Intermodal Containers Transportation: How to Deal with Threats?

Sergej Jakovlev[1,3][a], Arunas Andziulis[2][b], Audrius Senulis[1][c] and Miroslav Voznak[3][d]
[1]*Marine Research Institute, Klaipeda University, Bijunu str. 17, Klaipeda, Lithuania*
[2]*Department of Informatics and Statistics, Klaipeda University, Bijunu str. 17, Klaipeda, Lithuania*
[3]*IT4Innovations National Supercomputing Center, VSB-Ostrava Technical University, Studentska 6231/1B, Ostrava, Czech Republic*

Keywords: Security, Transportation, CSI.

Abstract: This paper provides an overview of the port container inspection techniques and procedures (standardized security procedures) relating to the detection of illicit material in containers. These procedures affect the duration of the containers transportation periods in different parts of the transport chain, according to the 2002 Container Security Initiative (CSI) regulations. The main object of this work – to demonstrate the inability of standard systems and associated technologies to deal with current threats and to propose solutions that are in line with the "intelligent containers" worldwide initiative.

1 INTRODUCTION

Intermodal container monitoring is considered a major security issue in many major logistic companies and countries worldwide (Scholliers et al. 2016). Current representation of the problem, we face today, originated in 2002, right after the 9/11 attacks. Then, a new worldwide Container Security Initiative (CSI, 2002) was considered that shaped the perception of the transportation operations, including sea, air and land transport. CSI consists of four core elements (inspection efforts):

1. Establish security criteria to identify high-risk containers based on advance information;
2. Pre-screen containers at the earliest possible point;
3. Use ICT to quickly pre-screen high-risk containers;
4. Develop secure and "smart" containers.

Now major ports all over the world contribute to CSI further development and integration into everyday transportation operations and improve the transport regulations for the developing regions (Carlo et al. 2014; Mark, 2019). Although, these new improvements allow us to feel safer and more secure, constant management of transportation operations has become a very difficult problem for conventional data analysis methods and information systems.

With the constant geopolitical and terrorism threats risks related to security violations grow at a rapid pace. The threat of a Chemical, Biological, Radiological or Nuclear Weapon (CBRN) being delivered using shipping containers has risen above other terrorist-linked threats to containerised transport all over the world and has become a single unifying driver of international transport security policy since 2001 (OECD, 2013). CBRN weapons handling requires much greater expertise and their development and deployment during container tampering is both a complicated and time-consuming process. It should be noted, that in many cases, the development of these weapons requires acquiring components and materials not through theft, but through official commercial transactions and in most cases using containerised shipments. This highlights the need to act not only to discover CBRN weapons in containerised shipments, but to also intercept CBRN weapon precursors (demonstration of the CBRN turn-around procedures in the transport chain presented in figure 1).

[a] https://orcid.org/0000-0002-1440-8221
[b] https://orcid.org/0000-0002-1735-8901
[c] https://orcid.org/0000-0002-4759-2707
[d] https://orcid.org/0000-0001-5135-7980

Jakovlev, S., Andziulis, A., Senulis, A. and Voznak, M.
Intermodal Containers Transportation: How to Deal with Threats?.
DOI: 10.5220/0007739805050512
In *Proceedings of the 5th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2019)*, pages 505-512
ISBN: 978-989-758-374-2

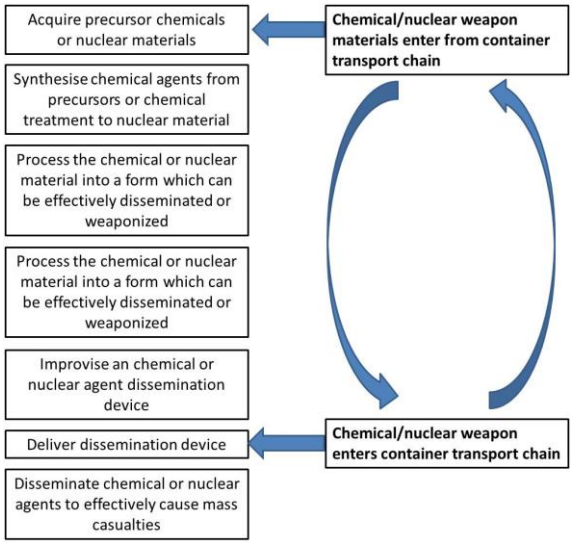

Figure 1: CBRN turn-around in the transport chain [Container transport security across modes, „European conference of ministers of transport. OECD 2013].

