is structured into two main parts; the first one enables the simulation of the CT operations. The second one represents the needed decision process for CT management. Furthermore, it integrates a risk management process and ensures the interfacing with external systems that provides our system with needed information.

The CTMS is interfaced with GOST (Geolocalisation Optimisation and Security of containers Transport). GOST was developed in case of an industrial partnership and it aims to ensure the tracing and tracking of transport in real time, particularly in the case of hazardous goods transport in a multimodal context. GOST is a web services platform coupled with technological solutions to track and secure container shipping. It is designed to monitor physical movements, administrative schedules and planned shipment information in real time based on information traceability, with possible interventions to prevent malfunctions and risks of failure. The GOST platform provides to the CTMS the needed information and alerts in real-time in order to identify risk situations [Boukachour *et al.* (2011)].

The following figure describes the global architecture of the CTMS:

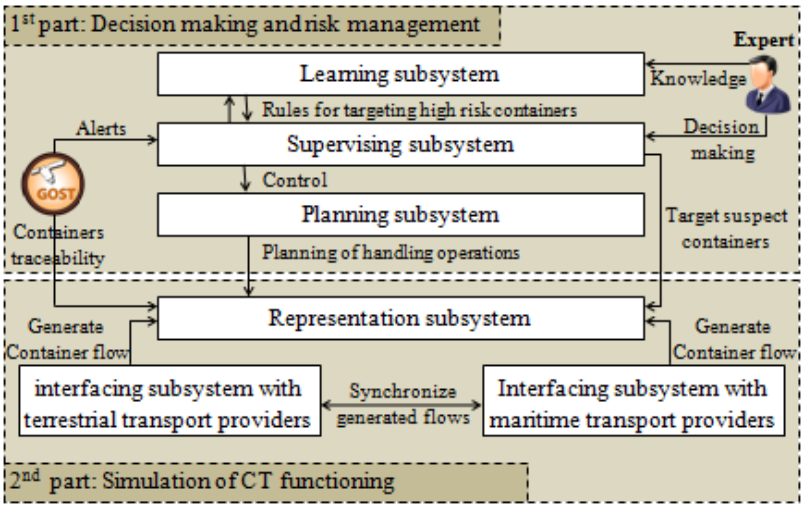

Fig. 3. Global architecture of the CTMS

The CTMS is classified into six subsystems that regroup agents with similar goals to form coherent groups:

- Interfacing subsystem with terrestrial transport providers: represents the functioning of the terrestrial gate of a CT by ensuring the generation of the inbound and outbound flows of containers. These containers are transported by trucks and trains.
- Interfacing subsystem with the maritime transport providers: ensures the generation of the inbound and outbound containers' flows in the maritime interface.
- Representation subsystem: is composed of agents representing the handling material. The aim of this subsystem is to simulate the container handling operations. In addition it allows the assessment of the CT performance.

- Planning subsystem: plans handling operations such as the routing of straddle carriers and trucks and the storage places allocation. This subsystem interacts with supervising subsystem in order to validate its decision.
- Supervising subsystem: serves to analyse the information provided by several systems to prevent risk occurrence. In our case the aim of this subsystem is to analyse container's information to target suspect ones.
- Learning subsystem: ensures the capitalization of information about high risk containers detected by the customs. In addition, it integrates information provided by experts to detect risk scenarios. This subsystem provides the supervising subsystem with needed information for the risk management process.

4. Case Study

The case study treats the export process of a container transiting through the *Terminal De France* CT in Le Havre seaport. The container is transported by a truck to the terrestrial interface of the CT. After the arrival of the truck to the terrestrial gate, customs officer checks the driver identity in addition to the condition of the container and its correspondence with the statement in order to validate its access. After that a place is assigned to the truck in the parking area. The next step consists of the allocation of a straddle carrier that discharges the container from the truck and transported to the storage area. Upon the arrival of the container vessel that will export the container, a straddle carrier transports the container from the storage area to the buffer of the quay where the vessel is berthed. Then the quay crane loads the container on the vessel. Figure 4 gives an overview of the handling process in the CT.

