

UNIVERSITY OF GENOVA

POLYTECHNIC SCHOOL

DIME

**Department of Mechanical, Energy, Management
and Transportation Engineering**



Ph.D. THESIS

in

**MACHINE AND SYSTEMS ENGINEERING FOR ENERGY, THE
ENVIRONMENT AND TRANSPORT**

Curriculum

**MATHEMATICAL ENGINEERING AND SIMULATION
XXXI CICLE**

**MODELLING VIRTUAL ENVIRONMENT FOR
ADVANCED NAVAL SIMULATION**

Supervisor:

Chiar.^{mo} Prof. Ing. Agostino Bruzzone

Candidate:

Riccardo Di Matteo

2018/2019

MODELING VIRTUAL ENVIRONMENT FOR ADVANCED NAVAL SIMULATION

Abstract

This thesis proposes a new virtual simulation environment designed as element of an interoperable federation of simulator to support the investigation of complex scenarios over the Extended Maritime Framework (EMF).

Extended Maritime Framework is six spaces environment (Underwater, Water surface, Ground, Air, Space, and Cyberspace) where parties involved in Joint Naval Operations act.

The amount of unmanned vehicles involved in the simulation arise the importance of the Communication modelling, thus the relevance of Cyberspace.

The research is applied to complex cases (one applied to deep waters and one to coast and littoral protection) as examples to validate this approach; these cases involve different kind of traditional assets (e.g. satellites, helicopters, ships, submarines, underwater sensor infrastructure, etc.) interact dynamically and collaborate with new autonomous systems (i.e. AUV, Gliders, USV and UAV).

The use of virtual simulation is devoted to support validation of new concepts and investigation of collaborative engineering solutions by providing a virtual representation of the current situation; this approach support the creation of dynamic interoperable immersive framework that could support training for Man in the Loop, education and tactical decision introducing the Man on the Loop concepts.

The research and development of the Autonomous Underwater Vehicles requires continuous testing so a time effective approach can result a very useful tool. In this context the simulation can be useful to better understand the behaviour of Unmanned Vehicles and to avoid useless experimentations and their costs finding problems before doing them.

This research project proposes the creation of a virtual environment with the aim to see and understand a Joint Naval Scenario. The study will be focusing especially on the integration of Autonomous Systems with traditional assets; the proposed simulation deals especially with collaborative operation involving different types of Autonomous Underwater Vehicles (AUV), Unmanned Surface Vehicles (USV) and UAV (Unmanned Aerial Vehicle). The author develops an interoperable virtual simulation devoted to present the overall situation for supervision considering also the sensor capabilities, communications and mission effectiveness that results dependent of the different asset interaction over a complex heterogeneous network.

The aim of this research is to develop a flexible virtual simulation solution as crucial element of an HLA federation able to address the complexity of Extended Maritime Framework (EMF). Indeed this new generation of marine interoperable simulation is a strategic advantage for investigating the problems related to the operational use of autonomous systems and to finding new ways to use them respect to different scenarios.

The research deal with the creation of two scenarios, one related to military operations and another one on coastal and littoral protection where the virtual simulation propose the overall

situation and allows to navigate into the virtual world considering the complex physics affecting movement, perception, interaction and communication.

By this approach, it becomes evident the capability to identify, by experimental analysis within the virtual world, the new solutions in terms of engineering and technological configuration of the different systems and vehicles as well as new operational models and tactics to address the specific mission environment.

The case of study is a maritime scenario with a representation of heterogeneous network frameworks that involves multiple vehicles both naval and aerial including AUVs, USVs, gliders, helicopter, ships, submarines, satellite, buoys and sensors.

For the sake of clarity aerial communications will be represented divided from underwater ones. A connection point for the latter will be set on the keel line of surface vessels representing communication happening via acoustic modem.

To represent limits in underwater communications, underwater signals have been considerably slowed down in order to have a more realistic comparison with aerial ones. A maximum communication distance is set, beyond which no communication can take place.

To ensure interoperability the HLA Standard (IEEE 1516 evolved) is adopted to federate other simulators so to allow its extensibility for other case studies.

Two different scenarios are modelled in 3D visualization: Open Water and Port Protection. The first one aims to simulate interactions between traditional assets in Extended Maritime Framework (EMF) such as satellite, navy ships, submarines, NATO Research Vessels (NRVs), helicopters, with new generation unmanned assets as AUV, Gliders, UAV, USV

and the mutual advantage the subjects involved in the scenario can have; in other word, the increase in persistence, interoperability and efficacy.

The second scenario models the behaviour of unmanned assets, an AUV and an USV, patrolling a harbour to find possible threats. This aims to develop an algorithm to lead patrolling path toward an optimum, guaranteeing a high probability of success in the safest way reducing human involvement in the scenario.

End users of the simulation face a graphical 3D representation of the scenario where assets would be represented. He can moves in the scenario through a Free Camera in Graphic User Interface (GUI) configured to entitle users to move around the scene and observe the 3D sea scenario. In this way, players are able to move freely in the synthetic environment in order to choose the best perspective of the scene.

The work is intended to provide a valid tool to evaluate the defencelessness of on-shore and offshore critical infrastructures that could includes the use of new technologies to take care of security best and preserve themselves against disasters both on economical and environmental ones.

Glossary

ABIED:	Air-Borne IED
AUVs:	Autonomous Underwater Vehicles
BBIED:	Body-Borne IEDIED
C-IED:	Counter Improvised Explosive Device
CASW:	Cooperative Anti-Submarine Warfare
CAPRICORN:	CIMIC And Planning Research In Complex Operational Realistic Network
CAX:	Computer Assisted eXercise
CBRN:	Chemical, Biological, Radiological e Nuclear
CIMIC:	Civil Military Cooperation
CIP:	Critical Infrastructure Protection
COA:	Course Of Actions
COIED:	Command-Operated IED
CTIA:	Common Training Instrumentation Architecture
CWIED:	Command-Wire IED
DACTYL:	Dynamic simulator of Autonomous robotic Carrier, Transporter, with hand for handling, Yanking and Loading
DAMA:	Defence Against Mortar Attack
DBNL:	Distributed Networked Battle Labs
DIES IRAE:	Disasters, Incidents and Emergencies Simulation Interoperable Relief Advanced Evaluator

DIMEFIL:	Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, legal
DIT:	Department of Technological Innovations
DON:	Distributed Observer Network
DVx2:	Distributed Virtual eXperience and eXercise
EMF:	Extended Maritime Framework
EOD:	Explosive Ordnance Disposal
FAO:	Food and Agriculture Organization
FOM:	Federation Object Model
FRC:	Fatah Revolutionary Council
GUI:	Graphic User Interface
HBM:	Human Behaviour Modifiers
HLA:	High-Level Architecture
HPP:	Harbour and Port Protection
HSS:	Health Service Support,
IA:	Intelligent Agent
IA-CGF:	Intelligent Agent Computer Generated Forces
ICT:	Information and communications technology
IDRASS:	Immersive Disaster Relief and Autonomous System Simulation
IDPs:	Internally Displaced Persons
IED:	Improvised Explosive Device

IPHITOS:	Interoperable simulation of a Protection solution based on ligHt Interceptor Tackler operating in Outer Space
IPIED:	Improvised Projectile IED
IRAM:	Improvised Rocket Assisted Mortars
ISM:	Improvised Sea Mine
ISRTA:	Intelligence, Surveillance, Reconnaissance and Target Acquisition
ISSEM:	Interoperable Security Simulation for extended Maritime framework
JEANS:	Joint Environment for Advanced Naval Simulation
LNG:	Liquefied Natural Gas
LVBIED:	Large Vehicle-Borne IED
MALICIA:	Model of Advanced pLanner for Interoperable Computer Interactive simulAtion
MANPADS:	Man-Portable Air Defence Systems
MEL/MIL:	Master Event List / Master Incident List
MCWS:	Marine Cyber Warfare Simulator
M&S:	Modelling & Simulation
MIMOS:	Movimento Italiano Modellazione e Simulazione
MMALT:	Moon and Mars Assets Location Tool
MoM:	Measures of Merits
MPA:	Maritime Patrolling Aircraft:
MS2G:	Modelling, interoperable Simulation and Serious Game

MTBF:	Mean Time Between Failures
MTTR:	Mean Time To Repair
NASA:	National Aeronautics and Space Administration
NATO DAT POW:	NATO Defence Against Terrorism Program Of Work
NLC:	Non-Lethal Capabilities
NGO:	Non Governmental Organization
NURC:	NATO Undersea Research Centre
OLP:	Organizzazione per la Liberazione della Palestina
OMT:	Object Model Template
PANOPEA:	Piracy Asymmetric Naval Operation Patterns modelling for Education & Analysis
PBIED:	Person-Borne IED
PIC:	Protection of Critical Infrastructure
PLC:	Programmable Logic Controller
PP:	Protection of harbours and Ports
RCIED:	Radio Controlled IED
ROV:	Remotely Operated underwater Vehicle
RPA:	Remotely Piloted Aircraft
RPG:	Rocket Propelled Grenade
RTI:	Run-Time Infrastructure

SA3C4:	Simulation of Autonomous systems to Augment scenarios Awareness and Capability in joint Cooperation within traditional assets to protect marine littoral and Coastal Critical infrastructure
SACLANTCEN:	Supreme Allied Commander Europe Atlantic Undersea Research Centre
SaaS:	Simulation as a Service
SATCOM:	SATellite COMmunication
SEE:	Simulation Exploration Experience
SIED:	Suicide IED
SIMCJOH:	Simulation of Multi Coalition Joint Operations involving Human modelling
SIMCJOH VIC:	Simulation of Multi Coalition Joint Operations involving Human modelling Virtual Interoperable Commander
SIMCJOH VIS:	Simulation of Multi Coalition Joint Operations involving Human modelling Virtual Interoperable Simulator
SISO:	Simulation Interoperability Standards Organization
SME:	Subject Matter Experts
SOM:	Simulation Object Model
SPIDER:	Simulation Practical Immersive Dynamic Environment for Reengineering
SVBIED:	Suicide Vehicle-Borne IED

T-REX:	Threat network simulation for REactive eXperience
TENA:	Test and Training Enabling Architecture
TOIED:	Timer-Operated IED
UAV:	Unmanned Aerial Vehicle
UGV:	Unmanned Ground Vehicle
UNCTAD:	United Nations Conference on Trade And Development
UNIFLI:	United Nation Force for Large Improvement of Eblanon
USV:	Unmanned Surface Vehicle
UVBIED:	Unmanned Vehicle-Borne IED
UVED:	Under-Vehicle IED
UWSIM:	UnderWater Simulator
UxV:	Unmanned Vehicle
V&V:	Verification and Validation
VBIED:	Vehicle- Borne IED
VLCC:	Very Large Crude Carrier
VOIED:	Victim-operated IED
VPN:	Virtual Private Network
VV&A:	Validation, Verification and Accreditation
WBIED:	Water-Borne IED

Table of content

1	OPERATIONAL ENVIRONMENT AND STATE OF THE ART	- 32 -
1.1	TERRORISM	- 32 -
1.1.1	<i>Maritime Terrorism</i>	- 35 -
1.1.2	<i>Counter-Terrorism</i>	- 43 -
1.1.3	<i>Major Maritime Terrorist Events of Recent Years</i>	- 45 -
1.2	COUNTER-TERRORISM SIMULATION	- 54 -
1.2.1	<i>Application Fields of the DAT (Defense Against Terrorism)</i>	- 54 -
1.2.2	<i>DVx2 and Crowdsourcing</i>	- 57 -
1.3	HYBRID WARFARE	- 70 -
1.3.1	<i>Hybrid Warfare Simulation</i>	- 71 -
1.3.2	<i>T-Rex & Cyber Attack</i>	- 72 -
1.4	OIL PLATFORMS	- 80 -
1.4.1	<i>Mobile Offshore Drilling Rigs</i>	- 80 -
1.4.2	<i>Fixed Offshore Drilling Rigs</i>	- 84 -
1.5	NATURAL GAS PLANTS	- 88 -
1.6	SUBMARINE PIPELINES.....	- 91 -
1.7	UXV & SAFETY.....	- 95 -
1.7.1	<i>CASE STUDIES ON UxV SIMULATORS</i>	- 100 -
2	PRINCIPAL UTILIZED TECHNOLOGIES	- 107 -
2.1	INTEROPERABILITY AND HLA.....	- 107 -
2.2	UNITY 3D	- 115 -

3	JESSI	- 118 -
3.1	MODELS	- 118 -
3.2	SCENARIOS	- 139 -
3.2.1	<i>Port Scenario: Port Protection</i>	- 141 -
3.2.2	<i>Oil Platform Monitoring</i>	- 142 -
3.2.3	<i>Glider Fleet</i>	- 144 -
3.2.4	<i>Military defense from a missile attack</i>	- 145 -
3.2.5	<i>AUV Fleet</i>	- 145 -
3.3	SEA GLIDER	- 147 -
3.4	VALIDATION AND VALIDATION	- 153 -
4	OTHER EXPERIENCES	- 155 -
4.1	SEE	- 155 -
4.2	SIMCJOH	- 173 -
4.3	MALICIA	- 188 -
4.4	DIES IRAE	- 196 -
4.5	SCUBA DIVER	- 213 -
5	CONCLUSIONS	218
	BIBLIOGRAPHY	221

Introduction

The following thesis project aims to provide a detailed illustration about how to create, implement and use an interoperable virtual environment closely connected to the problem of critical infrastructures protection and port facilities.

Maritime Security is a major issue that represent a strategic context for National and International interests. Indeed the evolution of the socio economic scenario even overstresses these aspects (Bruzzzone et al. 2015).

The steady growth of international maritime goods traffic is a very consolidated phenomenon. During the period between 2010 and 2016, world traffic increased in average annually in percentages about 4.16%. The United States confirms this growth trend, showing a positive trend with an import that sees in average an annual growth of 4,47% and an export that sees in average an annual growth of 4,89%. On the other hand, Europe, suffering from the effect of the recession, sees the trend of exports growing in average of 3,54% while imports show a more 'dancer' trend in a range that goes from a maximum of + 9.6% up to a minimum of -2.8% with an annual average of +2,67%. These figures are cumulative and represent a very significant overall increase, as proposed in Figure 1 (Rogers 2014).

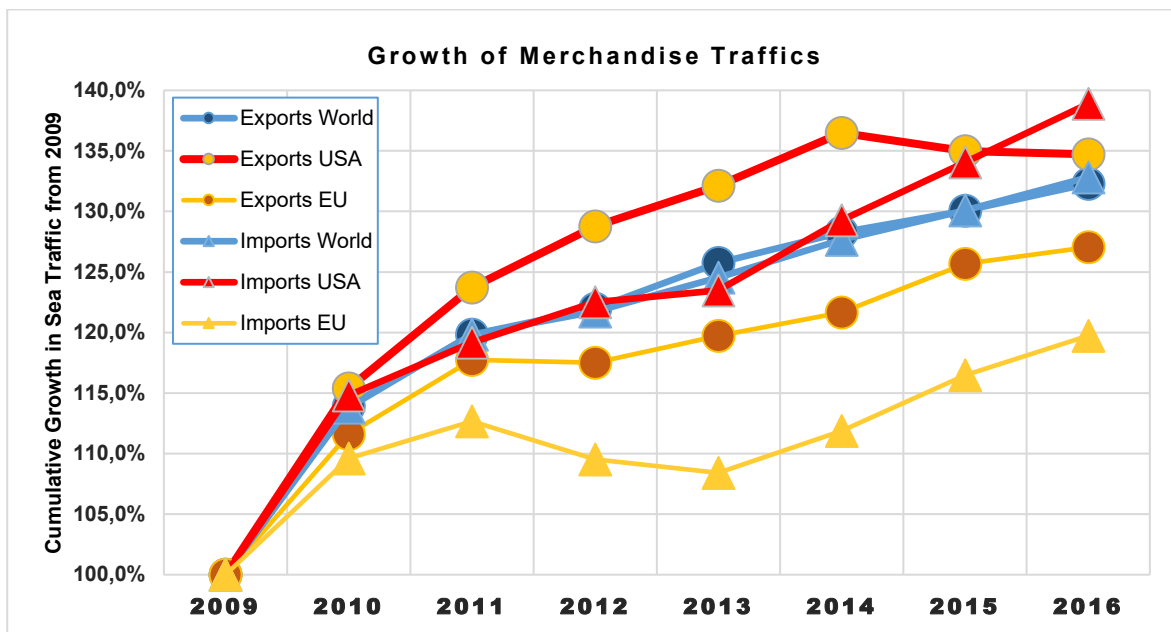


Figure 1: Increase in total world traffic (Source of Data UNCTAD: United Nations Conference on Trade And Development)

In fact, the logistics of the raw materials and goods flows is largely based on navigation lines. In this way, ports are strategic entry gates that are essential for the maintenance of industrial activities and just as indispensable for the sustainability of the vast majority of existing economies. Figure 2 provides an interesting overview of the increase in global maritime traffic between 2013 and 2014.

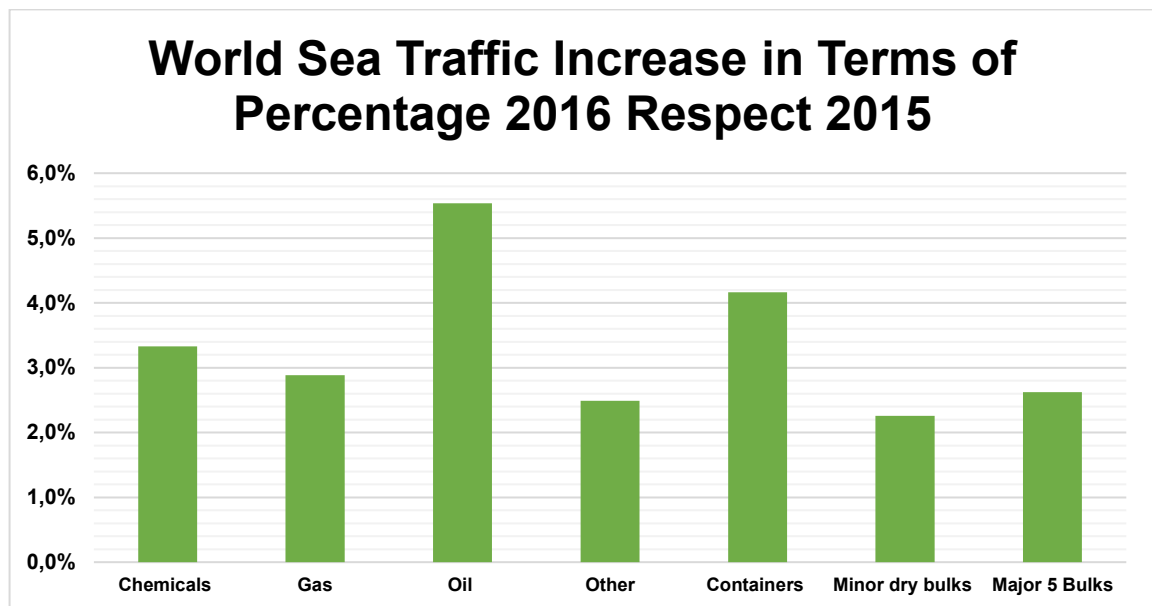


Figure 2: Trends in global maritime traffic between 2015 and 2016

It should also be considered that 44% of the world population resides near the coastline and that the trend of this data is growing (Choen et al 1997).

A large amount of critical infrastructures is located within coastal areas (e.g. power plants, fuel depots, refineries, water treatment plants, waste treatment, etc.) due to population density and / or logistical and technological advantages deriving from facing the sea.

In addition to these aspects, offshore resources for food (e.g. oil platforms, gas plants, wind farms) are normally located not far from the coast up to 200 nautical miles (Matrangelo 2005).

Finally, it is important to outline that the most strategic assets are concentrated near the coast and consist of critical infrastructures such as pipelines and underwater communication cables.

Before proceeding further, however, it is right to open a small parenthesis concerning the meaning of the term critical infrastructure. A first definition of critical infrastructures is given in Communication 702 of the Commission of the European Communities of 2004:

"Those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments" (Commission of the European Communities, 2004).

The decision of the European Commission to issue the aforementioned explanation arose following the meeting convened in June 2004 to establish a strategy to protect critical infrastructures from terrorist attacks.

