Security & Safety Training and Assessment in Ports based on Interoperable Simulation

Agostino G. Bruzzone MISS DIPTEM University of Genoa, Italy agostino@itim.unige.it URL www.itim.unige.it

Alberto Tremori

Simulation Team – DIPTEM University of Genoa, Italy alberto.tremori@simulationteam.com URL www.simulationteam.com

Enrico Bocca

MAST Savona, Italy enrico.bocca@mastsrl.eu URL www.mastsrl.eu

ABSTRACT

The present research proposes a Virtual Port Simulator based on an HLA technology, devoted to cooperative training in Harbor Security Procedures to support Maritime Security Transportation Act and International Ship and Port Facility Security Code (SOLAS). Within these frameworks a clear requirement for port security assessment & training is addressed, therefore the complexity of Harbors as well as the wide type of possible crisis create complex conditions to properly face this challenges. This paper presents a Virtual Port solution developed by the authors in term of architecture, model description, and configuration for training and security assessment. In fact, the creation of a common Virtual Port as synthetic environment with stochastic constructive and virtual simulation, where each federate represents an actor interoperating with other ones. By this approach the simulation supports both training and security assessment in term of procedures and considering the necessity to coordinate the different actors and to consider all the different issues. The final result is the definition of a new approach to face security by a joint simulation that involves concurrently all active actors for port protection.

INTRODUCTION

The paper proposes a Virtual Port Simulator based on an HLA federation devoted to cooperative training and assessment in Harbor Security Procedures. Port security requirements evolved after September 11 due to the 2002 Maritime Security Transportation Act (MSTA) in the USA. This act spurred a set of actions taken by the international community to mimic the US training regulations, such as International Ship and Port Facility Security (ISPS) Code under Safety of Life at Sea (SOLAS) Convention by International Maritime Organization (IMO). Within this framework a clear requirement for port security training is addressed, therefore the complexity of Harbors as well as the possible crisis creates hard limitations to develop realistic training sessions.

Ports are characterized by co-location and strong interactions among a large and diverse set of active actors. It is important to underline that the most of these actors are civilian. Organizations that work within port operations include Coast–Guard, other Navy agencies, as well as Port Authority, Terminal Operators, Shipping Companies, and Custom and Border Protection Agencies.

All these entities are active with different roles and Responsibilities. In addition to what we call "internal" active actors, Ports have significant interactions with external authorities. Ports, in fact, are part of complex logistic networks in crowded industrialized areas near large metropolitan areas (i.e. in case of a crisis heavy haul traffic to and from the port could strongly affect traffic patterns in the bordering town and requires effective coordination with transportation authorities, local police and the town administration). In port security interaction, coordination and communication among these entities are one of the critical aspects to be investigated during training exercises. Current security port training is based on simple, predefined live exercises. This training has significant limitations in capability and provides insignificant value for facing real threats. Usually, intensive operations are carried out in Ports, due to this fact, live training sessions, regardless of scale, are quite expensive. These factors provide the evidence that the development of training solutions based on simulation represents a highly reliable approach to replicate complex scenarios for the different actors without blocking port activities.

Furthermore, simulation approach is very useful in supporting strategic and operative assessments.

In order to support learning and assessment in decision making for critical security situations in ports, the authors developed a Federation where each active actor operates the respective resources and cooperates with others. For instance, it is possible to set up scenarios involving Coast Guard, Port Authority, Custom and Border Protections as well as Private Security agencies cooperating against different threats (i.e. smuggling, infiltration through ships, port attacks from ground, air or water).

By this approach the simulation supports the definition of security and Standard Operating Procedures (SOP) during the pre alert conditions; it supports distributed simulation to a relevant number of entities and low-cost training sessions in a cooperative manner.

Virtual Port was originally designed to support training of terminal operators (i.e. cranes and truck drivers); it evolved to an interoperable federation for extending the training from single vehicle/device to procedure and policies by supporting cooperative sessions. The paper proposes some aspects related to benefits and problems in developing simulators for security purposes from this legacy federation. It highlights the importance of proper design in interoperable models.