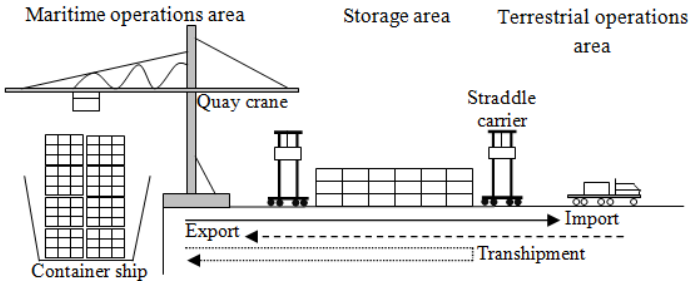

Fig. 4. Overview of container handling processes

4.1. *Functional analysis*

In order to simplify the case study we propose to focus on the export process of a container without detailed specification of the actor's tasks. Furthermore, the studied export process deals only with the inbound flow of containers transported by trucks. Thus, we will not treat the train transport of containers in this case. The use case diagram presented in figure 5 gives an overview of the principal tasks and actors involved in the export process.

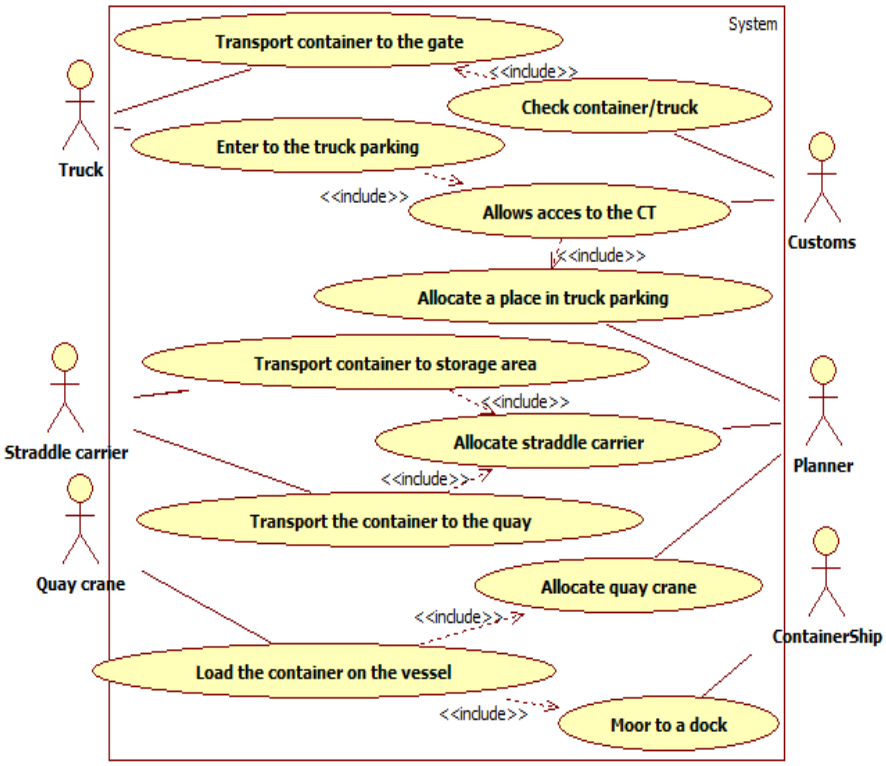

Fig. 5. Use case diagram of a container export process

This use case diagram gives a preliminary description of the container export process and specifies the six actors involved in this operation. There are two types of actors, the first set is composed of executive actors and regroup the handling equipment used in this process such as, straddle carrier and quay crane in addition to trucks and container ships. The second set represents the decisional actors that command the execution of the export process. These actors are the customs officers that ensure the inspection of containers and the planner actor which represents the port managers and their planning systems.

To give a dynamic view of the container export process and to present the tasks sequence executed to accomplish its goal, we propose the description of this business process based on the BPMN. The aim of this step is to ease the understanding of the process. We propose to model this process according to the descriptive level of the BPMN defined by Silver [Silver (2009)]. Thus, the following model gives a macroscopic view of the process without details of its sub-processes (figure 6).