This has had a direct impact on Transport authorities in many leading countries of the world, as they are constantly charged with ensuring both the flow of goods and ensuring the container transport chain security. In fact, there is no single information system governing the international movement of containers in the world, due to low level of cooperation between individual shipping companies, governments and even engineering working in this research area. No unifying security regulation is responsible for the entire process. Container transportation is done using multiple actors, industries, regulatory agencies, modes, operating information and management systems (IMS), liability regimes, legal frameworks, technological standards, ISO and etc., not to mention the standardization issues of documentation.

To combat illicit trafficking in maritime container transport, a good level of detection is essential, and should be approached with advanced data-driven or process-driven technologies. Although the process-driven technologies are done now with a large range of surveillance and active interrogation techniques, active sensors that register the threats during the transportation route and onsite might be an interesting supplement to the battle the rising threats. Data-driven characteristics will allow instantaneous recombination of all possible scenarios with a high certainty of risk detection under normal working conditions.

Analysis of scientific literature studying the intermodal terminal activity (Chung-Yee and Dong-Ping, 2017) revealed that there are many models helping to improve the terminal's operational activity, however there are no models helping to determine which technology would be the most rational (Rizzo et al. 2011). Integration of newer Information and Communication technologies (ICT) and procedures into the existing cargo handling operations is likely to be the main solution. As an example, some industrial applications and international regulations already consider adopting short range and long range communication through IEEE 802.11p and/or Cellular-V2X that are already used in industry, but with limited applicability (Masini et al. 2018; Xuerong et al. 2019). The choice of the applied communication technology often depends on the allowed control and communication frequency in the vicinity of the port. Frequency reflects numerous factors, including not only technical considerations, but also international availability and economic considerations. Application of most modern mobile technologies plays an important role in maximizing the performance, reducing the costs and risks of intermodal containers transportation and raises the efficiency of other transportation services in the supply chain. There are still many different opinions regarding the priorities of the supply chain and their involvement in the border security. One may notice that safety of the cargo is still the primary objective to the supply chain. This is due to the direct value input. Only the primary objective brings direct value and makes supply chain cost effective. Therefore, some of the adopted CSI regulations are not taken into account. In many cases, their expenses do not exceed the expenses of the possible risks. Nowadays, these regulations are becoming more obligatorily and therefore, in many security and safety applications worldwide, information management during the control operations is becoming the number one priority.

In general, most security threats arise mainly in the first few and last few links of the transport chain. Sometimes these small actors operate on tight margins, and pose higher security risks than their larger counterparts in the transport supply chain. Secure management of information and operations on these levels is crucial for the working stability of the entire transport operation for each container and good inside. An efficient unified and standardized information management system is needed to ensure the working stability of these actors, large and small, in terms of information retrieval, approval and forwarding. These systems must be incorporated into the existing IT infrastructures with less human interaction probability. Human-machine interaction

methods and technologies are needed to be adopted on various levels of process control. IMS must acquire and retransmit control commands within the working regulations in an optimal manner. Optimality must be achieved through constant update and improvement of local operating conditions at each separate transport chain position. In terms of terrorist attacks, terrorists will probably use one of two approaches:

1. Approach A (they will intercept a container and tamper with it);
2. Approach B (they will send a tampered container).

Not all technologies and methods are equally suited to counter both the A and B approach threats. Technical measures focusing on the integrity of the container and its environment are not of much use in the B threat approach. Constant containers scanning remain an effective measure to discover both threats. Intelligent information and communication technology based measures must be deployed to battle the B approach. To ensure the security from these approaches, specific measures are classified:

1. container scanning via X-Ray and etc.;
2. ensuring container integrity via E-Seal technology and etc.;
3. controlling access to the container via video surveillance technologies and etc.;
4. tracking containers via GPS and etc.;
5. assessing container risk using probability estimations, neural network modules for threat assessment and decision support.