STATE OF ART IN PORT SECURITY TRAINING

Even nowadays Training and Exercise on Security Procedures in Harbors are typically managed in traditional ways, mainly live events. The entire harbor operations are informed that on a certain date a training session for a particular kind of threat will be performed. For instance, the Genoa Harbor (the most important Italian Harbor and a primary Mediterranean port) identified 27 different kinds of incidents (related to both security and safety) and every year organized one or two training events focused on a specific accident. These events vary from simple safety procedure violations (i.e. accidents occurred to harbor operators, complex scenarios such as a ship approaching with alleged hazardous materials, dirty bomb threats). Simulation based training is diffuse but often with attention into a single actor (police, coast guard) and some specific kind of threats. Many efforts are done to carry out innovative researches to face traditional, symmetric attacks, i.e. glider, underwater unmanned vehicles, etc, but sometimes these do not represent the real danger. It is much more easy to prepare an homemade bomb with ammonium nitrate and bring it by car inside a ferry terminal rather than use a submarine; such events are hard to prevent as well train people to do that. Furthermore, prevention of "asymmetric" threats and, in general, after-disaster or after-attack operations requires strong co-operation among all the actors; training for this kind of distributed co-operative task is possible only by simulation.

WHY USING SIMULATION

The use of M&S to evaluate the impact of security matters on logistics/industrial facilities is justified by the need to analyze complex interactions among numerous factors. Simulation techniques are fundamental to test operators and agencies and evaluate impacts of security requirements on people and cargo flows. Security equipment and procedures for logistics facilities can usually be grouped into two major classes:

- Internal: Security control of logistics flow
- External: Security control of external component

The first class refers to all the additional operations that must be carried out to ensure that goods are not dangerous (i.e. container scanning, gate controls, custom checks, etc.). The second class refers to the fact that external entities (i.e. terrorists) might be introduced in some points of the facility's logistics flow (i.e. contamination of food along the supply chain) or may affect the efficiency of the entire infrastructure (i.e. attacks on a port/airport). One interesting aspect is that intensive logistic flows of entities (i.e. people, materials, etc.) have a mutual influence on one another and can be a potential threat. In fact, with regard to the security activity, intrusion models must be used to control potential interference between Cargo and people in various areas of ports. In this field of application, M&S is often used to study processes, performance levels and costs with regard to regular operating conditions. These simulation models can be used to support an assessment of impact that safety and security procedures may have on logistics throughput as well an evaluation of the role that human resources play in ensuring reliable surveillance and control during continuous and discrete monitoring (i.e. monitoring and inspections for facility border surveillance).

Such models enable managers and decision-makers to evaluate quantitatively the effectiveness of man/machine interactions during standard operations and emergencies (i.e. high and very high intrusion alert). Using these models for risk analysis purposes helps to identify the best practices for emergencies related to relevant targets. These simulators can be used to perform tests related to the effectiveness of different organizational models within critical structures, providing experimental results about the impact of the consequences with regard to interfacing with public institutions. In operative terms, the general experience obtained from simulation models helps to improve integration of automated control systems through ad hoc architecture design which combines the information coming from different sources and evaluating the impact resulting from the use of all possible alternative systems. Simulation tools can be used to carry out a comprehensive assessment of the system's security weakness by modeling its constitutive parts and providing the means for verifying the performance level for the system as a whole, during the simulation run.

