Simulation in Produktion und Logistik
Entscheidungsunterstützung von der Planung bis zur Steuerung
Wilhelm Dangelmaier, Christoph Laroque & Alexander Klaas (Hrsg.)
Paderborn, HNI-Verlagsschriftenreihe 2013

Simulation of a Logistics Network to Import Goods with Unknown Risk to Increase the Security in the Supply Chain

Simulation eines Logistik-Netzwerks zum Import von Gütern mit unbekanntem Risiko zur Stärkung der Sicherheit in der Supply Chain

Bernd Hellingrath, Carsten Böhle, Michael Middelhoff, Westfälische-Wilhelms Universität Münster, Münster (Germany), hellingrath@ercis.uni-muenster.de, carsten.boehle@wi.uni-muenster.de, michael.middelhoff@wi.uni-muenster.de

Abstract: The simulation model used in this paper compares potential setups of processes and screening devices for the identification of threats like weapons or explosives hidden in physical shipments transported by a logistics service provider (LSP). The model specifically addresses the problem of uncertainties in the occurrence and identification of threats considering type 1 and type 2 error probabilities. Scenarios varying in their use of buffers and screening technology are evaluated towards their resource occupation and resulting threat identification rates. The presented model is able to compute reliable results under uncertainty in threat occurrences and reveals influences on the behaviour of multi-tiered screening systems.

1 Introduction

The amount of goods imported into Germany accounts for up to 90 billion euros every month (Statistisches Bundesamt 2013). From the annual report of the Federal Customs Administration of the Federal Ministry of Finance one can quote that in 2011 about 30,000kg of drugs have been imported and discovered in the overall import of Germany (Bundesministerium der Finanzen 2012). In comparison to prior years this accounts for an increase of over 10%, not considering the possible unknown cases. Also, an increase in weapons and ammunition has been recoded. Likewise, a study organized in 2012 by the World Customs Organization targeted at drug trafficking via mail and express channels (Operation SKY-NET) lists 9.5 tonnes of different drugs that were sent in more than 941 parcels. The study lasted 19 days and was supported by 68 member countries (World Customs Organization 2012).

International trade and globally traveling passengers open up a variety of vulnerabilities for civil security. Each shipped item via logistics service providers

(LSP) and every passenger entering the country via air, land or sea might be a source of danger. This issue has been known since decades and especially considered in air travel and cargo transport. Considering these various possible points of entry into a country, one of the most important difficulties in securing civil security is the enormous amount of shipments and passengers each day. This results in huge uncertainties on threat occurrences and creates the need to find efficient and effective means to verify the security of incoming goods and people from outside the country.

Objects of interest to the presented approach are arbitrary physical goods which are imported by an LSP and might contain hidden threats. LSPs are considered as active agents, who implement security measures (here screening technologies) to protect civil security. At the same time they are also part of the infrastructure at risk. The LSPs have an own interest to protect their facilities, employees and customers, motivating investments in improved security means. The threats considered in this paper are dugs, weapons, radioactive matter and explosives. To protect the population from these illegal imports, different screening technologies next to handing over shipments to authorities, which are allowed to perform a physical inspection by opening shipments, can be used, that leave the item unopened and undamaged. Examples are imaging technologies like X-ray or molecule analysis with ion-mobility-spectroscopy. Providing security comes at high costs for the installation and operation of screening devices and time required for screening. For a cost driven LSP this leads to a conflict between cost minimal operations, the provided service level and the security level. Further, complex multi-tiered screening systems are influenced by dynamics like variations in the workload caused by arrival times and schedules. For an analysis of these factors it is reasonable to analyse the system behaviour in different scenarios using a simulation study. According to the guideline VDI 3633 of the Association of German Engineers, it is suitable to use simulation to analyse non-existing systems under high uncertainty, given in the unknown distribution of threat occurrences (Verein Deutscher Ingenieure 2000). Considering process durations influenced by waiting times and probabilistic routing decisions in a multi-tiered setup results in complex interdependencies, which can be observed using simulation (Rabe and Hellingrath 2001).