But, what technologies and methods work for one threat assessment, will not necessarily work for the other. Generally, technologies put into place fall into one of the following five groups.

- Measures seeking to scan or otherwise physically confirm the contents of the container;
- Measures seeking to ensure the physical integrity of the container;
- Measures aimed at ensuring the security of the container environment as it moves and is handled in the container transport chain;
- Measures seeking to track and trace the container in the supply chain;
- Measures centred on the provision, and use of, information related to the shipment.

Over the past few decades many securities related initiatives were proposed. In relation to Lithuania, they can be classified as International (including EU countries and US) and many other industry measures. Some of the most noticeable measures that that impact on the security and safety of the containers transportation process and the maritime sector are (see also table 1):

- International Maritime Organisation (IMO);
- International Labour Organisation (ILO);
- World Customs Organisation (WCO);
- International Standards Organisation (ISO)- ISO guidelines ISO/PAS 17712:2003 Freight containers – Mechanical seals; Radio Frequency Identification Tags (RFID) in conjunction with freight containers (ISO/WD 17363) as well as a draft standard outlining common communication protocols for RFID-enabled e-seals (ISO/DIS 18185);
- European Union (EU)- Maritime and port security;
- Secure Trade in APEC Region (STAR);
- United Nations Economic Commission for Europe (UN-ECE);
- Container Security Initiative (CSI);
- Customs-Trade Partnership against Terrorism (C-TPAT);
- 24 Hour Advance Manifest Rule;
- Bio-Terrorism Act;
- IEEE 802.11p and/or Cellular-V2X.

Table 1: Summary of current container security measures.

	Container scanning	Container integrity	Container environme	Container tracking	Container doc. and intelligenc
International (EU, US)					
IMO	x		x		x
ILO			x		x
WCO	x		x	x	x
ISO	x	x			
EU		x	x		x
APEC /STA R	x			x	x
UN-ECE/ TIR	x	x			x
UN-ECE	x	x	x		
CSI	x				
C-trap		x	x		x
24 hour rule	x				x
Bio-terrori sm act	x				x

Today many new and innovative technologies are not ready for commercial international deployment

throughout the transport chain, although some steps are being made in that direction (Masini et al. 2018). Generally, because of the incompatible operating standards and limited operational experience. In general terms, 100% of all containers can be scanned and screened in any given point (container terminals) using current policies and regulations.

2 OVERVIEW OF THE OPERATIONAL STRATEGIES

Similar security systems have already proven their direct value in many fields of operation. At present, companies all over the world are contemplating using it to benefit their business and overall processes to produce direct value for their customers while also improving operational performance in terms of cost, quality, security, speed, flexibility and optimal resource management (figure 2). Some of the new adoptions include e-seals and etc. An additional strategy element of operations was taken into account to improve the main strategy objectives by optimally utilizing the vast amount of direct and indirect resources that scattered within the transportation chain from the initial cargo to business processes. Optimality is ensured by operations strategies elements that include descriptors with inner resources reallocations. The additional benefit of the new developing key elements will use the known limited resources (e.g. time constraints, labour force) in advance to the IMS and control system by initial cargo transportation route planning in safer manner. Therefore, an additional operations strategy objective includes unnecessary business processes management and deals with the uncertainty about the effectiveness of basic operations strategy elements and their optimal usage. This optimum resource management mainly depends on availability of intermodal containers. It also ensures that once they are returned, they are redeployed as quickly as possible and never put to mixed use. This includes fast container turn around and ensures that containers are assigned to specific cargos are never put to mixed use. The additional optimum usage of quality elements will minimize the risks involved in data transfer within the security system. Additionally, currently applied Wireless sensor network (WSN) technology using active RFID tags include a variety of environmental monitoring capabilities such as the ability to track ambient temperature, vibration, radiation, to wirelessly collect information about containers inner environmental conditions. This could possibly introduce new opportunities to increase the intelligent container concept firstly proposed in the CSI. Concerning the legal framework to combat illicit nuclear trafficking, several major strategies exist. The legal definition of the acts committed during nuclear trafficking can be taken from the Conventions on the Physical Protection of Nuclear Material and for the Suppression of Acts of Nuclear Terrorism and include the unauthorized presence and unlawful possession and illegal disposal of nuclear material including the violation of the regulations for its obtainment, handling, and transportation.

