Kretschmann, Lutz; Münsterberg, Torsten

Conference Paper

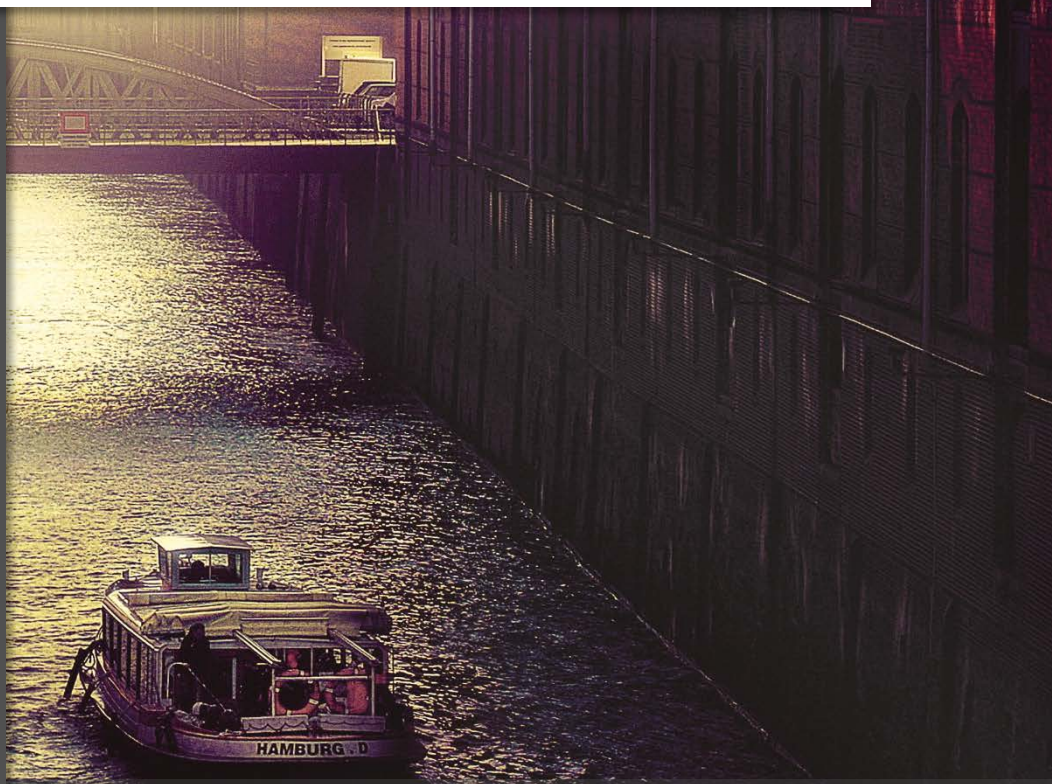
Simulation-framework for illicit-goods detection in large volume freight

Proceedings of the Hamburg International Conference of Logistics (HICL) – 23

Lutz Kretschmann, Torsten Münsterberg

Simulation-Framework for Illicit-Goods Detection in Large Volume Freight

HICL



Published in: Digitalization in Supply Chain Management and Logistics
Wolfgang Kersten, Thorsten Blecker and Christian M. Ringle (Eds.)
ISBN 9783745043280, Oktober 2017, epubli

Simulation-Framework for Illicit-Goods Detection in Large Volume Freight

Lutz Kretschmann[1], Torsten Münsterberg[1]

1 – Center für Maritime Logistik und Dienstleistungen (Fraunhofer CML)

Innovative non-intrusive inspection technologies can help customs prevent illicit trade in large volume freight. Validation whether technologies fulfill their intended purpose ideally takes place under real conditions. However, constraints limit the number and type of experiments performed during such field trials. Against this background simulation offers the opportunity to evaluate improvements in detection of illicit-goods without interrupting activities on site. A discrete event simulation framework in the context of large volume freight is introduced in this paper. It provides the means to compare alternative detection architectures - combinations of different detection technologies – regarding their effectiveness in identifying illicit goods in containers while at the same time the flow of goods through security checkpoints can be analyzed. The framework is applied to an exemplary case study comparing a single device detection architecture with a two device system. Results highlight the somewhat counter intuitive logic that adding a second device to the detection architecture either reduces the overall false clear probability at the cost of a higher false alarm rate or vice versa. Further the impact that adding another layer of detection has on the flow of containers through the detection architecture and in particular on process time is discussed. Findings described here are only a first step towards building a comprehensive simulation-framework for illicit-goods detection in large volume freight. Nonetheless, they illustrate how modelling and simulation can help customs identify the optimal use of innovative detection technologies to increase overall security at EU-borders.

Keywords: maritime security; illicit trade; detection architecture; discrete event simulation;

1 Introduction

Container transport has become an essential part of global supply chains and merchandise trade connecting Europe with markets around the world. Since ports play a key role within the European transport network, maintaining a high level of port efficiency is of great importance for continued economic prosperity throughout the EU.