4.2. *Risk analysis*

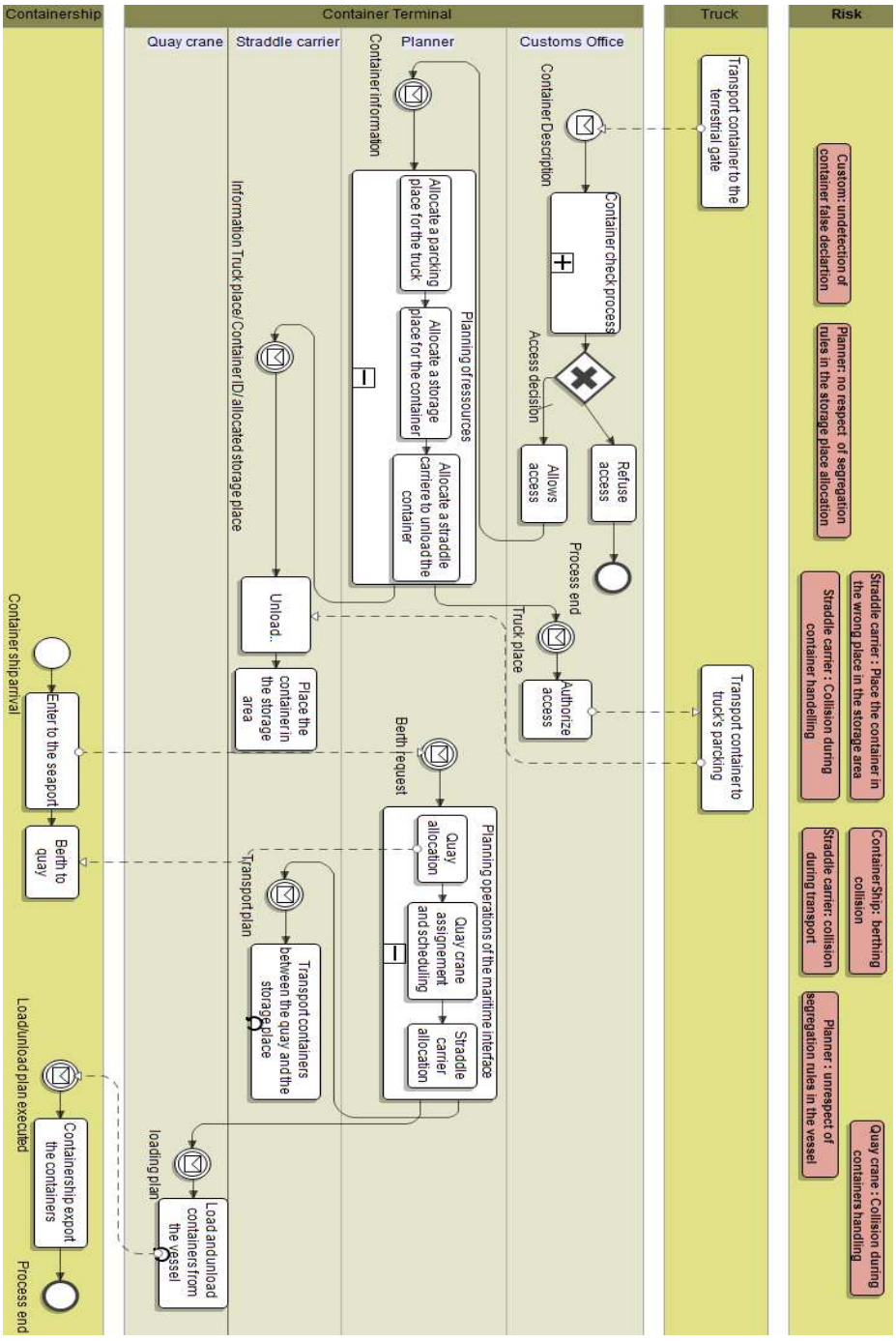

Fig. 6. Container export process BPMN diagram

The purpose of the risk analysis in the proposed risk management approach is to investigate the possible risk scenarios arising from the CT activities. However, CT is prone to a myriad of risks arising from both external and internal causes. Thus, the identification of the risk scenario's causes and its possible consequences are the basis for prioritization of the possible intervention actions. For this purpose, the aim of this step is to build credible risk scenario based on the bow-tie approach. This approach allows an accurate description of possible risk scenarios based on the specification of events on the upstream and downstream of the risk occurrence. Thus, the FTA is used to specify the sequence of events that triggered the risk event. The ETA is established to specify the evolution of events in order to assess the possible damages caused by the occurrence of a risk.

Until recently, the risk management in the CT was concentrated on accidental event that occurs during the handling process. The pool risk in the BPMN diagram of the export process integrates a set of possible risks principally arising from the handling activities (figure 6). However, the arising of the terroristic activities in the world imposes to take these risks into consideration. Consequently, the risk analysis phase focus on the study of the false declaration of containers content. There are many scenarios that may exploit this fraudulent action such as:

- The exploitation of containers and the CT facilities to transport weapons to attack other countries
- The exploitation of CT as a target to amplify the consequence of a terrorist attack due to its location, oil refineries existing in the seaport and the economical impact of the suspension of its activities
- To avoid the payment of expensive taxes for a type of goods.

The following figure presents a bow-tie diagram that shows the events on the upstream and downstream of the false declaration:

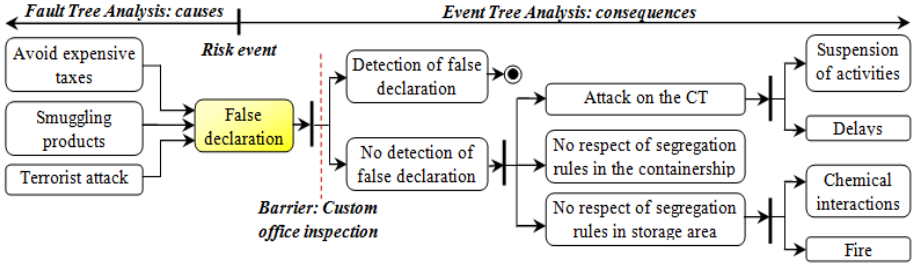

Fig. 7. A bow-tie diagram of false declaration risk

The combination of the events allows us to constructs a set of possible scenarios. The case of terroristic attacks on the CT is one of the most important scenarios because it leads to the suspension of activities and consequently it causes huge financial losses. For this purpose, we aim to mitigate the occurrence of this risk trough the adoption of a preventive solution. This solution consists of the integration of a barrier to control the inbound flow of containers. Thus, we propose to specify a decision support system that assists the customs officers to analyse declaration to target suspect containers.