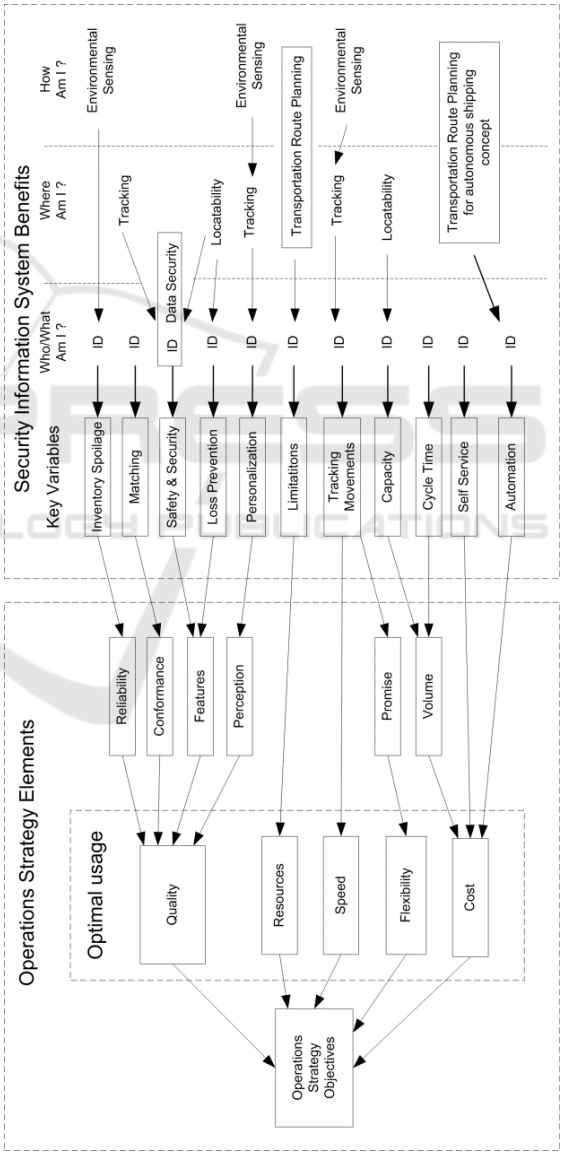

Figure 2: Proposed methods operations strategy framework.

The US favoured surveillance and monitoring techniques and advocated even a 100% scanning of shipments, but the EU took a data driven approach and fostered information exchange. A combination of both should guarantee continuity of knowledge, in particular of containers used in cargoes with suspicious routes. Since 2001-2002 inspections were made on a constant basis using various revisions, screening and monitoring technologies according to CSI, taking into account the 24-hour rule. Before any physical security inspection of the container, all the necessary information about the cargo is collected for containers targeting procedures during the unloading process. This is the first step of the security inspection. As an example, in the US the Automated Manifest System (AMS) offers information concerning the contents of the imported containers. Then the Automated Targeting System (ATS) computes the threat assessment of each container and makes decision support for the agencies and operators. Decision is done based on 300 weighted rules developed from the actual experience of Customs agents from screening and targeting containers. Identification of possible threat is done when a container is still on route. This is an „in advance security" method that provides the first general security measure before the actual container arrives to its final destination. Its information is used as a threat assessment tool for the IMS. When identification of containers with and without possible threats is finished, physical inspections are done. They are started with passive inspections followed by active inspections and manual inspections. In relation to current and proposed operations strategy elements improvement via optimisation, it is necessary to increase the effectiveness of operations speed in term of time of inspection. However, it must not have negative impact on the quality of operations via general security level and flexibility of procedures. Resources optimal dispersion over the transport chain should not be omitted as well, due to future autonomy increase.