Also within Communication 702 there is a notable classification of infrastructures belonging to this category:

- Energy plants and networks (for example, electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system)
- Systems communication and information technology (for example, telecommunications, broadcasting systems, software, hardware and networks including the Internet)
- Finance (for example, banking, securities and investment)

- The health system (for example, hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services)
- Food supply (for example, safety, production means, wholesale distribution and food industry)
- Water supply (for example, dams, storage, treatment and networks)
- Transport (for example, airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems)
- Production, storage and transport of dangerous substances (for example, chemical, biological, radiological and nuclear materials)
- The administration (for example, critical services, facilities, information networks, assets and key national sites and monuments) (Commission of the European Communities, 2004).

From the list just mentioned, it can be seen how these plants are very different and consequently, how difficult it is to adopt an adequate security strategy.

Therefore, from 2004 onwards, during the design of such infrastructures, the engineer is obliged to consider not only the different natural problems such as earthquakes, tidal waves and atmospheric cataclysms but also a further phenomenon that is constantly increasing: the terrorism. The latter has become so important to constitute one of the fields that arouses greater fears and complications.

Today we are witnessing an evolution of the terrorist threat and new forms of war defined as, for example, asymmetric (irregular forces using guerrilla methods and terrorist attacks against a conventional force) or hybrid (both conventional and suicidal, terrorist and media attacks).

Just recently we have witnessed the use of the first Cyber Weapon capable of physically destroying critical system components; since 2010 it is appearing a new virus, called Stuxnet, that, developed perhaps by Israel to hit the enrichment facilities of Uranium in Iran, has destroyed more than 1000 centrifuges. This cyber weapon specialized in attacking SCADA systems (Supervisory Control and Data Acquisition), recognizing the types and constructors (particular attention to Siemens systems), has led to the destruction of 10% of Iranian capacity without firing a single shot. Just to understand the entity of the cyber-attack, international analyses have shown that three years after the spread of the virus, Stuxnet is still present not only in the Iranian SCADA systems (47%), but also in 23% of the Indian ones and in over 2% of the Chinese ones. This virus is a real sleeper and intelligent weapon and today it affects about all other countries in the world. Indeed, the state with the number of maximum infected systems is USA where there is the 27% of the contaminated automation systems, but also Israel itself, India, England, Australia are highly contaminated. This cyber-attack highlights how the threat has changed and how crucial it is to develop new solutions capable of protecting critical infrastructures at 360 degrees compared to attacks from land, air, sea and even network.

Indeed, even in the real context there has been a proliferation of types of attacks linked to new types of threats born thanks to the easy availability of explosives with high potential and to the development of new techniques and technologies for the creation of primers:

- IED: Improvised Controlled Explosive
- ABIED: Air-Borne IED
- BBIED: Body-Borne IEDIED
- COIED: Command-Operated IED
- CWIED: Command-Wire IED
- IPIED: Improvised Projectile IED
- ISM: Improvised Sea Mine
- IRAM: Improvised Rocket Assisted Mortars
- LVBIED: Large Vehicle-Borne IED
- PBIED: Person-Borne IED
- RCIED: Radio Controlled IED
- RPG: Rocket Propelled Grenade
- SIED: Suicide IED
- SVBIED: Suicide Vehicle-Borne IED
- TOIED: Timer-Operated IED
- UVBIED: Unmanned Vehicle-Borne IED
- UVED: Under-Vehicle IED
- VBIED: Vehicle- Borne IED

- VOIED: Victim-operated IED
- WBIED: Water-Borne IED

In this context, the industrial plants and critical infrastructures often have a strategic value that makes them potential targets of the most diverse asymmetrical attack systems. Furthermore, it is evident that many of these plants are on the coast or in coastal waters (On-Shore and Off-Shore) for reasons of opportunity and necessity, making their protection critical with innovative tools such as autonomous systems.







VBIED	Type	Amount of Explosive	Overpressure Lethal Radius	Minimum Radius to evacuate	Wound risk for crystal and glasses
	Sedan	225 kg	30 m	460 m	460 m
	Big Sedan	450 kg	38 m	535 m	535 m
	Van	1800 kg	61 m	840 m	840 m
	Pickup Truck	4500 kg	91 m	1150 m	1150 m
	Tank Truck	13600 kg	137 m	1990 m	1990 m
	Articulated lorry	27200 kg	183 m	2135 m	2135 m

Figure 3: VBIED table

Often, we miss the meaning of asymmetric value of these threats, or the difficulty of reducing the vulnerability of a plant to these aspects. From this point of view, the table in figure 3 is very helpful.

It is evident that a VBIED based on a truck (trailer and trailer) potentially generates a lethal 180-meter wave with possible damage caused by glass breaking up to 2100 meters, requiring the evacuation of an area of 12 km². This means that the safety zone of a critical system, even compared to such a simple and brutal threat, is invasive in any installation in a modern western context. Just think about a port often adjacent (if not immersed) in the urban context and the transport network or look at the example provided in the proposed case relating to the LNG plant of La Spezia below.



Figure 4: Example of the explosion radius of a VBIED in the La Spezia coast It.

Therefore, it becomes necessary to develop new technological, operational and procedural solutions to face this threat.

From this point of view, NATO has activated since 2004 a special program for the Defence of Terrorism (DAT) that has gone to investigate some of the lines of intervention to mitigate this problem in relation to the threats felt by the Alliance countries with particular reference to:

- MANPADS Large Aircraft Survivability against Man-Portable Air Defence Systems
- PP Protection of Harbours and Ports;
- RPG Protection of Helicopters from Rocket-Propelled Grenades
- C-IED Countering Improvised Explosive Devices
- EOD Explosive Ordnance Disposal and Consequence Management;
- CBRN Detection, Protection and Defeat of Chemical, Biological, Radiological and Nuclear Weapons
- ISRTA Technology for Intelligence, Surveillance, Reconnaissance and Target Acquisition of Terrorists
- DAMA Defence against Mortar Attacks
- CIP Critical Infrastructure Protection
- NLC Non-Lethal Capabilities

The simulator developed in this research aim precisely at create support tools to address these issues with particular reference to the protection of Industrial Plants and Critical Infrastructures (Bruzzone et al. 2018c).

In order to achieve a good target in the field of security, large costs and a large consumption of human resources are often required.

Therefore, in this field, the research is very active and one of the most probable ways of overcoming these problems is to use self-guided vehicles. The latter are among the first candidates for these purposes also due the fact that the researches in this field are very active. Autonomous systems, nowadays, are provided of artificial intelligences that allows them to be able to patrol and identify possible threats very effectively and quickly, certainly less than those that would employ a human. In view of these considerations, their use in safety routines is seriously considered.

Autonomous vehicles are devices that, once programmed, are able to perform pre-established tasks, choose the priority of these and modify their routine in the event that something different from the pre-established occurs. However, we must always bear in mind that these are machines not equipped with real intelligence and therefore improvisation, for this reason, the programmer must first identify all the possible causes that could change the standard behaviour. Subsequently it will have to create a logic of behaviour in case these circumstances occur.

Now there is a multitude of autonomous vehicles that can fly, surf, go on land and even underwater. Many have already been developed, others are being tested and still others are being designed. The functions they can carry out are even more numerous and different, enough to consider the employment of them not only in the field of protection but also in different sectors: from military to transport, production, etc. etc.

In a maritime scenario the drone that can be used are very different, for example we can use underwater vehicles like AUVs (Autonomous Underwater Vehicles) (figure 5), ROVs (Remotely Operated underwater Vehicles) (figure 5) or Gliders (figure 6). The latter are AUVs of the latest generation with a completely innovative propulsion system: the normal autonomous underwater vehicles, in fact, use a propeller driven by an electric motor, the Gliders, moves using the currents and moving the position of its centre of gravity through a piston that longitudinally displaces a concentrated mass.



Figure 5: on the left an example of AUV (image taken from <https://www.offshoreenergytoday.com/tag/auv/>), on the right an example of ROV (image taken from <http://www.oceaneering.com/rovs/rov-systems/spectrum-rov/>)

The wings of the Glider behave similarly to those of an airplane generating lift in the direction of motion. This strategy allows to considerably limit the use of electric power for propulsion, thus conferring an autonomy of about one month, enormously greater than propellered propeller systems



Figure 6: Sea Glider (image taken from <http://auvac.org/configurations/view/49>)

It is necessary to consider that the sea trials necessary for testing the behaviour of underwater drones are quite expensive both in terms of resources and in terms of time. Due this reason, the simulation becomes fundamental: with modern technology, we are able to recreate the physical behaviours of self-guided vehicles very closely to the reality, thus avoiding the tests that would lead to wrong procedures. In this way, simulation is assuming a role even more decisive, since it saves time and resources.

At this point, it is natural to wonder about the meaning of Simulation: it is the imitation of one or more operations carried out over time by a process or a system of the real world. To simulate it is necessary to recreate a model that includes in itself all the key characteristics and behaviours (or functions) of what is being simulated. If this model represents the imitated system, the simulation reproduces the operations performed by it.

Thanks to the simulations, it is possible to evaluate and predict the behaviour of the real system under the imposition of specific conditions by the user. It is a very powerful experimental tool of analysis and for this reason it is used in many contexts including training, education, security engineering and in the videogames. Given its peculiarity in

predicting events, the simulation can also be used to show how a possible event could have been carried out differently, changing certain conditions or actions taken during the simulation. It is often used in the design phase for expensive systems or difficult and dangerous construction.

Very often, we make the mistake to exchange the simulators for videogames, in particular the models made with 3D graphics software: indeed, the simulator, in order to be recognized as such, must be tested as well as the veracity of the results obtained by it; the videogames, instead, do not require such procedures. There are three classifications for software that reproduce virtual environments:

1. Videogames: software based purely on entertainment and reproducing non-real facts.
2. Serious Games: software designed for user training / entertainment; the behaviours of the models recreated in the virtual environment, are the real ones but the chain of events is forced to be more dynamic than the reality, in order not to bore the user.
3. Simulators: software based on true imitation of reality. The real behaviour of models or chains of events are not altered in any way.

In essence, simulation is the logical-mathematical-procedural reconstruction of a real conceptual model. In general, this model is complicated and can be decomposed into several smaller and simpler sub-models, interconnected with each other; they are these interconnections that usually make the problem difficult to manage and analyse without the aid of simulation. Just think of the classic example of a simple production chain made up of

just two machines and we want to know their daily, monthly and yearly flow of output pieces.

In order to find them, we must take into account a large number of variables such as:

- processing and arrival times of raw materials;
- defects of raw materials;
- breakdowns of equipment;
- breakage of workpieces;
- absences;
- shifts;
- holidays and illnesses of workers etc.

All these variables are interconnected and influence the results searched by us.

Without the aid of a computer, it becomes very difficult to find the result of this example and, if the designer wanted to observe the change of the analysed variables by modifying some input data, it would be almost obligatory to develop a simulator on it. Indeed, with a simulator, it would be enough to make new runs of the software modifying the input variables and then analysing the effects on the results. This would allow him to make choices and, above all, to avoid errors during the design phase. Indeed, these kinds of errors are expensive to eliminate in case they are detected only after the start of the construction of the plant.

To develop a good, well-designed simulation model, it is almost mandatory to follow certain procedures. In the first instance, we must carefully study the problem to be reproduced in order to define the objectives and variables that we want to analyse. In this way, we can limit

the phenomenon and include superfluous things or, worse, forget fundamental details. In this phase, it is very important to define all the possible input and output variables: a careful study carried out in this first phase, saves time in the later stages and, at the same time, avoid future changes that could compromise the program structure.

Once we have finished the analysis, we move on to the development of a conceptual model, defining the entities, their behaviours and the variables associated with them in order to reproduce the model in computer language.

After this last phase, it is necessary to validate the model: to do it we have to compare it with the real simulated process and possibly asking subject matter experts whether the model reproduce faithfully the reality, or it should be modified.

To conclude, in order to have usable data from the simulator, that is they predict the behaviour of the analysed real system, it is essential to study the input data. Indeed, in this phase, it is necessary to collect and analyse the input data that will allow defining the operating parameters of the system (such as it can be the processing times in the example of the production chain). We have always reminded that a well-developed conceptual model but with one or more wrong parameters will produce completely wrong results that will lead to the invalidation of the simulator or, even worse, to wrong choices at design phase. If in the model there are stochastic and undetermined parameters, we have to use the techniques of probability calculation, thanks to which we can construct a probability distribution for each input data, in order not to neglect any possible eventuality.

At this point, we can finally write the model in computer-mathematical terms, calibrate it and evaluate it. The most used computer languages are the general purpose such as C++, C#, Java, Pascal, but there are also applications already developed such as Simul8, Arena Simulation, Micro Saint etc., that we can use depending on the problems examined. Obviously, the latter are very easy and quick to use but they have little versatility compared to general-purpose programming languages. To simulate small size problems, you can also use common programs like Excel or Spreadsheet.

Finally, once the simulation model has been created, it is necessary to validate it: to do this, it is not enough to start the simulation only once and check if it returns a true result, but we need to do many launches and analyse the results statistically. Indeed, a single run, if the developed simulator is stochastic and non-deterministic, represents only one of the various (almost infinite) possible evolutions of the system. The quantity and length of the iterations should be determined at this stage. Filtered the possible transients, we can estimate a range of values in which the analysed parameters of the studied problem can oscillate: this band is called the confidence interval.

When the simulation is very sophisticated, namely when the model to be simulated is sufficiently complex and includes more complicated sub-models, each requiring a multitude of calculations, there is the risk that the simulation becomes 'heavy' even for a modern computer and that it is inevitably slowed down. To avoid this inconvenience, it is useful to develop multiple simulators, one for each sub-model, designed to communicate with each other. In this way, the simulation instead of evolving along a purely sequential line, takes

place in separate and parallel tracks, drastically decreasing the calculation time for each single step. On the other hand, however, you lose the comfort and convenience of having the simulator in a single program and in one computer: if you want to simulate the process you will need as many PCs as the individual simulators. To obtain connectable and interchangeable programs, communication standards have been developed that standardize the information exchanged by the various software. These standards, HLA (High-Level Architecture) among all, are the architecture with which to structure the code using general-purpose languages, and they are devolved purely to the simulation. Using the HLA, the simulators can interact with each other, exchanging data and events to each other, in order to influence the respective simulations.

The interactions between the different software are managed by the run-time infrastructure (RTI: Run-Time Infrastructure) of which there are several types such as PITCH, MAK, PORTICO etc. These standards are widely used in the engineering sector and in civil and military training.

Therefore, the previously mentioned configuration, characterized by several simulators operating in parallel and by the mutual exchange of data and values, puts the time management as a critical issue: the simulators must be synchronized with each other so that they communicate correctly. In the case the simulators are not correctly synchronized, it could happen that a software, with less calculations to manage than another one interacting with it, performs its steps quickly and advance to the next steps before the other simulator. At this point, the fastest software would exchange with the second one data that do not

belong to the instant in which the other simulator is, but it would transmit results of computations that in time history are more advanced.

In this regard, it is fundamental to take into account the three different times that distinguish the simulation: the Wall clock Time, the Scenario Time and the Logical Time. The first is the real time, the current time in which we are, different depending on the location in which we find ourselves. The Scenario Time is the time in which the simulation is set that could have a precise date or not; its speed depends on the settings defined by the user or by the programmer and only in rare cases can it also coincide with the Wall clock Time. This second time is closely related to the simulation as it allows us to understand when the latter is set and especially how long the events that happened in the virtual world would take place, if they really happened. The third and last time, the Logical Time, is a value of the software used to indicate the Scenario Time: essentially it is the value of a single step of the calculation logic in terms of time, expressed in seconds or milliseconds. For example, if the Logical Time is 0.1 seconds and the simulation is at step 10, the Scenario Time is at 1 second after the start (we simulated a second of activity).

With this in mind, it is clear that the possibility of modifying the Logical Time is essential for the communication between two or more different simulators. Unfortunately, this is not always possible, and it is for this reason that some software to reproduce virtual environments are not compatible with interoperability.

When a simulator is federated to a federation, time is no longer managed by it but by the RTI. The latter sets the Logical Time and ensures that all the federates respect it: in practice,

the simulators must communicate to the RTI the term of the logical-mathematical steps to be performed in a single step, then wait for the permission of the federation to advance to next moment. This technique allows simulators to always be synchronized with each other and not to come across the problem described above.

There are different configurations of the simulation speed and the main ones are essentially three:

- Real Time: one second of the Logical Time corresponds to a second of the real one.
- Scaled real-Time: the simulation speed is higher or lower than the Wall clock Time, the real-world clock.
- As-fast-as-possible: the simulation speed is the highest we can have, in this configuration of course the progress of the time is dictated by the slower simulator.

Therefore, HLA is an excellent tool to let more simulators communicate with each other and it allows to recreate extremely complex environments that only one simulator would not be able to manage. This, together with the reusability of the model for future implementations and the versatility that in this way it is guaranteed to the simulator, led to the choice to use this type of architecture for the virtual environment we have developed.

Returning to maritime safety, it is evident due to the complexity of the scenario described, the need to use the simulation as a tool of investigation due to their intrinsic practicality.

In many maritime contexts, defence policies need to be reviewed taking into account the very dynamic nature of emerging threats, as well as the need to protect large infrastructure with multiple points of high vulnerability.

From this point of view the use of autonomous systems and heterogeneous sensor networks could allow the development of new sustainable solutions to improve security, reduce vulnerability as well as to increase safety. Indeed, for the latter motivation Industry 4.0 integrates all automation technologies and, among others the new category of the so-called UxVs (Unmanned Vehicles), i.e. all those remote ground, aquatic (surface or underwater) or aerial (fixed or rotary wing) vehicles operating with different levels of autonomy, from remotely operated to fully autonomous.

Unmanned vehicles are characterized by many advantages, ranging from their agility and speed in reaching places that would be otherwise difficult to access, to their potential in replacing humans in the presence of dangers and to their expendable nature. Due to these characteristics, UxVs are becoming popular and spreading exponentially among many different application fields, with special attention to the lightest and less expensive models (Salvini 2017). Such versatility is reflected by their dissemination which is monitored and studied with great interest by the authorities and agencies involved in security and prevention in all areas, and therefore also by INAIL, in particular by DIT, the Department of Technological Innovations (Clarke et al. 2014; Di Donato 2017).



Figure 7: IDRASS Simulator operating Autonomous Systems inside Industrial Plants

In Italy, DIT is also assessing its potential through research work aimed at promoting its diffusion for reducing the workers exposure to high risks and difficult tasks, where human presence was supposed to be indispensable up to now and to ensure safe inspections and monitoring to maintain the safety of hard-to-access structures and work equipment (Spanu et al. 2016).