Besides its integral role in the movement of legitimate cargo between countries intermodal container transport is also exploited in illegal trafficking activities (WCO, 2016). Table 1 shows the main categories of illicit trade as defined by Interpol (2014). The unlawful transport of illicit goods poses a threat to security, the environment and the economy. Container shipments are potentially misused in various ways including the movement of security sensitive goods like weapons, explosives or even radioactive materials as well as illegal trade in drugs, counterfeit products and environmentally sensitive goods which negatively affects citizens directly or indirectly. Moreover illegal trade is responsible for a loss of tax revenues, causes market distortion and can be associated with damages to the environment. For a discussion of negative socio-economic impacts of illicit trade see e.g. Hintsa and Mohanty (2014). Customs, as government organizations which control and administer the movement of goods across borders, play an important role in securing international supply chains by preventing illicit trade in large volume freight. Excluding intra-European trade the total number of containers imported to the EU in 2014 was 17.5 million TEU of which the vast majority is of legitimate nature (World Shipping Council, 2017). However, the sheer number of containers moved across EU borders highlights the challenge customs face in effectively preventing illicit trafficking without interfering unduly in the legitimate flow of goods. Contributing further to the difficulty of this task is the wide variety of risk materials that need to be detected both effectively and efficiently.

It is generally agreed that physically inspecting 100 percent of containers for illicit content is not practical. Instead detection technologies play an essential role for customs administrations to meet their responsibilities. Such non-intrusive inspection (NII) technologies enable a detection of possible anomalies within the container without having to open it.

At this point image based detection technology (X-ray) plays the central role in NII for most threats. However, several research projects currently underway will result in important advancements in NII technologies for checking maritime containers and other large volume freight for anomalies in port and at land borders (see e.g.

Table 1: The main categories of illicit trade

Main sectors of illicit trade
Illicit trade in chemical, biological, radiological, nuclear and explosive material
Illicit trade in arms and weapons
Illicit trade in narcotic drugs and psychotropic substances
Illicit trade in environmentally sensitive goods
Intellectual property crime
Pharmaceutical crime
Illicit trade in excisable products
Illicit trade in cultural property

ACXIS project, 2016; C-BORD project, 2017; CRIM-TRACK project, 2014). Through these initiatives a number of new and improved NII technologies will become available which customs can deploy at their respective border crossing sites in future.

As the number of principally suitable NII systems increases, identifying the optimal set of technologies for a particular border crossing gets ever more complex and thus challenging. More choices have to be evaluated under a specific set of requirements and constraints to identify which combination of technologies has the best cost to benefit ratio. In order to support this decision process, this paper introduces a discrete event simulation framework in the context of large volume freight. It enables customs to compare combinations of different NII technologies regarding their effectiveness and efficiency to detect illicit goods. At the same time logistical constraints at a particular border crossing point can be taken into consideration and the impact of new NII systems on the flow of container through security checkpoints can be analyzed.

The remainder of this paper is structured as follows. Section 2 introduces the term detection architecture and describes how the performance of a detection architecture can be described in terms of probabilities. Subsequently Section 3 gives an overview of different approaches in literature which analyze detection architectures in order to support their design. The developed simulation-framework for illicit-goods detection is introduced in Section 4 and applied to an exemplary case study in Section 5. Concluding remarks and possibilities for future research are given in Section 6.

2 Detection Architecture

Since customs face a wide variety of possible threats and NII technologies vary in their effectiveness of detecting different threats, ideally they are integrated in a detection architecture which makes sure that each technology is used according to its particular strength. The Customs Detection Technology Expert Group defines a detection architecture as "a construction of individual detection processes into a defined structure in order to determine whether a consignment is 'legitimate' or 'illicit"' (CDTEG, 2014).

In accordance with the WCO SAFE Framework of Standards detection architectures implemented by EU customs follow a risk based approach (WCO, 2012). This means that available information and intelligence relating to a cargo shipment is used to identify potentially high-risk containers in a first screening process. These high-risk containers are selected for one or more subsequent scanning processes where further information about the content of the container is collected e.g. by means of NII equipment. In case an anomaly is sustained based on scanning results the container is unpacked in a last step and the presence of illicit goods is checked by physical inspection. If a non-conformity is found the goods are stopped or otherwise released for further transport (see figure 1).

2.1 Objectives of Detection Architecture Design

When identifying a suitable detection architecture for a specific border crossing customs have to do justice to conflicting objectives. In the case a shipment is falsely cleared and thus a threat enters the country, society has to absorb the negative socio-economic effects associated herewith. Accordingly customs have to make sure certain acceptable detection thresholds for relevant threats are met.

In order to increase the likelihood of detection, one option would be to implement a more extensive screening, scanning and physical inspection regime (in effect inspecting a larger share of containers). Alternatively thresholds could be lowered beyond which the shipment is escalated to the next detection process instead of being released (in effect already a smaller suspicion leads to further inspection). However both will result in more disruptions to the flow of legitimate shipments and increase the number of cases where scanning indicates a threat that does not exist (false alarms).