4.3. *Risk prevention*

To prevent risk scenarios generated from the occurrence of false declaration of containers. Customs office controls the container flows and targets high risk cargoes for inspection and scanning. Thus, we use a rule based system to assist officers to choose suspect containers and the application of the Apriori algorithm to extract new rules from the previous interventions of customs. The classic application of rule based system tries to reproduce human reasoning based on rules engine and association rules that represents knowledge provided by expert of the domain. The aim of this section is to present a simplified example of Apriori method application to discover new rules.

The table 1 shows a set of four interventions of customs officers to inspect containers and the result of these inspections. Furthermore, it gives the principal properties of inspecting containers.

Table 1: Transactions describing the containers inspections

Rule ID	Attributes describing the intervention of customs officers
1	Less than a container load (LCL), the origin country is in Europe, not false declaration
2	LCL, not Authorized Economic Operator (AEO) transporter, the origin country in Asia, false declaration
3	Full container load, not AEO transporter, false declaration
4	Container of hazardous goods, AEO transporter, the origin country in Asia, false declaration

The first step in the Apriori algorithm consists of the generation of all the possible association rules based on the combination of the items on the table 1. To ease this step we propose to analyse the two following association rules:

- If the transporter is not AEO then there is a false declaration
- If LCL container then there is a false declaration

In the second phase of this analysis we will calculate the support of these association rules. For example the support for the first rule is the number of transactions, in this case we have four transactions (Table1), where the attributes **not AEO transporter** and **false declaration** exist together divided by the number of transactions (Eq. 1.a). Thus, the support of the first rule is 2/4 = 0.5 and for the second rule the support is 1/4 = 0.25.