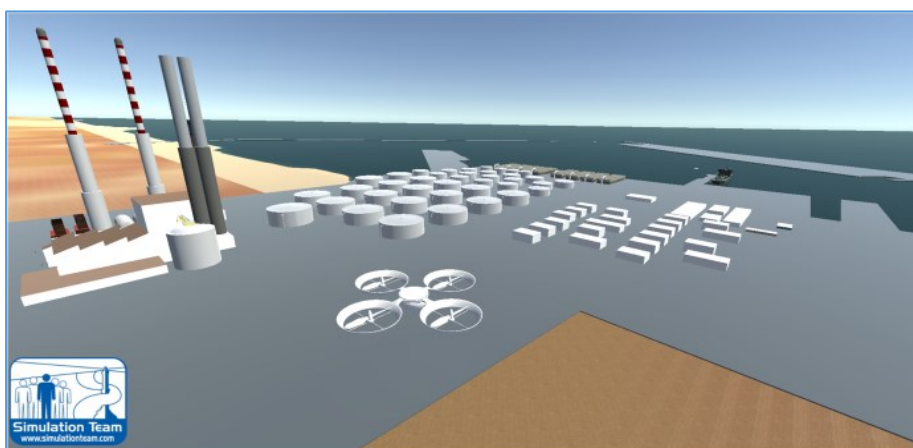


Figure 8: UAV overview within Critical Infrastructure Protection Simulator, T-REX

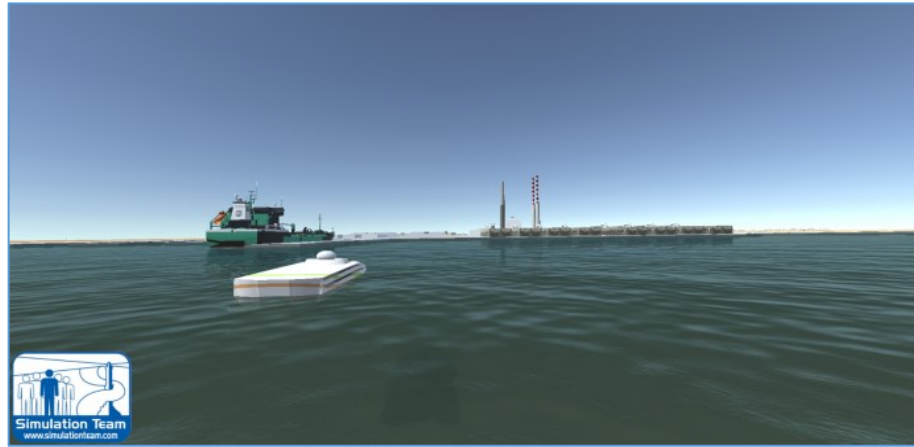


Figure 9 T-REX combined protection of Port Framework by USV and other Autonomous Systems

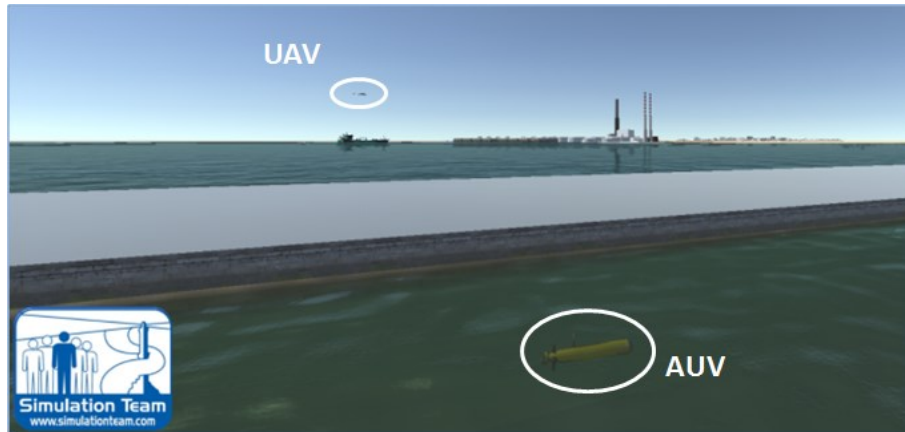


Figure 10: AUV patrolling around the Critical Infrastructure in cooperation with UAV

Today efforts are made to promote the spread of Autonomous Systems, given their possible employment for prevention on safety, therefore it is not possible to ignore the fact that the introduction of such a new technology, even though one of its objectives is Risk reduction, can result itself a carrier of new risks and dangers that require to be investigated.

Not being, these new solutions, still used permanently in this field, it is necessary to define the architecture, the technological requirements, the policies and the procedures of use, as well as their reliability and efficiency (Know et al 2008). For all these purposes, the

simulation represents a promising approach able to support the development of innovative training equipment, to promote the diffusion and service of new technologies (Waite 2001). Therefore, considering all these elements, it is fundamental for the development the use of simulators able to solve these problems and to adapt dynamically to the evolutions of these scenarios (2013c Bruzzone et al.).

For these reasons, we are evaluating the interoperable simulation to the state of the art, as the best approach in this field and they are measuring the numerous initiatives proposed through the networks of excellence and international organizations and institutions.

This work aims to examine the development of an interoperable simulation environment to study the combined use of autonomous and traditional systems in the Extended Maritime Framework (EMF) (i.e. the surface of the sea, the coast, the underwater environment, airspace, space, and cybernetic level) to protect critical infrastructures (Bruzzone 2015) and to investigate the possible employments of UxVs.

In fact, the concept of the Extended Maritime Framework (EMF) was developed to take into account the strong correlation between the different sectors and the need to include them in a single common setting (2013b Bruzzone et al.). The EMF represents a very critical environment in which the importance of interoperability is emphasized by the multiple nature of the battlefield and the complexity of specific heterogeneous networks among its members.

In addition to these elements, as anticipated, critical infrastructures are also present in this context, including strategic resources, such as submarine cables and pipelines, ports, as well as offshore and on-shore plants, terminals, etc.

The use of autonomous systems for the protection of critical infrastructures is very promising to reduce the vulnerability in this environment considering all the different domains. Therefore, it is clear the importance of investigating these solutions both with qualitative models and with extensive experimentation. Moreover, in this context it is fundamental to study the interoperability of autonomous systems with traditional vehicles (for example helicopters, boats, ships, MPA, etc.) which presents itself as a critical issue in this scenario. Probably simulation is the only method able to develop this ability to investigate and to evaluate a priori the most effective strategic solutions to face these challenges.

Furthermore, the adoption of HLA has also led to consider the idea of using this simulation to support education and training and therefore to adopt the SaaS (Simulation as a Service) paradigm already successfully tested in the DVx 2 simulator. (Bruzzone et al., 2014b).

Therefore, the objectives of this interoperable simulation on the protection of a complex maritime scenario (ISSEM: Interoperable Security Simulation for the Extended Maritime Framework) is to establish the guidelines for the combined use of autonomous systems and traditional vehicles. The simulator should be able to combine behavioural models and the data transmission network (i.e. the vehicles that communicate with each other) with the simulation of critical infrastructures. In this way, it will be a powerful tool for evaluating the effectiveness of the solutions studied regarding the protection of strategic resources in the

maritime framework extended to all environments (i.e. considering the surface of the sea, the coast, the underwater environment, the airspace, the space, and the cybernetic level).

Obviously, some of these models will have to be developed ad hoc to reproduce new elements (for example fleets or swarms of autonomous systems) and many traditional systems will require revisions in order to be usable in this context.

Therefore, the creation of this ISSEM federation represents the opportunity to develop a strategic capacity in the modelling and analysis of the Extended Maritime Framework for the protection of coasts, shores and related infrastructures present.

Another important contribution made by ISSEM is the possibility of coupling the simulation of critical infrastructures, including the effects deriving from compromised safety, with that of new autonomous systems and traditional solutions.

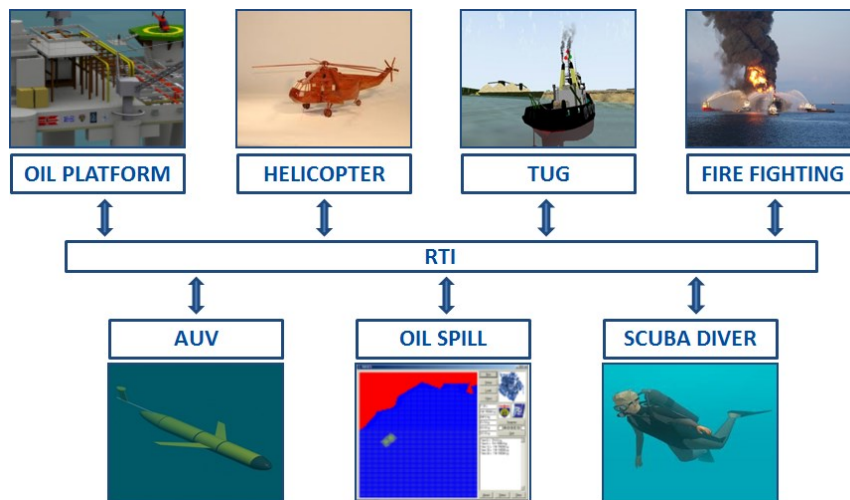


Figure 10: Example of an ISSEM federation ISSEM

The concept is based on the models already applied in the context of natural and industrial disasters (Giribone et al.1994, Bruzzone & Massei 2006, Bruzzone et al 2014d). In fact in this context it is necessary to be able not only to estimate the reduction of vulnerability, but also to assess the damage resulting from attacks to different targets through specific mathematical functions that take into account the strategic role of the affected activities, their costs, and their implications on society. This means that if a power plant is damaged so that it has to suspend its activities for a certain period, the damage would also affect urban activities that require its services, or in the case of oil and gas plants, their arrest could generate significant implications (Bruzzone et al. 2014a) direct and indirect on population and environment. An example of ISSEM federation designed to address these issues is presented in Figure 10.

Another important aspect to consider carefully, is the identification of the project requirements needed to create a collaborative simulation distributed to all potential users. Indeed, with this approach it becomes possible to evaluate the performances provided by unmanned systems when they are integrated with today's existing naval, air and surface devices, used in the protection of marine and coastal critical infrastructures (e.g. cables, submarine pipelines, harbours).

The final goal of ISSEM is therefore, the creation of an HLA federation of simulators and the related guidelines for making it able to extend it further respecting the standards for interoperability. The decision to use these reference standards for M & S is also motivated by the availability of software and a multi-simulation facility already developed on the

marine environment based on HLA (Massei et al. 2010, Bruzzone et al. 2013a, Bruzzone et al., 2013b, Bruzzone et al., 2013c).

In order to obtain valuable results and to create an effective demonstration with limited resources, it is crucial to define the boundary conditions of the scenario to be simulated in the ISSEM federation. This means that the virtual environment should focus on a specific scenario defined by common agreement between the different partners and it should analyse, therefore, only specific cases of strategic importance for maritime safety. In this context, the modelling of threats, as well as the simulation of the coordination of available resources, are critical because they are asymmetrical maritime scenarios (Mevassvik et al., Bruzzone et al. 2011a). To succeed in the exposed intentions, it is fundamental to federate objects with intelligence within the scenario, that is to use the IA-CGF (Intelligent Agent Computer Generated Forces) already used in the field of maritime security for other scenarios (Bruzzone, Tremori, Massei 2011b).

It is important to define this scenario in a way that allows ISSEM to demonstrate its general capabilities in relation to its dual use (defence and civil application). From this point of view it is advisable to combine the identification of the type of critical infrastructures to be studied (i.e. oil platforms, commercial ports) with the expectations of the business world on sectors related to industries and critical plants in this context (for example oil and gas, sea transport and terminals).

As anticipated ISSEM represents a first step also in relation to the activation of a maritime security initiative. The general objectives are to interface with industrial applications and

territorial security, and therefore it may be necessary to address the defence theme more specifically. Therefore, on this subject, a special version of the ISSEM federation should be adapted to deal with the details of this case.

The defence scenario should require a development plan to ensure stakeholder involvement and exploitation of results. The above could be achieved by activating various activities including:

- A survey on models and simulators that have the possibility of being integrated into the Federation
- Detailed definition of the objectives of the Federation, the Environment and the Scenario of the Mission and Architecture
- Definition of the configuration of the Federation for the first experimentation aimed at testing, presenting, and interactively exploiting the 'increased capacities' provided by the interoperable simulation.

In general, the potential Stakeholders of ISSEM are the national, national marinas, marine stakeholders, the Autonomous Community, the Simulation Community, Coast Guard, Internal Security Agencies and Industrial Agents (e.g. Industry Defence, Oil & Gas Industry, commercial and transport ports).

The customized ISSEM Federation and / or a specific version for the defence context could be implemented in synergy with existing projects and in cooperation with partners. This

could be made available as a new tool to improve maritime survey capabilities for NATO and the nations. Several components of the federation are currently operating within the simulation laboratories (i.e. Simulation Team Labs of Savona Campus); these examples could be further developed to be made available for the evaluation of possible solutions, as well as to be used as exercises and for further analysis.

The simulator proposed in this thesis is called JESSI (Joint Environment for Serious Games, Simulation and Interoperability) and proposes a virtual environment to investigate how to best use new technologies in a maritime scenario. The software also focuses on the aspect of communications that are critical in the marine environment.

The simulator is a member of a ISSEM federation and its goal is to give a clear view of the complexity of the scenario in which all types of existing automated vehicles (underwater, air and ground drones) and traditional vehicles (helicopters, ships, Submarines) are included in order to find the best configurations for a strategically successful plan. The latter aims to improve the security of critical infrastructures against possible attacks or terrorist attacks, providing for limited costs and above all the use of automated vehicles. The infrastructures can be power stations, ports, factories or warehouses overlooking the sea as well as oil platforms.

Giving a clear image of the maritime operations showing the communications that the various vehicles make between them is not at all banal, especially if we also consider the differences between the various communication channels. For example, if we consider aerial communication (those transmitted by radio waves), they travel at a very high speed, close to

light speed and are affected by a few disturbances; if instead we consider underwater communications, they travel at a lower speed than the sound speed and are affected by multiple disturbances that alter the signal. The physical rules governing these two types of signals are very different and should be taken into account.

1 Operational Environment and State of the Art

1.1 Terrorism

If we tried to provide a definition of terrorism, we would not be able to find a precise and unequivocal definition. The term is vague, it is often used and easily it lends itself to abuse. Both at national and regional level, there is no unequivocal definition of terrorism. However, a functional description of this phenomenon can be given: it is a form of criminal violence for political-military purposes, exercised through clandestine structures and methods (Di Matteo D. et al., 1998).

Over the centuries, terrorism has been used continually as a form of war, domination and coercion, by means of violent premeditated actions such as attacks, kidnappings, murders, massacres and sabotage. Therefore, it doesn't arise from nothing, but is influenced by situations of time and place.

Terrorism must be distinguished from the legitimate use of force, whose institutional limits are known; from common or organized crime, whose ultimate purpose is essentially economic; and from ordinary political violence, whose modalities manifest themselves out in the open.

Following a series of terrorist incidents that took place in the 1980s and multiplied in the 1990s and 2000s, various observers have also found a religious matrix, albeit radicalized, at

the base of the phenomenon. However, if we want to make an accurate analysis, we must distinguish between religion lived as faith and religion as ideology. Moreover, when religious practice goes beyond the threshold of ideology, it assumes distinctly political characters, objectives and programs.

For a complete perception of the argument, it is finally necessary to consider that terrorism is used in case of very strong structural imbalance and that it represents an indirect strategy, used when the weaker actor cannot prevail against a stronger opponent.

Without prejudice to the functional description of the phenomenon described above, further characters allow us to identify the contemporary terrorism contours.

It was born in the late sixties, is put in place 'from the bottom', or from private formations with or without the supporting State assistance and constitutes a stage in the non-conventional conflict spectrum, aimed at revolutionary international upheavals, or alternatively it is expressed as a simple tactic within the various stages of the conflict.

Internal Terrorism must also be distinguished from the International one: the first one is a phenomenon that is much more frequent than the latter and involves citizens and territories of two or more states. The International one, also called Transnational, on the other hand, normally coincides with the political struggle's encroachment, or it is connected to other causes, which occur in theatres characterized by particular geopolitical situations. It is routinely exercised at a tactic level to obtain an immediate or short-term result. Moreover, it often enjoys the support of one or more supporting States, sometimes qualified as 'patrons'.

1 Operational background and state of the art

Often the attitude of these advocating States is due to feelings of solidarity, but we must not overlook convenience calculations and exploitation tactics based on Regional interests.

The support activities for subversive groups come to fruition through propaganda favourable to their aims, with the granting of transit and asylum in the sovereign territory of the supporter State, in the provision of logistical and operational bases, in training, in financing, in the supply of documents and information and in the facilitation of links with other subversive elements.

Relations between terrorist associations and supporting States are not stable: the groups, in fact, can refer, in different periods, to different states.

It is also necessary to specify a peculiarity of the terrorist attacks that differentiates them from the common models of aggressive or violent actions: in these last ones a dyadic bond is outlined, whose constituent parts are the aggressor and the victim. Instead, in a terrorist action, the relationship is generally triadic because it also presents a spectator, usually defined as a target, to whom the terrorist act actually addresses, because it is from the behaviour of the latter that they expect significant consequences.

The victims affected play a passive role, they are generally chosen not for the value that their elimination has, but for the message that comes from an action against them. In fact, often one victim is worth the other, since only the effect produced on the 'target' counts. This type of goal is essentially composed of governments.

Terrorists choose individuals based on the function they perform in the bureaucratic complex of the system, even regardless of the amount of power they manage.

Since victims and 'targets' can be in relation for different reasons, the distinction between these two elements is not always clear. It is incontestable when people totally unrelated to the terrorist cause are involved, but in some cases victim and 'target' can coincide. Consider, for example, cases in which military bases are attacked, not to obtain significant immediate results, but for the repercussions that the attack may have on other military units or on political authorities. In other cases, the two elements still coincide completely, so the goal is achieved by removing the political scene victim.

The terrorist action therefore threatens or destroys the victim and aims to terrorize the 'target' to influence its political behaviour. In addition to this, it produces an impression on public opinion both at the national level (that is the nation affected) and at the international level.

In fact, in their actions, terrorists can eliminate a victim by immobilizing those who have common characteristics with it, such as to feel potentially endangered; at the same time, they are likely to influence the group subject to political demands and manipulate a broad public. The terrorist actions are conducted in such a way as to have maximum resonance and the terrorists claim responsibility for their actions, contrary to the common criminals.

1.1.1 Maritime Terrorism

Although a definition of 'maritime terrorism' doesn't emerge from conventional texts, it cannot be denied that it represents a form of violence exerted against maritime interests, with the aim of creating a situation of panic aimed at pursuing one, or more, of the following objectives:

- To obtain a concession for the pursuit of a cause.

1 Operational background and state of the art

- To acquire money for a cause.
- To elevate the weight of a request or claim in a cruel way.

The tragic previous experiences have made possible an 'identikit' of the protagonists of such episodes:

- Extremists.
- Common criminals.
- Fanatics (religious or ethnic).
- Mutineer crews (with purposes related to causes that support terrorism).

It is evident that we are faced with a brutal, effective and spectacular weapon, which has been present in the events of this century, adapting itself to the most different situations. A moving galaxy that is difficult but not impossible to probe.

This threat often presents itself as an action of 'commandos' or raiders, therefore it proposes itself with the same characteristics.

It has the great advantage of the action choice, or when to hit (freedom time), where to hit (freedom space), how and who to hit, the choice of the objective and how to achieve it.

The threat makes use of surprise as a decisive factor for the success of its interventions, so its main enemy is the information services (intelligence) of the various western Countries or an accurate preventive action, including security checks and patrols. The chosen objectives are different and 'easy', but they have a characteristic that unites them: they must strike the public, create panic and dismay at the political/managerial class of the Country or Countries affected.

Therefore, the terrorist instrument has also found in the maritime sector how to manifest its violence, in the same way as in the past, but also in current times, the pirates, for other causes, terrorized the civil navigation, stealing and looting.

The discriminating element between the two phenomena is constituted by the fact that the terrorist action is supported by a political or political-religious cause, while the 'less noble' is the end that underlies the pirate action.

From a technical point of view, terrorist actions at sea could be traced to models traceable to running wars, made of ambushes and attacks on merchant units not escorted by naval forces, because they are able to face military ships of the opposing power, with hope of success.

These references are cited to underline what serious effects would cause terrorist aims, if they were directed towards maritime objectives, ports and port facilities included.

There is no doubt that the terrorist phenomenon has effects very significant, and since the seventies onwards has assumed the connotations of a real front for many western States, with particular reference to the USA.

Terrorist actions, used to attack various kinds of interests, can attack areas of considerable importance, such as the maritime one, which is the cornerstone of every western nation. The latter, which base their economy on the free trade system, would be greatly damaged if targets such as ships, ports, oil terminals and related sectors were to be attacked.

In the most recent history of terrorism attacks on navigation in the strict sense have been relatively rare, but we mustn't forget that the consequences of this type of accident are potentially more serious than attacks on land-based objectives.

1 Operational background and state of the art

The removal of investments and the lower distribution of industrial products are the first and obvious effects that can be caused by the reduced potential of maritime traffic. These considerations consistently reflect their true meaning, if we consider that more than half of the commercial exchanges around the globe occur using the ship carrier.

According to experts, the reduced diffusion of the phenomenon is due to the difficulties with which a small group of hijackers can assume and maintain control of a large ship. On the other hand, in principle it is much easier for States to use their naval power to regain control of the ship. This is true if you think that many nations are equipped with particularly trained anti-terrorist forces.

The most vulnerable maritime objectives are ports, roads, estuaries and waterways, providing a variety of valuable and easily accessible targets.

The movements of the PLO (Palestine Liberation Organization) saw the possibility of carrying out such attacks. The Al Fatah group was planning to arrive with a merchant ship loaded with explosives to the Eilat port. The terrorists wanted to shoot forty-two rockets of one hundred twenty-two-millimetre at the port's fuel depots and then head for the crowded beach and cause a violent explosion. Fortunately, the plan was thwarted by a unit of the Israel Navy that sank the merchant ship, but the Palestinians, considering the 'goodness' of the plan, in the following years built special units for terrorist attacks on maritime objectives, including rocket attacks and missiles at Israeli targets on the coast. In some cases, they embarked on ships bound for Israel, in other cases they used their own means, starting from nearby bases.

