SIMULATION OF MANNED & AUTONOMOUS SYSTEMS FOR CRITICAL INFRASTRUCTURE PROTECTION

Agostino G. Bruzzone[1], Marina Massei[2], Giovanni Luca Maglione[3], Riccardo Di Matteo[4], Giulio Franzinetti[5]

[1, 2] DIME University of Genoa
URL: www.itim.unige.it

[3, 4,5,] Simulation Team
Email: {maglione, riccardo.dimatteo, ...}@simulationteam.com
URL: www.simulationteam.com

[1] agostino@itim.unige.it,[2] massei@itim.unige.it, [3]malione@simulationteam.com,
[4] dimatteo@simulationteam.com, [5] giulio.franzinetti@simulationteam.com

ABSTRACT
Critical Infrastructure Protection is a rising issues in today world; considering that most of the population live on coastal area it is not surprising the fact that several of these infrastructures are located within marine scenario. Ports, piping, cables, off-shore and coastal on shore plants are being more and more targeted by asymmetric threats. Employing Autonomous Assets allows to drastically reduce the protection costs but requires to design new solutions. This paper addresses this issues with special attention to off-shore platforms respect the opportunity to improve threat assessment by innovative solutions. Indeed the paper proposes an Agent Driven stochastic simulation for reproducing a combined used of autonomous and traditional assets devoted to identify threats as well as the possibility to use it for training Unmanned Aerial Vehicles (UAV) pilots. The authors present the results of the experimental campaign obtained on a test population of unskilled operators to evaluate the possibility to diffuse the use of such approach without requiring very highly qualified expertise.

Keywords: Simulation, Critical Infrastructures, Autonomous Systems, Training, UAV, Off Shore Platforms, Asymmetric Threats

INTRODUCTION

Nowadays the geopolitical situation and the technological evolution is emphasizing the impact of critical infrastructure. This is due to several reasons: general presence of heavy threats in terms of security related to terrorist organizations, vulnerability of existing critical infrastructures to easily accessible technologies operating on different layers, such as IED (Improvised Explosive Device) cyber-attacks, autonomous systems (Abrahams et al. 2005). The technology evolution is even further emphasizing this elements because is becoming more and more common to have critical infrastructures that are remotely operated, such as happens in energy sector, with many renewable energy solutions geographically widespread and lightly supervised and protected (e.g. wind farms). Another fact is the great need of energy for human societies (McKercher et al. 2004, Mastrangelo 2005) that promotes the growth of natural gas consumption and resulting risks connected with these facilities that are sensitive to terrorist attacks (e.g. NLG terminals). All these considerations highlight the problem of critical infrastructures protection (Bruzzone et al. 2013a) and their resilience also when connected along the supply chain (Longo and Oren, 2008). One factor that is strongly affecting countermeasures effectiveness is the sustainability in terms of reliability, operational costs, efficiency etc. For these reasons, it is evident that autonomous systems represent on one hand a potential threat and on the other an interesting resource for protecting critical infrastructures (Hill 1996, Hudson 1999, Mevassvik et al. 2001, Bruzzone et al. 2011a). It is worth to mention that actually, the autonomous solutions do not cover completely the mission spectrum; often protection, patrolling, block operations are expected to be carried out by traditional assets or at least in co-operation with them. This means that it is necessary to integrate these systems to evaluate the best configuration and even to identify how to cover the different spaces domains: cyber space, space, air, land, sea surface and underwater (Bruzzone 2013, Bruzzone et al. 2013b). An interesting observation is that many critical infrastructures are located in coastal areas due to the fact that ocean traffic supports most of logistics and connection and that the majority of the population live on urbanized coastal town.

1. OFF SHORE CRITICAL INFRASTRUCTURES

So many on-shore and off-shore installations are operating in this framework and need to be addressed; it is even important to outline that off-shore installation are even more complex to be protected with reasonable costs due to their configurations as happen with off-shore platforms, off-shore wind farms, underwater pipelines and cables. From this point of view, protective

solutions should be activated to cover different domains. It is evident the complexity of this framework and the necessity to integrate different domains, approaches, platforms, systems and procedures within a highly stochastic environment; so the use of simulation represents a very good opportunity to face these challenges and to model this context (McLeod 1982, Banks1998, Bossomaier 2000, Waite 2001).