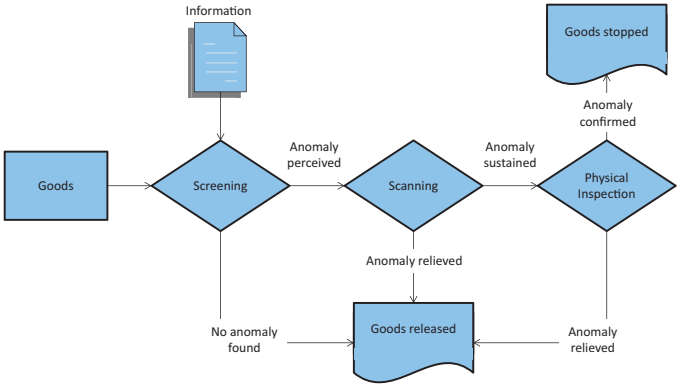


Figure 1: Detection architecture (CDTEG, 2014)

Any (unnecessary) inspection of legitimate cargo and in particular false alarms will be perceived as a nuisance by the parties involved in the transport chain. Moreover, ports with overlapping hinterlands stand in fierce competition for cargo with each other. If customs procedures in one port are extensive resulting in possible delays, generalized transport cost of moving good through this particular port will increase compared to other ports. This negatively affects the competitive position of the port and cargo is potentially shifted towards ports with lower standards (De Langen and Nijdam, 2008). Thus, customs have to maintain an appropriate level of security for one thing but also ensure that the impact of checking containers for illicit goods on the flow of freight is kept as low as possible.

2.2 Detection Capability of Detection Architectures

In order to describe the detection capability of individual scanning technologies as well as that of single or multiple-device detection architectures probability models can be used. In the simplest case an individual detection process can lead to two different outcomes: the presence of an anomaly in the container is sustained (alarm) or the presence of an anomaly in the container is relieved (clear). Following Kobza and Jacobson (1997) four possible cases have to be distinguished in this context (see figure 2).

To describe a devices capability of detecting a particular threat, probabilities of Type I and Type II errors can be used. The Type I error probability is the probability that a device raises an alarm under the condition that no threat is present in the container or P(Alarm|NoThreat). The Type II error probability on the other hand is the probability that a device does not raise an alarm under the condition

that a threat is present in the container or $P(NoAlarm|Threat)$. The lower both conditional probabilities are the better is the performance of the device.

Expected values of Type I and Type II error probabilities can be determined experimentally or, where test data is not sufficiently available, have to be estimated based on expert knowledge and information from system insiders (e.g. customs, technology providers).

The probability of a false alarm as well as the probability of a false clear is further influenced by the prevalence of non-conformities (probability that a threat is present in a container or $P(Threat)$) in the population that is being examined. Accordingly:

		Presence of threat	
		Yes	No
Response	Alarm	A true alarm – correctly detecting a threat within the container	A false alarm – detecting a threat within a container that does not exist
	Clear	A false clear – not detecting a threat within a container	A true clear – not detecting a threat within a container that does not exist

Figure 2: Possible results of detection process

$$P(FalseAlarm) = P(Alarm|NoThreat) * P(NoThreat)$$
$$P(FalseClear) = P(NoAlarm|Threat) * P(Threat)$$

Additionally a distinction between a device alarm and a system alarm is necessary for multiple device detection architectures:

— Case A – a system alarm is triggered if any device in the detection architecture raises an alarm

— Case B – a system alarm is triggered if all devices in the detection architecture raise an alarm

Probabilities of a false alarm respectively a false clear for a multiple device detection architecture under Case A and Case B are the combined conditional error probabilities of the individual devices.

3 Approaches for Analyzing Detection Architectures

Modelling and simulation methods increasingly gain acceptance in the overall security research landscape and particularly as effective tools for finding optimal detection architectures.

The primary use of discrete event simulation models, such as the simulation-framework for illicit-goods detection in large volume freight described in this paper, in this context is twofold:

— Simulate the detection performance of detection architectures

— Simulate the flow of goods through security checkpoints

Discrete event simulation can support the design process of adequate detection architectures by offering the opportunity to evaluate and assess improvements in detecting illicit goods without interrupting activities on site. Operational effectiveness, efficiency and detection performance of different system designs can be compared and analyzed according to the priorities and requirements at a specific border crossing. Moreover, as pointed out by Wilson (2005), the approach also allows determining the impact of different technology set ups on operation, logistics and cargo flow, identify bottlenecks and serves as a basis for specifying resources needed.

Several fields of research are relevant for the work presented in this paper which are briefly discussed in the following. Overall the interest in studying the design of detection architectures intensified significantly after the terrorist attacks of September 11, 2001 in New York (9/11). Understandably a large part of previous work deals with aviation and airport security as well as the detection of nuclear material smuggling as these are scenarios directly associated with terrorist threats.

Due to changes in aviation security after 9/11 explosive detection systems for 100 percent scanning of checked baggage were deployed at all US airports. Jacobson et al. (2006) apply probability modeling to evaluate the cost effectiveness of several single- and two-device explosive detection architectures at airports. While the work in this paper follows a similar approach to model the detection performance of detection architectures it focuses on a different transport system: sea ports and maritime container transport. Further it makes use of an event based simulation method which allows gaining insights into the dynamic performance of a detection architecture and thus reach a better understanding of bottlenecks and spikes in the workload

Comparable demands for a 100 percent scanning regime have also been enacted for containers entering US ports with the goal to prevent potential terrorist attacks on a port which would have devastating economic impacts (U.S. Congress, 2007). Several studies dedicated to 100 percent container scanning can be found in

literature. Martonosi et al. (2005) apply a cost-benefit analysis methodology in this context to compare different scanning regimes. They conclude that switching to 100 percent scanning is not cost-effective for most scenarios unless an attack is very likely to occur. Another example can be found in the work done by Bakshi et al. (2011) who develop a discrete event simulation model. They calibrate their model using historical data from two container terminals and assess the operational impact of different inspection policies. While their work focuses on 100 percent scanning and threats associated with terrorism there are some similarities with the simulation framework described here with regards to methodology and the modeling of detection processes. Further Bakshi et al. (2011) conclude that a "one-size-fits-all" approach does not work for all terminals. This underlines the need to develop a flexible simulation framework, as it is the case in this paper, which can be applied to the workflow at different border crossings.