The forms of armament used by terrorist groups are varied and sophisticated, in this regard sea-sea missiles could be used also on-board small boats. Moreover, the systems and tactics used by the Iranian 'pasdaran' are a clear example about it. Indeed, these terrorists, on board small motorboats and equipped with light armaments, have undermined the mercantile traffic system in the Persian Gulf region, with clear and understandable damages that affect above all the productive sectors of the western Nations. The damages were so huge that was necessary a naval deployment to protect the merchant fleets.

It has been pointed out that the use of naval force against the terrorist danger is certainly one of its possible uses. So far, there have been relatively few examples of maritime terrorism, but it is not only the most prudent to worry about the vulnerability of oil tankers, platforms, ports, port infrastructure and submarine installations.

Maritime terrorism can find its application in a series of criminal cases, such as:

- Capture and violent control of a ship or platform.
- Acts of violence against persons on board, when the act is likely to compromise the safety of navigation.
- Destruction of a ship or damage to it in such a way as to compromise the safety of navigation.
- Placement of devices capable to destroy the ship.
- Destruction or serious damage to services related to maritime navigation.
- Communication of false information, thus endangering the safety of maritime navigation.

1 Operational background and state of the art

- Killing or wounding a person in connection with one of the criminal facts mentioned above.
- Threats against ports, port shipping offices and depots.
- Mutiny of political inspiration.
- Extortion (often never reported for retaliation).
- Mining of cables and submarine pipelines.
- Attacks against the marine environment (ecoterrorism).
- Attacks against ships and military vehicles.

The privileged tool terrorism can use with extreme ease (in relation to the high level of danger) is the threat. In fact, these weapons are currently available on the market in a wide range of models ranging from the most sophisticated to the simplest versions and obsolete, whose deterrence effect cannot be eluded.

For example, around the 'Enlarged Mediterranean', there aren't few Countries able to lay mined fields by means of:

- Ships - vessels (military and otherwise).
- Airplanes (military and otherwise).
- Submersible (including those with a low technological profile).

The use of commercial vectors in the release of mines, makes it particularly difficult to monitor their movements and to identify areas of possible release. The contrast to a threat of this kind would be a crime that could not be punished with acts of reprisal or retaliation due to the intrinsic clandestinity of the authors.

For terrorist attacks, various forms of explosive devices are used:

- bombs, mines and conventional throwing weapons.
- Letters and parcel bombs.
- Explosive charges.
- Conditioned Ordinaries (IED Improvised Explosive Device).

In particular, maritime terrorist actions can use the following devices:

- Contact loads under the hull.
- Mines positioned on the bottom.
- Self-propelled or wire-guided underwater weapons.
- Explosive vessels positioned near targets located at sea.
- Individual throwing weapons.
- Charges of circumstance and not positioned on board or in areas of maritime interest.

Regarding any ship in port/moored, terrorist actions can be carried out by:

- The positioning of various systems such as cars, explosive containers or bins placed in the immediate vicinity of the mooring place.
- Abandoning explosive bags or packages, or armed attacks by visiting personnel on board.
- Tiling or mooring of boats loaded with explosives.
- Delivery of parcels or bomb letters on board.
- Attacks conducted with individual, anti-tank and anti-aircraft throwing systems.
- Intrusion on board.

1 Operational background and state of the art

From 1978 to 1998, more than a hundred terrorist or rebel actions were registered against ships and/or harbours. About ten ships in navigation were subjected to attacks and captured, another dozen was destroyed. Some shipping companies and oil companies have paid large sums to terrorist organizations to safeguard their commercial interests without informing the police authorities.

But let's see now why the choice of a 'maritime' target. A goal of a maritime nature currently represents an optimal choice since in addition to presenting intrinsic defensive difficulties, due to a lack of vigilance compared to airplanes, airports, trains, etc., provides a greater choice of action for terrorists. In fact, the latter will have to reach the target with more difficulty (ships in navigation, platforms on the high seas) using more men, with little knowledge of the environment in which they operate.

In summary:

- Total surprise.
- Initial contrast almost nil.
- Possibility of many hostages.
- Goods to be exploited (loading merchant units).
- Threat of ecological disaster (oil tanker, gas carrier, toxic waste transport, chemical)
- Difficulty of international cooperation due to lack of regulations.

All the points listed above make a marine target very attractive for a possible terrorist attack, and that's why the problem should not be underestimated.

1.1.2 Counter-Terrorism

According to many experts in the sector, an anti-terrorist policy "should be aimed at making the organization less efficient rather than fighting it militarily".

The contrast can therefore be made essentially in two ways:

- Preventive Measures.
- Actions of contrast.

Preventive measures are all those designed to counteract the terrorist action before it manifests itself. However, it must be kept in mind that there are no "totally unreconcilable" defence systems, but protection measures, even if partial, can often be decisive to discourage potential attackers.

They are articulated in:

- Intelligences.
- Patrols.
- Close radar surveillance.
- Video surveillance.
- Sonar surveillance.
- Electronic countermeasures.
- Adequate counter-terrorism plans.

The contrast actions are the responsibility of the police and military bodies.

Basically, the procedure is:

- Reporting the threat to the competent authorities, carried out by civilian, military, intelligence or directly by the terrorists themselves.
- Detection and location of the threat.
- Military intervention procedures.

As already mentioned, the decisive point for the success of a terrorist action is the surprise effect that does not allow time for the defence bodies to intervene promptly. The reports arrive too late or are not done, and this facilitates the task of the bombers.

So, the key to combating these criminal attacks is the timely detection of threats and this can only be done with the intensification of preventive measures. The latter, however, have intrinsic difficulties, such as the reduced number of available means and the multitude of possible 'targets' and the high costs. For this reason, to increase the security of the marine scenario, alternative ways should be found to make them more efficient with sustainable costs.

Autonomous vehicles lend themselves very well to anti-terrorist practices because they are equipped with sophisticated sensors, such as sonar, cameras and radar, can easily patrol large areas in a short time with reduced costs, being able to alert the defence organs in time from such threats.

Therefore, this thesis project has as one of its objectives to seek a convenient use of such drones in order to prevent any massacres and economic damages deriving from terrorist attacks and attacks.

1.1.3 Major Maritime Terrorist Events of Recent Years

Maritime terrorist events happened in recent years are very different; the principals are listed below in chronological order and then a brief description is also given:

- 1961: taking possession of a transatlantic of Portuguese nationality off the coast of Venezuela.
- 1974: seizure of a Greek merchant ship in Karachi.
- 1980: closure of the Sacramento port for three days due to a false bomb on board a Soviet freighter.
- 1981: unsuccessful attack on an offshore platform off the American coast.
- 1981: capture by pirates of a container port and three oil tankers in the Strait of Malacca.
- 1982: high redemption paid to protect one of the six off-shore platforms from risks of attacks.
- 1983: boarding of a cargo used by the American navy in the Strait of Malacca, by a group of pirates.
- 1984: occult mine-laying of the Suez Canal and Red Sea by a merchant in transit.
- 1985: similar episode against an oil tanker.
- 1985: murder of three Israelis on board a yacht in Larnaca.
- 1985: sequestration of the Achille Lauro.
- 1986: murder of 2 Israeli sailors in Barcelona.

1 Operational background and state of the art

- 1987: attack in the Aegean against a Greek ship by a member of the FRC of Abu Nidal.
- 1987/88: mines for the prohibition of mercantile traffic during the Iran/Iraq war.
- 1991: reclamation of more than 1200 war items posed by Iraq in the Persian Gulf.
- 1993: attack on the Italian merchant Lucilla in the port of Oran.
- 2000: attack on the USS Cole destroyer in the port of Aden by a terrorist group linked to Al Qaeda.
- 2005: missile attack by a terrorist group, linked to Al Qaeda, against the port of Aqaba.

Achille Lauro Case



Figure 1.1: Cruise ship Achille Lauro (image taken from https://en.wikipedia.org/wiki/Achille_Lauro_hijacking)

1 Operational background and state of the art

Cruise ship Achille Lauro (image taken from https://en.wikipedia.org/wiki/Achille_Lauro_hijacking)

The most striking example is the hijacking of the ship Achille Lauro, in that case some Palestinian terrorists seized the Italian cruise unit with five hundred eleven passengers aboard predominantly American and British nationality demanding in return for the release of fifty terrorists imprisoned at Israeli prisons threatening in case of denial, killing all subjects on board.

The Italian Government, after an initial moment of surprise, tried to solve the terrorist emergency by following one side, the diplomatic way with an attempt to negotiate with the official representatives of the PLO, on the other, to prepare an intervention with the departments special to use as extrema ratio.

On the scene of action, the units of the Italian Navy were surveilling the Achille Lauro. Even the United States in the circumstances, were ready to intervene with their special department (Delta Force) stationed in Malta, if necessary.

The situation was resolved thanks to the mediation of moderate Palestinian groups belonging to the PLO Directive (Arafat).

The negotiations were conducted thanks to the solicitations of Italian diplomacy, also belonged to members of the PLO (Abu Abbas, mind of the organization, head of the front for the Liberation of Palestine and firm supporter of the policy of terror of the subversive movement).

1 Operational background and state of the art

The ship and the hostages, although not all of them unharmed (there was in fact an American victim) were released while the terrorists and the mediators were captured intercepting the plane that was bringing them back to Tunisia, an operation carried out by the Americans.

Portuguese Transatlantic Capture

In 1961, some exponents of the IND. NAZ. Portuguese movement, they took possession of a Portuguese transatlantic off the coast of Venezuela. Also in this case there were victims, the third officer of the ship was killed. Subsequently, the favourable outcome of the negotiations allowed the release of passengers in Brazil.

A Merchant Ship Karachi Seizure

Another incident to remember is the seizure of a Greek merchant ship in Karachi: the terrorists threatened to kill the crew and blow up the ship, if the Greek authorities had not freed two Arab terrorists detained in Hellenic land. Greece surrendered to blackmail and with a judicial artifice, freed the two prisoners who reached Libya. Although the diversion of a ship may seem easy due to the poor controls, generally carried out at the embarkation, in fact these events are extremely rare, in fact, it is to be considered that in a span of thirty years, less of a dozen ships were seized.

Sinking the Rainbow Warrior

1 Operational background and state of the art

A particular case, although not part of the strictly 'terrorist' type, is the case of the Rainbow Warrior, in which agents (probably French) could easily organize with an underwater operation, the sinking of the flagship of Green Peace: 'Rainbow Warrior' in Auckland Harbour in New Zealand.

The destructive event resulting from the attack, caused enormous psychological and symbolic effects. It is clear that although the French intent had no terrorist purpose, in fact it had suggested a tactic of certain success towards the public, as well as terrorist groups that could have exploited similar circumstances for the completion of new attacks.

This case underlines how in the maritime scenarios the underwater actions constitute a real weak point for safety. This is due to the difficulty for ordinary means in patrolling submerged areas and therefore in identifying potential threats.

Red Sea Mines

The western intelligence experts, in several cases have been able to assert that a new and deadly form of terrorism was born, characterized by the laying of mines at the crucial points of maritime traffic. In particular, in July 1984, some areas of the Red Sea were an exemplary theatre of this type of sabotage: eighteen merchant ships of various nationalities were damaged by mines. From what has been said, it is noted that the maritime objectives are not immune to the destabilizing and destructive effectiveness of terrorism.

1 Operational background and state of the art

Attack on the Merchant Ship Lucilla

A classic Italian example is constituted by the attack of Islamic fundamentalists in the tricolour Lucilla merchant. On that occasion the ship stopped in a port from Algeria, was assaulted and the whole crew was slaughtered. The strategy used by terrorists aimed at achieving a general isolation of the Algerian state. The episode hides in itself potentiality of phenomenon evolution that could bring as hypothetical evaluation to the aggression of naval units in roadstead or even in transit in order to discourage any relationship with foreign countries.

Massacre on board a Yacht in Cyprus and Barcelona

On September 25th, 1985, three Israeli citizens were murdered on board their yacht in Larnaca (Cyprus) by an Al Fatah group. This episode shows that even sectors that are not connected to important systems of the State can be the object of the "terrorist impetus" as a tool to make the essence of their cause heard and spread.

The same terrorist group has repeated, later, in Barcelona, the terrorist action mentioned, causing the death of two unarmed Israeli sailors.

Attack on a Greek Ship

On November 7th, 1987, a Greek ship was attacked by a single terrorist member of the FRC (Fatah Revolutionary Council) of Abu Nidal in the Aegean Sea. The episode caused the death of nine people, while over eighty sailors were injured.

1 Operational background and state of the art

Shortly before the untimely explosion of a car bomb had failed a plan for an attack on an American Navy ship.

Attack on US destroyer USS Cole



Figure 1.2: USS Cole destroyer after the attack (image taken from https://en.wikipedia.org/wiki/USS_Cole_bombing)

On October 12th, 2000, the US destroyer ship USS Cole was the victim of a terrorist attack by the Al-Qaeda terrorist organization. The ship was moored at the port of Aden in Yemen, intent on a routine refuelling after navigating the Persian Gulf. A few hours after his landing, a small fiberglass boat carrying a considerable amount of explosives and two suicide bombers, approached the destroyer's port and exploded. The explosion created a gap in the hull of twelve meters in height and eighteen in length.



Figure 1.3: Gap in the hull of the USS Cole due to the terrorist attack (image taken from https://en.wikipedia.org/wiki/USS_Cole_bombing)

The burst charge was estimated at between two hundred and three hundred kilos of C-4. Seventeen American sailors lost their lives in the explosion and thirty-nine were injured. After three days of work to temporarily repair the hull, the crew was able to secure the ship and determine the amount of damage. Fortunately, the keel of the ship came out unscathed from the explosion and therefore the ship could be repaired, avoiding its demolition.

It is interesting to note that if the ship had not been a new generation one, designed to support such an eventuality, it would almost certainly have suffered irreparable damage, risking sinking or disarming and demolition.

The destroyer was subsequently loaded onto the Norwegian Blue Martin pontoon for the return trip to the United States. Here after months of repairs, he was able to return to service to demonstrate the effectiveness of design measures aimed at surviving such attacks.

Missile Attack on the Port of Aqaba

On the morning of July 19th, 2005, the port of Aqaba was targeted by two Katyusha missiles. The missiles, launched by a terrorist group linked to Al Qaeda, fell on an American warehouse used to store materials and supplies and near the Jordanian guard. Also in this case, the attack caused the victims: a Jordanian soldier lost his life and another was seriously injured. It is thought that the target of the attack was in fact an American ship moored in port at the time of the attack, but it came out unharmed not reporting any kind of damage.

Shortly thereafter, a third missile was launched on the airport area of the city of Eliat, fortunately without causing victims.

This episode underlines the importance of finding mechanisms of effective defence against possible missile attacks.

1.2 Counter-Terrorism Simulation

After the attack on the twin towers in 2001, many Nations and International Organizations set up new research programs to tackle the terrorism, that has continued to evolve over the last decade (Benney et al., 2009).

In particular, NATO established in 2004 the NATO DAT Pow (Defence Against Terrorism Program of Work) to develop innovative solutions in various sectors to address these threats. One of these proposes the development of an innovative simulation solution based on MS2G (Modelling, interoperable Simulation and Serious Game) to tackle the complex sector of defence against terrorism (Bruzzzone et al.2014a). This project has also been developed, based on the Paradigm of the SaaS (Simulation as a Service), in order to make it available on the web as a cloud service.

The main objective of this project was to evaluate the reduction of the vulnerability against terrorism in relation to the results of NATO research in recent years (Bruzzzone, Tremori 2014b).

1.2.1 Application Fields of the DAT (Defence Against Terrorism)

The operational requirements and weaknesses of the defence against terrorism have been summarized in 11 elements presented in the DAT Pow during the Conference of National Armaments Directors (CNAD 2004 and following):

- Large-Body Aircraft Against Man-Portable Air Defence Systems (MANPADS)
- HPP: Harbour and Port Protection

1 Operational background and state of the art

- Helicopter Protection for jet rockets RPG (Rocket Propelled Grenade)
- Protection from improvised explosive Devices (C-IED: Counter improvised explosive Device)
- Reclamation of explosive devices (EOD: Explosive Ordinance Disposal) and consequences management
- Precision Air-Drop Technology for Special Operations Forces, Detection
- Protection and defusing of CBRN weapons (Chemical, Biological, Radiological and Nuclear)
- ISRTA: Intelligence, Surveillance, Reconnaissance and Target Acquisition
- DAMA: Defence Against Mortar Attack
- PIC: Protection of Critical Infrastructure
- NLC: Non-Lethal Capabilities

Simulation has been identified as the best solution for virtual demonstration and presentation of the results of the research carried out on this topic during the last 10 years. An important advantage, deriving from the use of simulation, is the possibility of supporting Subject Matter Experts (SME) with an interactive tool that allows them to conduct experiments (Longo 2010, Longo 2012).

This capability becomes even more significant in the case where the innovative MS2G paradigm is applied, because SME could remotely access to the simulator and share not only the results, but also hypotheses and scenario configurations in order to compare their

hypotheses and validate mutually their conclusions (Bruzzzone et al., 2014a, Bruzzzone, 2018).

This aspect is very important for the defence against terrorism, both for the complexity of the scenario and for the uncertainty in the determination of many factors. In fact, when we talk about terrorism, there are no reliable statistics concerning probabilities of attack or about their effectiveness and effectiveness of defensive solutions (McKercher et al.2004). This is due not only to safety-related issues, but also because these aspects have a constantly changing nature, that reduces the size of the samples available, as well as the possibility of conducting valid experiments live.

In 2002, during a Panel on M&S organized by MIMOS (Italian Movement Modelling and Simulation) a question was asked about "how simulation could support counter-terrorism, considering the inventiveness and creativity of human beings in the preparation of these attacks "(MIMOS 2002); on this occasion Prof. Bruzzzone stated that "while it is impossible to predict terrorist attacks, it could be quite feasible to simulate them, obviously, not to support terrorist plans, but to evaluate the reduction of vulnerability obtainable with alternative solutions".

After several years, the DVx2 simulator is proposed to respond exactly to these problems with the use of the advantages of the currently available technologies and the new methodologies (for example SaaS, MS2G).

In fact, the simulation aims to create a consolidated reference point for the reduction of vulnerability and how to reach it, on the basis of evaluations carried out by experts.

Considering the complexity and the dimension of the defence against terrorism, it is obviously necessary to define the limits for the development of the model. In fact, the authors decided to start modelling, focusing only on three important elements of the above list: C-IED / EOD, CBRN, JISR (Bossomaier 2000, Bossomaier et al 2009).

In fact, the simulation could be used to address many aspects: from the assessment of skills to the training of personnel. In this context, an important innovative point is the use of MS2G to create a distributed network that could support crowdsourcing (Bruzzzone 2014A et al.). The latter, in anti-terrorism, is an important issue because it allows Subject Matter Experts to interact with each other and to share estimates, ideas and solutions. There are clear possibilities offered by the proposed interactive simulation environment that could be used through secure networks for such purposes. Another aspect, not to be overlooked, is the possibility of using these models for the exploitation of results by decision makers or a general public. Obviously, all these issues involve data of a sensitive nature and, in this document, we only report releasable public information related to the conceptual modelling of the initiative.

1.2.2 DVx2 and Crowdsourcing

As already mentioned in previous chapters, the idea of creating simulation models for Counter-Terrorism (and even in asymmetric conflicts) has been studied for many years and has become increasingly popular since 11 September (Moscow et al 1996, Smith 2002, Petrova and Camponeschi 2002, Abrahams 2005 Oren and Longo 2008, Bruzzzone et al.2009a, 2009b).

1 Operational background and state of the art

With regard to this topic, therefore, the use of simulation has been proposed within an innovative paradigm corresponding to M2SG (2014a Bruzzone et al.).

A project developed on this topic is the DVx2 simulator (Distributed Virtual eXperience and eXercise). This software was created for specific areas of application (for example C-IED, Joint Intelligence, surveillance and reconnaissance against chemical, biological, radiological and nuclear weapons) to tackle the difficulty of defence against terrorism through a modular approach shown in Figure 1.4.

