SIMULATION FOR ASSESSING SECURITY-BASED POLICIES IN IMPORT/EXPORT OPERATIONS

Pasquale Legato[a] **and Rina Mary Mazza**[b]

[a], [b]Department of Electronics, Computer and System Sciences (DEIS)
University of Calabria
Via P. Bucci 42C
87036 Rende (CS), Italy

[a]legato@deis.unical.it, [b]rmazza@deis.unical.it,

ABSTRACT

In today's business environment, manufacturing and distribution companies have elevated their concern for security. They are working hard to ferret out risks and inefficiencies that may occur as their products and services move along the supply chain network. In this study we consider security issues from the stand point of a shipping agency providing import/export services. The objective of our study consists in the evaluation of security-based operating procedures and modalities that can lead to significant reductions in the controls that occur within the company activity due to both inside and third-party formalities (e.g. controls performed by the local Customs Office). The costs and benefits related to the adoption of new security-based policies and practices are estimated via discrete-event simulation. In the output analysis of multiple simulation replications, significant computational savings are achieved by introducing a fixed-point procedure to generate confidence intervals for the security-based performance measures of interest.

Keywords: logistics, security, discrete-event simulation, output analysis

1. INTRODUCTION

It is common knowledge that, ever since the September 11 attacks on the World Trade Center, governments, most branches of industry and citizens alike have drastically elevated their concern for safety and security. Although both deal with preventing negative events and conditions, these terms are normally regarded as representing distinct properties: safety deals with non intentional (accidental) negatives, whereas security deals with intentional (malicious) one (Gkonis and Psaraftis 2010). Methodologically speaking, this difference is significant enough to require an approach that spans across the increasingly specialized sub-disciplines of law, commerce and science.

These words ring especially true in the supply chain arena as many companies are working hard to ferret out risks, inefficiencies and, thus, costs of both safety and security efforts. In particular, the globalization of most industries has sparked heightened awareness of the various risks and vulnerabilities that products are exposed to as they move along the supply chain continuum from design and sourcing to manufacture, transportation, distribution and final sale to the consumer. Supply networks are long and complex. Many entities, including outsourcers and subcontractors located world-wide, handle the product as it moves across geographical and national borders, thereby creating many physical and temporal threats that pose a risk to product safety and security (Maruchecka et al. 2011).

Research theories and methodologies, as well as regulations and standards have addressed these problems to provide fresh insights and innovative solutions. Here we consider security issues from the stand point of a shipping agency providing import/export services. The objective of our study consists in the evaluation of security-based operating procedures and modalities that, in terms of performance, can lead to a 30% reduction in the controls that occur within the company activity due to both inside and third-party formalities, such as the controls performed by the local Customs Office. The costs and benefits related to the adoption of new security-based policies and practices will be evaluated via simulation. The paper is organized as follows. In the Problem Description paragraph, the security problem at hand is described by considering both internal and external influences ranging from technical solutions to national and international initiatives. Special attention is then given to the company's so-called import process, the most important for growth and exposure to security threats. In the Simulation paragraph, the convenience of using a fixed-point procedure against a two-stage procedure when generating interval estimates during the output analysis of the simulation study is examined. In the Numerical Experiments paragraph, *as is* simulations and *to be* scenario analyses are presented to assess and compare the before and after status of the company's security orientation. Finally, conclusions are drawn in the last section.

2. PROBLEM DESCRIPTION

A shipping agency providing import/export services is called to interact with carriers, customs, harbor offices, warehouses, forwarding agents, stevedores, border controls, port authorities, terminals and any other sorts of bodies and organizations belonging to the so-called port community. The information flows generated by the interactions among the above actors of the container supply chain are certainly a major concern when taking into account security issues for a company whose main activities are based on information processing, rather physical transformations and/or transfer operations. In this sense, we follow a two-stage approach to model and analyze the security problem within the container supply chain from the standpoint of the shipping agency. In the first stage, recognition and formalization activities of the logistic processes in the container supply chain are carried out in order to: *i*) represent rules and operation modalities used by actors when dealing with containers; *ii*) define interactions and information exchanges; *iii*) build a formal model with the objective of reorganizing the logistic processes in the container supply chain and evaluating performance measures in terms of specific security issues. In the second stage, the overall system developed in the first stage (i.e. control and communication procedures among the actors, data exchange and decision control along the container supply) is tailored to the shipping company under analysis and assessed via simulation.