The authors have investigated since long time the protection of critical infrastructures in marine domain and in energy sector as well as there are a number of research works that show the potentials of Modeling & Simulation based approaches in this area, not only for protection but even for performances improvement (Longo et al. 2013). In this paper, the authors propose a systemic approach devoted to integrate innovative technologies over different kind of platforms to guarantee high level of protection with low costs based on the integration of autonomous systems and AI (Artificial Intelligence).

The paper proposes a case related to the protection of off-shore platforms by using autonomous systems able to identify threats through innovative procedures; for instance the use of specific algorithms and sensors on these platforms could allow to conduct face recognition of the crew of suspected boats at large distance reducing the risk of false alarms and extending protective area. In this context the use of non-lethal weapon is crucial and this approach represent a very good example to improve the protection and improve safety and reliability.

Indeed the drones could be employed to extend the range where it is possible to identify the threats, to anticipate them and to increase the time available to adopt countermeasures (Ören & Longo 2008, Bruzzone et al 2011c). As anticipated this approach is beneficial also to reduce the false alarms, furthermore increasing the capacity to discriminate between real and false alarms improve protection system credibility.

Therefore the innovative drone technology is often not completely autonomous, but needs to be integrated other traditional assets (e.g. equipment devoted to be used to intercept, discourage or engage threaths) often operated by humans; in addition the drones require usually operators and the procedures are driven by the decision makers (Longo et al. 2014). In this paper the authors adopt the MS2G (Modelling and interoperable Simulation Serious Game) for addressing these aspects in order to create a framework that could be used in multiple ways: evaluator of capability assessment for these innovative solutions, training equipment for drone operators and simulator for the definition of policies and procedures (Mosca et al 1996, Kuhl et al. 1999, Massei & Tremori 2010, Guo et al. 2011, Bruzzone et al. 2012). Indeed the authors decided to carry out an experimentation to evaluate the potential to easily train not very skilled operator in conducting such scanning procedures; the experimentation carried out with drone users allowed to evaluate the effectiveness of the MS2G solution proposed to train the operators as well as to evaluate the benefits provided by augmented reality aid and other specific algorithms (i.e. face recognition) for what the authors name wide range detection (Raybourn 2012, Bruzzone et al. 2014).

2. CURRENT SITUATION AND RELATED R&D

Among critical infrastructures that ones related to energy industry are very important and it is interesting to note that while technological accidents in the energy industry have been deeply investigated over the last decades, the issue of attacks on energy infrastructures is gaining increasing importance as production and transit areas are evolving into politically unstable and unreliable frameworks. It is necessary to consider energy domain under the security perspective for risk assessment (Burgherr et al. 2015). Indeed the discussion arises on how to optimize security of critical infrastructure facing budget constraints, technological innovation and new competitive threats. The fields of investigation include Patrolling, Sensor Coverage and Interference, Domain Protection and Blocking (Bruzzone et al. 2009, Megherbi & Xu 2011, Kranakis & Kriznac 2015). To this end, many actors (e.g. EC, US DoD, NATO and Academic Institutions) are investigating innovative options (e.g. Autonomous Systems, Manned Patrolling Assets) for protecting critical infrastructures against asymmetric threats in the maritime environment using multi-agent simulation and interoperable simulation (Enters et al. 2002, Smith 2002, Lucas et al. 2007, Matusitz 2013, Massei et al. 2014, Bruzzone et al. 2015a). Ongoing researches are even oriented to the definition of multi-layered architectures for reconfigurable autonomous assets (Brdys 2014), as well as models to support decision making process based on innovative techniques such as Artificial Neural Network and Genetic Algorithms (Bruzzone et al 2015a) and Game Theory (Ordónez et al. 2013, Vorobeychik & Letchford 2015). The diffuse employment of drones in new operative scenarios implies the necessity to design innovative training sessions for operators through LVC Simulation (Live-Virtual-Constructive) (Vince et al. 2000, Ratliff et al. 2010, Bruzzone & Longo 2013c) capable of providing rapid and efficient knowledge and skill development for drones operators (Rowe et al. 2015). This necessity is even underlined by the availability of new technological contents, such as Augmented Reality, with which operators need to interface (Miller et al. 2014). Indeed one issue is to manually pilot the unmanned aircrafts remotely by using camera image streaming and sensors information (Yang et al. 2010) in particular for complex operations such as docking or low altitude flight. Over the years, in order to avoid catastrophic damages to assets and increase missions success rate, simulation-based procedures have been designed for training operators on mission specific operational scenarios in advance (Javaid et al. 2013). Often simulation for adaptive learning is adopted to improve time-critical decision making skills (Abhyankar et al. 2014). So the development of common standard in military training and computer game simulators domains to simplify