Other scholars including e.g. Gaukler et al. (2012) and McLay and Dreiding (2012) apply operations research methods to the problem of detecting nuclear material in cargo containers in port. Gaukler et al. (2012) compare the existing inspection system for nuclear materials detection in containers with two alternatives which make use of radiography information to decide on the routing of containers through the detection architecture. They find systems which utilize additional information gained through X-ray to outperform the current approach for a wide range of scenarios. The work by McLay and Dreiding (2012) deals with identifying optimal strategies for escalating containers to a secondary scanning stage given multiple devices in the first stage such that the overall detection probability is maximized within certain budget constraints. In contrast to the research on linear programming in the context of container scanning this paper focusses on event simulation to analyze security issues and cargo screening problems.

Research comparable to this paper regarding the methodology applied – discrete event simulation - has been done by Siebers et al (2009). They describe a first approach to develop a cargo screening process simulator which enables customs to identify optimal technology set ups given certain commodity-threat combinations in order to maximize the likelihood to detect illicit cargo. In subsequent work the outlined concept is applied to a case study for cargo screening facilities in the Port of Calais (Siebers et al, 2011; Sherman et al., 2012). For a very specific threat - clandestines trying to cross the UK border hidden in lorries – they compare different methods for conducting a cost-benefit analysis one of which is discrete event simulation.

4 Simulation-framework

EU border crossing sites are characterized by unique conditions and face individual challenges. Logistical settings such as available space and the specific flow of containers at each border crossing is different. Further, illicit trade of goods is a dynamic field with constantly changing routes and adjustments in modality, quantities smuggled per load as well as concealment methods. Accordingly, customs deal with different types of threat scenarios in terms of a combination of legitimate cargo and illicit goods. Against this background, customs have to identify a detection architecture which best fulfills their specific needs and requirements while taking into consideration conflicting objectives (balancing security and the impairment of legitimate cargo flow) within given constraints regarding budget, capacity and available resources.

Considering the above, a systemic European solution how to make best use of innovative NII technologies to prevent illicit trade and smuggling must be adaptable to different types of borders and be able to take into account the local risk profile representing the flow of illicit goods and respective threats in one location. A one-size-fits-all solution or methodology cannot cope with this challenge.

The simulation-framework for illicit-goods detection in large volume freight presented in this section is supposed to be a flexible tool which can help customs configure the detection architecture and workflow concept for a specific border crossing point. Discrete event simulation provides a practical way to compare different technology set ups and combinations and analyze their respective detection performance. Further the approach makes it possible to determine how innovative NII technologies can be integrated best into the overall flow of containers through the detection architecture and evaluate important performance measures such as total lead times, waiting times experienced in the inspection process or NII system utilization. Thus, the simulation framework supports identifying economically and practically effective technology combinations and scanning sequences for a given threat profile at a certain border crossing and within specific local logistics and workflow requirements.

Any model is a simplified representation of a real world system. Accordingly certain assumptions are necessary to transfer the actual system into a simulation environment. In order to represent a detection architecture within the proposed simulation framework the following three elements are defined and transferred into the simulation model:

- Individual detection performance values for all detection processes
- Decision making logic linking individual detection processes
- Logistical process between individual detection processes

The detection performance value represents the probability that a particular technology will correctly identify different commodity-threat combinations or produce a false alarm. Within the simulation framework detection processes are modeled as “servers” with dedicated properties. Servers are predefined modules in the simulation software, which represent a generic process step. With regards to the detection performance of individual technologies the logic of probability models as introduced in Section 2 is applied. Accordingly an expected value of the probability that an alarm is raised although no threat is present and an expected value of the probability that no alarm is raised although a threat is present is defined. If several threats or commodity-threat combinations are to be modeled at the same time, respective detection performance values for different technologies can be integrated in a detection rate matrix as proposes by Siebers et al (2009).

The decision making logic between individual detection processes within the simulation framework determines the routing of objects (containers) through the model. In the simplest case a detection process has two possible outcomes: an alarm is raised or the object is cleared. The decision making logic defines the next step within the overall detection architecture for both outcomes. A more complex decision making logic is required in case a detection process has more than two possible outcomes (e.g. a high, medium or low detection sensor reading) or in case additional information (e.g. from manifest or previous scanning process) is taken into consideration to make a decision about the routing of the object through the detection architecture.