In this section, we first provide some general background on security matters by considering both internal and external influences ranging from technical solutions to international initiatives. We then focus on the representation and discussion of the shipping company's major service: the import process, the most important for growth, third-party interaction and exposure to security threats. The objective of adopting security-based policies consists in pursuing a 30% decrease in the number of controls performed by the company and the local Customs Office when carrying out activities related to the import process.

2.1. Background Information

Technology can certainly aid any company in its struggle to improve security in the management of container import/export flows. Driven by the increasing importance of pervasive computing, information technology (IT) can especially provide support via comprehensive and flexible hardware and software applications. To fix ideas, one may choose from a variety of solutions among which, but not limited to:

- electronic seals;
- biometric technologies;
- closed circuit TV systems;
- RFIDs, radio frequency identification;
- other systems (acoustic, gamma-ray, x-ray, radiation detection, vapor/trace detection);
- GPSs, global positioning systems;
- A-GPSs, assisted global positioning systems;
- extended tracking technologies.

Whatever the solution implemented, the real challenge consists in keeping data and information exchange along the supply chain fast, lean and secure. From a quantitative perspective, the size and awareness of the problem runs back in time and can be summarized by the following figures (Infotransport 1994):

- 70% of the documents pertaining to transport is automatically generated, printed and sent on paper and then manually reintroduced into other computer-based processing systems;
- error rates in documentation reach 50%;
- the cost for providing paper document management in container transport operations lies between 7% and 10% of the value of the product itself.

Therefore, it is quite clear how an accurate and computer-based data and document processing can cut the general costs and time loss in logistics.

As a result, the competitiveness of the overall (Italian) transport system can benefit from the introduction of these IT solutions. However, even greater benefits can be achieved when similar solutions are implemented with respect to the initiatives that customs and governments from countries worldwide are promoting. Examples are the SAFE framework of standards, the ISO standards, the Transported Asset Protection Association (TAPA), the International Ship and Port Facilities Security Code (ISPS), the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), the Operation Safe Commerce (OSC), the Secure Freight Initiative (SFI), and the Bioterrorism Act.

In particular, for the purposes of our study, we consider the ISO/PAS 28000 specification for security management systems for the supply chain. ISO/PAS 28000 specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain: financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations, as well as personnel training and emergency procedures in case "security events" happen to occur.

A schema for designing a system compliant with the ISO/PAS 28000 standard must include:

- security planning and management;
- risk planning and management;
- a formal and shared description of the activities and processes carried-out by the organization, including the definition of the instructions and procedures set by the organization for security management (e.g. operational controls, emergency management, security programs and objectives, monitoring and measurements);

- management of preventive and corrective actions;
- (ongoing) review of activities and continuous improvement.

When adopting a management model compliant with the ISO/PAS 28000 standard, a risk analysis should be performed to identify the risks that can compromise container security. Rather than discussing how the risk analysis is carried out (Haimes 1998), here we report on the critical issues that have been brought about in the shipping company's activity. First of all, although the organization is aware of the need of tools for security monitoring, it normally exploits time-proven company practices and simply focuses on the recruitment of qualified personnel. Second, synergies seem possible between security and pre-existing systems compliant with quality standards and/or to-be systems for the automatic management of the company document workflow. Last, but not least, although interest for security is manifest, there is little knowledge allowing the implementation of a "formal" security system based on rigorous tools and methodologies.

This stated, in the following, special attention is given to the shipping company's so-called import process, the most important for growth, third-party interaction and exposure to security threats.

2.2. The Import Process

The import process plays a leading role in the shipping company's business. It features both company and third-party control policies (i.e. Customs) that affect the overall complexity of the process. The actors involved include: *i*) customers meant as final addressees of the imported goods or their intermediaries (i.e. subjects demanding a service); *ii*) the shipping company as shipper and representative of the customer by carrying out on his/her behalf all the necessary formalities related to the import of the goods (i.e. subjects offering a service); *iii*) Customs, the authority that is responsible for collecting and safeguarding customs duties and provides clearance for the goods that enter (exit) the Nation's territory and whose controls are an integrated part of the import service; *iv*) the container terminal, the concessionaire of the area in which container handling and interchange of goods in cargo units, as well as inspection activities in cooperation with the Customs Office are carried out. A flowchart (see Figure 1) and a step-by-step description of the import process follows.