In this paper we present a simulation model of an import hub in a national network of an LSP. The hub is supplied with imports from outside Europe. Different scenarios observe the system's behaviour under varying process configurations and installed technology. Shipments are filtered according to a prior risk assessment. First, section 2 introduces related studies of similar multi-tiered screening systems. Section 3 introduces the context of the LSP and lays out general conditions the simulation is based on. After this, section 4 gives details on the simulation model, explains underlying assumptions and describes the screening technologies. The different scenarios and results are presented in section 5. Finally, section 6 summarises the findings and gives an outlook on the further development and open research questions.

2 Aviation Security Screening

A variety of related studies is published in the context of aviation security. This is driven by the historical evolution of protecting civil security from terrorist activities like the attack on the World Trade Centre in the USA on September 11, 2001. Sewell et al. recently presented a mathematical security screening device allocation model for optimal allocations of aviation security screening devices across a set of airports (2013). They show that the problem is mathematically solvable under time and budget conditions including a passenger pre-screening to assign passengers to groups of a perceived risk level. Each group is assigned with a specific screening program, which the passengers have to undergo to get cleared for boarding. The importance of a risk-based assessment of passengers and an according screening plan for each group is especially stressed by Butler and Poole (2002). They compare different screening technologies and argue on the high amount of passengers and low capacities of screening devices. Following their argument, a prior risk assessment and group specific screening resource assignment is crucial to address the amount of passengers. In aviation security, the allocation of screening devices and a risk based grouping is widely used to develop effective and efficient screening models (Nie et al. 2009; Sewell et al. 2002). Earlier, Kobza and Jacobson showed the effectiveness of multiple-device systems compared to single-device systems and the importance of error probabilities of type 1 (false positive) and type 2 (false negative) in general access security systems (1997). No approach has been found that is able to take the dynamics of the screening process into consideration. Due to the high number of items and the huge uncertainty, some dynamic characteristics will become important, e.g. arrival times and the resulting fluctuations in workload. Further, none of the approaches considered a dynamic screening based on the item information and the current system state. The situation in the logistics context is also different from aviation in so far as private data might be concerned, which is particularly protected for certain shipments and cannot be used for pre-screening.

3 Problem Statement

The model is loosely based on a real world case of a logistics company importing large amounts of shipments from various countries into Germany. Criminals and terrorists try to ship drugs, explosives, weapons or radioactive material via the LSP by abusing its service. Considering the total amount of shipments, the cases of items actually containing threats can be seen as very low. To address the high uncertainty of threat occurrences, an assumed threat distribution over countries of origin was defined. Based on the long term experience of the LSP, the developed distribution is structured as follows. Each origin is assigned with a general threat probability and conditional probabilities determining the chance by which a specific threat is present. The origins are divided into three categories of secure (5% of all origins), dangerous (5%) and medium risk countries (90%). Countries known to be secure have low general threat probabilities (~1%), whereas the majority of countries have medium (~5%) and dangerous countries relatively high probabilities (~10%). An example is the USA, which are considered to deliver secure shipments, leading to a low general threat likeliness of about 1%. The distribution of threats is 60% drugs, 10% explosives, 5% radioactive matter and 25% weapons.

The import hubs receive different amounts of shipments via air and land transport during the day, sorts them according to their destinations and finally directs them into the national network, which is omitted here. Potential threats are supposed to be detected at the point of entry in the network. The LSP is not informed about single items before they arrive, so prior filtering based on information is not possible. Therefore, the risk of a single item can first be assessed once the item has been received in an inbound gateway and the relevant information like the origin is recorded. The risk assessment will create a risk profile for each item based on the presumed threat distribution of the country of origin and additional know-how in assessing visible indications. It is not supposed to analyse any personal information such as names and addresses of the sender and the receiver. It will specify for an item the likeliness for each of the threats. Based on the risk profile, items are routed individually through the screening devices in case a multi-tiered screening setup is installed. Screening technologies are characterized by their ability to detect certain threats (cf. Table 1). They are assigned with type 1 errors, the likeliness of false threat detection, and type 2 errors, the likeliness of false clearance, for each of the threats. This influences the routing of each item and the capacity utilization of screening devices. The set of available technologies consists of X-ray, terahertz spectroscopy (THz) and ion-mobility-spectroscopy (IMS). These have been selected, because they are candidates to be implemented at the hub and are different in their mode of operation, required time, and detection quality, but also costs for acquisition and operation. Detailed information on the screening technologies is given in the next section.