3 ANALYSIS OF SECURITY ASSURANCE PROCEDURES

The baseline container flow within the transport chain is presented in figure 3. It is presented from the process view perspective. Such procedure was prevailing in most parts of the world, eliminating most security procedures. This container flow example is a general representation for most container flows in the world and up to 95% of containers arriving to the US borders. In reality, however, much lower container scanning and inspections are provided. In US, by the year 2002, of the more than 7 million containers, approximately 10% was inspected and scanned. In general in EU roughly 5% of all import containers are subject to an inspection (*Risk Analysis of Container Import Processes, Virtuele Haven; "Seacurity" Improving the Security of the Global Sea-Container Shipping System, Rand Europe*).

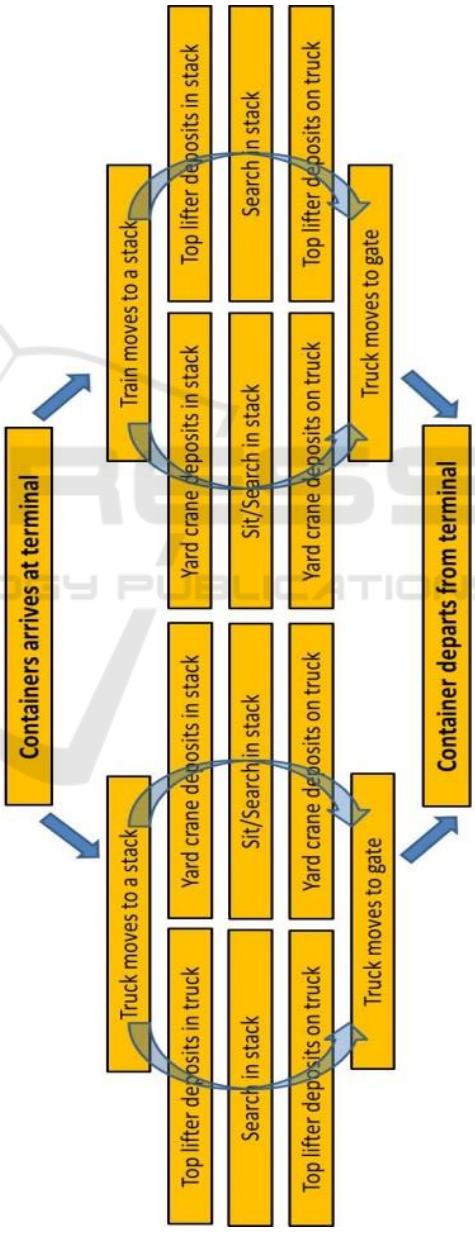

Figure 3: Baseline container flow without inspection procedures.

For the rest of the 5%, expensive security measures are applied, using technologies like huge X-Ray machines. However, they are very costly and their maintenance requires a certain degree of knowledge and certification and operator experience. Thus is not considered in many port of the world. This may also be due to lack of firm regulations from the local customs and other regulatory services. In general, such regulations are mostly omitted and only basic visual inspection policy is applied. In most cases, terrorist threat is considered relevant only when something happens in that region. In all other times, omission of some general rules is constantly present. It should be mentioned that all the decision are done manually transporting a 5% risk container to the inspection site and performing the inspection: non-intrusive (visual) and intrusive.

The following figure 4 presents the whole process of container turn-around in a container yard with all inspection policies and procedures currently used for incoming containers in the US (as an example). Final decision based on scan photography's is performed by a single operator. Therefore, its accuracy may prove to be faulty in some of the cases. In the case of radiation monitoring, same principle is applied. A top lifter is used to transport a pre-determined container to a check location and then same procedures using emission monitoring equipment. Operator is also responsible for the accurate perception of the received parameters. Many other regions of the world use same principles and from a near future perspective EU strategy will also include the application of the CSI objectives on a mandatory basis for all ports.