A customer applies for a request to import goods and the shipping company issues a so-called *bill of lading* (in the following bill). As required by the company procedure, the bill is first assigned an "open" position. It is then (eventually) processed according to two main sub-processes: the *forwarding* option and/or the *verification of sanitary formalities* option. The former is a marketing-like process intended to extend the transportation service beyond the terminal and way on to the final destination indicated by the addressee. The latter is a process referring to the fito-sanitary and veterinary controls of the goods required at border crossings.

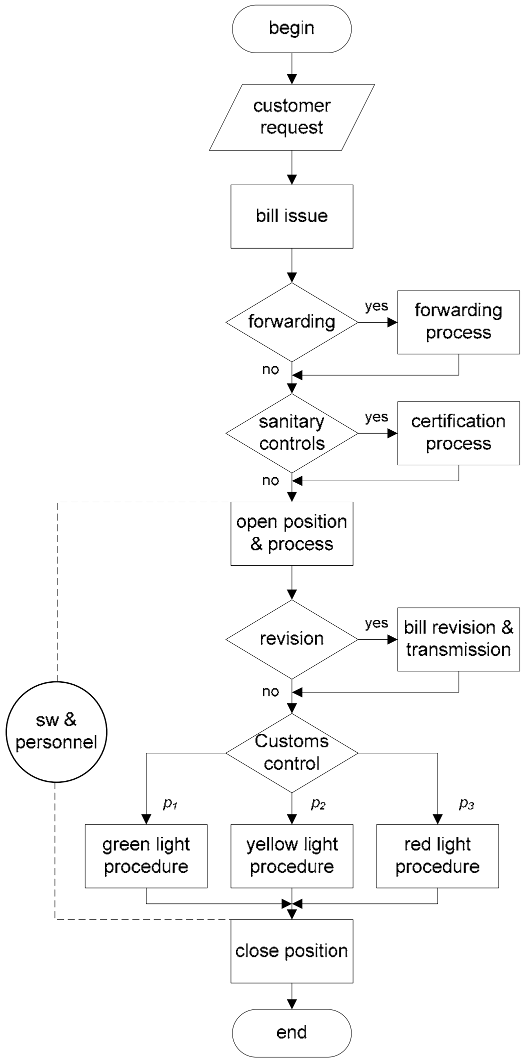

Figure 1: The Model of the Import Process

The opening and processing of the bills requires both active resources, such as qualified company personnel, and passive resources, such as software systems that provide for the electronic management of the bills.

Table 1: Skills of Company Personnel

	Skills			
Unit	Import	Export	Transits	Marketing
1	✓	✓	✓	
2	✓	✓	✓	
3	✓	✓	✓	
4	✓	✓	✓	
5	✓	✓	✓	
6		✓	✓	
7		✓	✓	
8		✓	✓	
9				✓
10				✓

For each unit belonging to the first category of resources, the number of employees and types of skills of each employee must be specified. As shown by Table 1, in the shipping company under analysis, both *single-skilled* and *multi-skilled* personnel are available.

Once the resources for bill processing have been assigned (i.e. management software and technical personnel, but also marketing personnel if the bill undergoes the forwarding option), the classification of the goods and the customs declaration must be fulfilled. The effort required in this part of the customer service, depends on both the number of containers and the number of customs codes that need to be considered in each bill. Observe that custom codes may be updated by the competent authorities during the actual bill processing. As a result, some fields of the bills may require a revision (nearly 6% of the times). Bill revision is also necessary every time a misinterpretation of customer information leads company personnel to commit an incorrect completion of customs documentation (11% of the times). According to the historical data of the company under examination, inaccuracies refer to.

- number of packages (42%);
- package weight (4%);
- country of origin (41%);
- value of goods (12%);
- addressee/shipper (1%).

