Proceedings of the 2005 Winter Simulation Conference
M. E. Kuhl, N. M. Steiger, F. B. Armstrong, and J. A. Joines, eds.

DEVELOPING DATA FUSION SYSTEMS DEVOTED TO SECURITY CONTROL IN PORT FACILITIES

Enrico Bocca
Simone Viazzo

McLeod Institute of Simulation Science
Via Opera Pia 15
Genoa (GE) 16145, ITALY

Francesco Longo
Giovanni Mirabelli

Mechanical Department, University of Calabria
Cube 44C, via P. Bucci
Rende (CS) 87036, ITALY

ABSTRACT

The paper presents an innovative approach to seaport security problems. In particular the authors propose the Modelling & Simulation and Data Fusion integration to provide an efficient tool to test and improve the container inspection reliability taking into consideration – at the same time – the impact of different security level on system performances.

In this context the opportunity given by new standards and normative, in terms of sharing information, highlights the possibility to use Simulation as well as Data Fusion for analyzing different aspects (related to security) enhancing the container selection approach based on container risk evaluation (as strongly required, for instance, by Customs-Trade Partnership Against Terrorism, C-TPAT).

1 INTRODUCTION

It's well known that the 90% of world cargo moves by containers and the economic interests involved in such activities are the basis of global economy. At the same time the recent events testify that one of the fundamental terrorism goals is the complete destruction of these economic interests.

The seaports face today the same security problems of airports after September the 11th.

Issues concerning with seaport security regard several aspects such as perimeter security, internal security and operative controls, maritime security, port community systems, decision support systems, prevention and emergency management and so on.

Answers to these issues obviously look in different directions such as access control and fencing surveillance, internal area monitoring, cargo equipment control as well as passenger and baggage control, water surveillance in front of piers and traffic control, risk analysis, emergency alarm systems.

Normative and standards are extremely clear about the guidelines for securing seaport activities; at present the most important normative and initiatives are the following:

- U.S. Custom service's Container Security Initiative (CSI);
- Customs-Trade Partnership Against Terrorism (C-TPAT);
- International Ship and Port facility Security code (ISPS code);
- U.S. Maritime Transportation Security Act of 2002.

It's important to stress that standards and normative help keep events like September 11 from happening establishing the right guidelines but they don't offer explanations about the choice of all the possible tools, methodologies and technological advances to secure seaport and relative activities and above all they don't directly deal with the impact of the security procedures on system performances.

Among the security issues previously mentioned, the container inspection phase plays a critical role because of threats that by means of containers can enter or exit a seaport. Focalizing on this aspect, the only way to jointly consider security and efficiency is the integration of all available container information in order to evaluate a container risk factor. The container risk evaluation allows to reduce the inspection times guarantying no additional delay for low risk container as well as detailed inspections for containers that may pose a risk for terrorism.

The intrinsic difficulties related to tune such type of approach can be faced using simulation in order to estimate inspection phase effects and reliability as well as the impact on performance system of an emergency situation.

2 CONTAINER RISK EVALUATION

In order to evaluate a risk index for each container entering the port it is necessary to consider several information sources.

Suppose to subdivide the information sources in three main categories:

- container history information;
- container configuration information;
- alert information.

The container history essentially groups four information sub-categories:

- *vectors*, logistic companies that have transported the container until the present port;
- *nodes*, destination points before entering the present port;
- *vendor*;
- *regions*, previous country passed before entering the present port.

The container configuration reports information about the following characteristics:

- *container type*, such as 20 feet, 40 feet, reefer containers and so on;
- *good type*, goods characteristics transported inside the container;
- *manifest of non-conformity* noticed on container
- *security NC*

Finally the alert is defined by the following information:

- *security level* inside the port;
- *intelligence police* e relative reports about security issues;
- *port location*;
- *ship entering the port.*

All these information – opportunely used and combined by means of Data Fusion – bring to container risk index definition. Such risk index must be used in order to plan the container inspection.

Obviously, as previously mentioned, this type of approach cannot be tuned directly on the real system. An optimal solution is to test and tune the approach by means of a virtual environment.