VIRTUAL PORT FEDERATION CHARACHTERISTICS

Virtual Port is a distributed interoperable stochastic simulator which includes different players representing port security active actors. The threats are playable characters, therefore the authors are evaluating the adoption of their Intelligent Agents to drive CGF for representing both the menacing behavior as well as other elements (i.e. passengers behavior, other ships, terminals, etc). Stochastic components are affecting internal and external flows of the port, in addition they affect detection, tracking or engagement. This federation includes a federate devoted to Control & Debriefing that supports After Action Review (AAR), as well as online review during the exercise. It generates a local parallel virtual port based on recorded actions until the present moment and moves in space and time to investigate while the simulation is still running on the federation, then eventually closes it and join back to the evolving scenario. The instructor controls environmental conditions (i.e. daytime, fog, rain, sea, wind) as well as scenario and situations, (i.e. number and type of ships involved). This federation automatically controls all the trucks and carriers not directly used by operators. Currently the following objects are part of virtual Port (Fig.1):

- Vessels (i.e. cargo ships, boats, coast guard)
- Cranes (i.e. mobile cranes, reach stackers, gantry cranes, etc.)
- Vehicles (i.e. internal and external trucks, as well as police and custom cars, security, ambulances)
- Aircraft (i.e. helicopter and planes)
- UAV (air, water and underwater)
- Cameras and Sensors (i.e. terminal camera, radar, sonar).
- Gates (i.e. port access gate and terminal gates).
- People (i.e. passengers, workers, threats).



Figure 1. Sample of Virtual Port Federates

Being originated by training solution for port operators this environment is a virtual simulator supporting immersive solutions (i.e. scalable cave from 270° to 360°) and it is integrated with motion platforms (6 degree of freedom), therefore due the modeling approach it is scalable on laptop and operator can navigate the virtual world with mouse and/or joysticks.

The federation allows relocating control of the objects among the different federates by a quick configuration system and scalable solutions for different training sessions.

Virtual Port includes the integration with biomedical devices measuring stress levels. These systems were originally integrated in order to support research for crane operator performances; being compact they support training and investigation even in port security. Virtual Port includes a High Performance Computer (HPC) federate developed to support the integration with complex computational models running on an computer grid that eventually can take care of simulating complex phenomena (i.e. fallout).

Currently the Virtual Port operates on workstations and laptop. The authors developed a mobile solution for training in ports based on a shelter obtained from a 40' high cube container; this solution is very easy to move and include cave, instructor workstation, multiple training stations, equipped area for connecting laptops, as well as debriefing area with interactive board for AAR and exercise overview.

The use of Virtual Port as a synthetic environment for training in Security and Safety procedures is in an early phase. Authors are developing research activities based on a scenario definition devoted to support Training procedures and configuration of the whole architecture for safety and security assessment in Ports using the federates and models proposed in figures 2-9.

In this initial phase, authors focus on the use of the Federate SEAPORTS (fig. 9) in order to calculate the throughput of containers according to different security procedures.

The example proposed in the following paragraph Virtual Port Test MOP and MOE Experimental Analysis regards the study of the port behavior and relative resources under the effect of different security levels. The performance indexes taken into consideration are defined as *moved TEUs per structural unit*. These indexes measure the total efficiency of the terminal container in terms of available resources utilization.

The most important resources (structural units) are: berth length, dimensions of the yard area, number of portainers. The equations (1), (2), (3) define the performance indexes from a mathematical point of view.

$$Index1 = \frac{TEUs}{BerthLenght}$$
(1)

$$Index2 = \frac{TEUs}{YardArea}$$
(2)

$$Index3 = \frac{TEUs}{PortainerNumber}$$
(3)



Figure 2. Virtual Port HLA Simulation of Custom Operations



Figure 3. AUV (Autonomous Underwater Vehicle) Federated in the Virtual Port



Figure 5. Helicopter Checking Terminal and Port Situation



Figure 6. New Generation UAV (Unmanned Aerial Vehicle) Federated in the Virtual Port



Figure 7. Virtual Model of Terminal Fences and Cameras



Figure 8. Oil Spills Simulation



Figure 9. Terminal Operation and Inspection Procedures Simulation (i.e. Gamma Rays and Manual Inspections) for Container Terminals

VIRTUAL PORT TEST MOP AND MOE EXPERIMENTAL ANALYSIS

Definition of Measure of Performance (MOP) and Measure of Effectiveness (MOE) play a fundamental role, especially when high level of complexity arises from the necessity to train several organizations different by nature to cooperate together on new complex scenarios. The authors propose some preliminary metrics for supporting these aspects and guaranteeing the capability of measuring individual progress and combined capabilities along the training process as well as the effectiveness of the procedures for facing specific threats.