The DVx2 simulator was developed with the aim of gathering knowledge and experience on the Counter-Terrorism of experts in the field through the use of the MS2G. The simulator combines interoperable simulation with web serious games to create a distributed environment where simulation could be provided as a service.



Figure 1.4: DVx2 scenarios

One of the main advantages in this case is the use of AI-CGF (Intelligent Agent Computer Generated Forces), developed by the Simulation Team, to direct terrorists and defenders (Bruzzzone et al 2011a, 2011b).

This intelligent force generator allows carrying out numerous simulations automatically, extending the simulator's testing capabilities. In doing so, from this approach, experts in the field could use DVx2 to test the effect of independent variables and hypotheses on reducing vulnerability.

DVx2, is currently quite efficient, so you can perform these interactive experiments by investigating different configurations and immediately analyse the results that are displayed within the virtual environment. DVx2 shows the situation both by reproducing a 3D view of

1 Operational background and state of the art

the city, and by presenting the distribution of damages, accidents and evacuation areas (Figure 1.5). All these parameters evolve dynamically during the simulation allowing the understanding of the succession of events. But this may not be appreciated in a classical experimentation, due to the too high simulation speed.

Moreover, special 3D detailed scenes are generated to reproduce the critical points, so that they can be used to propose to the SME possible attack sites and/or the possibility to modify the parameters by clicking on the appropriate virtual objects.

In fact, the simulation results regarding scenario configuration, risk analysis and key performance indicators on vulnerability reduction, are stored in the cloud. This database allows the creation of a constantly updated knowledge on defence against terrorism that could contain several dynamic experiments simulated on different scenarios, carried out by Subject Matter Experts. In fact, the synthetic environment of DVx2 is allowing access to many important variables related to the areas of investigation. By combining different aspects, heterogeneous scenarios could be developed. In fact, DVx2 uses the IA-CGF to dynamically simulate the evolution of the threat network (Figure 1.6).

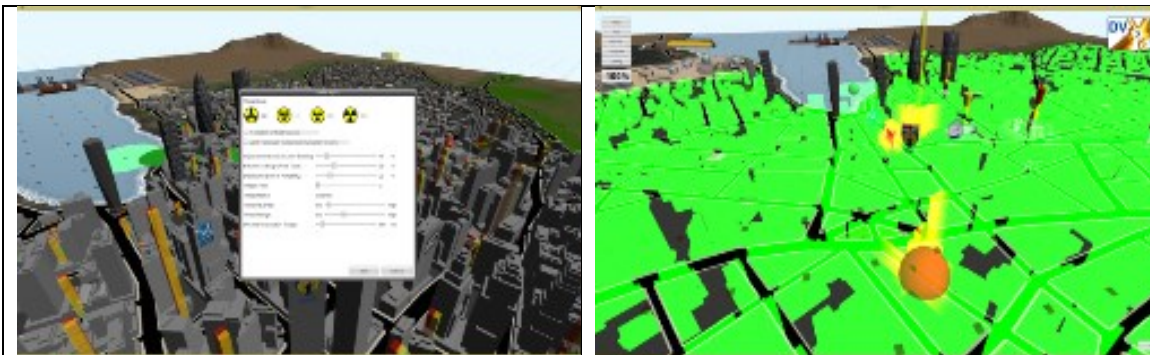




Figure 1.5: Virtual representation of the parameters of the scenario (top left), of the damage due to the attacks (top right), of the setting of countermeasures (bottom left) and of the critical points (bottom right) of DVx2

DVx2 was developed to address only some specific elements of those listed in the DAT PoW, however, it is clear that the interoperability approach to modelling allows to add other simulators, or meta-models, to the purpose of extending the validity of the simulator to new fields, or to modulate its resolution and its details towards specific elements (Kuhl et al.1999).

Within the specific case selected (for example C-IED), DVx2 allows users to set parameters and make decisions, while the simulator independently assesses risks and impacts in terms of reducing vulnerability.

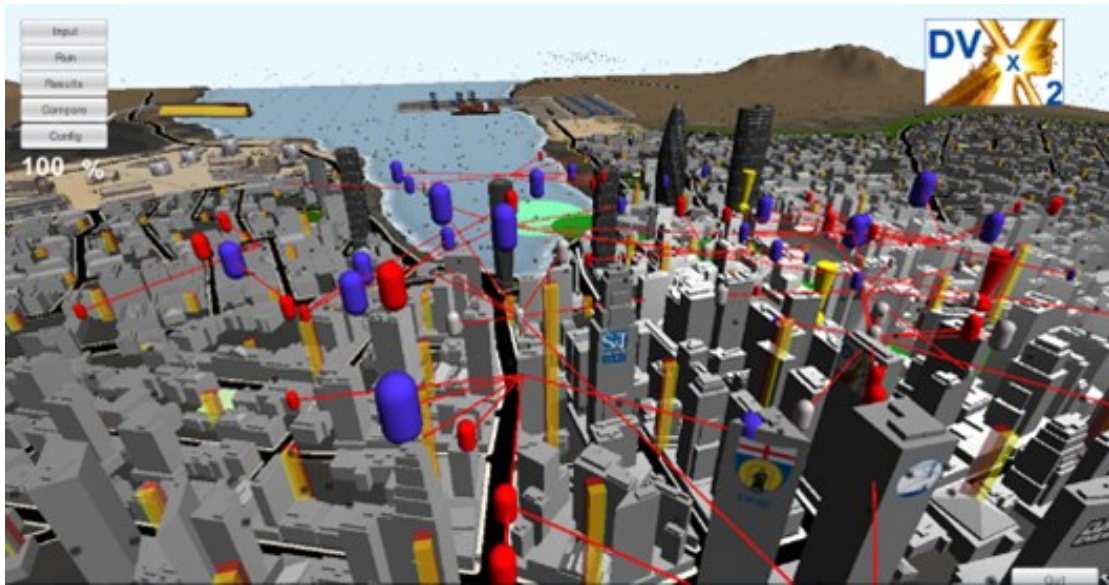


Figure 1.6: Network of simulated threats in the JISR module of DVx2

The virtual world of DVx2 is also used to propose the final results within an effective graphical representation that allows users to grasp the approximate results of the simulation. The simulator is implemented as a Web serious game capable of operating on secure networks. It is important to underline that the DVx2 conceptual model has been developed considering the use of HLA as a reference standard for interoperability to allow expansions to be reused in the future as it could for example be federated within a large federation of simulators (Bruzzzone et al.2011).

Moreover, through a correct authorization and access scheme at different levels, users can access the DVx2 database and dynamically compare their experiments with others carried out by their colleagues based on different hypotheses. This allows us to understand how

conservative or optimistic hypotheses are used by them, and also to evaluate the efficiency and effectiveness of the various alternatives on the different simulated scenarios.

In this way, DVx2 provides very effective support for Crowdsourcing and interactive distributed experimentation. Obviously, the simulator also has great potential as a tool to be used for staff education and training (Tremori et al.2012); in fact, the use of this software could support the development of virtual distributed exercises (Raybourn 2012).

So, the use of MS2G in this context is destined to become a solid approach and a point of reference for the other issues listed in the defence against terrorism. DVx2 could evaluate the implementation of DAT initiatives, in terms of reducing vulnerability, for future planning and recognition of its results, while the distributed nature of this approach would allow the networks of experts in this field to be strengthened.

The general structure and architecture of DVx2 are based on the combination of stochastic simulation with discrete events with intelligent agents in the role of terrorists, as well as with DAT resources (Hill 1996; Banks 1998; 2011b Bruzzone et al.). The user of DVx2 by accessing this simulation service is able to specify the actions, activities and policies to be followed. In this way he can select the hypotheses to be adopted in relation to the different DAT scenarios.

The generator of artificial intelligent forces directs terrorist actions and countermeasures throughout the simulation. The risks and the reduction of vulnerability are measured during the whole evolution of the scenario (Bruzzone et al 2011a.). In fact, the estimates given by

the simulator on damages, costs and victims allow the comparison of various alternatives and/or estimates made by SME.

The VV&A process (Verification, Validation and Accreditation) is applied to the simulator using informal techniques and dynamic experiments. In fact, the approach for development and validation is based on the "lean" simulation concept (Bruzzone, Saetta 2002a): the validation of the correctness of the conceptual models contained in the Simulation (the framework simulated by our virtual models) must be checked by expert's simulation during the revision process (Balci et al 1996, McLeod 1982). In addition, it is necessary to verify the consistent implementation of the software code with respect to the conceptual models (Balci et al.2011). Therefore, the validation and numerous dynamic tests on DVx2 were conducted by the anti-terrorism and simulation experts. In this way, it was possible to validate the simulator as suggested by the established techniques (Amico et al. 2000).

The DVx2 architecture is based on simulation as a service that allows users to experience the serious game DVx2 directly on the web through a web browser, by downloading a plug-in (Guo, Bai, Xu 2011, Tsai et al 2011). This solution is more flexible than the operating systems in use. To ensure full access to all potential users, a stand-alone version was developed that can be run locally or in a web browser. This configuration was also useful both to test the GUI (Graphic User Interface) and the simulation engine, and also to ensure the usability of the software from workstations, operating within secure networks under heavy restrictions on access to the Internet.

To this end, the DVx2 architecture includes conceptual elements, such as the management users and system accesses (UMAS) and the Discrete Event Simulator (DES), as shown in fig.1.7.

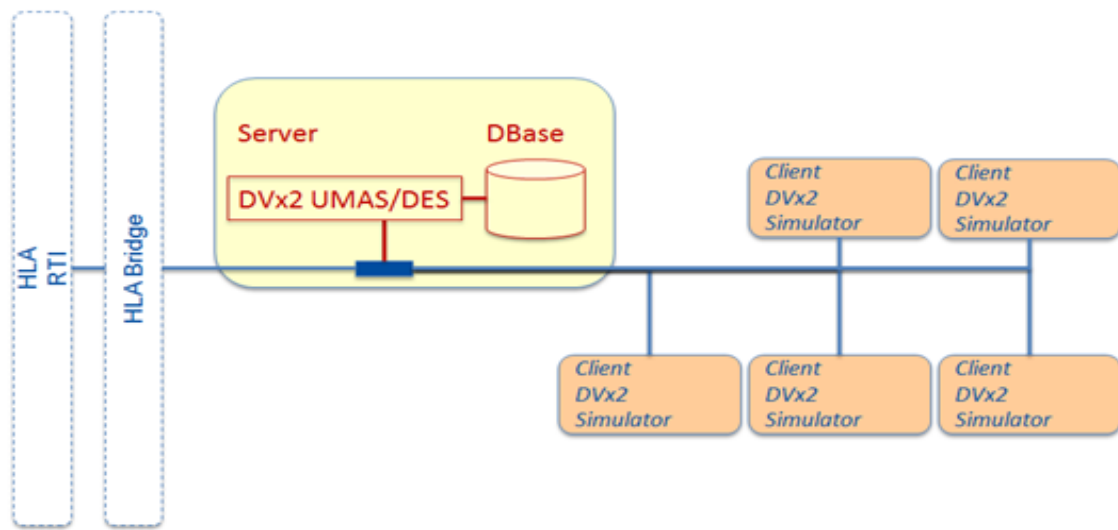


Figure 1.7: DVx2 Architecture

The UMAS of DVx2 is dedicated to providing users, as well as administrators, an easy-to-use system that allows the creation and management of user accounts. It was initially developed using PHP, while the main database, used to store data (both user data, as well as simulation inputs and outputs), was built with MySQL. Two main roles were created as part of the UMAS of DVx2: the administrator user and the reader user.

DES is a simulator (written in Java programming language) that deals with the evolution of the game according to a stochastic simulation to discrete events that evolves according to the variables and set-up parameters (made by the player users at the Client level).

1 Operational background and state of the art

Finally, the DVx2 architecture also includes an external bridge that allows you to connect to a federation according to the IEEE 1516 HLA standard. This part is dedicated to ensuring the possibility (for future developments) of linking the serious game DVx2 as a federation of an HLA federation.

With this approach, DVx2 users can compare the results obtained by modifying the parameters and changing different hypotheses. The simulator could operate on the web in such a way as to allow the study of a wide range of alternatives through an approach that allows interactive crowdsourcing (Bruzzone et al 2012; Elfrey 2006).

In terms of implementation, the decision to allow the use of the virtual world through the web has introduced some constraints of computational efficiency and issues related to bandwidth availability. In doing so, during the development of DVx2, the importance of providing the user with an interactive and effective control, on the virtual representation of the obtained results, emerged: due to the high volume of data, the final structure of DVx2 was forced to take into account the requirements to operate on the web and to be more interactive. According to these considerations, different models have been moved from the DES to the original DVX2 GUI that has evolved into a real simulator (as we will see in the structure described below) representing the final architecture of the simulator.

This solution is very effective in case more experts perform more independent simulators, while, in the case in which it is a single interactive multiplayer simulation, an improvement in the DVx2 DES should be made. In the current version of DVx2, different users are enabled to run multiple scenarios in competition, for example, you can replicate the simulation to

test the reliability and measurement of resistance and robustness against stochastic factors, or to see the effects of changes on hypotheses and parameters. Therefore, the intelligent agents participate in each execution separately and the comparison is only on the results of the initial and final simulation. DVx2 supports the processes and game logic shown in figure 1.8.

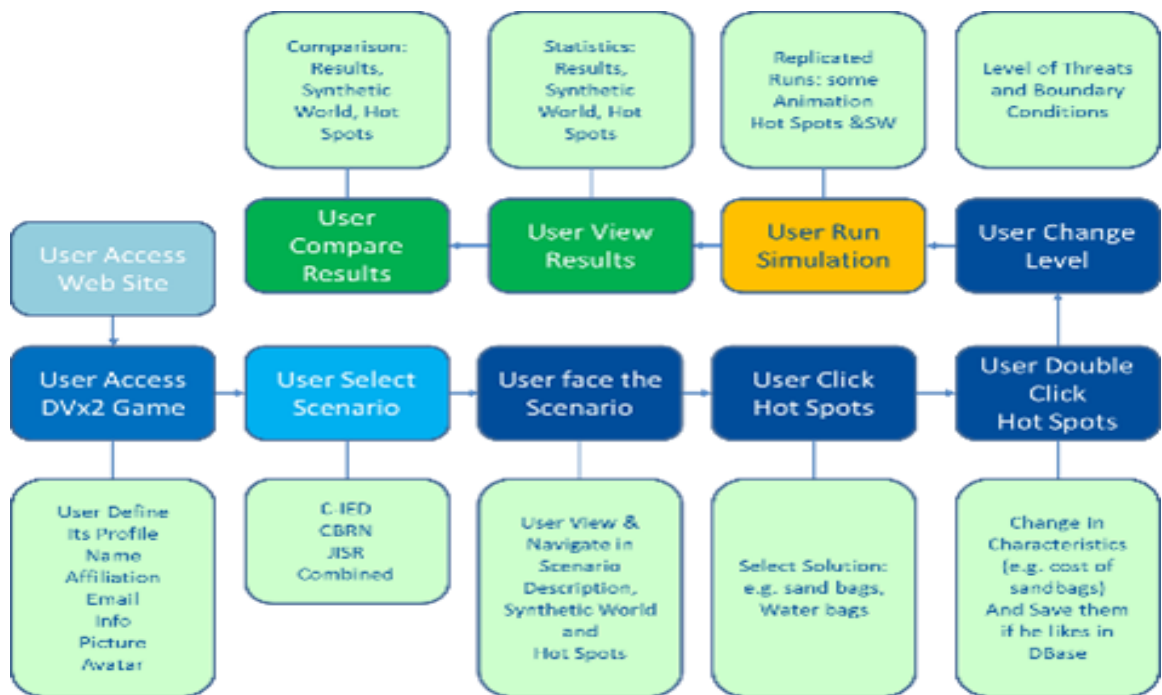


Figure 1.8: Processes and gaming logic of DVx2

Obviously in stand-alone mode, compared to crowdsourcing mode, DVx2 only deals with the part of the simulation, avoiding taking care of the management of the profiles and integrating the results of the Data Base. In the currently implemented version of DVx2, the user accesses the DVx2 environment by selecting game alternatives and then proceeds to

1 Operational background and state of the art

prepare and analyse the simulation. These activities are carried out in the virtual environment created by the simulator, while the results are proposed both in numerical and graphic form. DVx2 implements several target functions that allow interactive evaluations of successes in DAT POW in terms of vulnerability reduction. In this sense the use of the simulation allows to estimate a wide spectrum of target variables able to provide a complete picture of the vulnerabilities using many alternatives. So, in crowdsourcing mode, the user has only the main variables available in the 3D GUI, otherwise it would risk confusing him if there were too many factors. For example, in this case, among the parameters estimated by the simulator you can see: Casualties, Injured, Reaction Time, Suspicious or Clean Areas, Evacuation Time, Total Evacuation Costs, Success Rate, Correct Evacuation Distance.

The success of the DVx2 demonstration shows the opportunity to use it for experiments dedicated to strengthening its validity and accrediting it among the communities of SME. It would be interesting to conduct further experiments to measure model efficiency by working with other experts. In fact, it is already a strategic advantage to have access to this simulator that offers the possibility to share and evaluate crucial and interactive experiments on scenarios concerning the defence against terrorism. The community of experts could use this simulator to create a dynamic archive of their knowledge on this topic.

So, the innovative approach, proposed on the basis of the MS2G, allows to use the crowdsourcing and extraction of the data obtained from the simulation through the combined use of the Modelling and Simulation, the Intelligent Agent and the Serious Games. In this way, it becomes possible to involve a large number of people to keep their knowledge

continuously updated through the interactive and engaging environment of the Serious Games.

The architecture of DVx2 allows to collect the data and information needed to fill the databases useful for a better understanding of the phenomena analysed, by sharing the various hypotheses of the experts with their consequences estimated by the simulation. The authors of the software focused the analysis on specific areas listed in the DAT PoW and the scenarios realized by them were useful to test the concepts and to investigate how the Modelling and Simulation, the Intelligent Agent, the Serious Games and the immersive technologies could be effective in this constantly changing and hardly predictable environment.

An important follow-up, ensured by the MS2G approach, is the ability to create a distributed interactive simulation that could be successfully used in various fields such as training, education, dissemination, capacity assessment, testing and trial of different users. In fact, in the case of DVx2, there is an interesting potential, in terms of general use, in the application of the simulator in the training and education of both military and civilian personnel, as well as for achieving the objectives of NATO DAT PoW.

One of the main advantages of DVx2 is the possibility of supporting the development of new concepts and solutions through Virtual Interoperable Testing. In the same way DVx2 could be used for the development of new functionalities for the strategic evaluation of the scenarios with the use of the new simulation models.

1.3 Hybrid Warfare

The security environment is changing continuously and rapidly along last years; indeed, the evolution of internet and media channels as well as globalization emphasize the impact of specific concurrent actions carried over different channels (e.g. political, social, financial, cyber, etc.). For these reasons, the Alliance is studying intensely these new phenomena often aggregated under the name of Hybrid Warfare (Baker 2015, Bruzzone et al. 2016b). Even if the concepts are very well known also in the past and there are controversial on the name, it is evident that new technologies (e.g. Internet of Things, Social Networks) are changing the way this multi-channel approach could be applied and confirm the importance to address this context (Di Bella 2015).

Indeed, one of the main characteristics of this kind of warfare is that it includes several types of means, activities and actors combined each other, civil as well as paramilitary, military and irregular actors, try to achieve political and strategic objectives through overt and covert actions and conventional and unconventional means (Marszal 2013; Wintour & Shahee 2016). The Hybrid Warfare focuses often to destabilise Command chains and complicate the decision-making being especially effective against organization that are slow in their decision process due to their democratic or multinational nature. In this context, the subjects of war activities are often intentionally ambiguous in order to avoid a direct military confrontation, triggered by article 51 of the UN charter. It is evident that the modern concept of Hybrid Warfare is pretty complex and requires specific models and studies; due to these reasons the Alliance Foreign Minister in the December 2015 meeting approved a specific

strategy addressing hybrid warfare. In this case, the Asymmetric, Information and Cyber Warfare evolve in critical domains considering that the Hybrid Warfare involves all the full Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, legal (DIMEFIL) spectrum. In this case, the war is conducted in all battlegrounds such as international community, home front population and conflict zone population; so, the models of engagements are the most different.