development of new concepts and to increase capability to achieve common goals reducing negative crossover (Kuhl et al. 1999; Svane & Karisson 2003).

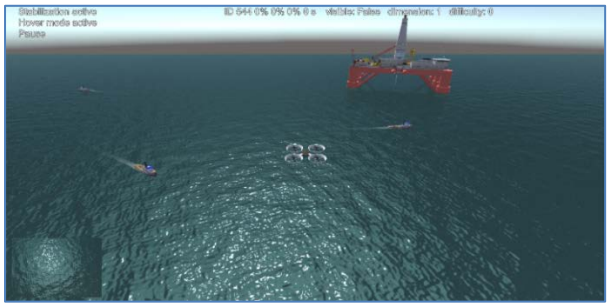

Figure 1 Scenario

3. PURPOSE OF THE SIMULATION

The authors are proposing an approach that integrates AI algorithms for face recognitions with sensors mounted on rotary wings as support for protecting offshore platforms. In this case the simulation is devoted both to understand the operative advantage of a rotary wing drone employed on off-shore platform for the decision maker and to provide a test-bed to train drones operator performing recognition activities in a hostile environment facing unconventional targets.

The simulator proposed for this case is titled SO2UCI (Simulation for Off Shore, On Shore & Underwater Critical Infrastructure) and it has been developed by the authors within the Simulation Team; SO2UCI is a simulation able to support training on protecting Off-Shore Platforms (e.g. oil rig, gas rig), On-Shore Critical Infrastructures (e.g. ports, power plants, refineries, desalinators) and Underwater Critical Infrastructures (e.g. cables, pipelines) from Asymmetric Threats using conventional assets and autonomous systems (e.g. RHIB, Helicopters, Sensors, UAV, USV, AUV, Gliders, etc.). The simulator is interoperable by using HLA (High Level Architecture) and support integration with real equipment as well as with other simulators and solutions as the SPIDER. SO2UCI integrates scenarios for training the use of specific sensors on rotary wing UAV to discriminate suspect boats invading the perimeter of Oil Rig (e.g. face recognition, thermal camera, etc.). The models have been verified by applying VV&A Procedures (Blaci et al. 1996).

In the proposed experimentation the user of the simulator is the Drone Operator. The control system of the drone is very basic and adopts simple on game interface; indeed this is due to the experimental nature of the project, but also to the consideration that most of future operators could be more familiar with this solution. Further development might possibly include the setting of a more specific control system and integrated framework with other protection systems.

The user main goal is to pilot the rotary wing drone close enough to the boats in order to activate recognition sensors, entering their range and within a specific relative position to catch the crew face. The user has to remain within the sensor range until sensors data acquisition process is over; the process is supported by information and alert provided by speakers to the boat from the drone; it is evident that for many reasons non cooperative behaviour could be expected and could lead to alert just based on additional evidence of suspect behaviours. The purpose of the experimental campaign, on the other hand, is both the evaluation of the impact of simulation for training purposes and the influence of augmented information provided by the simulation to pilots such as enabling the visibility of sensors range and of the required profile to successfully approach a suspect boat.