The logistical process between individual detection steps describes the flow of containers within the model. It includes all main logistical drivers of system performance. The following parameters are defined:

- The rate at which containers arrive over time
- The time it takes for an object to move from one server to the next
- The capacity of individual servers (number of objects which can be handled simultaneously)
- The time required for a server to complete a process

Probability distributions are used to characterize process and arrival times respectively. Additionally site specific logistical constraints and characteristics such as available space and the flow of containers at a particular border crossing can be considered accordingly.

5 Case Study

This section gives results for an exemplary case study comparing a single device detection architecture with a two device system by applying the proposed simulation-framework for large volume freight introduced in the previous Section 4. Different performance measures are calculated for each scenario in order to illustrate the tradeoff between reducing the overall false clear probability or reducing the false alarm rate in case a second device is added to the detection architecture. Additionally the logistical impact is highlighted by means of lead time (total inspection time), waiting times experienced and system utilization. In case the simulation framework is applied to an actual detection architecture both can support customs management in making an informed decision with regards to performance and cost factors.

The simulation framework is implemented in the discrete event simulation software Enterprise Dynamics by the company INCONTROL. This particular software was selected due to its high flexibility regarding nonstandard processes on the one hand and the comprehensive library of modules for standard processes on the other hand. Different simulation modules, like sources, queues, servers and sinks, are used to build up the detection architecture and, where necessary, amended with specific program code to match the desired process logic and behavior. Sources are the origin of containers entering the detection process. Queues represent waiting or storage areas, if for example containers line up in front of a scanning facility, because only one container can be scanned at a time. Servers take on the role of any time consuming process, like scanning, analyzing or transportation. Sinks are the final destination of containers after completing the detection process. Based on these modules detection architectures can be created and modified quickly. Results of simulation runs are exported to Microsoft Excel for a comprehensive analysis.

5.1 Design

X-ray imaging detection technology is the central component in almost all customs detection architectures (CDTEG, 2014). In the case study it is represented as “Scanning A”. Scenario A represents the single device detection architecture where only Scanning A is used. For the two device detection architecture in Scenario B and Scenario C, X-ray is complemented with another detection device “Scanning B”. Due to logistical reasons (lower process time) Scanning B takes place previous to Scanning A. Naturally other arrangements are possible. The corresponding decision making logic between individual detection processes for all three detection architectures is shown in figure 3.

All three scenarios are analyzed for a hypothetical border crossing point with a simulation run having a time horizon of five years. The process of screening is not modeled explicitly. It is assumed that containers entering the system had previously been selected as high-risk and thus forwarded to further scanning. Only one type of threat is considered. Scanning results of each detection process are based on the true classification (threat/no threat) of the container. Alarm respectively clear probabilities are calculated as introduced in Section 2. Individual device responses are assumed to be independent.

The actual share of containers arriving in a given port that contain a threat is highly sensitive information. The same applies to detection performance values of individual NII technologies. Conditional probabilities used in this calculation are partially estimated based on discussions with customs organizations. Because of the sensitive nature of some of the data used in the simulation the values itself are not reported. For a validation results and behavior of the simulated system were compared with available customs data. A further refinement of the model is foreseen once customs feedback on simulation results becomes available.

It is not the intention of the case study to calculate the exact detection performance. Rather results of the case study are supposed to illustrate the general behavior of single compared to multiple device detection architectures. For this purpose Scanning A is assumed to produce a higher rate of false alarms compared to Scanning B. Scanning B on the other hand is assumed to produce a higher rate of false clears compared to Scanning A. Physical inspection is considered to be 100 percent successful in detecting illicit goods.

About 250 000 container enter the detection architecture during each simulation run. The arrival time is characterized by a negative-exponential probability distri-

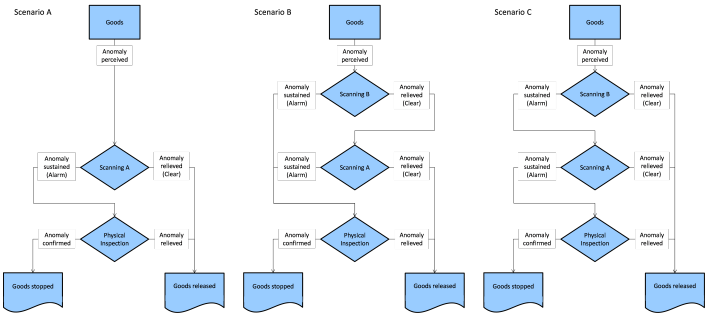


Figure 3: Detection architectures considered in case study

bution. During nighttime the arrival rate is lower by the factor of ten. Process-time distributions of individual servers in the model are approximated based on system insider judgements about average, maximum and minimum process time and as well as observations made at border crossing points. The capacity of individual servers (number of objects which can be handled simultaneously) assigned to Scanning A and physical inspection is defined in a way that waiting times during the day are the exception. For Scenario B and Scenario C the capacity assigned to Scanning A and physical inspection is not changed. Scanning B capacity, again, is defined in a way that waiting times at associated servers are the exception. Several different performance measures are calculated for each scenario:

- Number of false clears
- Share of containers sent to physical inspection
- Time containers spend in the detection architecture
- Utilization rate of physical inspection resources

5.2 Results

Table 2 shows important results of the simulation experiments for the three considered scenarios. The results are given as relative values compared to Scenario A. Accordingly, Scenario A has a value of 1 for all three key indicators.