The Hybrid Warfare is not only an actual activity; in addition to actual conflicts, it was used also in historical cases (Lamb & Stipanovich 2016). Indeed, considering the nature of the hybrid Warfare, it is necessary to conduct an analysis over a spectrum of alternative multiple layers (McCuen 2008; Weitz 2009; Gerasimov 2013; Bachmann & Gunneriusson 2014; Davis 2015).

In facts, also the actors of hybrid warfare belong to different types including both state and non-state players. Hybrid warfare is a concrete and actual phenomenon, in many conflict zones and it is supposed that belligerents are using hybrid strategies. One of the main objectives of hybrid warfare, is avoid the direct military conflict when possible, but to use overt military actions as coadjutant to the whole plan.

1.3.1 Hybrid Warfare Simulation

In order to investigate this context and study scenarios, it is evident the potential of Modelling and Simulation (Christman, Di Giovanni and Wells, 2015; Schmidt 2015). Indeed, simulation is an important methodology to study a such complex environment that include different domain and layers as well as stochastic factors; for instance, the human

behaviour as well as cyber, conventional and information warfare should be covered by specific models. All these aspects have been studied extensively in modelling and simulation, even if the complexity related to their mix within Hybrid Warfare is still a new subject of investigation (Davis 2015). Several researches about complex scenarios had led to the creation and the use of Intelligence Agent for recreating model of human behaviour since many years (Shonkwiler et al. 1986; Avalle et al. 1996. 1999; Castelfranchi & Conte, 1996; Dascalu et al. 1998). The intensification of the use of the IA conducted to the development of several tools to support modelling development (Resnick 1996; Ferber et al. 1998; Parunak et al. 2006; Cayirci & Ghergherehchi 2011; Bruzzone et al 2014a; Zhang 2016). More recently the use of Multi Agents and Intelligent Agents allowed to reproduce complex situation including human behaviour (Takadama et al. 2007, Takadama et al. 2008; Bruzzone & Massei 2010; Macal et al. 2010; Joo et al. 2013; Cai et al. 2013). The Simulation Team is extremely active in the Human Behaviour modelling: it developed complex models about PSYOPS, CIMIC Operations, Civil Disorders, Decision Making, etc. In particular, the peculiarity of IA-CGF NFC (Intelligent Agent Computer Generated Simulator Non-Conventional Framework) is that his IA are able to take advantage of specific events for their operational planning (Bruzzone 2013; Massei & Tremori 2014; Bruzzone et al.2015; Di Bella 2015).

1.3.2 T-Rex & Cyber Attack

During this research, the author participates, with the Simulation Team, to the development of T-REX (Threat network simulation for REactive eXperience) an interoperable MS2G

(Modelling, interoperable Simulation & Serious Game) solution that address this context (Bruzzone & Cayirci 2016a). T-REX is a stochastic discrete event simulation able to act in stand-alone way or to be federated with other HLA simulators. T-REX could be executed in real time or fast time; in this second case it allows to conduct multiple runs to investigate alternative solutions for vulnerability reduction respect Hybrid Warfare.

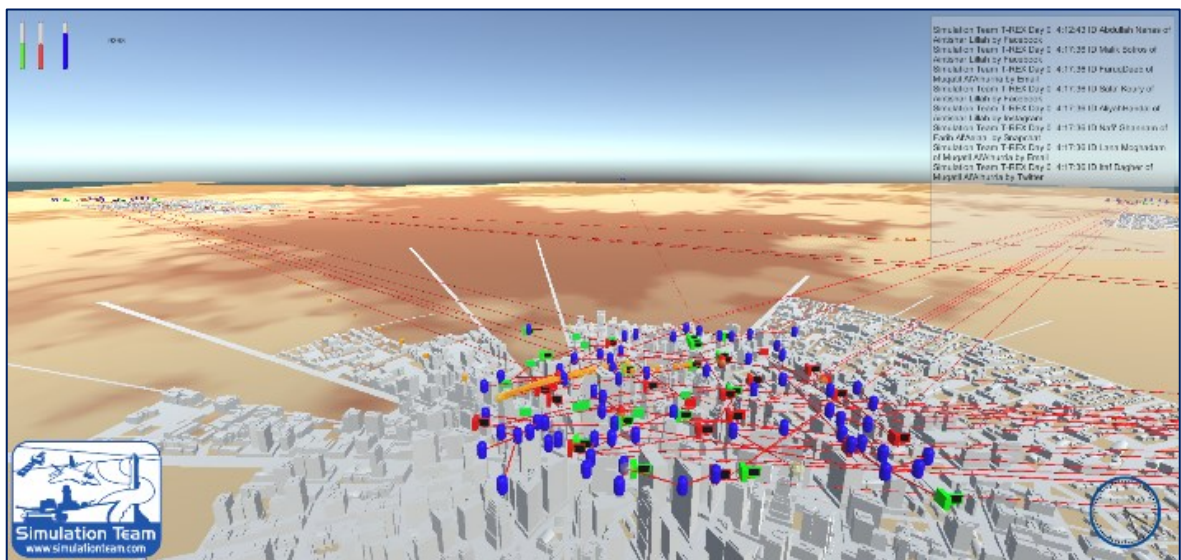


Figure 1.9: T-Rex

The simulator is currently demonstrated over a scenario related to a desert area bordering with sea and including five towns; the simulation includes multiple layers simulating population (e.g. individuals and/or families) as well as interest groups (e.g. industrial sectors, religious groups, social classes). These elements are structured within social networks and regulated by mutual relationships expressed by fuzzy variables in terms of attitude and intensity.

1 Operational background and state of the art

T-REX includes also other layers interoperating with the socials, in particular the Entity & Units reproducing military units and assets that influence population behaviours. The case proposed includes also the power grid, cyberspace and communication network. Indeed, the Cyberspace is reproduced modelling the IP address of all fixed and mobile ICT (Information and communications technology) elements as well as their related interconnections; each node and link could be attacked by compromising its availability, integrity and/or confidentiality and it is possible to conduct defensive, offensive and restoring actions.

In T-REX all elements evolved dynamically and are driven by the IA-CGF reproducing Hybrid Warfare situation; in addition, the simulator could be federated within an HLA Federation with other models. Currently the scenario includes also traditional and virtual assets on the area as well as a Power Plant, a Desalination Plant, and a Tank Farm that are critical infrastructures in the area.

The proposed simulation deals with modelling different actions on real and Cyber layer. In particular, concurrently with conventional terrorist actions, a Viral attack is considered, targeting ICT Critical Infrastructure, such as security systems, Surveillance systems, Command and Control of Autonomous Assets; this cyber could be coordinated during the simulation with a conventional attack to the strategic infrastructures of the area.

In facts, the diffusion of the virus follows a specific logic, described in the following, devoted to maximizing its effect minimizing the possibility to intercept it. Simulation starts with a small number of infected machines by pen drives; indeed, the diffusion takes place mostly by pen drives, but also by information exchange through web (e.g. infected e-mails, attached

files). The virus stays dormant to be hardly detectable until the ICT Critical Infrastructure is infected. The Virus is thus activated only in critical ICT nodes resulting in the overall shut down of the Security network, Surveillance network etc. The virus capability to activate itself in the only computer for which it has been designed and its approach not disabling functionalities, but compromising the integrity of data, makes the virus very difficult to be intercepted and removed by regular antivirus scan, making its diffusion rapid and effective. This diffusion model and virus behaviour has been modelled by authors reproducing the existing virus called Stuxnet (Langner 2011), described in the previous paragraph, that caused in recent years great damages in the industry sector, targeting PLC (Programmable Logic Controller) like SCADA systems.

The strength of the Antivirus protection is controlled by a reliability parameter. The higher the reliability the more probable the virus detection and removal, avoiding threat diffusion. Diffusion is further influenced by the attitude of humans operating PCs; the simulator reproduces human activities during the daytime (e.g. wake up, go to work, lunch break, work with partners, move to other office) increasing scenario realism.

The Entities simulated within the T-REX model include among the others:

- People: This category is divided into terrorists and regular persons. They are characterized by status, condition, real nature, social network connections; in the simulation they are represented by icons able to change colour and size based on their condition; for instance, if they are recognized as normal population, dormant

1 Operational background and state of the art

terrorist, active terrorist, intercepted terrorist, neutralized terrorist, terrorist planning attack.

- ICT Nodes: all the ICT elements including Laptop and Desktop computer as well as smartphone
- USB Pen Drives
- Autonomous Systems: for instance, UAVs (Unmanned Aerial Vehicles), flying over the scenario, in charge of intercepting communications and UUVs, UGVs (Unmanned Underwater and Unmanned Ground Vehicles) assigned to patrolling roles.
- Conventional Military Assets: for instance, Navy Ship and ground vehicles and units patrolling the area
- Critical Infrastructures: Oil Platform, Tank Farm, Oil Terminal, Power Plant, Desalination Units
- Civilian Entities: such as Cargo Ship arriving into the oil terminal
- Cyber Attacks and Cyber Defensive Actions defined in terms of efficiency, reliability, responsiveness and effectiveness; each of the ICT nodes and links is considered in terms of confidentiality, availability and integrity.

All the entities listed are vulnerable to real and cyber-attacks and are simulated both in their cyber connections and physical operation.

The Simulation allows the visualization of Communication link and data package exchange.

The communications considered in T-REX include voice, E-Mails, Phone call, SMS, MMS, What's App text, Snapchat, Facebook, Twitter and other Social Networks.

Through the GUI the User can set the following parameters:

- Simulation Speed
- Autonomous System Configuration (e.g. UAV number)
- Initial Number of Infected Computer
- Virus Strength in Attacking a Node
- Antivirus Reliability
- Virus Diffusion Speed
- Percentage of Unprotected PC
- Percentage of PC adopting Weak Antivirus
- Percentage of PC adopting Strong Antivirus
- Number of Active Entities (People and ICT Nodes) in the Scenario

T-REX provide through a basic GUI the User with the capability to observe, dynamically over the runtime, the following controlled variables:

- Simulation Time
- Instantaneous percentage of infected computer

1 Operational background and state of the art

- Instantaneous percentage of uninfected computer
- Time for shutting down Critical Infrastructures
- Situation of Critical Infrastructures
- Threat Network Status
- Asset Situation
- ICT Node Status
- Intercepted Communication Log
- Reliability of Communication Links
- Working status of ICT critical infrastructure

The experimentation carried out allowed to obtain a validation of the experimental error in terms of target function by applying ANOVA technique.

Therefore, it emerges that the most innovative researches within modelling and simulation community could be strategic for addressing almost all the areas of different layers of Hybrid Warfare (Bruzzzone et al. 2018b, 2018d).

The preliminary results achieved by the authors of T-REX demonstrated the possibility to conduct multiple actions over different layers to destabilize an area by compromising the ICT, Critical Infrastructures and by conducting asymmetric warfare actions. The extraction of the threat network communications over the different social networks and channels is a good example of how this approach could support also use in CAX (Computer Assisted exercise). Indeed, by simulating the detected and undetected activities of the threat network

1 Operational background and state of the art

and the dynamic intelligence results based on the used assets, it becomes possible to provide to such exercises a much more complex representation of these activities.

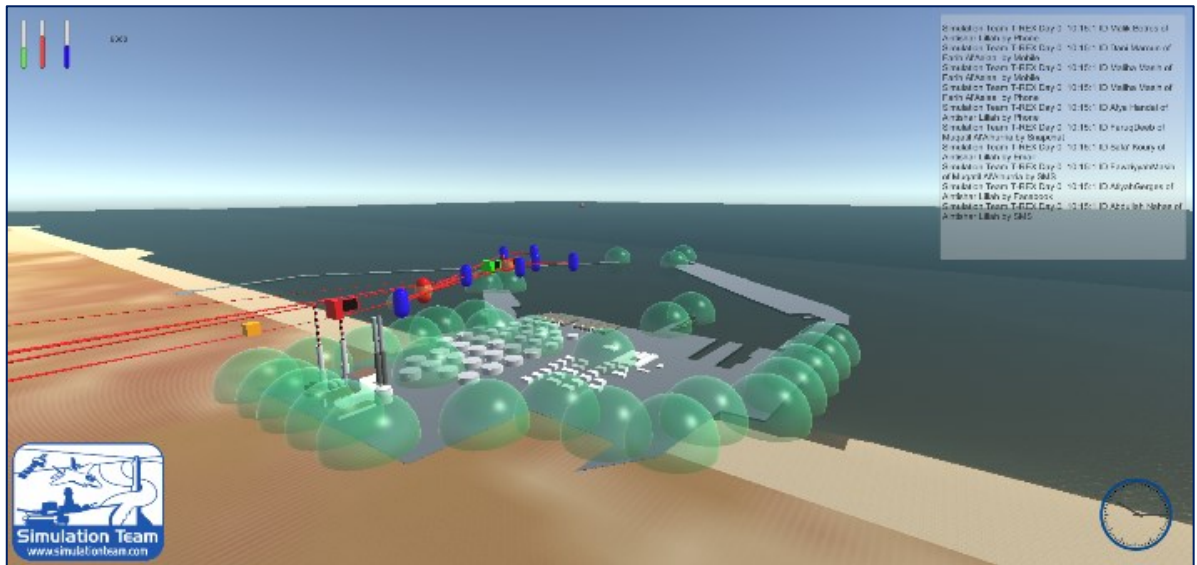


Figure 1.10: The port with his security system in T-REX

The simulator was also paying special attention to autonomous systems considering the growing use of these elements as well as their strong connections with cyber defence.

The simulation Team is currently working on further extending the simulator T-REX to represent additional Hybrid Warfare elements.

1.4 Oil Platforms

A particular case of critical infrastructure for security are offshore platforms. These buildings due to their intrinsic nature, how they are built and their operational location, can easily be the object of terrorist attacks and sabotage.

Their safety is very difficult to guarantee and therefore, in order to better understand these difficulties, it is useful to provide a description of the various existing types of such structures.

First, off shore drilling can be divided into two broad categories:

- Movable
- Fixed

1.4.1 Mobile Offshore Drilling Rigs

The main feature of these platform is that they aren't permanently anchored to the seabed. For this reason, they can be moved from one point to another, depending on the needs. There are several different types of this infrastructure, the main characteristics of which are presented below.

Drilling Barge

The Drilling Barges are mainly used for drilling in inland seas with shallow water. Typically, they are used in lakes, swamps, rivers and canals. These structures are large floating

1 Operational background and state of the art

platforms that can be towed by tugs. Designed for shallow and calm waters, they are not able to withstand the marine motions that are found far from the coast (K. Sadeghi 2007).

Jackup Platforms (raised platforms)

Jackup Platforms are similar to Drilling Barges, with only one big difference: once towed on the site to be drilled, three or four 'legs' are lowered to touch the seabed. This system allows to raise the platform above sea level, unlike the barges that instead float, reducing the sensitivity of the platform to the marine weather conditions. This converts into a condition of better safety during work. However, this type of structure can be used only in shallow waters, up to about 150 meters of depth, since it is not possible to extend its legs more than a certain length.

Submersible Platforms

Submersible Platforms provide, such as those raised, a contact with the seabed. They consist of two hulls positioned one above the other. The one at the top contains the rooms reserved for the crew just like a normal platform. The one on the bottom instead, has the same function as an external hull of a submarine: when the platform is moved, it is filled with air in order to float the entire structure, while when it is stationary at the point of the installation, it floods with water so as to sink the platform until it touches the bottom.

This type has the advantage of being easily moved into the sea, but, like the others described so far, it is limited to shallow waters.

1 Operational background and state of the art

Semi-submersible platforms

This type of platform is the most used because it combines the advantages of submersible platforms with the ability to operate in deep water. The structure is made up of columns and hulls that, similarly to the lowest of the submersible platforms, can be flooded with water or filled with air. The operating principle is the same as the type described above with the difference that the submerged hulls do not reach the bottom, but only up to a certain depth. So, the platform does not rest on the ground but continues to float on the sea.

During the operation of the auger, the stability is given by the part of the submerged platform and to avoid drifts are used large anchors, weighing at least ten tons. So, the latter, combined with the submerged hull, allow the use of the platform even on the high seas, ensuring its safety even during adverse weather conditions. Currently, with modern technologies, these platforms can be used easily in the deep seas more than 1800 meters.

Drillship

As the name suggests, drilling vessels are ships specially designed to perform drilling operations. The drillship, in addition to all the features and equipment of a transoceanic ship, have a drill located at the centre of the whole hull, where there is a well, called 'moonpool', which vertically crosses the whole hull. This hole allows the head of the auger to come out from underneath the hull so as to be able to extend the machine to the desired depth.

1 Operational background and state of the art

To remain on the drilling site, these large ships use a sophisticated dynamic positioning system. Using electric azimuthal propellers capable of moving the ship in any direction, sensors placed on the auger and a computer that uses positioning satellites, the ship corrects its position at all times so that it always remains at the pre-set point.



Figure 1. 11: A typical drillship (image taken from <http://www.2b1stconsulting.com/drillship/>)

These structures, thanks to their characteristics, are used in very deep waters.

1.4.2 Fixed Offshore Drilling Rigs

These infrastructures are permanently anchored to the seabed and therefore, once installed, can no longer be moved.

There are many types of fixed platforms and all have the same advantage over mobile ones: higher stability.

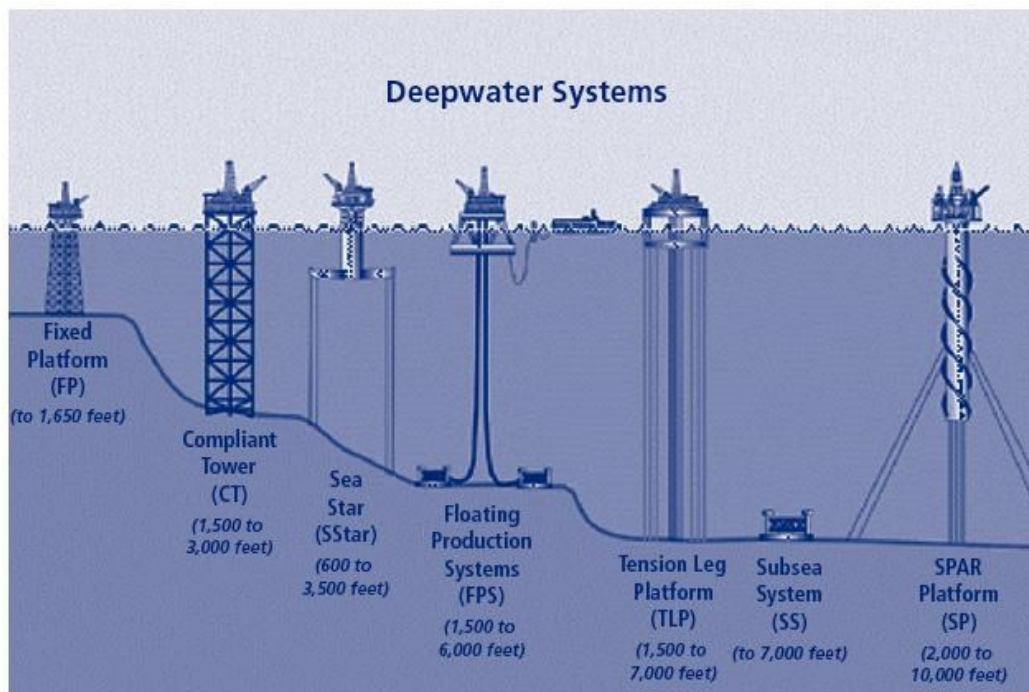


Figure 1. 12: Various types of Fixed Platforms (image taken from <http://uniquemoments.ro/wp-admin/fpso-turret&page=4>)

Fixed Platforms

In certain cases, and in not very deep waters, it is possible to physically attack the platform at the seabed.

1 Operational background and state of the art

Anchoring to the seabed can be done in two ways: either with concrete or steel 'legs', fixed to the bottom with pylons, or through imposing concrete structures constrained by their own weight at the point of installation.

Since they are anchored to the seabed, they suffer very little from the effects due to wind and marine motions. On the other hand, as already mentioned, they cannot be used in deep waters because the costs would be excessive.

Compliant Towers (Tower Platforms)

These platforms are similar to the previous ones. The distinction with these lies in the structure that connects it to the seabed: instead of having 'legs', they have a narrow tower attached to the foundations on the ground.

Unlike the structure of fixed platforms that is very rigid, this tower is flexible and allows the construction to absorb the high pressures exerted by winds and marine motions. In this way the Compliant Towers are very robust and allow their use in deep water, up to almost 1000 meters, even withstanding the adverse conditions caused by a hurricane.