4. SCENARIO AND MODEL DESCRIPTION

The authors propose a scenario for training operators in controlling a remotely operated patrolling asset for an off-shore critical infrastructure protection. The scenario is set in deep water and the entities involved are:

- A Semi-Submersible platform
- Piping Infrastructures
- Small-Medium Size Boats
- Rotary Wing UAV (Umanned Autonomous Vehicle) and its Sensors
- Autonomous Underwater Vehicles

In facts the use of AUV in this testing is limited, but in other cases this allowed to cover also submerged threats and it is maintained; the simulation adopts High Level Architecture to support interoperability and could be connected with other simulators.

The simulator reproduces the physics of the entities and their control and actions. Sophisticated Intelligent Agents developed by Simulation Team are devoted to drive the entities and to reproduce behavioural model of small-medium size boats controlling their routing and speed (Bruzzone et al. 2011b).

The models of the sensors embedded in the Drone are devoted to perform crew face recognition and overall boat identification and classification in order to finalize the threat assessment based on these aspects and the boat behaviour analysis.

During the Simulation it is possible to present an augment reality where the sensors range and boat approach profile are proposed by a 3D visible volume, displayed around the fore part of the boats to help the UAV operator (Figure 2). Furthermore the simulator gives the user the possibility to visualize, at run-time, the percentage of completion of the sensors acquiring process computed as in Eq. 1

$$Completion\ \% = \frac{Time\ inside\ Working\ Range}{Nominal\ Working\ Time} \cdot 100$$

The Acquisition Process is cancelled in case the pilot exits the sensor range or adopt improper flight profiles before acquisition completion and restarts when entering the range again; the computation is referred to the single specific boat in the vicinity of the drone. Once face recognition is completed the Simulator provide a report about the time spent in performing the activity and an overall evaluation. In general the test iis

considered failed when the drone impact the water or is damaged due to a crash.

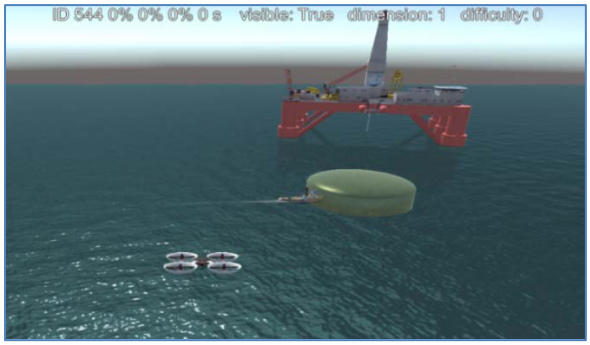

Figure 2 Simulation settings on screen top

Through the User Interface it is possible to act on the following settings:

- Augmented Reality for Sensor Range and Profile:
  - Non-Visible
  - Visible Range
- Dimension of the Sensor Range:
  - Small Range
  - Medium Range
- Difficulty Level:
  - Boats keep almost constant heading and adopt cooperative behaviour
  - Boats manoeuvre to evade the drone and adopt not cooperative behaviour

5. EXPERIMENTAL CAMPAIGN

The experimental campaign has been performed on a test population of 12 operators. The operator used were unskilled people and students, with limited or no experience in operating UAV; this approach was devoted to investigate the possibility to quickly train this kind of user to operate such procedures; it is evident that the sampling is very reduced and the results are limited and specific of the proposed case, so no general considerations could be finalized, therefore the study provide an overview about interesting consideration that actually the authors are using to conduct further development and testing. In the experimentation the operators performed 6 attempts each with constant difficulty and Sensor Range. The experimental campaign is designed to evaluate the influence of two target functions: Number of Successful Recognitions and Time to Accomplish Recognition respect the following independent variable:

- Sensor Range
- Augmented Evidence of Sensor Range
- Difficulty level

In the following each target function is analysed.

Number of Successful Recognition

From the analysis of experimental simulation data it is interesting to notice a higher number of successful recognitions for smaller Sensor Ranges. The reason behind this trend is the increased operator accuracy during the experimental tests.