Whatever be the cause, the technical staff must perform a sort of re-processing of the bill in order to carry out the corrections required. After the revision process is completed, a communication pertaining to the revised bill is sent to the Customs Office for approval. Bill processing may be considered closed only after receiving an acknowledgement to the above procedure.

As for inspection activities performed by the Customs Office, in a broader sense the representation of this control is placed in relation to the outcome returned from the Customs IT system. This outcome, in turn, can be classified as:

- green light or AC - Automated Control ($p_1 \approx 31\%$ of the cases) in which no further forms of control are carried out by the Customs officers assigned to the inspection activity;
- yellow light or DC - Document Control ($p_2 \approx 36\%$ of the cases) in which the related documentation is considered respondent to the Customs declaration or the eventual differences are of limited significance and, thus, considered immediately remediable;
- red light ($p_3 \approx 33\%$ of the cases) in which an SC - Scanner Control is performed or a GV - Goods Visit operation is carried out, meaning a real physical control of the goods inside of the container. In both cases (SC and GV), a request must be sent to the terminal to apply for control services. These occur in cooperation with the local Customs Office in order to guarantee the presence of the Customs officer delegated to hold the hearing on the terminal premises. The terminal provides for container transfer in the inspection area and, concomitantly, prearranges all that is necessary to carry out the inspection (e.g. container opening, handling of containerized goods, etc.).

Given the complexity and stochastic nature of many of the features in the above model, simulation has been chosen to evaluate the adoption of new security-based policies and practices within the import process.

3. SIMULATION

The design and implementation of the “import process simulator” has been carried-out in compliance with the conventional steps used to guide a thorough and sound simulation study (Banks et al. 2001). Rather than providing a general description of these steps, here we focus on the output analysis of simulation. In particular, we present and discuss the convenience of using a fixed-point procedure against the classic two-stage procedure (see from page 511 on in Law and Kelton 2000) in order to limit the standard error when generating interval estimates for the security-based performance indices examined in the Numerical Results paragraph.

Let X be the normal random variable representing the performance index of interest and $\mu \hat{=} E(X)$ the mean value that we want to estimate by an interval of random width, centered on the sample mean $\overline{X}(n)$. Using standard notations for Student-t quantiles, confidence level and sample variance, the interval estimator at the $1-\alpha$ level of confidence is:

$$\overline{X}(n) \pm t_{n-1;1-\alpha/2} \frac{S(n)}{\sqrt{n}} \tag{1}$$

In our case, the *n* parameter corresponds to the number of simulation replications to be set by the modeler before actually performing the simulation study. Hence, we want to determine the value of *n* that allows the modeler to keep the half-width of interval (1) within a predefined limit. The resulting fixed-point procedure provides an estimate of μ that satisfies the so-called relative error criterion (Nakayama 2002). In this respect, observe that

$$\left|\overline{X}(n) - \mu\right| = \left|t_{n-1;1-\alpha/2} \frac{S(n)}{\sqrt{n}}\right| < \varepsilon|\mu| \tag{2}$$

where $\varepsilon > 0$ stands for the target relative error. Thus, a fixed-point procedure may be set as soon as the dependence of both ε and the standard deviation from *n* is highlighted as follows:

$$\left| \frac{t_{n-1;1-\alpha/2}}{\overline{X}(n)} \frac{S(n)}{\sqrt{n}} \right| = \varepsilon(n) \quad (3)$$

where the sample mean is used instead of μ. The fixed-point schema is illustrated in Table 2.

Table 2: The Fixed-Point Procedure

1	set $k=0$, read n_k and ε_{target}
2	compute $\varepsilon(n_k)$
3	$\overline{X}(n_k)$, $S^2(n_k)$
4	$\varepsilon(n_k) = \frac{t_{n-1;1-\alpha/2} * S(n_k)}{\sqrt{n_k} * \overline{X}(n_k)}$
5	if $\varepsilon(n_k) > \varepsilon_{target}$
	Compute
6	$n_{k+1} = \left\lceil \frac{t_{n-1;1-\alpha/2} * S^2(n_k)}{\varepsilon^2_{target} * \overline{X}^2(n_k)} \right\rceil$
7	$k = k+1$ and go to Step 2
8	else STOP.
9	return $\left[\overline{X}(n_k) \pm t_{n-1;1-\alpha/2} \frac{S(n_k)}{\sqrt{n_k}} \right]$

To fix ideas, if the target average waiting time of a bill before actual processing is meant to be within 5% of the real value with probability $1-\alpha$, then ε is set equal to 0.05.