We suppose that the minimum support value to keep a rule association is equal 0.25, then we will keep the two studied rules for the calculation of confidence. This step consists of determining the certainty of an association rule and its relevance. Thus, the confidence for the first rule is equal to the number of transactions where both **not AEO transporter** and **false declaration** exist divided by the number of transactions where the attribute **not AEO transporter** exists (Eq. 1.b). Consequently, the confidence of the first rule is 2/3 = 0.66 and the confidence of the second rule is 1/3 = 0.33. Therefore, if the minimum confidence of a rule is 0.5, only the first association rule will be added to our rule based system.

The application of the Apriori algorithm to discover association rules allows the establishment of a learning process that allows us to add new knowledge to the system and to remove old rules which are no longer relevant.

4.4. *Risk management impact*

The application of risk management approaches in the CT is important to improve its reliability and to attract new container flows. However, the application of these measures may slow down the handling operations and consequently affect the CT performance. Thus, in order to assess this impact we propose the integration of the decisional process for targeting suspect containers in the functioning of the CTMS. The following figure gives an overview of the integration of the process for targeting risky containers in the learning and the supervising subsystems of the CTMS:

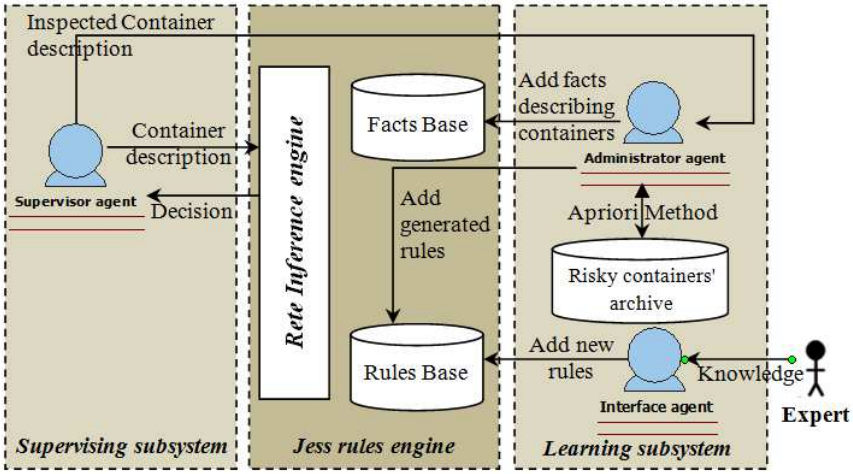

Fig. 8. Process of targeting high risk containers

The learning subsystem is composed of an interface agent that ensures the integration of knowledge provided by experts. In addition to the administrator agent that manages the rule database and ensures the application of the Apriori algorithm to specify new rules. The second subsystem ensures the control of container flows and target suspect containers for further inspections based on a rules engine. Furthermore, it communicates the results of its inspections to the administrator agent in order to enrich the facts base.

In reality, suspect containers targeting by the customs officers is based on the analysis of numerous attributes describing the cargo. Furthermore, the experience acquired by the customs officer and its ability to analyse numerous attributes are the key factors for the success of this decision process. We have implemented this decision process using the JESS [Friedman-Hill (2003)]. JESS is a rule engine used to develop rule based computer programs that has the capacity to reason using knowledge. Thus, the experience of the customs officer is represented by the association rules stored in the rule base. In addition, the decision for the inspection of a container is ensured by the RETE inference engine [Friedman-Hill(2003)] provided by JESS. The RETE inference engine controls the whole

process of applying the rules and specifies the order in which the rules will be fired. This Inference engine gets the container description from the supervisor agent and checks the possible combination of rules to take a decision.