This virtual environment is made up by two fundamental parts:

- *Virtual Cargo Generator*
- *Seaport Simulation Model*

In the following part of the paragraph is reported a detailed description of *Virtual Cargo Generator*, please refer to next paragraph for *Seaport Simulation Model*.

The *Virtual Cargo Generator* provides virtual security scenarios to analyze by means of port simulation model and it is based on the information sources previously described. The logical steps followed by the *Virtual Cargo Generator* are:

- *Virtual Path* generation containing all the information relative to container history;
- *Virtual Cargo Configuration* reporting information about container characteristics;
- *Virtual Alert Scenario* regarding report and alert in a specific period of time;
- *Virtual Threat*, such as radioactive substances, narcotics, weapons (and so on) sitting in a container.

Figure 1 shows a graphic representation of the *Virtual Cargo Generator* and risk evaluation procedure.

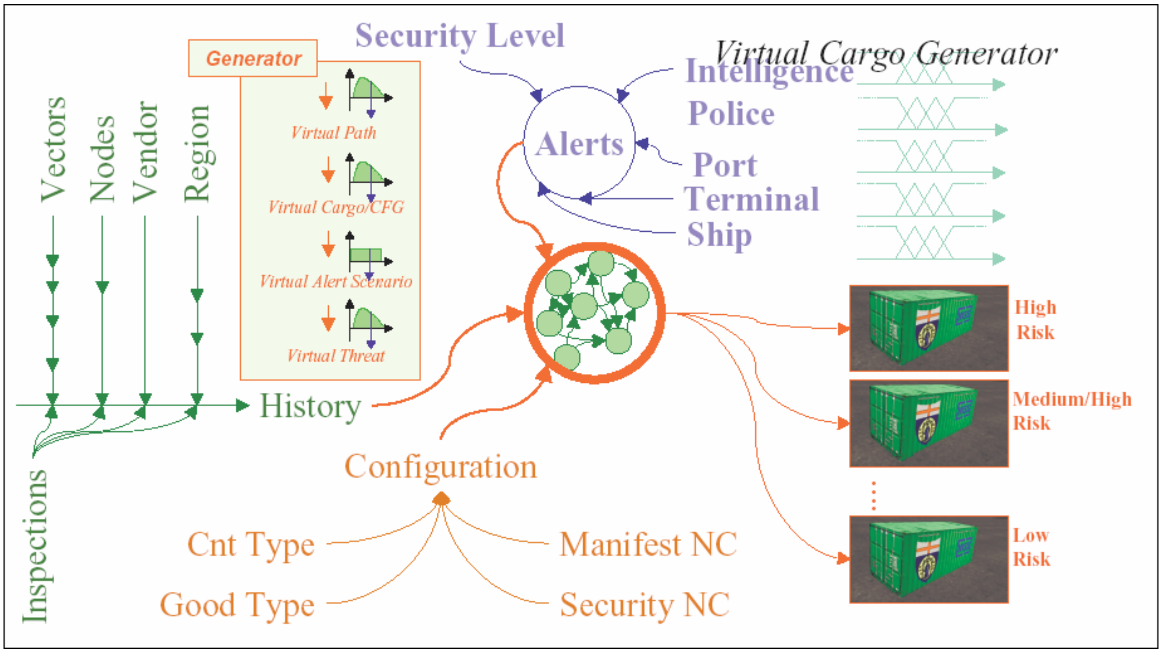

Figure 1: Risk Analysis Evaluation

The Virtual Path, the Virtual Cargo Configuration and the Virtual Alert Scenario allow to define the container risk level, distinguishing between high risk, medium/high risk and low risk. The Virtual Threat could be discovered by means of inspection phase.

3 SEAPORT SIMULATION MODEL

If from one side a *Virtual Cargo Generator* has been created, providing in this sense several and different security scenarios, it is now necessary – from the other side – a *Seaport Simulation Model* that will be used to monitoring the container inspection phase reliability as well as the impact of different security level on the port performances.

In other words the entire virtual environment (union of *Virtual Cargo Generator* and *Seaport Simulation Model*) is used to carry out integrated distributed control with input consisting of various information flow opportunely combined by means of Data Fusion.