The above scheme is able to account for the changes in mean and variance estimation and, thus, it allows to dynamically adjust the number of runs required to generate the confidence interval within the predefined error. Practically speaking, this can enable significant savings from a computational point of view which, in simulation, always represents a major issue.

4. NUMERICAL EXPERIMENTS

The purpose of the simulation experiments is to compare the "as is" organization of the import process with its "to be" organization based on policies compliant with security assurance. As a result, the company management should be able to choose the operating procedures and "optimal" security-oriented modalities for the import process that, in terms of performances, can lead to a 30% reduction of the controls sampled out on the shipping company's work-flow within the related container supply chain network.

The experiments are carried out under Rockwell's Arena simulation package (version 11) and run on a personal computer equipped with an Intel® Core™2 Duo 1.58 Ghz processor and 2.93 gigabytes of RAM. The models in Arena include VBA (Visual Basic® for Applications) blocks that allow to insert user-defined code. In this study, these blocks are used to interact with worksheets under Microsoft® Excel 2002 in order to record the output data produced by the simulator and generate 95% intervals estimates according to the fixed-point procedure previously described in the Simulation paragraph.

4.1. As Is Simulation Model

In order to reproduce the import process as it is currently run by the company, the experiments use data from the first semester of 2009. This data is represented by means of synthetic estimators, once lag-correlation type mathematical procedures based on the mutual distance between data have been used to support the prerequisite of independence. Different types of distribution forms are then identified as "candidate" representations of the data models. Finally, the goodness of these distribution functions is verified by employing frequency histograms, p-p plots and the proper goodness-of-fit tests in which a comparison occurs between the empirical distribution forms and the theoretical distribution forms.

For illustrative purposes, some modeling examples of the bill processing times are given in Tables 3 and 4 and Figures 2 and 3. Obviously, to complete this part of the study, the previous steps are applied to obtain models for all the input data required by the import process (i.e. bill issuing, forwarding, certifications, software updates, bill revisions and green light, yellow light and red light responses)

Table 3: Data for Bill Processing

Semester I 2009	
number of observations	644
min observation	23
max observation	65
mean	24.45
median	23
variance	13.43
lexis ratio	0.15
skewness	6.62
data independence	yes

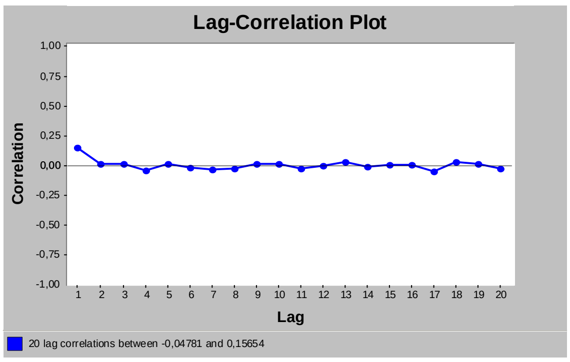

Figure 2: Verification of Absence of Correlation among Bill Processing Times

Table 4: Input Models for Bill Processing Times

Semester I 2009		
Model	Score	Location, Scale, Shape
Weibull	85.71	22.96, 0.46, 0.42
Gamma	79.76	22.96, 5.09, 0.29
Log-Logistic	77.38	0.00, 23.75, 22.53