Table 2: Results of case study

	Scenario		
	A	B	C
Number of false clears[1]	1.00	0.62	12.20
Number of false alarms[1]	1.00	1.47	0.02
Physical inspections[1]	1.00	1.39	0.09

1 - relative to Scenario A

The results underline the previously described effect that adding a second device to the detection architecture either reduces the overall false clear probability at the cost of a higher false alarm rate or vice versa. In Scenario B, where any device alarm results in a physical inspection, the number of false clears is reduced by 38 percent on the one hand, but on the other hand the number of false alarms increases by 47 percent. Further the number of physical inspections increases as well compared to Scenario A (plus 39 percent).

The reverse effect can be observed for Scenario C where any device clear results in goods being released. The number of false alarms is reduced significantly compared to Scenario A and the demand for physical inspections declines in the same order of magnitude. However, at the same time the number of false clears increases by a factor of 12 compared to the level calculated for Scenario A.

Accordingly, adding a second device to the detection architecture is associated with a benefit in terms of reduced false clears or reduced false alarms. However, it always comes with the price of increasing the other figure respectively.

The lead time of containers passing through the system for all considered scenarios is illustrated in figure 4. The boxplot shows the distribution of lead times per container. The lower whisker indicates the 2.5 percent quantile, the upper whiskers marks the 97.5 percent quantile. Values given in the figure represent the time a freight forwarder can expect the overall inspection process to take, once the container has arrived at the location where inspections take place. Adding a second scanning device to the detection architecture increases the median lead time in Scenario B (53 min) compared to Scenario A (31 min) because a larger share of containers undergoes physical inspection. On the other hand median lead times in Scenario C (28 min) are less than in Scenario A since Scanning B has

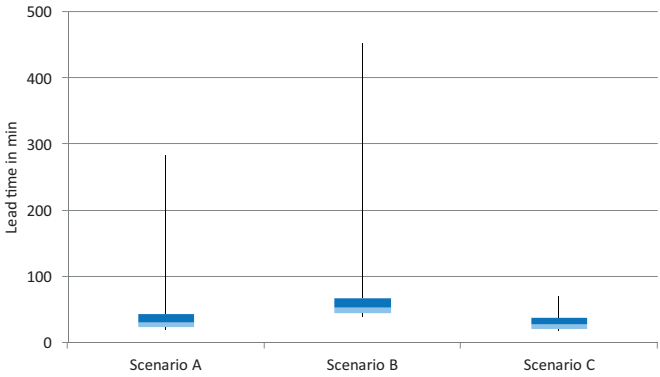


Figure 4: Lead time for all containers

a shorter process time than Scanning A and a more containers are released after the first scanning process.

The distribution of lead times shows a positive skew in all three scenarios. The reason for particular long lead times is the physical inspection process. The dispersion of lead times is highest in Scenario B where a large share of containers undergoes physical inspection and, in addition, containers experience waiting times where the physical inspection capacity is fully utilized. In contrast, Scenario C is characterized by smaller deviations in lead time compared to Scenario A and Scenario B.

Subsequently lead times for containers which did respectively did not go through physical inspection are discussed in detail.

Figure 5 contains a boxplot only for those containers which were subject to physical inspection. The median lead time for these containers is 275 min in Scenario A, 334 min in Scenario B and 288 min in Scenario C. The difference between Scenario A and Scenario C is approximately the time required for Scanning B. In Scenario B the median of 334 min is already affected by the increased number of cases that experience waiting times due to full utilization of physical inspection capacity. Of course this effect could be reduced by an extension of the physical inspection

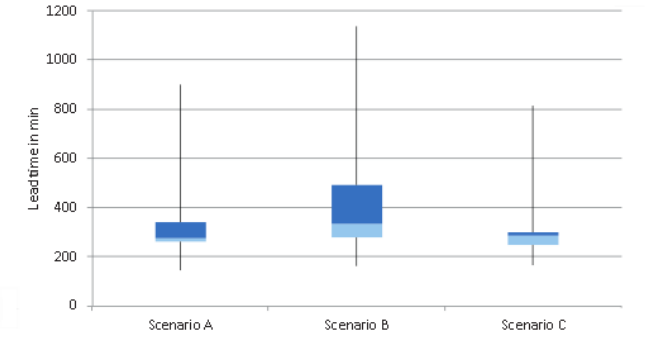


Figure 5: Lead time for containers that went through physical inspection

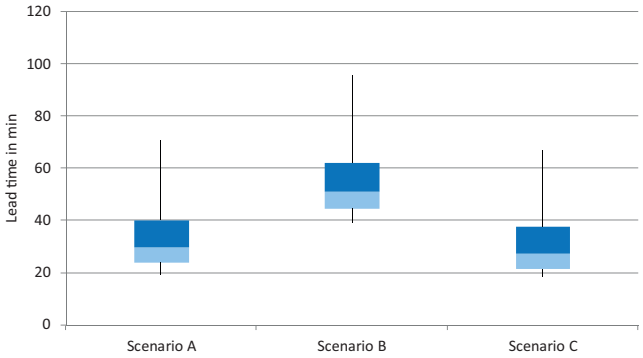


Figure 6: Lead time for containers that did not go through physical inspection

facilities. The high values of the 97.5 quantile in Scenario A and Scenario B (900 min and 1140 min) are a combination of waiting times for physical inspection and a long physical inspection process itself which occurs for some containers. The latter effect also explains the position of the 97.5 percent quantile in Scenario C. It is lower than in the other scenarios though since fewer containers undergo physical inspection in Scenario C and accordingly it is less likely for a container to experience waiting time prior to physical inspection.