We applied this solution to analyse data describing 1.000.000 containers transiting trough TDF CT. Among these containers only 0.6% of them are fraudulent with different occurrence probabilities. The resources existing in the studied CT allows to inspect only 1.6% of these containers. Furthermore, the decision process is started with an empty knowledge base. The Apriori algorithm is executed for every 100.000 containers analysed in order to generate new decision rules. Figure 9 provides a comparison between the number of containers targeted by the decision support system and the number of risky containers detected in each step. This comparison allows us to understand how the system improves its decisions based on the rules generated in each step by targeting pertinent containers. Consequently, it improves risky containers number relatively to the targeted containers number.

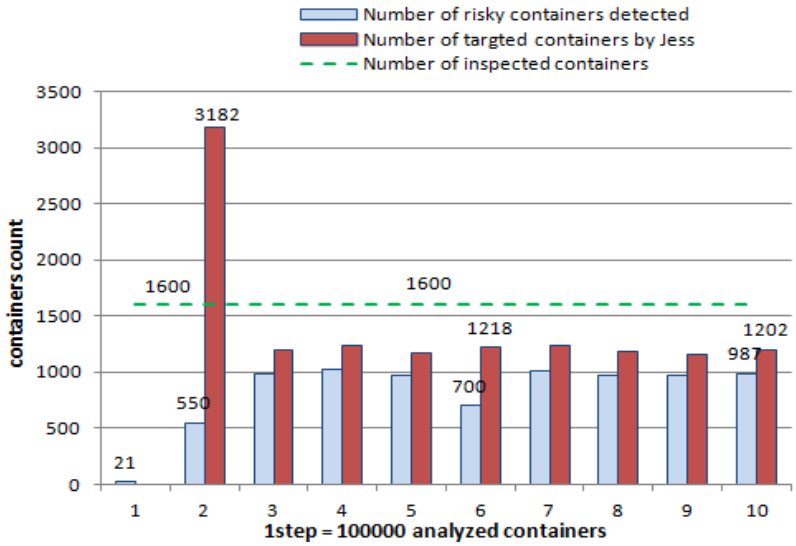

Fig. 9. Comparison of risky containers number and targeted containers number

The execution of the learning process one time after the analysis of each 100.000 containers guaranties the update of the knowledge base. Thus, we ensure the adaptation of the decision process by deleting irrelevant rules and enriching the knowledge base by new rules. Figure 10 illustrates how the system update the decision rules during its functioning and how these updates improve the right decisions rates.

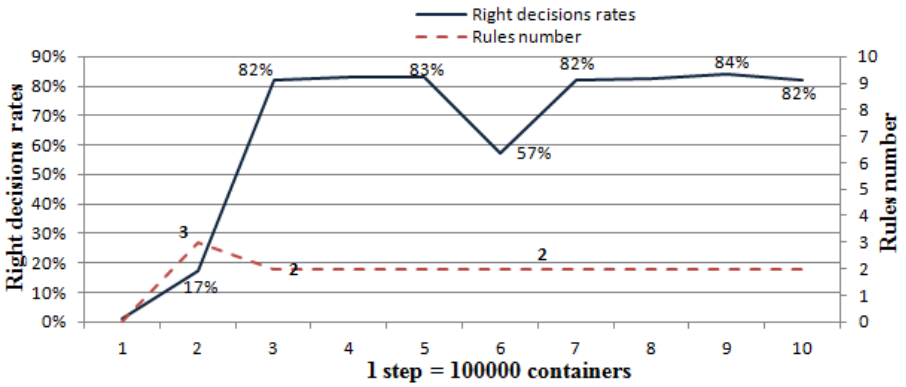

Fig. 10. Evolution of right decision rates and rules number

In the first step, the right decision rate is 1% percent because the system's knowledge base is empty and containers to be inspected are targeted randomly. In the second steps, the system generates three rules and improves the right decision rate to 17%. This wake rate is justified by the generation of irrelevant rules due to the wake number of containers stored in the inspections archive. The third step shows that the system use only two new rules and the right decision rate has evolved to 82%. This result means that the new generated rules are adequate to identify risky containers hidden in the data set describing containers. The results generated in the other steps keep the same rules with an average right decision rate equal to 77.6%.