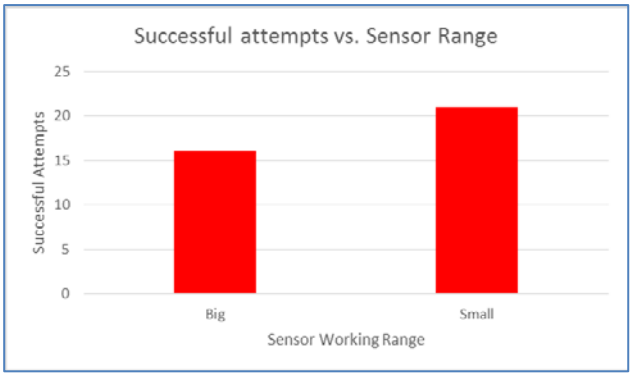

Figure 3 Successful Attempts vs. Sensor Range

Figure 4 Successful Attempts vs. Difficulty Level

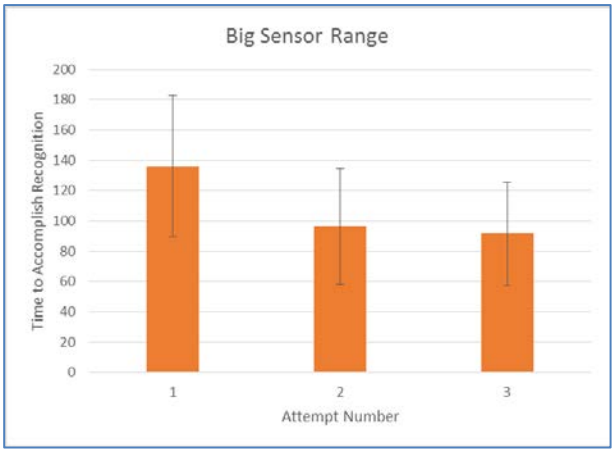

Figure 5 Time to Accomplish Recognition vs. Attempts

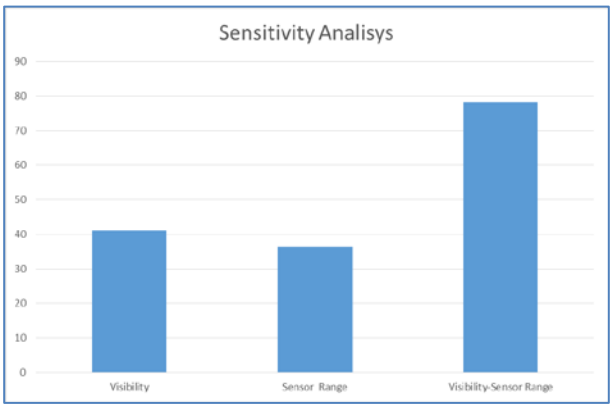

Figure 6 Influence of Visibility and Sensor Range dimension on Time to accomplish the mission

The Difficulty Level is another important aspect; in deed as expected, by increasing the not cooperative attitude of the boat to evade drone controls, the success rate of the UAV operator decreases.

Average Time to Accomplish Recognition

UAV operator performance has been evaluated in terms of time required to accomplish the first successful recognition in the scenario. The analysis of the experimental simulation data shows a positive reduction of the average time required to recognize the target over the different attempts. This result is significant even though the relative confidence band is pretty wide; the reason behind the amplitude of the confidence band is to be found in the heterogeneous nature of the UAV operator population involved in the testing campaign, indeed some of them were more keen on using serious games and were better experienced with the HMI (Human Machine Interface) than others.

The Sensitivity analysis on Time to Accomplish Recognitions, shown in the figure 6, highlights the positive influence of the Augmented Evidence of Sensor Range; indeed the average time required to perform recognitions improves when the Evidence of the Sensor Range is visible to the UAV operator through an augmented representation while flying.

The same considerations apply to Sensor Range size, in other words the higher the sensor range, the lower the average time to accomplish recognition. From the same figure it is possible to notice the influence of the combination of the two parameters, so to say, users provided with visible sensor range, needs less time to complete the mission if drone sensor range is high.

The experimental campaign has been performed using SPIDER (Simulation Practical Immersive Dynamic Environment for Reengineering) Interactive CAVE (Cave Automatic Virtual Environment) developed by Simulation Team. The SPIDER intended use is to support Live Virtual Constructive Simulations and even Augmented and Virtual Reality for single users or for multiple users for immersive and collaborative use of simulators (Figure 7).