For what concern the *Seaport Simulation Model*, the authors, using virtual reality and simulation based on technology advances (new tools, platforms, software utilities and procedure experience), are able to realize and propose different type of simulators for analyzing different aspects of the seaport activities such as load and unload operations, internal transportations, ship arrives and departures. Figure2 shows a simulation of internal transportations while in Figure 3 is proposed a terminal activities simulation.

Figure 2: Simulation of Operations in Detail

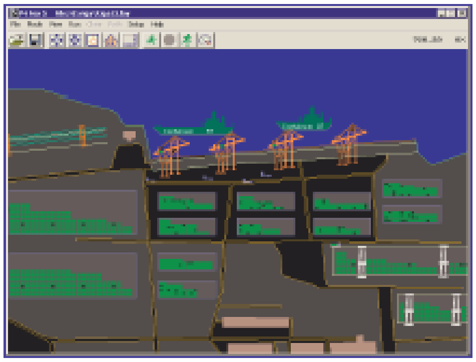

Figure 3: Terminal Activities Simulation

As application example port analyzed in this work, in particular a terminal container, was modelled using a discrete event simulation package. Movement equipment of the port is made up by portainers used for ship unloading and loading phase and straddle carrier and truck plus top loaders for containers movement in yard area.

Table 1 reports some information about the movement equipment technical characteristics.

Table 1: Equipment Technical Characteristics

	C	PC	TS	MP (SD)
ID	*[Kg]*		*[m/s]*	*[Cont.s/h]*
PT-1	35.000	5	0,50	25 (15%)
PT-2	50.000	5	0,75	30 (15%)
PT-3	60.000	5	0,75	30 (15%)
SC	From 2500	2	7	25 (20%)
TT	30.000		15	
PT=Portainer; **SC**=StraddleCarrier; **TT**=Truck+Top loader; **C**=Capacity; **PC**=Pile of container; **TS**=Translational speed, **MP**=Mean Productivity; **SD**=Standard deviation				

The terminal container works 24 hours per day and 365 days per year. The reference ship has a length of 250 m, width 35 m, draft 9 m, with a capacity of 4500 TEU.

The import flow (60% of total containers flow) is subdivided between trucks (70%), train (20%) and local ship (10%). The amount of time for docking and sailing operations is about two hours.

The terminal container modeled guarantees an average containers flow about of 1 million per year.

One of the most critical issue during the modelling phase is the number of entities moving in the simulation model. It' evident that the problem is caused by the high number of containers that could bring to have a simulation model computationally to heavy (with problems during the graphic animation as well as the speed of the simulation).

This type of problem can be solved substituting the entity flow with an information flow. Consider, for instance, the containers directed to the yard area, actually this containers must not be inspected. Consequently it's only necessary to model the movement toward the yard area and to store in a data base all the information relative to the container without generate an entity corresponding to the container.

A similar method can be used during the ship unloading or loading phase. A single entity making a loop between berth and ship successfully model this activity.

Obviously the situation is quite different for what concern the containers inspection phase. In this case, due to the approach used to study the problem, it's necessary to create the entity container as well as the relative information.

It's extremely clear that a terminal container is a non-terminating system, the duration of a simulation run is not fixed. The first objective in this type of simulator is to understand the optimal length of a simulation run.

To this purpose the *Mean Square Pure Error* Analysis (MSpE) has been used. Considering that the attention is focalized on the security problem and in particular on container inspection phase, the container mean waiting time before inspection and the container mean service time during the inspection were chosen as performance measures in order to establish, by means of MSpE, the optimal simulation run length.