If only the lead time of containers that did not go through physical inspections are analyzed, the results look somewhat different (see figure 6). The median lead time per container is shorter with 30 min in Scenario A, 51 min in Scenario B and 28 min in Scenario C. The difference of approximately 20 min between Scenario A and Scenario B corresponds to the process time of Scanning B plus waiting time experienced by some of the containers. Lead times on the upper bound (97.5 percent quantile) in Scenario A and Scenario C are around 70 min and 95 min.

The different detection system architectures designs also have a large effect on the utilization of individual system components and in particular on the utilization of the physical inspection process. In the base case, Scenario A, the median of

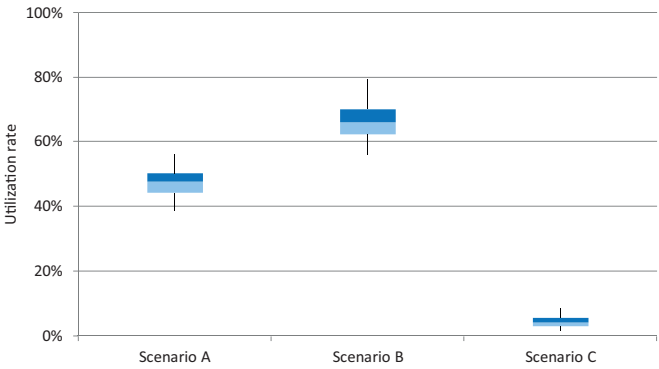


Figure 7: Average utilization rate of physical inspection per month

the average utilization rate per month at the physical inspection facilities is 48 percent (see figure 7). This is relatively high considering that the majority of the containers arrive during daytime and only few during night. As discussed before, the facilities for physical inspection are in little use in Scenario C where the median utilization rate is 4 percent. In Scenario B, on the other hand, the overall number of physical inspections is high. Consequently the utilization rate of the physical inspection facilities goes up and containers frequently experience waiting times. This increases costs either in terms of higher generalized transport costs or due to an extension of the physical inspection capacity to reduce waiting times. On the other hand the number of false negatives is lower in Scenario B which represents a comparative benefit. Fewer shipments are falsely cleared, thus the cost which society has to absorb in terms of negative socio-economic effects associated with illicit trade is reduced. This underlines that comparing the cost to benefit ratio of different detection architectures can be a suitable basis for decisions by customs management and policy makers.

6 Conclusion

Overall the role of maritime container trade in the transportation of illegal goods across borders is characterized by a comparatively low number of seizures but generally larger consignments of illicit goods than in other transport modes (see e.g. WCO, 2016). At the same time scholars have highlighted the potentially devastating impact that terrorist attacks could have in the maritime context overall and associated with maritime container transport in particular (see e.g. Greenberg et al., 2006; Schneider, 2011). Both emphasizes the importance of constantly improving detection architectures and thus effectively and efficiently preventing illicit trade while facilitating free flow of legitimate cargo across EU-borders.

This paper introduces a simulation-framework for illicit-goods detection in large volume freight. The framework represents an effective and flexible tool for customs to analyze different NII technology set ups - detection architectures – against their requirements without interrupting activities at a border crossing point. At the same time the applied method, discrete event simulation, provides the means to take logistical settings such as available space and the specific flow of containers into account and analyze important performance indicators such as average inspection times but also its variation e.g. expressed by inspection times in the upper quartile.

An illustrative case study demonstrated how a detection architecture can be analyzed with the simulation-framework. It compared a single device detection architecture with two variants of a two device architecture regarding the overall detection performance. Results show that by adding a second device to the detection architecture it is not possible to increase the relative chance to detect a threat (lower probability of false clears) and reduce the share of containers which unnecessarily undergo physical inspection (lower probability of false alarms) at the same time. It was demonstrated that a multi device detection architecture where any device alarm results in physical inspection will reduce the probability of false clears while a detection architecture where any device clear results in goods being released will reduce the probability of false alarms compared to the single device architecture.

Furthermore the impact of adding a second device on lead times and capacity utilization was shown in the case study. A multi device detection architecture does not inevitably mean that lead times increase. Whether they do or not depends on the logical structure of the detection architecture. The same applies for the utilization rate of e.g. the physical inspection resources which can either increase

or decrease compared to the single device architecture depending on the logic linking individual detection processes.

Findings described here are only a first step towards building a comprehensive simulation-framework for illicit-goods detection in large volume freight. There are several possible extensions to this work. A first extension is to implement different types of threats and specific capabilities of technologies to detect these threats in the model in order to analyze the full range of illicit trade customs deal with. A second extension is to consider information gained in one scanning process in the decision how the container is routed through subsequent scanning devices. This implicates a more complex decision making logic linking individual detection processes which might also take into account the current utilization of NII scanning equipment and physical inspection stations to reduce waiting times during peaks. A third extension is to quantify direct and indirect cost associated with different detection outcomes (true alarm, false alarm, false clear, true clear), the detection process itself as well as increases of generalized transport cost due to potential delays. This way changes in different cost factors could be weighed against each other, adopting the concept of cost-benefit analysis, to provide a more comprehensive basis for customs management and policy makers to take informed decisions. Work is in progress to address these extensions.