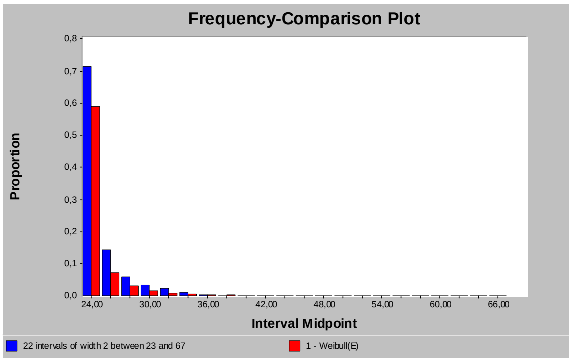

Figure 3: Histogram for Bill Processing Times

Thanks to the validation of the "as is" model (Sargent 2007), it is possible to assess whether or not the operating model is an accurate representation of the real system and, thus, continue with the experiments for the "to be" model. As for this matter, the simulator returns performance measures based on both intermediate and final check points (e.g. monthly and semiannual). This output is then compared with the real performance measures recorded by the company for the period of interest. These include, but are not limited to, the average number of *i*) bills completed, *ii*) forwarding operations, *iii*) sanitary verifications, *iv*) outcome of the inspections carried out by the Customs Office classified according to one of the three categories previously defined (i.e. green light, yellow light and red light), as shown in Table 5.

Table 5: Validation on a Selection of Average Monthly Results

Index	Results	
	Real Data	Simulator
N° of bills completed	107.33	[106.25 - 109.11]
N° of forwardings	35.83	[35.03 - 36.10]
N° of certifications	24.67	[24.55 - 25.43]
N° of green lights	33	[32.80 - 34.08]
N° of yellow lights	38.83	[38.43 - 39.35]
N° of red lights	35.5	[34.76 - 35.94]

The above results appear to be satisfactory. Therefore, the simulator can be used to perform the what-if analyses planned to evaluate future key security-based company policies.

4.2. To Be Simulation Model

The objective of achieving a 30% reduction of the controls sampled out on the import process calls for the evaluation of alternative organizations for the corresponding document workflow. In particular, as pointed out in §2, for this purpose the current and, most of all, the future company security-oriented policies rely on monitoring activities whose effectiveness mainly depends on the recruitment and training of company personnel. To realize the importance of this matter, one may consider the correlation between the presence of qualified personnel and the correct use of the software that supports the company workflow. As a matter of fact, this business function will be considered as one of the key elements on which what-if analyses will be performed to estimate the effect of the controls carried out by the local Customs Office on the different scenarios under examination.

From a general point of view, the Customs Office (or, more precisely, the Customs of the European Union) has set the objective of finding an equilibrium point between the speed of exchanges and the effectiveness of controls based on anti-illicit trafficking, fraud and counterfeiting actions. The related control systems use modern technologies for an automatic risk management based on a constant analysis of the traffic flows. The corresponding control policies involve a subjective risk assessment of every operation in order to favor "reliable" economic operators (i.e. "white lists" vs "black lists").

According to the data collected from the customs declaration, an IT process is used to verify the documentation related to the aforesaid declaration. Practically, the reliability of an operator is estimated through a series of prefixed parameters on which the Customs Office performs its own controls. In particular, the so-called "risk profiles" are closely correlated to the combination of the following elements of the Customs declaration:

- origin and destination of goods;
- addressee of goods;
- sender of goods;
- type and characteristics of goods.

This stated, here we will consider parameters on which the company can act with some degrees of freedom: the number of errors in the customs declaration and, as a consequence, the number and types of revisions required. In brief, the higher the result of *n° of revisions/total n° of bills*, the lower the reliability of the operator and, thus, the higher the number of the controls. The logical nexus between these two factors leads to test a series of hypothesis that, if verified, draw a corollary that supports the decrease in Customs controls. The latter is the overall goal of the simulation study.

In the case study under examination, out of the 644 bills processed in the first semester of 2009, the company recorded:

- 30% of inspections;
- 11% of revisions, followed by inspections in 33% of the cases;
- 33% of demands for certifications, followed by inspections in 33% of the cases.

According to what was previously stated on the reliability of the operator, one may assume that a decrease in the number of (bill) revisions is followed by a decrease in the number of inspections as well. In particular, the decrease could be pursued by *i*) training the technical personnel with the objective of reducing the number of errors in the documentation or *ii*) planning the update operations of the company software with the objective of drastically reducing the number of revisions. Since the effect of neither of the above actions is known *a priori*, the "to be" simulation model consists in a sensitivity analysis based on total error reduction (i.e. 100%) or partial error reduction (i.e. 50%, 25% and 10%) and, thus, the estimation of the consequences of these reductions in terms of company or Customs controls.