5. DISCUSSION

The establishment of a risk management approach to improve the security of the logistic systems is in the keen interest. The complexity of these systems imposes to focalise on the main nodes of the global supply chain. Thus, we have treated the case of a CT due to the dependency of the international trade to the maritime transport. However, the specificity of the studied case imposes the adoption of an approach that reconciles the application of a risk management process with its impact on the CT performance.

In fact, by taking into account the importance of understanding the functioning of the studied system. We considerate that use case diagram is appropriate for the modelling and the specification of the principal actors and their interactions with the system. Thus, the activity for modelling the CT business process is driven by the results issued from the use case diagram [El Fazziki *et al*. (2012)]. In addition, to overcome the lack of adaptation of use case to present a dynamic view of the business process we have adopted the BPMN. This notation allows us to achieve an accurate description of the tasks sequence structured according to the involved actors. Consequently, BPMN presents a rigid foundation to tackle a functional analysis to specify the risk events.

The proposed risk management approach aimed to assist the customs office by the implementation of a decision process for targeting suspect containers. For this purpose,

we have opted for the development of a rule based system because it presents many similarities with the real reasoning of the customs officers. Moreover, we integrate the Apriori rule mining method to extract new association rules from the archives describing the inspection activities. Consequently, we enrich the proposed decision process with a continuous learning process that improves the effectiveness of its rules base.

The last part of the proposed approach deals with the integration of the decision process for targeting suspect containers in the CTMS. Moreover, it aims to understand how the application of the risk management slows down the handling operations and consequently affect the CT performance. To this end, we used the CTMS platforms to integrate our risk management process in the management policy of the CT. This platform is based on the agent paradigm which is appropriate for the representation of the complex and distributed nature of the CT.

6. CONCLUSION

This paper aims to analyse the risk management in CT and to investigate the integration of these measures in its management policy. We adopted a structured approach to ease the analysis of the studied system and the establishment of a risk management process. We focused on the improvement of the CT safety by the integration of a decision process for targeting suspect containers. This process is based on the use of Jess rules engine and enriched by the Apriori rule mining method. Furthermore, we integrate the process for targeting suspect containers in the functioning of the CTMS in order to assess its effectiveness.

7. ACKNOWLEDGMENT

This research was funded by the region of *Haute-Normandie* in France.

8. REFERENCES

Agrawal, R.; Srikant, R. (1994). *Fast Algorithms for Mining Association Rules.* Proceedings of the 20th VLDB Conference Santiago, Chile.

Bandeira, D. L.; Becker, J. L.; Borenstein, D. (2009). *A DSS for integrated distribution of empty and full containers*. Decision Support Systems, volume 47, issue 4, pp. 383–397.

Barjis, J. (2008). *The importance of business process modeling in software systems design*. Science of Computer Programming, volume 71, issue 1, pp. 73–87.

Boukachour, J.; Fredouët C-H.; Gningue, M.B. (2011). *Building an Expert-System for Maritime Container Security Risk Management*. International journal of applied logistics, volume 2, issue 1, pp.35-56.

Cariou, P.; Mejia, M. Q.; Wolff, F. (2009). *Evidence on target factors used for port state control inspections*. Marine Policy, volume 33, issue 5, pp. 847–859.

Chatterjee, A. (2003). *An overview of security issues involving marine containers and ports*, The Annual Conference of Transportation Research Board, Washington, USA.

Chinosi, M.; Trombetta, A. (2012). *BPMN: An introduction to the standard*. Computer Standards & Interfaces, volume 34, issue 1, pp. 124–134.

Dahlman, O. *et al*. (2005). *Container Security A Proposal for a Comprehensive Code of Conduct*, Defense & Technology Papers. Web site last visit 31/05/2013: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA434718.

Darbra, R. M.; Casal, J. (2004). *Historical analysis of accidents in seaports*. Safety Science, volume 42, issue 2, pp. 85–98.