6. CONCLUSIONS

The experimental campaign obtained on the test population shows the effectiveness of simulation both for training drones operators in using such unconventional asset to perform strategic tasks such as critical infrastructure patrolling and to evaluate the impact of additional information provided to operators during flights.

It is worth to notice, from experimental data, how the size of the sensor range have a negative impact on the number of success while it has a positive impact on the time to accomplish recognition; the operator of the drone with smaller sensor range configuration results often more careful, paying more attention to accomplish recognition, successfully completing more missions, but spending quite some time; on the other hand, the operator flying with large range configuration is often more proactive, failing more attempts, but resulting faster (in average) when succeeding.

The positives results obtained during the testing campaign show the potential use of this simulation as training tool as well as means of evaluating the effectiveness of employing an autonomous system in such a complex scenario.

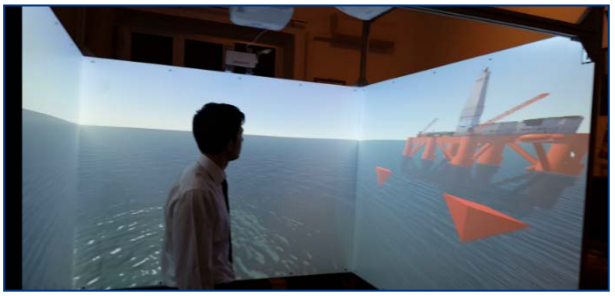

Figure 7 Testing facility, the SPIDER

REFERENCES

Abhyankar, K., Polakonda, R., Ganapathy, S., & Barrerra, K. (2014, June). Model-based simulation systems for adaptive training in time-critical decision making. In NAECON 2014-IEEE National Aerospace and Electronics Conference (pp. 149-152). IEEE.

Abrahams A., Boisot M., Bharathy Gnana (2005) “Simulating the Knowledge Transfer Dilemma: Lessons for Security and Counter-Terrorism”, Proceedings of SCSC, CherryHills, NJ, July

Amico Vince, Guha R., Bruzzone A.G. (2000) "Critical Issues in Simulation", Proceedings of Summer Computer Simulation Conference, Vancouver, July

Balci O., Glasow P., Muessig P, Page E.H., Sikora J., Solick S.,Youngblood S. (1996) "DoD Verification, Validation and Accreditation (VV&A) Recommended Practices Guide", Defense Modeling and Simulation Office, Alexandria, VA, November

Banks J. (1998) “Handbook of Simulation: Principles, Methodology, Advances, Applications, and Practice”, John Wiley and Sons, NYC

Bossomaier T., Green G.D. (2000) “Complex Systems”, Cambridge University Press, Cambridge

Brdys, M. A. (2014). Integrated monitoring, control and security of Critical Infrastructure Systems. Annual Reviews in Control, 38(1), 47-70.

Bruzzone, A., Cunha, G., Elfrey, P., & Tremori, A. (2009). Simulation for education in resource management in homeland security. Proc. of SCSC, Istanbul, Turkey, July, pp. 231-238

Bruzzone, A. G., Massei, M., Madeo, F., Tarone, F., & Gunal, M. (2011a). Simulating marine asymmetric scenarios for testing different C2 maturity levels. Proceedings of ICCRTS2011, Quebec, Canada, June

Bruzzone, A. G., Tremori, A., Tarone, F., & Madeo, F. (2011b). Intelligent agents driving computer generated forces for simulating human behaviour in

urban riots. International Journal of Simulation and Process Modelling, 6(4), 308-316.