4 Model Definition

Based on the problem we created a discrete event-simulation model, which represents the screening setup from receiving the item until passing it on to sorting, i.e. assuming that there is no threat, or physical inspection. Each physical shipment is observed as a distinct item. The model is reduced to one hub location as all hubs in the network of the LSP share the same setup and processes. By omitting the internal network procedures, there are further no interdependencies among the hubs. The model starts with the creation of items according to a fixed plan, describing the amount of shipments routed to the hub for each day over one year. From an initially defined general threat distribution by origin, a specific threat from the four categories is drawn by chance. This distribution is constant and simulates the threat likeliness unknown in reality.

After the items are routed to the hub, they are processed by a risk assessment function, which will probabilistically ascribe a risk based on the presumed threat distribution of the origin. Additionally, the risk assessment makes use of further individual item information. It is assumed that information like size, weight and declared content can be evaluated to assess the risk. As this information is not part of the model, it is replaced by a probability to identify an occurred threat. This is uniformly distributed between 1% and 13%. That means, any parcel has a basic threat level depending on its origin, and in case it actually does represent a harmful item, the threat level is additionally increased. As a result, a harmful parcel from a dangerous country (10% threat likeliness) is at most considered to be risky with a probability of 26%. This low number is justified by the scarce information available to assess the risk. Since high risk items therefore would mostly not be sent to screening, the assessed risk is additionally scaled up to 100% likeliness to be selected for screening. The highest threat level of 26% is consequently always routed to screening in case of item-level risk assessment. An overview of the simulation model is given in figure 1.

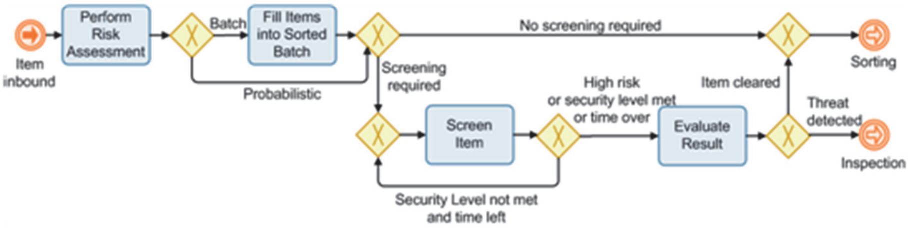

Figure 1: *Overview of Simulation Model Sequence*

Depending on the created risk profile, each item is then routed through the available screening devices, considering error probabilities of false positives and false negatives. Routing decisions are based on the current most likely threat of an item and the detection capabilities of devices. The model defines a screening accuracy of 90% as termination criterion for the screening. This causes items to pass screenings until the presumed risk for each of the four threats falls below 10% or one of the risks increases to over 90%. Screening technologies influence the item's risk values based on their error probabilities. The lower the error probability, the stronger is the increase or decrease of the risk values, since the result is more reliable. Thereby the most likely threat might change over time. Additionally, each item has to be processed at the day of arrival in order to maintain service quality. The maximum processing time is therefore 24 hours. Items are ascribed to contain a threat, if at least one of the screening devices has detected it and the risk value for this threat is above the security level of 90%. In case a threat is detected, the item is sorted out for further physical inspection by authorities. Secure items proceed in the regular sorting process of the LSP. If an item has not reached 90% accuracy and there is no time left, it will be cleared and no further screening is performed. This increases the influence of dynamics like schedules and arrival times.

The model does not evaluate cost factors of the screening system in the scenarios. It can be assumed that increased effort will also increase the cost of a given configuration. In case of successfully introduced threats into the supply chain, there are not clear economic losses available. Considering that for instance explosive devices put several human lives at risk and imported drugs cause severe socio-economical costs, it is very difficult to relate the system costs to the prevented damage. Therefore, it is more suitable to argue on the percentage of prevented threat instances. The cost estimation is thereby only a limitation of investments. Due to the huge uncertainty, the model does not address an optimization of the effort-to-cost relation, as related mathematical models do. It rather seeks to analyse dynamic components and in later studies intelligent attackers.