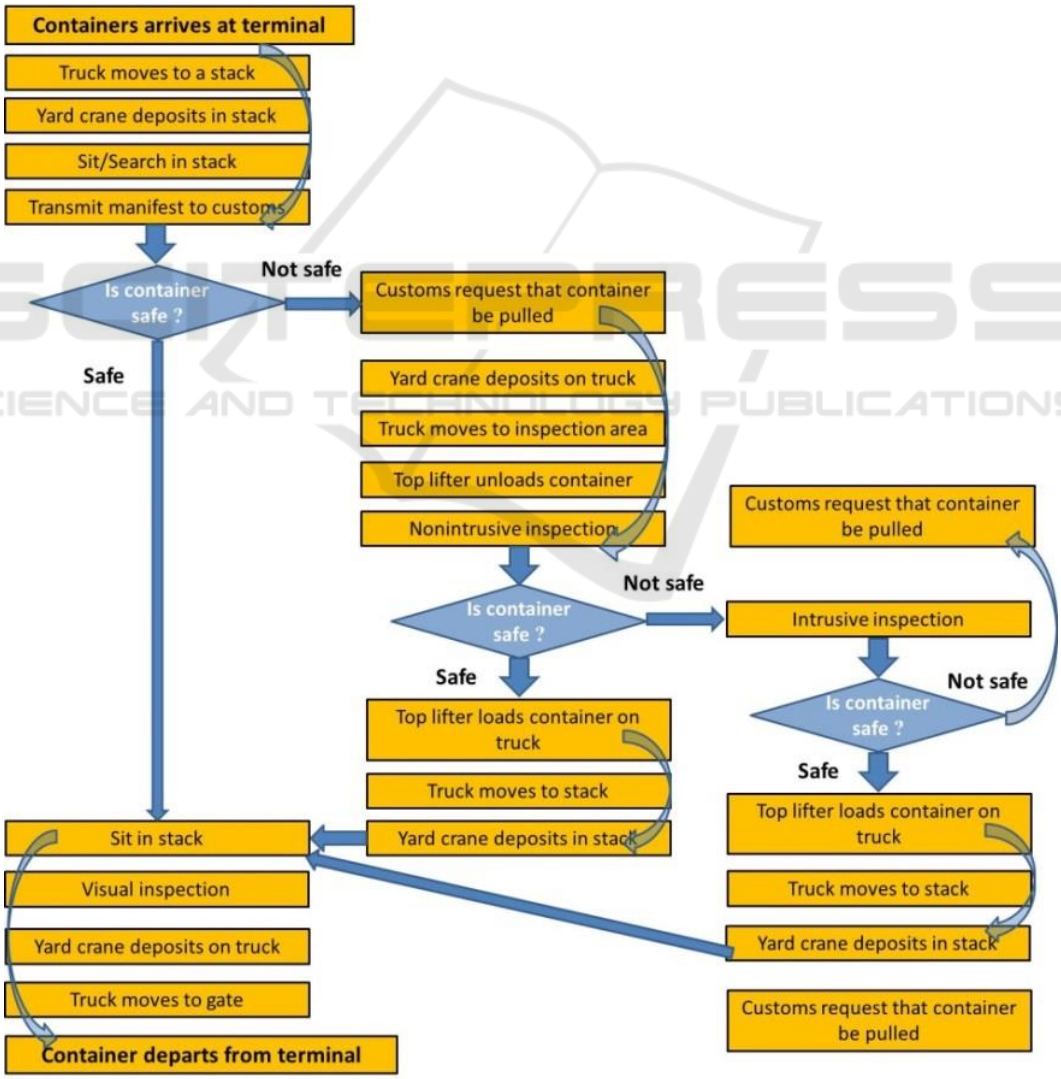

Figure 4: Casual inspection procedure according to CSI.

In figure 5 data acquisition algorithm is presented for the casual inspection procedure when all procedures are done.