In hypothesis n°1 based on personnel training, each simulated scenario returns estimates for the average reduction in the number of bills to undergo a revision process each month. The total number of hours during which the above bills are held in detention by Customs waiting for approval is estimated as well. Observe from Table 6 how both of these factors affect controls and the productivity of the related company departments which is slowed down by Customs detentions. It is quite clear that a reduction in bill revisions from [11,60 - 12,16] to [5.71 - 5,98], on one side, results in a reduction of company controls and, on the other, it additionally cuts the 33% of revised bills followed by Customs controls. Therefore, this "medium" scenario (i.e. 50% option in Table 6) has a significant impact on the company's operating efficiency and is coherent with the objectives of the simulation study.

Table 6: Results from What-if Analysis based on Security-driven Training Activities

Training	Monthly Analysis	
	N° of revisions	Customs Detention (h)
Pre-training	[11.60 - 12.16]	[46.88 - 49.08]
10%	[10.30 -10.79]	[42.48 - 44.11]
25%	[8.60 - 9.07]	[35.40 - 37.05]
50%	[5.71 - 5.98]	[23.41 - 24.56]
100%	0	0

Figure 4 illustrates the trend in the reduction of the total number of hours (per month) of bill detention by Customs, according to more frequent and regular percentage variations.

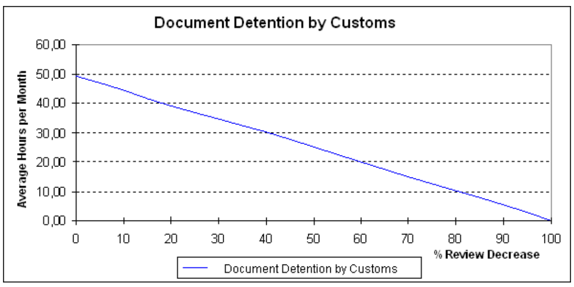

Figure 4: Trend of Document Detention by Customs based on Security-driven Training Activities

In hypothesis n°2 based on planning software update operations, one must consider the following factors. Update operations can be necessary due to software bugs, a phenomenon which is normally negligible, or variations in the data used for calculations in Customs charges. In the latter case, the software devoted to such purpose features a heavy use of third-party archives that, in turn, require continuous updates (e.g. the archives containing customs duties, currency change, variations of agreements between countries, etc.). As a result, errors can be forced from delays in updates which, due to organizational deficiencies, are often left to the good will of a single company operator who may not have the skill to perform such update.

The related what-if analysis is carried out by estimating the average number of revised bills (per month), along with the time required to carry out the software updates and subsequent bill revisions. By analogy with the first what-if hypothesis, Customs inspections follow the software updates, therefore, further reductions are brought about in both company and Customs controls. In this sense, for each scenario Table 7 records the average number of bill revisions related to software updates, as well as the total time effort that, in turn, holds back the productivity of the corresponding company department.

Table 7: Results from What-if Analysis based on Security-driven SW Maintenance

Maintenance	Monthly Analysis	
	N° of Revisions	Time Effort (h)
Pre-maintenance	[6.21 - 6.69]	[1.57 - 1.73]
10%	[5.26 - 6.29]	[1.08 - 1.84]
25%	[4.15 - 5.72]	[0.65 - 1.55]
50%	[2.71 - 3.73]	[0.29 - 0.97]
100%	0	0

Figure 5 illustrates the trend in the reduction of the total number of hours required to perform software updates and the revision of those bills for which processing activities were interrupted due to the software update.

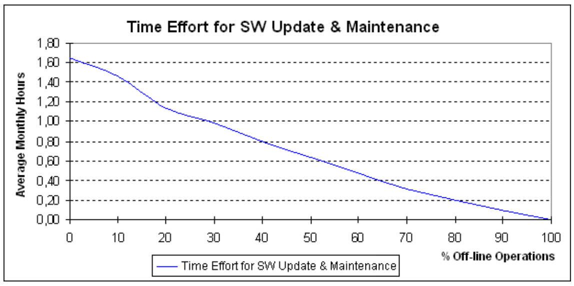

Figure 5: Trend of Time Effort for Security-driven SW Update and Maintenance

The present simulation study is completed with some key considerations on the estimates reported in Tables 6 and 7. These 95% confidence intervals have been generated according to our fixed-point procedure for keeping the error (1) within a predefined limit (2), rather than a classic two-stage procedure. Since the proposed scheme accounts for the changes in the mean and variance estimation, it allows to dynamically adjust the number of runs required to generate the confidence intervals within the predefined error.