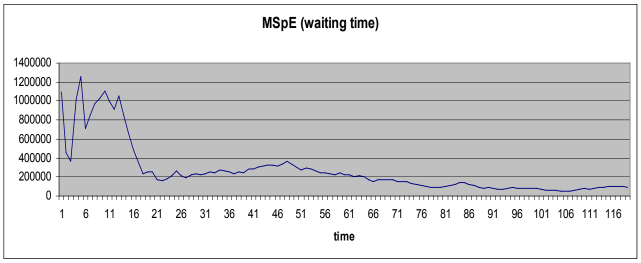

Figure 4: MSpE Analysis for Waiting Time

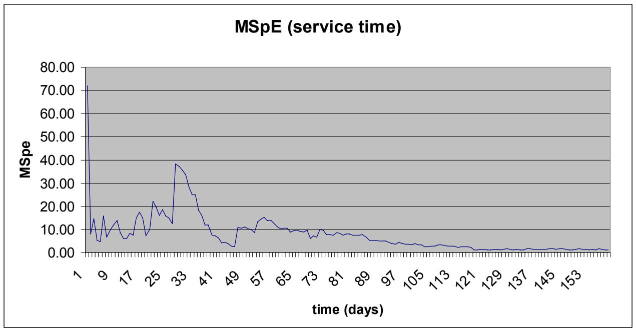

Figure 5: MSpE Analysis for Service Time

Figure 4 shows that the reduction of Mean Square pure Error relative to container waiting time becomes negligible after 120 days. From figure 5 it's possible to see that for what concern the container service time the MSpE becomes negligible after 160 days.

As recommended by the theory of the Mean Square pure Error analysis, in case of comparison, it's necessary to choose the greater interval of time that is 160 days for each simulation run.

4 CONTROLS RELIABILITY AND SYSTEM PERFORMANCES

In relation to value assumed by the container risk index (in output by the container risk evaluation phase) the container itself will be subjected to a particular type of inspection.

The inspection phase implemented in the *Seaport Simulation Model* is made up by five stations, respectively:

- Radiation Screening;
- Chemical Screening;
- Biological Screening;
- Gamma Ray Inspection;
- Full Inspection.

It's extremely clear the possibility to jointly use the *Virtual Cargo Generator* and the *Simulation Model* to test and improve the control reliability.

In fact if from one side it is not known the potential threat inside a container, from the other side all the container information are used in order to classify the container dangerousness and choose the right order inspections. Several simulation runs have been made to monitor the inspection phase reliability in terms of discovered threats.

Besides taking into consideration some performance indexes (such as moved TEU per Portainer or moved TEU per berth length) it's possible to analyze the impact on the system performances of different security level (see Figure 6).

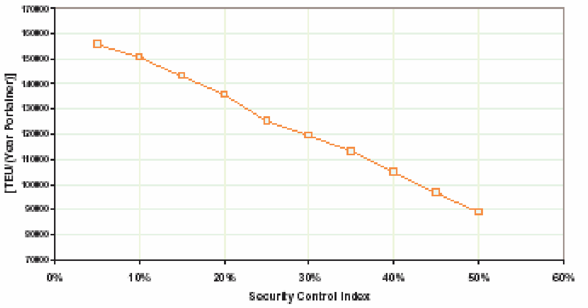

Figure 6: System Performance versus Security Level

The simulation model allows to compare different solutions for the inspection phase. A particular scenario has been analyzed introducing some new portable equipment for the inspection phases and grouping (thanks to new equipment) the radiation screening, the chemical screening and biological screening in one phase. The consequence is a container waiting time and container service time reduction. The effects can also be seen on system global performances.

Figure 7 show the difference per year per portainer between the two different inspection solutions underlying the positive effects of new portable equipment as well as grouping phases.

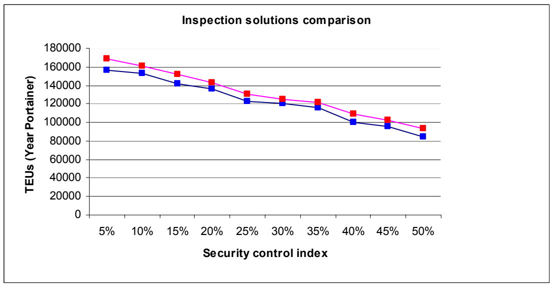

Figure 7: Two Possible Inspection Solutions

REFERENCES

Altiok T. 2005. "I-GERT", NSF Report / Rugters University, Piscataway NJ

Ballou R. 2003. *Business Logistics/Supply Chain Management*, Prentice Hall, Readings.

Banks J., Handbook of simulation, Wiley Interscience.