Bruzzone, A.G., Massei, M., Tremori, A., Longo, F., Madeo, F., Tarone, F. (2011c) “Maritime security: emerging technologies for Asymmetric Threats”, Proceedings of the European Modeling and Simulation Symposium, EMSS, Rome, Italy, September, pp.775-781

Bruzzone, A., Longo, F., Nicoletti, L., & Diaz, R. (2012). Traffic controllers and ships pilots training in marine ports environments. In Proceedings of the 2012 Symposium on Emerging Applications of M&S in Industry and Academia Symposium, SCS, Orlando, FL, April

Bruzzone A.G. (2013) “New Challenges for Modelling & Simulation in Maritime Domain”, Keynote Speech at SpringSim2013, San Diego, CA, April

Bruzzone A, Longo F, Tremori A (2013a). An interoperable simulation framework for protecting port as critical infrastructures. International Journal of System of Systems Engineering, vol. 4, p. 243-260, ISSN: 1748-0671

Bruzzone A.G., Fontaine J., Berni A., Brizzolara, S., Longo F., Dato L., Poggi S., Dallorto M. (2013b) "Simulating the marine domain as an extended framework for joint collaboration and competition among autonomous systems", Proc. of DHSS, Athens, Greece, September

Bruzzone, A. G., & Longo, F. (2013c). 3D simulation as training tool in container terminals: The TRAINPORTS simulator. J.of Manufacturing Systems, 32(1), 85-98.

Bruzzone A.G., Massei M., Agresta M., Poggi, S., Camponeschi F., Camponeschi M. (2014) “Addressing Strategic Challenges on Mega Cities through MS2G”, Proc.of I3M2014, Bordeaux, France, September

Bruzzone, A. G., Massei, M., Tremori, A., Crespo Pereira, D., Franzinetti, G., Oddone, M., Carrera, A., Camponeschi, F., Dato, L., (2015). Autonomous system simulation to improve scenario awareness and capabilities to protect marine, off-shore and coastal critical infrastructure. In Proceedings of the 8th International Workshop on Applied Modeling and Simulation, WAMS, September Bergeggi, Italy.

Burgherr, P., Giroux, J., & Spada, M. (2015). Accidents in the Energy Sector and Energy Infrastructure Attacks in the Context of Energy Security. European. Journal of Risk Regoulation, 6, 271.

Enders, W., & Sandler, T. (2002). Patterns of transnational terrorism, 1970–1999: alternative time-series estimates. International Studies Quarterly, 46(2), 145-165.

Guo S., Bai F., Hu X (2011) "Simulation software as a service and Service-Oriented Simulation Experiment", Procededings of IEEE International Conference on Information Reuse and Integration, August, pp.113-116

Hill David (1996) "Object-Oriented Simulation", Addison Wesley, Reading MA

Hudson, R. A., & Majeska, M. (1999, September). The sociology and psychology of terrorism: Who becomes a terrorist and why Washington, DC: Federal Research Division, Library of Congress.

Javaid, A. Y., Sun, W., & Alam, M. (2013, December). UAVSim: A simulation testbed for unmanned aerial vehicle network cyber security analysis. In 2013 IEEE Globecom Workshops (GC Wkshps) (pp. 1432-1436). IEEE.

Kranakis, E., & Krizanc, D. (2015). Optimization Problems in Infrastructure Security. In International Symposium on Foundations and Practice of Security (pp. 3-13). Springer International Publishing.

Kuhl F., Weatherly R., Dahmann J. (1999) "Creating Computer Simulation Systems: An Introduction to the High Level Architecture", Prentice Hall, NYC.

Longo, F., Ören, T. (2008). Supply chain vulnerability and resilience: A state of the art overview. Proceedings of the 20th European Modeling and Simulation Symposium, EMSS 2008, pp. 527-533.

Longo, F., Huerta, A., Nicoletti, L. (2013). Performance analysis of a Southern Mediterranean seaport via discrete-event simulation. Strojniski Vestnik/Journal of Mechanical Engineering, 59 (9), pp. 517-525.

Longo, F., Chiurco, A., Musmanno, R., Nicoletti, L. (2014). Operative and procedural cooperative training in marine ports, Journal of Computational Science, 10, pp. 97-107.

Lucas, T. W., Sanchez, S. M., Sickinger, L. R., Martinez, F., & Roginski, J. W. (2007). Defense and homeland security applications of multi-agent simulations. In 2007 Winter Simulation Conference (pp. 138-149). IEEE.