Table 8: Fixed-point versus 2-stage Procedure for Error Control in Confidence Intervals

Scenario	Performance	Δ%
1	N° of Revisions	37.50%
	Customs Detention	47.37%
2	N° of Revisions	47.37%
	Customs Detention	44.44%
3	N° of Revisions	16.67%
	Customs Detention	9.09%

In terms of (average) computational savings (Δ% is the n° of runs saved in percentage), Table 8 shows how the fixed-point procedure outperforms the 2-stage procedure in error control during the generation of interval estimates for the security-based performance measures across the three scenarios under analysis.

5. CONCLUSIONS

Security-based procedures compliant with the ISO/PAS 28000 standard have been tested via simulation with respect to the import process of a shipping company. The what-if approach adopted to evaluate the impact of the above procedures has returned promising estimates as far as reducing the number of bills to be revised by the company is concerned. These (interval) estimates have been obtained with a reduced computational effort, by using a fixed-point procedure to determine the number of simulation replications which ensure a standard error below a target value. Besides the general objectives of the study, an additional research opportunity has risen from a methodological point of view: the quest for advanced techniques of *importance sampling* that allow to properly analyze scenarios by means of simulation when an insufficient quantity/quality of data is available.

ACKNOWLEDGMENTS

This work has been partially supported by the Italian Ministry for Education, University and Research (MIUR) under the e-Log Project, grant n° DM28145.

REFERENCES

Banks, J., Carson, J.S., Nelson, B.L., and Nicol, D.M., 2000. *Discrete-Event System Simulation*. 3rd ed. Upper Saddle River, New Jersey: Prentice-Hall, Inc.

Gkonis, K.G. and Psaraftis, H.N., 2010. Container transportation as an interdependent security problem. *Journal of Transportation Security* 3:197–211.

Haimes, Y., 1998. *Risk Modeling, Assessment and Management*, New York: John Wiley.

Infotransport, 1994. *Stato dell'arte dell'informatica nei trasporti*. Infotransport 22/04/94.

Law, A.M. and Kelton, W.D., 2000. *Simulation Modeling and Analysis*. Third Edition. McGraw-Hill: New York.

Maruchecka, A., Greisb, N., Menac, C., and Caid L., 2011. Product safety and security in the global supply chain: Issues, challenges and research opportunities. *Journal of Operations Management* 29:707–720.

Nakayama, M.K., 2002. Simulation Output Analysis. *Proceedings of the 2002 Winter Simulation Conference*, 23-34, San Diego, CA, USA.

Sargent, R.G., 2007. Verification and Validation of Simulation Models. *Proceedings of the 2007 Winter Simulation Conference*, 124-137, Washington, DC, USA.

AUTHORS BIOGRAPHY

Pasquale Legato is an Associate Professor of Operations Research at the Faculty of Engineering - University of Calabria, Rende (CS, Italy), where he teaches courses on simulation for system performance evaluation. He has published on queuing network models for job shop and logistic systems, as well as on integer programming models. He has been involved in several national and international applied research projects and is serving as a reviewer for many international journals. His current research activities focus on the development and analysis of queuing network models for logistic systems, discrete-event simulation and the integration of simulation output analysis techniques with combinatorial optimization algorithms for real-life applications in Transportation and Logistics. His home-page is www.deis.unical.it/legato.

Rina Mary Mazza received her Laurea degree in Management Engineering and obtained a Ph.D. degree in Operations Research at the University of Calabria, Rende (CS, Italy). She is currently head of the "Research Projects Office" at the Department of Electronics, Computer and System Sciences (DEIS) of the above University. She has a seven-year working experience on Knowledge Management and Quality Assurance in Research Centers. She is also a consultant for operations modeling and simulation in terminal containers. Her current research interests include discrete-event simulation and optimum-seeking by simulation in complex logistic systems. Her e-mail address is rmazza@deis.unical.it.