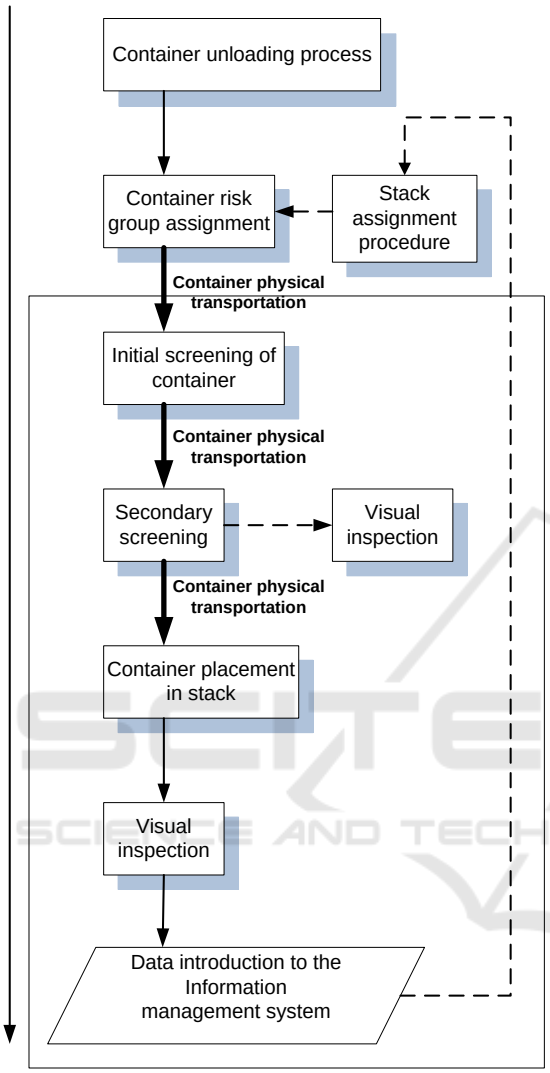

Figure 5: Security procedures.

As one may notice, during these procedures, vital information retrieval is done only after the final visual inspection procedure. Algorithm loop is made beginning with the initial screening of the container to demonstrate the containers rearrangement cycle. IMS is used only after the final revision procedures and its expert support functionality is not adopted at full scale. In many cases, data introduction to the information management system is done manually using human operators' onsite when a 100% screening policy is applied. ATS then collects this data for further container management. Was that data correct? It depends on the human experience level. Therefore, this link between external decision support systems and operators working onsite must be adopted in a new technological solution via intelligent container concept, previously proposed by the CSI. Only then, IMS and the supporting systems will bring the highly anticipated security level to the transport whole transport chain and will utilize the ATS at full scale.

In this case, a 3 stage container check is done to ensure the security at 100%. In other words, in order to obtain the vital security information in due time, statistical data introduction to the information management system must be done prior to the operator intervention to ensure security of the personnel in the vicinity of the stack and to minimize the response time, if such needed. Container risk group assignment procedure for the ATS is done at a new terminal after the previous container security check was performed and data was collected. Stack assignment procedure is casual for every case. It depends on the security threat and transportation timetable. Casualty must be changed with the new initiatives to stack each container accordingly with its level of security. As one may notice, many decisions, physical activities and procedures are still done by the operators on-site. This means that human errors are still likely to occur on a daily basis due to fatigue, concentration loss, harmful intentions and etc.