Seastar Platform

Seastar platforms are a compromise between semi-submersible and fixed ones. They are equipped, in fact, with a submersible hull depending on whether filled with water or air as the first, and a series of 'legs' that anchor them to the bottom like the second. In this way they

1 Operational background and state of the art

have the advantage of stability due to the attached hull, and the little mobility due to the anchorage.

The 'legs' are cables always kept in tension by the residual float of the platform immersed body that do not allow the vertical movement of the platform, but instead allow the side one. In this way the structure can counteract the force of the sea and wind without breaking the anchor.

Starfish platforms are used for small deep-water basins when building a platform is not economically viable. They can operate at a depth of more than 1000 meters.

Floating Production Systems

Floating Production Systems are essentially semisubmersible platforms that have inside them, in addition to drilling machines, also equipment for oil extraction. In this type of ships are also allowed that can be used as floating production systems (FPSO).

The platforms are held in the place of extraction or through large and heavy anchors and/or using the dynamic positioning system used by the drilling vessels.

With the floating production system, once the site is drilled, the drill head is not retracted aboard the platform, but remains attached to the seabed.

The oil is then transported from the head of the drilling rig to the production system on the floating platform through vertical pipes (risers).

These structures can operate up to more than 1800 meters of depth.

Tension Leg Platforms

The Tension Leg Platforms are basically a larger version of the starfish platforms. They have 'legs' made up of live cables that connect the platform directly to the seabed. So, these 'cords' also limit enormously the vertical movement and allow a wide lateral movement (more than 6 meters).

Thanks to this semi-mobile structure, they can operate up to more than 2000 meters of depth.

Subsea System

Subsea Systems are oil extraction wells located directly on the seabed unlike the structures already described, located on the surface.

These structures don't have drilling machines and therefore the drilling of the ground is delegated to a mobile platform. The extracted oil or natural gas is then sent through marine pipelines to existing platforms or directly to nearby port facilities.

These underwater platforms are strategically convenient when a field consists of several extraction points: a single floating extraction system is built and many Subsea Systems that send their extraction products to this single platform.

Submarine extraction systems are typically used at depths greater than 2100 meters.

Spar Platforms

The Spar Platforms are the largest offshore platforms used so far. They are characterized by a large cylinder that supports the platform. However, this cylinder does not arrive directly at

1 Operational background and state of the art

the sea floor but up to a certain altitude. The connection to the ground is guaranteed by a series of cables and pipes.

The large supporting structure stabilizes the platform at sea and allows movements to absorb the forces exerted by a hurricane.

There are three different types of such platforms, diversified by the shape of the hull.

The classic spar is the one described above: the hull is composed of a single large cylinder.

The Truss Spar instead, has a tubular system that separates the part that serves only ballast at the base of the platform, from the top also cylindrical on which the platform is resting.

Of the last type, the Cell Spar, there is a single example in the world. It is characterized by the replacement of the only platform supporting cylinder, with a system of several cylinders that surround a central one. This structure is the most economical because of a smaller size and therefore a smaller quantity of raw materials.

The spar platforms can operate up to 3000 meters deep.

1.5 Natural Gas Plants

Natural Plant Plants deserve special attention because of their intrinsic hazard. They arise, on the average, onshore on sea coast or offshore not excessively seaward, as they require a large amount of water to subtract or bring heat into the transformation processes that undergoes natural gas (NG).

The GN, as we know, at room temperature and atmospheric pressure is in the gaseous state. Since in the liquid state it occupies about 1/600 of the volume occupied by the aeriform state, once extracted it is liquefied to allow a more advantageous transport and storage.

During the liquefaction process then it is also possible to remove those components such as powders, acid gasses, helium, water and heavy hydrocarbons, which are polluting or/and lower the heating power and/or damage the instruments with which the gas is then used.

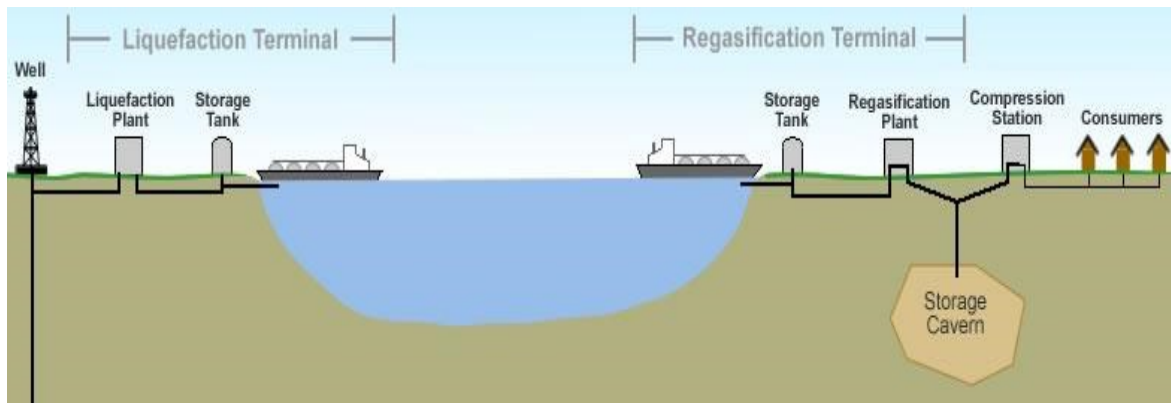


Figure 1.13: Typical Natural Gas production chain (image taken from <http://geology.com/articles/lng-liquefied-natural-gas/>)

Mainly composed of methane, the Natural Gas passes to the liquid state at a temperature of -162°C at atmospheric pressure. To reach these temperatures a large quantity of coolant is used, on average water, and therefore the infrastructures suitable for this process arise near the sea, in the ports. Then in liquid form it is then transported to the destination point where there is a regasification plant. This structure performs the opposite action of the previous one: it returns the fuel to the gaseous state. This transformation, however, releases a large

1 Operational background and state of the art

quantity of heat that must be removed in some way. For this reason, even these plants are born near the sea in such a way as to be able to exploit sea water as a coolant.

Basically, both the arrival and departure terminals see large tanks where they store the gas Natural Liquefied, of a structure used for the physical transformation of the fuel and of a quay equipped with special pipes, built at Hoc for the loading and unloading of LNG (Liquefied Natural Gas) on transport vessels called gas carriers.

These infrastructures therefore deal with a substance which in itself is very dangerous because it is explosive, and a possible attack against them could have a considerable destructive effect. Therefore, it is very important to increase the safety of the port areas in order to protect these infrastructures which for their task fall into the category of critical safety.

An explosion of these plants could lead to immeasurable collateral damage, both in terms of human and economic and social lives. Suffice it to say that all modern buildings and houses are connected to the Gas network. This is used in kitchens and heating systems in private homes, as fuel for creating heat for generating electricity or for triggering chemical reactions in industries.

For all these reasons, a possible interruption of the supply service, nowadays, would cause serious social and economic damage as well as the loss of income of the owner of the plant. Moreover, such facilities often arise near commercial ports and therefore other activities could directly imply the destructive effects of a detonation of these plants.

Fortunately, nothing like this has ever happened to these plants, but they certainly represent an excellent target to strike many of the industrialized countries alive. So, a policy of greater security is not at all advised but rather is greatly encouraged by many governments.

1.6 Submarine Pipelines

When the distances are not too long and when the Earth's morphology allows it, instead of the traditional means such as trucks or ships, pipes are used to move oil and natural gas. These ducts, if necessary, to cross small stretches of seas, lakes or rivers, can be underwater. If you want to install this type of piping you have to choose carefully the route to be carried out because they contribute several problems that include several factors, including:

- Background state: it can be flat or irregular presenting bumps or dips or submarine canines. In these cases, you have to be careful because connecting the pipeline from side to side, in addition to having the weight of it itself that causes it to flex, there are very often also vibrations from currents (Von-Karman). The corrective measures for these cases include the levelling of the seabed made by injecting sand under the pipes, and a constant monitoring of the pipelines. Another factor to consider is also the resistance of the bottom, in fact it can be yielding causing the sinking of the pipe in it to a depth that makes maintenance work difficult or, on the other hand, too hard to create abrasions and damage to the outer coating of the pipeline at the points of contact between it and the submarine rock.

1 Operational background and state of the art

- Mobility of the seabed: on the seabed there can be some sand dunes just like in the deserts that with time move because of the currents. So, if you support a pipe from one of these it could happen that after a period of time it remains without support and can break. So, backdrops with these characteristics are to be avoided.
- Underwater landslides: in the sloping seabed with high sedimentation rates, landslides may occur due to seismic events, which may cause the pipes to be inflated by bending them and/or causing breakages on them.
- Currents: in the same way as the winds present on the surface, in the water there are currents that encourage conduits even in a costly manner. They can be very strong even in shallow seas, and therefore it is preferable to avoid areas where they are present with high insistence.
- Waves: In shallow water, waves could be a problem both in setting up and for stability during the entire life of the pipeline due to the forces that can exert on it and the corrosiveness of the water.
- Problems in the Arctic environment: in areas with cold climates, additional problems can be created. First, icebergs could be harmful to pipelines. In fact, by drifting in shallow water, the seabed is crossed with the keel in such a way as to damage the pipelines or hit directly with them. Another possible problem may be the vortices that could either break the pipes due to the strong currents generated and remove the ground at the base of them causing their collapse.

1 Operational background and state of the art

- Other pipes: along the chosen route you could intersect other pipes. In this case a bridge structure should be built in such a way as to avoid and pass over it. This resolution must be well designed because both the direct contact between the pipes and that due to displacements due to the currents must be avoided.
- Fishing vessels: fishing boats often scrape the seabed with their nets, and these could damage both boats and pipes if they collide with them.
- Anchors of the ships: the anchors of the ships could be one of the possible causes of breaking of the marine pipes.
- Military activities: some marine areas, which were theatres of military clashes, could still be scattered with explosive devices such as mines. Other areas could be used to try new weapons and other anchors may have sensors for detecting submarines, on the bottom. All these areas must be avoided.

So, taking all these issues into consideration, it is easy to understand that the paths to be followed are hardly ever the most direct, but to have 'safe' traces, there are continuous detours that increase the mileage.

These pipes can have different dimensions depending on what they are carrying and their capacity. Their main characteristic is that they consist of several concentric tubes, generally two, in such a way that only the outer cylinder moves, thus limiting the displacements of the innermost one, in which the extracted material actually flows. In other words, the external piping serves as protection for the internal one.

1 Operational background and state of the art

It has been calculated that for the transport of gas and oil, the submarine pipelines are advantageous up to a distance of about 25,000 km, beyond which the transport via methane tanker is cheaper.

So, in the seas there are great distances covered by these pipes that are exposed to possible sabotage attacks. In fact, at the moment it is very difficult to be able to monitor all the kilometres that they travel, and this makes them highly vulnerable. An attack on them would bring all the economic and social problems already exposed for on-shore infrastructures, with the addition of possible environmental damage due to the leakage of the transported fuels.

The constant monitoring of pipelines is very expensive with traditional means and for this reason they are only occasionally checked. This, of course, is a great danger that should be avoided. Autonomous vehicles would lend themselves very well to this task: once left at sea, in fact, they would patrol the pipelines throughout their run until they are exhausted. Then they could be fished to recharge the batteries while replacement drones would continue to perform their task. In this way there would be a constant monitoring of the pipelines that would significantly increase their overall safety. In fact, the instruments that make up the payload of autonomous vehicles have, in addition to monitoring the presence of possible threats, could constantly monitor the conditions of the waters they pass through, also detecting the presence of pollutants deriving from possible undetected spills.

1.7 UxV & SAFETY

Safety is a major issue as well as one of the major driver, along with security, for the extensive use of UxV in civil and military applications; in facts their low operational cost and expendable nature make them ideal for being used in dangerous environments and almost all case studies proposed in the paper deal with these topics (Apvrille et al.2015; Merwaday & Guvenc 2015; Altawy et al. 2016). Due to the complexity of these context the use of M&S (Modelling and Simulation) is considered often the most promise methodology for investigating modern UxV problems (Bruzzzone et al. 2016e).

In facts, Simulation Team is working on up-to-date simulation technologies and has acquired a large experience in autonomous systems within a broad set of applications with special attention to collaborative multi domain cases (Bruzzzone et al. 2014a, 2016f). Along last years, the Simulation Team has activated several projects for Industry and major Agency in using UxV in industrial plants (Bruzzzone et al. 2016e).

From another point of view, INAIL-DIT is a Department that, in line with its mission, is approaching these new UxV and remote pilot systems while also keeping in mind the safety aspect. The safety measures to be taken in the design and use of drones are just some of the topics that will need to be addressed in order to get products up to all applications where they can be effectively used; among these topics for instance it could be useful to develop studies on materials suitable for protecting the drone itself as well as the people around, or the development/adoption of sufficiently advanced safety equipment, beyond the ones required to fulfil the functional requirements of the drone (Valavanis et al. 2014; Sanchez-

1 Operational background and state of the art

Lopez et al. 2016). Finally, it is desirable that regulatory and technical standards follow, or rather support, this innovative process within Industry 4.0 and its technologies, including remote pilot systems (Kehoe et al.2015). INAIL-DIT is committed to being ready to support the National Authorities in every step when collaboration would be necessary. For instance, the use of remote pilot systems involves remote control by a human and, sometimes, the presence of other personnel engaged in carrying out work in close proximity to the areas where autonomous vehicle operations take place; this introduces issues about training among the others. In addition, this scenario implies also the need to apply the relevant legislation for the protection of the health and safety of workers, as well as the rules of transposition of applicable product and other relevant National or International regulations (Djellal & Gallouj 1999). This implies that the authorities and bodies involved are plural; in addition to the European Commission, which is responsible for the issuance of directives/product regulations, many National Departments and Ministries as well as Public Organizations are involved, such as, for instance in Italy, the Ministry of Labour and Social Policies, the Health and Safety of Workers, the Ministry of Labour Infrastructure and Transport, for Aviation Security or Navigation and the National Agency for Civil Aviation. In the following it is proposed an overview of different application fields for UxV where remotely operated vehicles and autonomous systems might positively affect the health and safety of workers. Given the succession of serious and fatal accidents occurred over the past few years during the conduct of activities in suspected or confined environments (Spillane et al. 2012; Nano et al.2013; Leão et al. 2015), which in many cases highlights an inadequate risk assessment

of the possible presence of hazardous substances, one of the first uses of remote pilot systems is definitely about air quality control in confined environments such as silos, tanks, holds, and other environments (Valavanis et al. 2014).

In this case, it might be useful to equip drones with "smart" sensors for evaluation, for example, of the conditions that may allow operators to enter in dangerous areas (Floreano & Wood 2015). It is clear that, in order to operate these systems, it is necessary to carefully consider the characteristics that these systems to check consistency with presence of liquids, vapours or dust and, more generally, hazardous areas (such as areas subject to the ATEX Directive). These analysis and requirements are devoted to ensure safe and adequate use of UxVs under critical conditions that may occur in confined environments, or in general, within the areas where they should operate during emergencies; for instance in avoiding the accident escalation from fire scenarios in case of upper tier Seveso plants (Palazzi et al. 2017).

In order to ensure its safe and adequate use in difficult conditions that may occur in confined environments or in general in environments where drones should intervene for emergency management (e.g. in case of Accidents at high risk companies). Another useful application of UAVs for the protection and safety of workers is their use for inspections at relevant heights or at least in difficult-to-reach areas for structures and equipment in order to check their integrity and stability through a visual examination assisted by optical systems (cameras, thermal sensors etc.) or checks performed using other equipment (Jones 2006). In addition, UAVs can be utilized for environment surveys through high-resolution

1 Operational background and state of the art

photographic capture, enabling visual 3D mapping and thus the knowledge of orographic features (e.g. slopes of the ground) as well as to detect, in real time, the presence of obstacles and particular conditions of danger determined, for example, by climatic factors which may change the orographic conditions already observed (Siebert & Teizer 2014). Another important, but less known application of UxV is monitoring of infrastructure using GPR (Ground Penetrating Radar). Unlike other mentioned types of sensors, the GPR allows to control conditions of infrastructures hidden under soil; for instance, it is possible to detect flooding or voids, furthermore, being installed on a UAV, the GPR allows to perform this operation in short time (Kovacevic et al. 2016). Of course drones could operate not only individually, but also in a swarm which allows to install different kinds of sensors on the platforms and it could enhance drastically data acquisition capabilities of the whole system; this swarm collaborative use represents one of most promising directions of research in this field (Burkle et al. 2011). The data acquired in this way are available for being communicated instantly to the control unit of a bulldozer or any other moving machine that, through the help of a GPS system, could "alert" the driver if it is approaching to danger zones; it becomes possible also to develop a smart guiding support, in an assisted way, by providing automatic corrective actions, such as speed reduction until stopping or finding an alternative route, as a dynamic new risk point or area is approaching (Kim et al. 2015). To do this, the remote pilot system should be equipped with appropriate instrumentation (sensors, radar, cameras, etc.), now largely present on the market, which can be utilized with the specific task.



Figure 1. 14: Man on the Loop Supervising Operations within SPIDER special CAVE

As already mentioned, another useful area of employment is the acquisition of information through drones for the management of emergency relief activities (Doherty et al. 2007).

In facts, aerial reconnaissance with drones allows to have a direct view of the situation of places where it is not easy to access, at least for a first assessment process to drive first responders, thus facilitating assistance and recovery through, for example, identification of a possible access path to the affected area.

Other possible applications are those related to the evaluation of the various emissions of the machines and machineries (Gardi et al. 2016).

1 Operational background and state of the art

This includes also the use of microphone on drones that could prevent the placement of microphones on fixed positions difficult to be implemented due to the constraints of the machineries themselves (Ishiki et al. 2014). In addition, it has been studied the possibility to use drones to evaluate drift of fertilizers applied to irrigation machines in herbaceous and tree crops (Pulina et al. 2016).

This kind of testing could involve drift tracking using UAV equipped with high definition (HD) visual recording systems (Pizzarella 2014); the related images could be acquired by different profiles: from top, back and side, by using a water-based liquid mixed with a red powdered food for distribution analysis; once the drift motion is tracked the same is replicated graphically through the GIS support on an aerial photo.

More replicated tests in different climatic conditions could simulate different drift situations. In these cases, further focused analysis could be carried out on the specific weight of the distributed product, as the weight of the treated molecules that have different behaviour even with same meteorological conditions.

In facts, it is now possible to extend the scope and use of new autonomous system technologies, including the remote pilot systems, to increase safety and health levels through specific studies and research that allow to evaluate and promote their effectiveness.

1.7.1 CASE STUDIES ON UxV SIMULATORS

The challenges previously presented represent often new application fields for UxV or specific implementations of new solutions; so, it is evident that to complete their test and experiment and to evaluate related risks in terms of safety, it is necessary to recreate a

realistic mission environment. Usually this requires to be addressed by M&S (Modelling and Simulation) in order to be effective (Bruzzzone et al. 2014a); in facts the adoption of MS2G paradigm (Modelling, interoperable Simulation and Serious Games) represents a very strategic advantage allowing to combining different models, simulators and also real equipment within a common synthetic environment. These simulation environments should be intuitive and interactive by using most advanced Mixed Reality solutions such as the SPIDER (Simulation Practical Immersive Dynamic Environment for Reengineering), developed by Simulation Team, in order to support the Subject Matter Experts (Bruzzzone et al. 2016e). In the following case studies are proposed.

IDRASS

Indoor Operations in industrial Plants are critical especially in case the environment is contaminated, so they represent an ideal example to apply UxV; from this point of view, the support during disasters in industrial facilities is a very popular area for R&D on UxV due to the challenges represented by these environments (Bruzzzone et al. 2016e); some of the authors developed IDRASS (Immersive Disaster Relief and Autonomous System Simulation) to address this context in case of CBRN (Chemical, Biological, Radiological and Nuclear) contamination due to accidents or man-made disasters (see figure 7); IDRASS simulates both operations indoor and outdoor within different industrial facilities such as chemical and nuclear plants (Bruzzzone et al. 2016e). In these contexts, it is usually necessary to introduce many actors to reproduce the whole crisis scenario and, obviously, the use of

1 Operational background and state of the art

IA (Intelligent Agents) is a fundamental resource for being able to develop realistic mission environments. The safety issues in using drones within industrial facilities deals with the challenges due to these context (Mobley 2001): cables, cable trays, pipelines, tanks are physical obstacles that populate the area with high density. Therefore, in several cases there also relief venting systems and safety valves that could create streams challenging for UxV in terms of blast as well as temperature; in the plants often, the atmosphere could include dusts, corrosive agents as well as high temperature elements dangerous in terms of irradiations (Bruzzzone 2017).