Financial Disclosure

This work has received funding from the European Union's Horizon 2020 research and innovation programme, under grant agreement No 653323. This text reflects only the author's views and the Commission is not liable for any use that may be made of the information contained therein.

References

Acxis project (2016). *ACXIS Automated Comparison of X-ray Images for cargo Scanning*.
Bakshi, N., S. E. Flynn, and N. Gans (2011). "Estimating the Operational Impact of Container Inspections at International Ports". In: *Management Science* 57.1, pp. 1–20.
C-BORD project (2017). *Effective Container Inspection at BORDer Control Points*. www.cbord-h2020.eu.
CDTEG (2014). *Detection Architecture*. Brussels.
CRIM-TRACK project (2014). *CRIM-TRACK*. www.crimtrack.eu.

Gaukler, G. M., C. Li, Y. Ding, and S. S. Chirayath (2012). "Detecting Nuclear Materials Smuggling: Performance Evaluation of Container Inspection Policies". In: *Risk Analysis* 32.3, pp. 531–554.
Greenberg, M. D., P. Chalk, H. H. Willis, I. Khilko, and D. S. Ortiz (2006). *Maritime Terrorism: Risk and Liability*. Santa Monica, CA: RAND Corporation.
Hintsa, J. and S. Mohanty (2014). "A Literature-Based Qualitative Framework for Assessment of Socio-Economic Negative Impacts of Common Illicit Cross-border Freight Logistics Flows". In: *Innovative Methods in Logistics and Supply Chain Management: Current Issues and Emerging Practices*. Ed. by T. Becker, W. Kersten, and C. M. Ringle. Berlin: epubli, pp. 319–340.
INTERPOL (2014). *Countering Illicit Trade in Goods: A Guide for Policy-Makers*. Lyon.
Jacobson, S. H., T. Karnani, J. E. Kobza, and L. Ritchie (2006). "A Cost-Benefit Analysis of Alternative Device Configurations for Aviation-Checked Baggage Security Screening". In: *Risk Analysis* 26.2, pp. 297–310.
Kobza, J. E. and S. H. Jacobson (1997). "Probability models for access security system architectures". In: *Journal of the Operational Research Society* 48.3, pp. 255–263.
Langen, P. W. d. and M. N. Nijdam (2007). "Charging Systems for Waste Reception Facilities in Ports and the Level Playing Field: A Case from North-West Europe". In: *Coastal Management* 36.1, pp. 109–124.
Martonosi, S. E., D. S. Ortiz, and H. H. Willis (2005). "Evaluating the viability of 100 per cent container inspection at America's ports". In: *The Economic Impacts of Terrorist Attacks*. Ed. by H. W. Richardson, P. Gordon, and J. E. Moore II. Cheltenham: Edward Elgar Publishing, pp. 218–241.
McLay, L. A. and R. Dreiding (2012). "Multilevel, threshold-based policies for cargo container security screening systems". In: *European Journal of Operational Research* 220.2, pp. 522–529.
Schneider, P. (2011). *Maritimer Terrorismus: Tätergruppen und Anschlagstypen 1968 – 2010. PiraT Arbeitspapier zur Maritimen Sicherheit Nr. 13.* Hamburg.
Sherman, G., P.-O. Siebers, D. Menachof, and U. Aickelin (2012). "Evaluating Different Cost-Benefit Analysis Methods for Port Security Operations". In: *Decision Making in Service Industries: A Practical Approach*. Ed. by J. Faulin, A. A. Juan, S. E. Grasman, and M. J. Fry. Boca Raton, FL: CRC Press, pp. 279–303.
Siebers, P.-O., U. Aickelin, and G. Sherman (2009). "Development of a Cargo Screening Process Simulator: A First Approach". In: *21st European Modeling and Simulation Symposium (EMSS 2009), Volume I*. Ed. by R. M. Aguilar, A. G. Bruzzone, and M. A. Piera.
Siebers, P.-O., G. Sherman, U. Aickelin, and D. Menachof (2011). "Comparing Decision Support Tools for Cargo Screening Processes". In: *The 10th International Conference on Modeling and Applied Simulation (MAS 2011)*. Ed. by A. Bruzzone, C. Frydman, M. Massei, M. McGinnis, M. A. Piera, and G. Zacharewicz.
U.S. Congress (n.d.). *H.R.1: Implementing recommendations of the 9/11 commission act of 2007: Pub. L. No. 110-53, 110th Congress*.
Wilson, D. (2005). "Use of modeling and simulation to support airport security". In: *IEEE Aerospace and Electronic Systems Magazine* 20.8, pp. 3–6.
World Customs Organization (2012). *SAFE Framework of Standards to Secure and Facilitate Global Trade*. Brussels.
World Customs Organization (2016). *Illicit Trade Report 2015*. Brussels.
World Shipping Council (2017). *Trade Statistics*.