In case of the future terminal autonomy and shipping autonomy, these procedures must be eliminated and ATS system must be reconfigured. Nonintrusive inspection may vary between the applied systems for screening. Despite the fact that physical inspection of the contents of a container remains the most effective security measure, it is also one of the costliest and unsafe measures available to authorities. Although 100% physical inspection would be ideal in all situations, this remains an impossible goal given current trade volume and used standardised technologies. Information update rule applies to all incoming containers. Detection of threats and specific cargos is done in advance to eliminate unnecessary time for container introduction to the general inspection procedures to save transportation time. This could benefit the overflowing data streams within the organizations and minimize the risks of faulty information acquisition by the information management system when working without human interference. It must be done before the introduction to the stack, during the unloading procedure. On the other hand, intrusive inspection can only be performed by operators and the problem of false data interpretation and introduction to the containers management system

still exists. Both scenarios are ended in the same manner when each container is stored in terminal in a stack. Human interaction elimination and sufficient time resource optimisation can be achieved using remote and autonomous monitoring of the environment by each container individually. This security measure eliminates human visual inspection procedure from the process and transforms it into system inspection. It is safe to assume, that each container interaction with a human operator increases the risk level of the procedure in the whole conception of intelligent and autonomous container initiative.

4 CONCLUSIONS

Analytical research of resources and other study opportunities in container terminals all around Europe showed that existing container security screening equipment and procedures for intermodal cargo terminals does not assess the available ICT resources and their higher efficiency in solving the problems of terrorism. Attention is drawn to the lack of embedded cargo detection systems in the key parts of the transport chain. Particularly in the transportation of containers between several ports. It implies the presumption that only new technological components integration into a single ITC infrastructure is the only solution to achieve higher security level and to ensure the competitive position in the global market for separate larger and even smaller logistics companies. New containers revision and screening intelligent mechanisms must be developed for container terminals and can be integrated into the existing CSI concept.

Additional regulations, procedures and legal measures must be placed in case of possible detection with a high probability level. Therefore, a suggestion is made, that the adoption of new methods and their full integration, up to the working standards, is possible only when there is a certain degree of trust in the new technologies from all actors of the transport chain. For instance, new systems integration must be done in a step-by-step manner. It could be done locally in a single port for experimental reasons using single company's IT infrastructure for containers security investigation up to the working standards. This mixture could present practioners' with all the relevant adoption information that is now so crucial to the working environment of the entire transport chain operation. Disregarding the probability of ineffective usage of new methods may result in further stagnation in the area of new standard development within the CSI objective and could cause even further stagnation in the development of the intelligent container concept.

DISCLOSURE STATEMENT

Authors acknowledge that there is no financial interest or benefit arising from the direct applications of this research.

ACKNOWLEDGEMENTS

This research is/was funded by the European Regional Development Fund according to the supported activity 'Research Projects Implemented by World-class Researcher Groups' under Measure No. 01.2.2-LMT-K-718-01-0081.

REFERENCES

Scholliers, J., Permala, A., Toivonen, S., Salmela H., 2016. Improving the Security of Containers in Port Related Supply Chains. *Transportation Research Procedia*, vol. 14, p. 1374-1383.

CSI: Container Security Initiative. U.S. Customs and Border Protection, 2018.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 2013.

Mark S.S.H., 2019. Chapter 8: Perspectives on Security of Nuclear Material in Transport. *Nuclear Safeguards, Security, and Nonproliferation (Second Edition)*, p. 231-253.

Chung-Yee L., Dong-Ping S., 2017. Ocean container transport in global supply chains: Overview and research opportunities. *Transportation Research Part B: Methodological*, vol. 95, p. 442-474.

Rizzo, F., Barboni, M., Faggion, L., Azzalin, G., Sironi, M., 2011. Improved security for commercial container transports using an innovative active RFID system. *Journal of Network and Computer Applications*, vol. 34(3), p. 846-852.

Carlo, H.J., Vis, I.F.A., Roodbergen, K. J., 2014. Storage yard operations in container terminals: Literature overview, trends, and research directions. *European journal of Operations research*, vol. 235, p. 412-430.

Masini, B.M., Bazz, A., Zanella, A. 2018. A Survey on the Roadmap to Mandate on Board Connectivity and Enable V2V-Based Vehicular Sensor Networks, Sensors, vol. 19(7), p. 2207.

Xuerong, C., Jingzhen, L., Juan, L., Jianhang, L., Tingpei, H., Haihua, C., 2019. Improved Vehicle Ranging Method for the IEEE 802.11p. *Procedia Computer Science*, vol. 147, p. 389-393.