4.1 Assumptions

To reduce model complexity to the most important influences, it is based on assumptions which address the occurrence of threats and the application of screening technologies as well as their evaluation. 1) Each shipped item can contain at most one threat. Driven by the experience of the LSP, it is very unlikely that a mixture of threat categories is contained in one item. 2) No dependencies exist between screening technologies or multiple executions of the same technology. Previous screening results might improve further screenings due to combined information, which his omitted in the model 3) The quality of the screening is independent of the single object. The model does not differentiate physical properties of items, which might influence threat detection probabilities.

4.2 Screening Technologies

This section shortly introduces the screening technologies, which are used in the model. The technologies are outlined by their screening procedure and characterized with error probabilities for the threat types. Roentgen radiation or X-ray is a well-researched technology, which makes use of the property that radiation is penetrating matter in different strengths. By analysing the amount of radiation, which was able to pass through an object, it is possible to infer the materials beneath surfaces. Analysing hidden outlines of objects and matter density allows concluding on threats. Terahertz spectroscopy (THz) also makes use of matter’s property to react differently to radiation. THz radiation does not penetrate dense matter but is able to give precise images of objects beneath clothes or packaging. By varying radiations, it is possible to detect objects beneath different layered materials. THz will be used in two configurations with different processing times and accuracy. Ion-mobility-spectroscopy (IMS) is the only air sample screening technology applied in this context. It utilizes the property of molecules to retain a certain drift velocity in a magnetic field. Simplified, this velocity is lower the lager a molecule is. Thereby it is possible to determine the contained matter components of an object in very short times. It cannot be used to give a visual insight into an object, but it is precise in identifying matter, which diffuses substances into air. Table 1 shows the approximate detection rates of the different screening technologies by specifying the error probabilities for false threat detections and false clearance. Based on these values, the model will make probabilistic detection decisions. Note that IMS cannot be used for the detection of radioactive matter and weapons.

Table 1: *Screening Technologies Detection Rates*

Tech.	Time [min]	Drugs			Explosives			Radioactive			Weapons		
		Able	E 1	E 2	Able	E 1	E 2	Able	E 1	E 2	Able	E 1	E 2
X-ray	0.5	Yes	0.20	0.25	Yes	0.20	0.25	Yes	0.05	0.25	Yes	0.10	0.25
IMS	1.0	Yes	0.01	0.01	Yes	0.01	0.01	No	0.00	0.00	No	0.00	0.00
THzA	10.0	Yes	0.10	0.20	Yes	0.10	0.20	Yes	0.05	0.25	Yes	0.05	0.10
THzB	30.0	Yes	0.01	0.05	Yes	0.01	0.05	Yes	0.01	0.05	Yes	0.01	0.05

5 Simulation Scenarios

Simulation scenarios observe the system's behaviour to examine interdependencies under changing conditions. Each scenario is defined by a set of parameters and input values. To retain comparability, the environmental parameters remain constant. The following gives information on the scenario definition.

Constant among all scenarios is the arrival plan of items in the simulated year. Under realistic assumptions, about 1.5 million items have to be processed per year, which is an average daily workload of a little more than 4,000 items. Second, the screening termination criterions for each item are equal, which is the lower and upper bound of risk values and a time restriction of items to be processed on the day of arrival. Further, the evaluation of screening results and the decision on a detected threat is constant as defined by the model. Finally, each scenario has two variants. Variant A makes an item-based decision on whether to screen a parcel or not. The probability of being screened is then dependent on the perceived risk consisting of country-specific risk and additional information. Variant B uses a buffer to which 100 parcels are stored. When the buffer is full, 15% of all items with the highest risk assessment are forwarded to screening. The rest is cleared and routed to sorting. This split-up is similar to the percentage of screened items in the item-based decision of variant A, resulting from the underlying threat distribution. Therefore, screenings in both variants operate on an equal amount of items to retain comparability. Batched sorting has the effect that items with high risks are definitely screened, whereby the item-based selection always bears the chance that a high risk item is omitted due to the probabilistic decision.