El Fazziki, A. *et al*. (2012). *Une approche agents pour la modélisation des processus métiers*. 6ème conférence francophone sur les architectures logicielles, Lyon, France.

Ellis, J. (2011). *Analysis of accidents and incidents occurring during transport of packaged dangerous goods by sea*. Safety Science, volume 49, issues 8–9, pp. 1231–1237.

Fabiano, B. *et al*. (2010). *Port safety and the container revolution: A statistical study on human factor and occupational accidents over the long period*. Safety Science, volume 48, issue 8, pp. 980–990.

Friedman-Hill, E. (2003). *JESS in action rule based systems in Java*. Manning publication Co, ISBN 1-930110-89-8.

Kim, K. H.; Gunther, H. (2007). *Container terminals and terminal operations, Container terminals and cargo systems*. Springer-Verlag Berlin Heidelberg New York, ISBN 978-3-540-49549-9.

King, J. (2005). *The security of merchant shipping*. Marine Policy, volume 29, issue 3, pp. 235–245.

Longo, F. (2010). *Design and integration of the containers inspection activities in the container terminal operations*. International journal production economics, volume 125, issue 2, pp. 272–283.

Marhavilas, P.K.; Koulouriotis, D.; Gemeni, V. (2011). *Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000 à 2009*. Journal of hazardous materials, volume 24, issue 5, pp. 477–523.

Milazzo, M. F. *et al*. (2009). *Risk management of terrorist attacks in the transport of hazardous materials using dynamic geoevents*. Journal of loss prevention in the process industries, volume 22, issue 5, pp. 625–633.

Muehlen, M. Z.; Indulska, M. (2009). *Modeling languages for business processes and business rules: A representational analysis*. Information systems, volume 35, issue 4, pp. 379-390.

Najib, M.; ElFazzik, A.; Boukachour, J. (2012). *A container terminal management system*. The 14th international conference on harbor, maritime & multimodal logistics modelling and simulation, Vienna, Austria.

Notteboom, T. (2006). *Chapter 2 strategic challenges to container ports in a changing market environment*. Devolution, port governance and port performance research in transportation economics, volume 17, pp. 29–52.

Orphan, V. J. *et al*. (2005). *Advanced ray technology for scanning cargo containers*. Applied Radiation and Isotopes, volume 63, issues 5–6, pp. 723–732.

Papa, P. (2012). *US and EU strategies for maritime transport security: A comparative perspective*. Transport Policy, DOI: 10.1016/j.bbr.2011.03.031.

Rigas, F.; Sklavounos, S. (2002). *Risk and consequence analyses of hazardous chemicals in marshalling yards and warehouses at Ikonio/Piraeus harbour, Greece*. Journal of loss prevention in the process industries, volume 15, issue 6, pp. 531–544.

Roach, J. A. (2004). *Initiatives to enhance maritime security at sea*. Marine Policy, volume 28, issue 1, pp. 41–66.

Ronza, A. *et al*. (2003). *Predicting the frequency of accidents in port areas by developing event trees from historical analysis*. Journal of loss prevention in the process industries, volume 16, issue 6, pp. 551–560.

Silver, B. (2009). *BPMN method and style*. Cody-Cassidy Press, Aptos, California. pp.236. ISBN: 0982368100, 9780982368107.

Nedyalkov, T.; Andreeva – Nedyalkova.(2011). *Trends in the container shipping and need of a new generation container terminals and container vessels*. International virtual journal Machines, technologies, materials, volume 5, issue 3, pp. 20-23

Vergidis, K. (2008). *Business Process Analysis and Optimization: Beyond Reengineering*. IEEE Transactions on Systems, Man, and Cybernetics, Part C, volume 38, issue 1, pp. 69-82.

Vis, I. F. A.; Koster, R. (2003). *Transshipment of containers at a container terminal: An overview*. European journal of operational research, volume 147, issue 1, pp. 1–16.

Wein, L. M. *et al*. (2006). *Preventing the Importation of Illicit Nuclear Materials in Shipping Containers.* Risk Analysis, volume 26, No. 5, DOI: 10.1111/j.1539-6924.2006.00817.x.