Some preliminary analysis have been made in order to validate the simulation model. The results show that in this configuration of Virtual Port are processed 100.000 TEUs/month. Such values are very similar to the statistics recorded in several terminal containers with comparable berth, yard area and movement equipment.

The objective of the application example is the evaluation of the impact on the system of different security levels. Increasing the security level, the percentage of inspected containers increase as well.

Considering the stochastic aspects implemented in the model SEAPORT part of the Federation (movement equipment productivity, time between arrivals of ships, and so on) many simulation runs are needed to obtain significant results.

The mean values of the performance indexes, output from the simulation model, versus the different security levels (from 0% to 32 %) are summarized in table1.

Security Level	Index 1	Index 2	Index 3
[%]	[TEUs/month]	[TEUs/heactares]	[TEUs/Portainer]
0.00%	1,459	15,424	166,582
1.00%	1,447	15,307	165,321
2.00%	1,436	15,189	164,040
4.00%	1,413	14,946	161,422
8.00%	1,366	14,442	155,981
16.00%	1,264	13,370	144,403
32.00%	1,047	11,067	119,525

Table 1 – Results of simulation runs

The decrease of performance indexes in correspondence of higher security level highlights the system propensity to reach the block of all the main activities. The values taken by index 3 (that expresses the portainers efficiency) change from 155901 TEUs/n°portainers (security level 5%) to 88969 TEUs/n°portainers (security level 50%), with an efficiency reduction of 43%. The decreasing trend is also shown on the graph in figure 10.

Security Impact on Terminal Performances



Fig. 10 – Performance Indexes vs Security Alerts

Starting from the analysis of the performance indexes it's possible to make some economic considerations to define the right tools to achieve the goal in term of security, (i.e. more technology advances or better reorganization of internal logistics).

The results show that several parameters influence a target function of a port, underlining again the importance of considering all the agents operating in a harbor to reproduce realism of such a system.

CONCLUSIONS

In Port Protection, and in Homeland Security, it is important to analyze and be trained to asymmetric threats. Technology advances allow to identify any kind of weapons or technological threat. It is a big issue to detect one glider but it is of course much more difficult to detect one in a thousand trucks with a bomb made up by simple commercial bag of 50 lb ammonium nitrate entering into port area. It is clear that the security procedures are fundamental for all the actors operating in a port, for this reason a new concept of simulation based training has to be developed and diffuse to support this co-operative approach. At the same time we have also to consider that the port cannot be closed or its operations reduced without big impacts on the whole logistic network. Decision makers have to take into consideration even this aspect, both in training and analysis.

The goal of Virtual Port Federation is to provide a high level of complexity and "asymmetry" of threats but a simple way to develop exercises in order to provide numerous and realistic Training Events involving a huge number of people or actors, in order to represent the real entropy of a port.