5.1 Scenario 1: Single Device X-Ray Screening

The screening setup in scenario 1 only contains one X-ray device. This technology is one of the most common means and is very fast, but bears high error probabilities. With one device, the results give unaffected insights on the influence of the variant A and B, in which the process for the selection of items to be screened is modified.

The results shown in table 2 indicate a moderate ability to identify threats in the items. The occurred threats depict the fraction of items, which contained an actual threat. Screened items are the amount of items, which have been screened at least once. Evaluating the screening results, assumed threats are the percentage of all items declared as threat. In case the processing time of an item exceeds six hours, it is regarded as delayed and the percentage of such items is given. Finally, the identified threat percentage depicts the fraction of correctly identified threats. Note that the occurred threats and screened items will remain similar across the scenarios, because of the constant probabilities for threat occurrences and constant presumed risks. Variant A uses an item-based selection, using the presumed risk from the risk assessment. In 7% of all items, a threat is assumed which is nearly twice as much as threats have occurred overall. Of these, only 31% of the occurred threats have been identified correctly. Variant B has throughout all categories equal or improved rates. Threat detection obviously increased in accuracy, because fewer threats have been assumed and more threats have been identified. Additionally, the percentage of delayed items has decreased by 3%, which indicates an improved service level.

Table 2: *Scenario 1 Results*

Variant	Occurred Threats [% of all]	Screened Items [% of all]	Assumed Threats [% of all]	Delay > 6 hours [% of all]	Identified Threat [% of threats]
A	0.0351	0.1485	0.0636	0.1875	0.3088
B	0.0352	0.1482	0.0419	0.1587	0.4553
Difference	+0.0001	- 0.0003	- 0.0218	- 0.0288	+0.1465

With the same screening setup for both variants, the scenario results show that the use of a batched sorting by presumed risks has huge impact on the efficiency and accuracy of the system. Given the low required effort and investments for such a batched sorting, it is a suitable mean to improve the assignment of screening resources to the most risk-prone items.

5.2 Scenario 2: Multi-Tiered Technology Screening

Due to the high error probabilities of X-ray screening, it frequently occurs that a potential threat is assumed in an item, although this is not the case. This requires additional screenings to make precise decisions. In scenario 1 the item would have passed the X-ray device multiple times, each time affected by the high error rates. Scenario 2 therefore introduces the other two technologies, IMS and THz. In a first analysis, variant A again uses the item-based screening selection. This will give insights in the potential of the multi-tiered screening setup without the positive influences of the batched sorting. Variant B finally combines the multi-tiered screening with batched sorting.

Table 3: *Scenario 2 results*

Variant	Occurred Threats [% of all]	Screened Items [% of all]	Assumed Threats [% of all]	Delay > 6 hours [% of all]	Identified Threat [% of threats]
A	0.0353	0.1500	0.0734	0.1930	0.5236
B	0.0352	0.1500	0.0531	0.1493	0.8280
Difference	±0.0000	±0.0000	- 0.0203	- 0.0437	+0.3044

First, one can see in table 3 the improved identification rates of threats. Variant A even exceeds the batched sorting from scenario two. This shows that the multi-tiered screening has the higher improvement impact. The longer processing times of the advanced screening technologies become visible in the slightly increased percentage of delayed items. Remarkably, variant B exceeds all previous results with significant improvements. With 83% of identified threats and the lowest delay of 15%, it is a very accurate and effective configuration. The batched sorting combined with an improved allocation of screening resources to the threat categories bears high potential. Compared to the first results from scenario 1A the identification rate has been increased by 50% with at the same time fewer assumed threats and delays.

The increased complexity of the multi-tiered screening setup demands an efficient assignment of items to the screenings. Items with high risks are forced to enter the screening because of batched sorting. Item-based routing decisions enable a targeted use of the system's screening capacities.

5.3 Evaluation

Over the scenarios it has been shown that there are different possibilities available to increase the quality and efficiency in screening systems. The model further revealed influences of the uncertainty in the distribution of threats. Variant A probabilistically selected items to be screened, based on the assumed threat distribution, which by no guarantee has to be accurate in real scenarios. To cover this lack of information, the presented batched sorting can be applied. This results in setting information in context so that items with the highest risk level within a subset of all items will always be screened. It has been found that both batching and using multiple screening technologies positively influence detection probabilities. The effect of multiple technologies is stronger under the assumptions made for this study. A combination of both leads to the best results.