Bruzzone A.G., S. Viazzo, F. Longo, G. Mirabelli, E. Papoff, C. Briano, M. Massei. 2004. Discrete event simulation applied to modelling and analysis of a supply chain, *Proc. of MAS 2004*, Bergeggi (Ge).

Bruzzone A.G 2005. *GLOWS*, DIPTEM Press Genoa, Italy

Bruzzone A.G., Reverberi A., Rocca A., Brandolini M., Massei M. 2005. Security management systems in logistics: an innovative approach in solution design, *Proceedings of ASTC2005*, San Diego.

Bruzzone A.G., Brandolini M., Briano C., Petrova P. 2004. Poly-functional intelligent agents for computer generated forces, In *Proceedings of the 2004 Winter Simulation Conference*, ed. R .G. Ingalls, M. D. Rossetti, J. S. Smith, and B. A. Peters. Piscataway, NJ: Institute of Electrical and Electronics Engineers.

Bruzzone A.G., Brandolini M., Viazzo S. 2004. Massive training based on virtual reality equipment applied to logistics and heavy haul tracking, *Proc. of SCSC2004*, San Jose', CA.

Bruzzone A.G, Orsoni A., Giribone P. 2003. Fuzzy and simulation based techniques for industrial safety and risk assessment, *Proc. of ICPR*, Blacksburg VA.

Bruzzone A.G., Brandolini M., Briano C., Procacci V. 2001. FLODAF: Fuzzy logic applied to a multi-sensor data fusion model", *Proceedings of FLODAF2001*, Montreal.

Bruzzone A.G, Mosca R., Revetria R., Rapallo S. 2000. Risk analysis in harbour environments using simulation, *International Journal of Safety Science*, 35.

Bruzzone A.G., M.E., Cotta G., Cerruto M. 1997. Simulation & virtual reality to support the design of safety procedures in harbour environments, *Proceedings of ITEC97*, Lausanne (CH).

Fischer R., Green G. 2003. *Introduction to security*, Butterworth-Heinemann

Merkuryev Y., Bruzzone A.G., Merkuryeva G., Novitsky L., Williams E. 2003. Harbour maritime and multimodal logistics modelling & simulation 2003, DIP Press, Riga.

Marine Log. 2004. *Jitters as ISPS/MTSA deadline nears*, Simmons-Boardman Publishing Corporation, Omaha.

Marine Log. 2004. *MTSA and ISPS: final rules issued*, Simmons-Boardman Publishing Corporation, Omaha.

Marine Log. 2003. *IMO wants early ISPS implementation*, Simmons-Boardman Publishing Corporation, Omaha.

Mosca R., Bruzzone A.G. & Costa S. 1996. Simulation as a support for training personnel in security procedures, *Proc. of Military Government and Aerospace Simulation*, New Orleans, LA.

Safety at Sea International. 2003. *What will be the cost of ISPS? As ports and shipping companies race to comply with an extremely tight deadline to meet the IMO security requirements*, DMG World Media, London.

Security Management. 2003. *IMO sets course for port security*, American Society for Industrial Security, Alexandria.

Sennewald C. 2003. *Effective security management,* Butterworth-Heinemann.

Shepard S. 2004. *RFID*, McGraw Hill, NYC.

Tyska L., Fennelly L. 2001. *Cargo theft prevention: a handbook for logistics security*, American Society for Industrial Security.

AUTHOR BIOGRAPHIES

ENRICO BOCCA is a researcher in the Department of Production Engineering at Genoa University. His research interests include business plan related R&D projects, logistics and project Management. His e-mail address is enrico.bocca@liophant.org.

SIMONE VIAZZO is a researcher in the Department of Production Engineering at Genoa University. His research include simulation of supply chain, inventory management policies and forecasts methodologies. His email is viazzo@itim.unige.it.

FRANCESCO LONGO is a researcher in Mechanical Department at University of Calabria. His research interests include simulation of supply chain and terminal container with particular attention to security problems. His email is f.longo@unical.it.

GIOVANNI MIRABELLI is a researcher in Mechanical Department at University of Calabria. His research interests include simulation of human activities in manufacturing and logistic systems. His email is mirabellig@tin.it.