REFERENCES

- Amico Vince, Guha R., Bruzzone A.G. (2000) "Critical Issues in Simulation", Proc.of SCSC, Vancouver, July
- Bocca E., Bruzzone A.G., R.A. (2006) "Algorithms devoted to Reproduce Human Modifiers in Polyfunctional Agents", Proc.of SCSC, Calgary, Aug
- Bruzzone A.G., Reverberi A., Cianci R., Bocca E., Fumagalli M.S, Ambra R. (2009) "Modeling Human Modifier Diffusion in Social Networks", Proceedings of I/ITSEC2009, Orlando, November 30-December 4
- Bruzzone A.G., Giribone P. (1998) "Decision-Support Systems and Simulation for Logistics: Moving Forward for a Distributed, Real-Time, Interactive Simulation Environment", Proceedings of the Annual Simulation Symposium IEEE, Boston, 4-9 April
- Bruzzone A.G., Cantice G. (2008) "Software Agents Italian Army Developments and Researches", Technical Report GESI User Group, Wien, October
- Bruzzone A.G., Mosca R., Massei M., Bocca E. (2008) "Critical Issues in HLA Integration: PIOVRA CGF vs. Wargaming System", Proceedings of Summer Computer Simulation Conference, Edinburgh, June
- Bruzzone A.G., Massei M., B.M. (2007) "Demonstration for HBM within Civil Disorder Scenarios", Proc. of SCSC, San Diego CA, July
- Bruzzone A.G., Williams E.(2005) "Summer Computer Simulation Conference", SCS Int., San Diego
- Bruzzone A.G., Page E., Uhrmacher A. (1999) "Web-based Modelling & Simulation", SCS International, San Francisco, ISBN 1-56555-156-7
- Chait R., Sciarretta A., Shorts D.(2006) "Army science & Technology analysis for Stabilization and Reconstruction operations", Tech. Report Center for Technology and National Security Policy. October
- Fishwick, P. (1995) "Simulation Model Design and Execution", Prentice Hall, New Jersey
- Hamilton John A. Jr., Nash David A., Pooch Udo W. (1996) "Distributed Simulation", CRC Press
- Henscheid Z., Middleton D., Bitinas E. (2007), "Pythagoras: An Agent-Based Simulation Environment", Proc.and Bulletin of the International Data Farming Community, Issue 1

- Kuhl F., Weatherly R., Dahmann J., Kuhl F., Jones Anita, (1999) "HLA: Creating Computer Simulation Systems", Prentice Hall; ISBN: 0130225118
- Longo F, Bruzzone A.G., (2005) "Modelling and Simulation applied to security systems", Proc. of SCSC, Philadelphia, July
- Massei M., B.M., B.C. (2007) "Human Behavior Model for an HLA Federation", Proceedings of EUROSIW2007, Santa Margherita, Italy, June
- Marburger J.H., Ozolek D., Cooperstein T., Reichle S., Miller R.T., Anderson W.A., Dobrianski P. (2008) "Research & development challenges for regional Stability and Capacity Building - Executive Office of the President of the United States", Report of the NSTC on Homeland and National Security, Feb.
- Mosca R., P.Giribone & A.G.Bruzzone (1994) "Simulation & Automatic Parking in a Training System for Terminal Container Yard Management", Proceedings of ITEC94, The Hague, April 26-28
- Raybourn E.M., Roberts B., Diller D., Dubow L. (2008) "Honing intercultural engagement skills for stability operations DARWARS Ambush! NK Game Base Training", Proc. of ASC2008, Orlando
- Rizzoli A.E., Gambardella L.M., Bontempi G. (1997) "Simulation of an Intermodal Container Terminal to assist Management in the Decision-Making Process", Proc. of MODSIM9, International Congress on Modeling and Simulation, Hobart, Tasmania
- Ross-Witkowski C. (2005) "Agent-Based Models and Other Analytic Tools in Support of Stability Operations SAIC" Proc. of MORS, McLean, VA,
- Surdu J.R. Parsons D., Tran O.(2005) "The Three Block War in OneSAF," Proc. of I/ITSEC, Orlando, FL, Dec
- Viazzo S., M.B. (2004) "Simulation to Support Design and Training of Operative Procedures in Intermodal Terminals", Proceedings of HMS2004, Rio de Janeiro, Brazil, 25-30
- Zeigler B.P., Ball G., Cho H.J., Lee J.S. (1999) "Implementation of the DEVS Formalism over the HLA/RTI: Problems and Solutions", Proc. of Spring SIW, Orlando, June