The results proof that the model is trustworthy and allows observations of the system behaviour and the influencing factors. Yet the model has been applied to a fixed arrival plan over the scenarios and the threat probabilities have been known for the occurrence of threats. Thereby, it becomes interesting to consider the dynamics of arrival plans and work load fluctuations and to introduce intelligent attack scenarios with insight knowledge on the system and routing decisions, using this information to strategically introduce threats into the system to minimize the change of detection.

6 Conclusion

The results from the simulation scenarios have shown that process configurations and technology availability have significant influence on threat detection. For the high amounts of individual items, a complete screening would require resources and efforts which most likely exceed capacities. LSPs face the same problems as aviation travel and transport, where next to resources also the service level is an important constraint. Delays have to be as short as possible and shipments should only slightly be affected by screenings. The presented results are in line with the related studies and clearly indicate the potential of risk-based screening. Furthermore it has been shown that risk assessment can be supported by process design. The availability of diverse screening technologies and their optimal allocation are an additional tool to improve the level of security.

In further studies we will reduce the assumptions for the model, like introducing interdependencies of screening technologies. Additionally, we will study variations of the probability distributions of the risk assessment. Also, adding more details of the processes in the hub, e.g. parcel handling and storage, might become necessary.

But also for the existing model, interesting variants can be tested, e.g. the effect of the buffer size on the detection of threats or a coupling of the likeliness to be screened with the current workload of screening devices.

The simulation model is a first step towards an analysis of the influence of environmental dynamics. The internal routing decisions based on the constantly adapted individual risk profile of items are valuable for defining and evaluating attack scenarios. This is especially important in case the attacker does have knowledge about the dynamics of the risk assessment and scanning procedures. It is then possible to deduce information on how to introduce malicious parcels in the supply chain. In the configuration presented in this paper (which is exemplary and in no way similar to a real one!), it would be preferable to send items in a plane which is scheduled to land shortly after a plane from the United States carrying a great number of safe parcels. Also, the average probability for a malicious parcel to be detected is less for an item the later it arrives during the day. Therefore, more advanced configurations might be necessary.

Acknowledgement

The research leading to these results has received funding from the German Federal Ministry of Education and Research in the context of the project “InPoSec” (FKZ: 13N12298).

References

Bundesministerium der Finanzen (Hrsg.): Die Bundeszollverwaltung Jahresstatistik 2011. Berlin: Bundesministerium der Finanzen, 2012.

Butler, V.; Poole Jr., R. W.: Rethinking Checked-baggage Screening. Los Angeles: Reason Public Policy Institute, 2002.

Kobza, J. E.; Jacobson, S. H.: Probability models for access security system architectures. Journal of the OR Society (1997) 48, pp. 255-263.

Nie X.; Batta, R.; Drury, C. G.; Lin, L.: Passenger grouping with risk levels in an airport security system. European Journal of Operational Research 194 (2009), pp. 574–584.

Rabe, M.; Hellingrath, B. (Hrsg.): Handlungsanleitung Simulation in Produktion und Logistik. Erlangen: SCS European Publishing House, 2001.

Statistisches Bundesamt (Hrsg.): Deutsche Ausfuhren im November 2012 unverändert zum November 2011. Wiesbaden: Statistisches Bundesamt Pressestelle, 2013.

Sewell, E. C; Lee, A. J.; Jacobson, S. H.: Optimal allocation of aviation security screening devices. Journal of Transportation Security 6 (2013) 2, pp. 103-116.

Sewell, E. C.; Attagara, J; Kobza, J. E.; Jacobson, S. H.: Allocating explosive screening devices for aviation security. Journal of Transportation Security (2012) 5, pp. 141–155.

Verein Deutscher Ingenieure (Hrsg.): VDI 3633 Simulation von Logistik-, Materialfluß- und Produktionssystemen. Düsseldorf: Verein Deutscher Ingenieure, 2000.

World Customs Organization: Customs operation nets exceptional quantities of drugs in postal parcels. Brussels: 20 November 2012.