Massei, M., Tremori, A. (2010) “Mobile training solutions based on ST_VP: an HLA virtual simulation for training and virtual prototyping within ports”, Proc. of International Workshop on Applied Modeling and Simulation, St.Petersburg, Russia, May

Massei, M., Tremori, A., Poggi, S., Nicoletti, L. (2013) “HLA-based real time distributed simulation of a marine port for training purposes”, Int. Journal Simul. Process Model. 8, 42

Mastrangelo, Erin. (2005) "Overview of US Legislation and Regulations Affecting Offshore Natural Gas and Oil Activity." Energy Information Administration, Office of Oil &Gas, www.eia.gov/pub/oil_gas/natural_gas/feature_articles/2005/offshore/offshore.pdf, September

Matusitz, J. A. (2013). Terrorism & communication: A critical introduction. Loa Angeles: Sage.

McKercher, B., & Hui, E. L. (2004). Terrorism, economic uncertainty and outbound travel from Hong Kong. Journal of Travel & Tourism Marketing, 15(2-3), 99-115.

McLeod J. (1982) "Computer Modeling and Simulation: Principles of Good Practice", SCS, San Diego

Megherbi, D. B., & Xu, D. (2011). Multi-agent distributed dynamic scheduling for large distributed Critical Key Infrastructures and Resources (CKIR) surveillance and monitoring. In Technologies for Homeland Security (HST), 2011 IEEE International Conference on (pp. 426-433). IEEE.

Mevassvik, O. M., Bråthen, K., & Hansen, B. J. (2001). A Simulation Tool to Assess Recognized Maritime Picture Production in C2 Systems. In Proc. of the 6th International Command and Control Research and Technology Symposium, Annapolis, USA.

Miller, B.E., Fewer, J.H., Riggs, W.C., (2014) JHU/APL augmented reality training systems (arts) Proceedings in Fall Simulation Interoperability Workshop (pp. 309-316); September; Orlando; United States.

Mosca, R., Bruzzone, A. G., & Costa, S. (1996). Simulation as a support for training personnel in security procedures. Simulation Series, 28, 251-255.

Ören T., Longo F., (2008). Emergence, anticipation and multisimulation: Bases for conflict simulation Proceedings of the 20th European Modeling and Simulation Symposium, EMSS 2008, pp. 546-555

Ordónez, F., Tambe, M., Jara, J. F., Jain, M., Kiekintveld, C., & Tsai, J. (2013). Deployed security games for patrol planning. In Handbook of Operations Research for Homeland Security (pp. 45-72). Springer New York.

Ratliff, D.A., Fedak, O.S., Geis, D.P. (2010) UAS deployed live training: Perception or reality? In Proceedins of 66th Forum of the American Helicopter Society (pp. 2576-2582), May, Phoenix, AZ.

Raybourn, E.M. 2012. Beyond serious games: Transmedia for more effective training & education, Proc. DHSS2012, Rome, Italy

Rowe, L. J., Conwell, S. L., Morris, S. A., & Schill, N. P. (2015). Using Best Practices as a Way Forward for Remotely Piloted Aircraft Operators: Integrated Combat Operations Training-Research Testbed. In Handbook of Unmanned Aerial Vehicles (pp. 2505-2523). Springer Netherlands.

Smith, R. (2002, March). Counter terrorism simulation: a new breed of federation. In Proceedings of the Spring 2002 Simulation Interoperability Workshop.

Svane, T., & Karlsson, L. (2003). Suggesting a Common Framework for the Classification of Military Training and Computer Game Simulators. In SCSC (pp. 271-278). Society for Computer Simulation International; 1998.

Vorobeychik, Y., & Letchford, J. (2015) “Securing interdependent assets”, Autonomous Agents and Multi-Agent Systems, 29(2), 305-333.

Waite, Bill (2001) "M&S Professional Body-of Knowledge", Proc. of SCSC, Orlando Fl, July

Yang, J., Jiang, G. H., & Chao, J. G. (2010). A cross drone image-based manual control rendezvous and docking method. Journal of astronautics, 31(5), 1398-1404.