It is evident that there are solid, thermal and gaseous barriers not easy to detect and creating complex environments; sometime the UxV could be required to operate also in confined environments where the air mix could turn to be dangerous for explosions respect the characteristics of some of the robotic system components. In facts, the whole industrial plant could include several systems that could create risks and domino effect in case of UxV collision or even just interaction; indeed, the electronic interference between UxV controls and DCS (Digital Control System) could affect plant safety. In facts, it is also necessary to remind the very crucial aspect of electromagnetic compatibility. These aspects are common just to the presence of high voltage lines and equipment in the industrial plant and becomes even more intense in presence of ionizing radiation caused by nuclear spills and contamination, which could lead to loss of connection as well as drone malfunctions in case of its insufficient radiation hardening (McCurry 2017). In addition, it is also necessary to consider the presence of “natural” communication barriers, caused by reflection and

1 Operational background and state of the art

interference of electromagnetic waves due to the high density of metallic infrastructures; these are affecting UxV communications and operations.

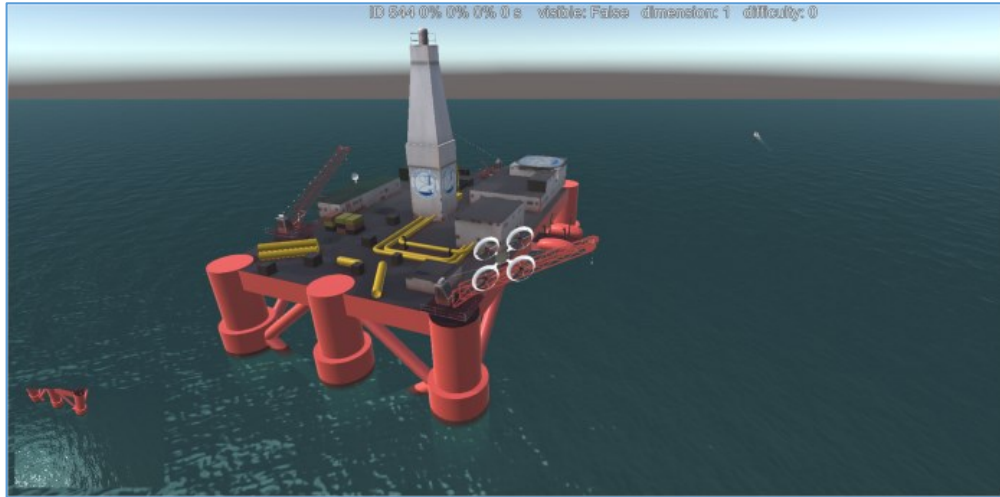


Figure 1. 15: SO2UCI with Drone supervision of the Off-Shore Platform

From this point of view, it is expected to require a high level of autonomy to the UxV considering the risk to lose contact with central control.

In IDRASS also the issue related to battery autonomy are raised, considering that to move within an industrial plant and to carry out data collection and sensor measures it could be challenging to have time to complete the whole mission, especially when moving indoor and/or in confined spaces. Finally, the industrial plants include presence of humans and the UxV should be able to operate avoiding injuring them by collision or indirectly by generating other accidents.

1 Operational background and state of the art

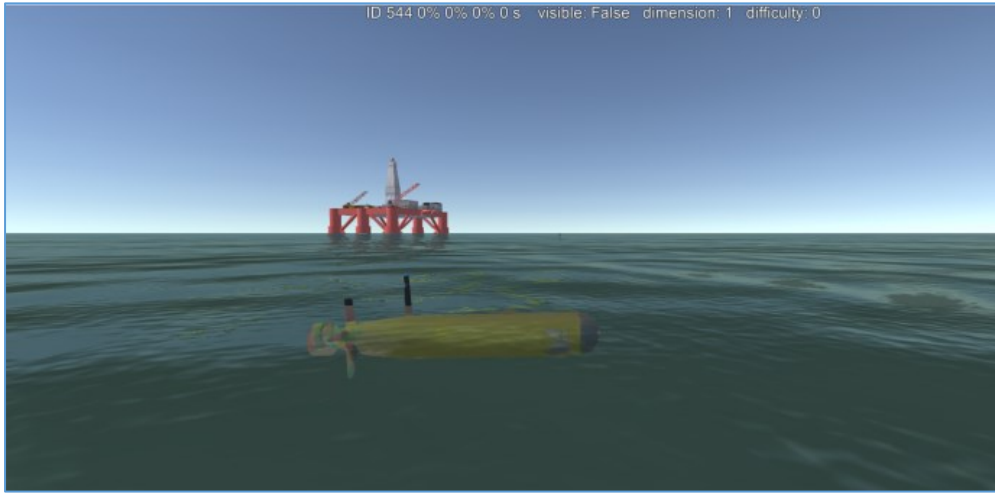


Figure 1. 16: AUV in SO2UCI patrolling around the Off-Shore Platform

From this point of view, an interesting idea is to assign the role of supervisor to humans instead than directly making them to pilot each single UxV as expressed by the man-on-the-loop concept supported by SPIDER solution as seen in Figure 1.14 (Magrassi 2013).

This is a great opportunity, reducing drastically the number of people required to support complex operations, but also a challenge for safety and security and introduce new challenges in terms of technological solutions and training (Bruzzone et al. 2016e). In the case of critical infrastructure protection, a major issue is related to false alarms; indeed, the large majority of suspect events are related to case dealing with harmless conditions due to general traffic, civilian unintentional infractions, birds or animal misclassification, etc (Bass 2000; Cardenas et al.2011). In addition to these considerations it is also possible to face sensor errors and failures that could create critical conditions in the protection systems (Merabti et al.2011).

In facts, this problem requires to cover 24/7 in presence even of challenging weather and boundary conditions (Kastek et al.2012).

Indeed, the use of UxV could be useful to reinforce the protection of critical infrastructures, considering that could be a robust solution supported by multiplatform, multisensory data fusion and that could allow to conduct further investigations directly approaching to the alerts in order to discriminate real threats from false alarms.

Obviously, these elements suggest specific requirements in terms of collaboration capabilities, redundancy and responsiveness of the multi UxV system.

SOU2CI

Operation on board of Off-Shore Platforms are very complex and the environment inside and outside the rig is very challenging due to the complexity of the platform and to the extreme boundary conditions where it operates (e.g. sea and weather); in this case the use of USV, UAV and AUV/UUV, in combined way, could be very useful; due to these reasons it has been developed a simulator called SOU2CI (Simulation for Off Shore, On Shore & Underwater Criticall Infrastructure) (see Figures 1.15 & 1.16) for investigating the capabilities of heterogeneous networks of autonomous systems within this application field (Bruzzzone et al. 2013c).

Indeed, the coordination among UxV operating in different domains is a crucial element for addressing these kinds of complex missions (Stilwell et al. 2004; Shafer et al. 2008; Tanner et al. 2007b).

1 Operational background and state of the art

In facts in this case the use of AUV coordinated with air assets is fundamental (Grocholsky et al. 2006; Bruzzone et al.2016d); therefore, the use of UUV (Underwater Unmanned Vehicles), such as gliders, introduces additional challenges due to the difficulties related to the underwater communications (Jans et al. 2006).

The collaboration capabilities are strongly related with the introduction of advanced AI solution and potentially by the human on the loop concept already mentioned (Sujit et al.2009; Bruzzone et al.2013c).

2 Principal Utilized Technologies

2.1 Interoperability and HLA

Interoperability in Modelling and Simulation (M&S) was conceived with the aim of developing distributed simulations and facilitating the reuse of models. In fact, it is one of the pillars of model development for many organizations, such as NATO, which require effective integration of latest advances created in different institutions and research centres all over the globe. Obviously, such solutions are developed independently, hence they are typically implemented using different paradigms and approaches, are written in distinct programming languages and supposed to operate in different operation systems, hence, could be pretty difficult in integration. To address such issue and provide interoperability among various solutions it was developed HLA (High Level Architecture) standard, although there are other standards such as DIS (Distributed Interactive Simulation), CTIA (Common Training Instrumentation Architecture), TENA (Test and Training Enabling Architecture), (IEEE, 2010a, IEEE 2015, 2012; DoD 2010; Lanman et al 2011). Despite variety of standards and technologies, the use of HLA is typically preferred, in fact, it has become an international standard after being proposed and used by the US Department of Defence (US DoD). This architecture has evolved in recent years and has been the subject of intense research on improving its potential.

High-Level Architecture is a general-purpose architecture for computer simulation systems which unifies integration of distinct simulators. In this case, the interaction between the simulators is managed by a Run-Time Infrastructure (RTI), which is capable to coordinate operation of models. In fact, RTI is a middleware run by every participant of a distributed system and allows them to connect and communicate with each other; such approach allows to participants (federates) to create a distributed simulation (federation).

It is important to consider, that the federates do not necessarily have to be connected in a Local Area Network (LAN), but they can communicate with each other through Wide Area Network (WAN), for instance, internet, which allows creation of geographically distributed federations. For example, in a project IPHITOS, which is described later, we connected our simulator from Genoa to a federation created in Alexandria, Virginia, in the United States and we successfully interacted with other simulators, one of which is located in Calabria.

As already mentioned, the High Level Architecture was originally developed by the US Department of Defence (DoD) and became the main standard for distributed simulations of the entire Modelling and Simulation community. The HLA is used in various fields for both military and civil applications, addressing most important aspects of simulation: learning and analysis (Massei and Tremori, 2010; Massei et al, 2013). The HLA is widely used in defence and homeland security, however, it is also used in civil applications, for instance in logistics and aerospace production, (Boer et al, 2008; Bruzzone et al 2008, Longo et al 2013, Longo et al 2014). In fact, currently, HLA is a key component in the development of large

distributed simulations and was successfully utilized for modelling in various industrial sectors (Anagnostou et al, 2013; Bruzzone, 2002).

In order to provide interoperability between simulators, HLA introduces a set of specific rules, which are indispensable for management of federations, in addition, HLA provides a standard API for communication between a federate and Run Time Infrastructure (RTI). However, the HLA does not give any indication about the management of data communications within the federation regarding the possession of the information and its specific use.

Originally the DMSO (today MSCO, Modelling and Simulation Coordination Office, US DOD) freely distributed (through a controlled authorization process) the first versions of the RTI as well as related libraries. The release process was centrally controlled and supported in terms of updates and maintenance by the DMSO RTI promoting the spread of HLA (McGlynn, 1996). Since the release of the first version of the RTI, many private companies have created and released commercial versions of the RT, however, open source alternatives are available as well. Considering the fact that commercial products took over control over the sector, after only few years of development the US DoD stopped support and updates of the DMSO RTI. Currently, there are several implementations of RTI created by different developers and manufacturers, that use different communication protocols and algorithms that unfortunately lead to their incompatibility (Ross, 2014, 2012). This complication can cause some problems when a federate is designed to operate with a specific RTI while it is

necessary to adapt it to another one, but also has the advantage that different implementations can be optimized for different purposes.

An important and well studied in literature aspect of HLA is related to its performance. In fact, latency or transmission and bandwidth limitations are one of the major concerns when it comes to large federations operating in real time or in scaled time, in particular, when there is hardware in the loop (De Grande et al, 2011; Cavaliere et al, 2015; Malinga and Le Roux, 2009). Time management mechanisms presented in the HLA ensure that the federation time is consistent among all the federates. However, this requires that time advances for each federate in the federation are blocked until the RTI grants authorization. Obviously, if delays due to latency and calculation times are too big, the simulation time may no longer follow the desired ratio with real time. For this reason, it is very important in the development of the simulation architecture to know how to deal with time management in the right way.

Some key factors that determine the efficiency of a federation are:

- Time management algorithms. The HLA ensures the coherence of the time between the federates with a request / permit mechanism that blocks each member until the RTI authorizes it, ensuring that the entire Federation has reached the next time step required by the federation. Furthermore, the HLA supports guided events, time divided by steps, parallel discrete event simulation paradigms (Fujimoto, 1998). In the last case, it guarantees to each simulator a conservative or optimistic synchronization.

- The protocol of messages exchange and handling is managed by the RTI (Ross, 2014, 2012). The different RTIs use both TCP and UDP unicast and multicast protocols and often have different size limits, for the exchanged. Both the reliability and the message latency requirements differ between the versions of the RTI while difference between their specific values is sometime very significant.
- The workload is distributed among the various federates. However, some federations may not allow the calculation workload to be distributed among the federates because they perform tasks of a different nature. Scheduling algorithms, where possible, can help to balance the workload and thus prevent a federate from becoming the bottleneck that delays the entire federation. De Grande's works are a good example of strategies that reduce impact of the problem (De Grande and Boukerche, 2011; De Grande et al, 2012, 2011; De Grande and Boukerche, 2010).

In this research, three different RTI implementations have been tested to evaluate their influence on the efficiency of specific simulation frameworks. Thus, this work contributes to the HLA literature by analysing performance problems in case of a complex federation, as well as demonstrating the synergies that can be achieved through the integration of HLA between existing simulators addressing different fields. The interaction between specialized simulators from different sectors makes it possible to increase the fidelity of entire model in complex scenarios.

Before discussing more in detail about HLA it is useful to propose some definitions of some specific terms used:

Federate: is a single simulator that complies with HLA standards and connects to the federation.

Federation: two or more federates that are connected by means of RTI, share data and interact with each other, thus forming a federation.

Object: is a data structure with logically connected items which could be exchanged between the various simulators.

Attribute: is a single data item of an object. An object can have multiple attributes.

Interaction: is a momentary event that the simulators share to interact with each other.

Parameter: is a single data of an interaction.

It is essential to understand the substantial difference between an object and its attributes and an interaction with its parameters: the two concepts are in fact very similar and differ only in terms of duration; indeed, when an object is created it exists until a federate destroys it. In the same time, an interaction is momentary and dissipates immediately after it is created. Attributes and interactions belonging to them accordingly.

All the objects and interactions that can be created and shared in the federation are contained in a file called FOM (Federation Object Model) that all the federates must necessarily possess if they want to connect. In fact, all the objects and interactions that can be exchanged are presented in the FOM, however, in some cases a single federate is not interested in elaboration of all the objects and interactions published during the simulation. For this reason, there is a second critical configuration file, called SOM (Simulation Object Model), which indicates which particular objects and interactions will be monitored by a federate.

Obviously, in order to connect to a federation, federate needs both of these files. If these requirements are satisfied, a federate could connect to the federation and subscribe to required attributes, having possibility to create objects and to modify their attributes. If a federate have specific object indicated in its SOM, at each logical step it will receive update of its attributes; obviously, a federate can modify attributes only of objects it possesses. Federates can also send interactions that others can read and use. The various simulators connected to the federation never exchange data directly between each other but interact y means of RTI, which manages communications.

As shown, the communication logic is generally simple but must always respect certain conditions so that everything works correctly. Some of main aspects have been already mentioned, while the complete list is presented below:

- The federation must have a FOM written with the rules of the OMT (HLA Object Model Template)
- During the execution of the federation, the federates must not communicate between each other directly but through the RTI;
- In a federation only one federate can be the owner of an attribute or an instance of a given object and have the power to modify it. An object owned by a federate cannot be changed by another one, if such operation is required to be carried out, it is possible to request possession of an object and modify its attribute.
- Each participant must share FOM and possess its SOM, written in accordance with the rules of the OMT.

- The representations and the management of the objects, in particular update of the belonging variables, is left to the individual federates and not to the RTI. The latter only provides a link for communications.
- During the execution of the federation any modification of the FOM must take place through the RTI.
- Each participant must be able to modify its clocks so that it can synchronize it with the other simulators and accelerate or slow down the simulation speed in accordance with the rest of the federation.
- Each federate must be capable to read, modify, send and receive all the attributes of the objects present in his SOM as well as the interactions with their parameters.
- All federates must be able to transfer and / or accept possession dynamically throughout the duration of the simulation of all the attributes of the objects present in their SOM.
- All the federates are required to change the conditions with which they update the attributes of the various objects present in their SOM.

If all these conditions are met, the simulator can connect to the federation and interact with the other federates. To implement the HLA in a simulator, it is necessary to use libraries present in the RTI. The latter are typically written in JAVA or C ++ and contain all the classes and methods required for correct functionality of the API provided by the RTI. With these classes it is possible to request to connect to a federation or to create it as well as requesting updates of object attributes, instantiating objects and updating it etc. This fact

causes problems with software that uses other programming languages, such as C# and JavaScript utilized by Unity 3D. Fortunately, this limitation could be overpassed by creating an appropriate software Bridge. This software acts as an interpreter, in fact, it receives messages from the simulator and then translates them into JAVA or C ++ commands and sends them to the RTI. Same thing, but with reverse procedure, it happens when it receives communications from the federation.

One of the biggest problems in the use of HLA, as already mentioned, is the extreme diversification of RTIs and their libraries, which are not interchangeable. In fact, if it's necessary to federate simulators, they must inevitably use the same Run-Time Infrastructure. Moreover, in various circumstances, it is not enough to use only the same software because the version used is also influential, for instance, from one update to the other the libraries could change. Despite such problems, the HLA is an excellent tool to provide the interoperability of the simulators, in fact, it is widely used in many fields in engineering and training for both civil and military uses.

2.2 Unity 3D

Unity 3D is a flexible and powerful game-engine, which allows development of both 2D and 3D simulators. Furthermore, it is capable to work with different target platforms, from PC to consoles up to mobile phones and virtual reality headsets. Another important advantage of Unity is related to the Graphic User Interface (GUI), which is very intuitive and easy to use. In order to be able to utilize various 3D models, Unity provide support of numerous file

formats, which allows import directly from CAD software, even if some cases such models are too complex for the engine. For these reasons, the created simulator was developed using this software.

The interface is composed of a virtual environment, where 3D models are imported, or are created directly from simple geometric shapes, and a series of utilities that allow to modify, move, assign characteristics and behaviours to all that is present in the created world. The behaviour logics of the various objects present in the environment are defined by means of the scripts assigned individually to the various models; such scripts can be developed in JavaScript and / or in C#. The software contains all the standard libraries of these languages with the addition of other own libraries, while corresponding documentation is available online. Unity utilizes its own physical engine named PhysX, that allows to manage dynamic models that regulate the behaviour of objects. With this software it is possible to assign positions, velocities, displacements, accelerations, forces and moments to the various entities. Furthermore, it manages collisions between the various objects, calculating the forces and moments generated by the collisions; moreover, it also includes functions to move objects autonomously from one point to another, identifying the fastest route and avoiding obstacles encountered along the way.

In the virtual environment, objects can be autonomous otherwise be "children" of other objects. In this second case, the centre of the coordinates is no longer the absolute centre of the virtual world but that of the "father" object, that is, the "children" objects have the coordinate axes of the "father" as an inertial reference system. Hence, if parent object is

moved, the child objects move accordingly, however, through script it is possible to obtain the absolute coordinates of the child object and, if necessary, free it from the father. This behaviour could be illustrated by the following example. A person who is walking down the street, heading to his car: until the man is outside the car the two systems (the car and the person) are totally unrelated and both are allowed to move independently, without influencing each other. When the person enters the car and it begins to move, they move together. To transmit the motion from the car to the person, it is therefore sufficient to set the person as the children of the vehicle, and it consequently will follow all the movements of the machine, even if it can move inside the machine. When the passenger gets out of the car once he has reached his destination, it is sufficient to remove this constraint and the two systems return to be completely autonomous.

The cameras and lighting are another important aspect of this software: it is possible to recreate directional lights that do not influence the vision of the camera, dynamically recreating shadows and brightness.

With this development environment it is possible to recreate various types of settings for the most varied purposes: for this reason, it was chosen for the purpose of the realization of the research project, at the base of precision, good graphics and excellent visualization which were required.

3 JESSI

3.1 Models

In the recreated virtual environment, there is a great variety of 3D models, of which a brief description is given below:

- **Aircraft Carrier:** the British Aircraft Carrier Queen Elizabeth is reproduced. This is still under construction and is expected to enter service in 2020.



Figure 3.1: British Aircraft Carrier Queen Elizabeth 3D Representation

- **AUV MUSCLE:** electric propeller underwater drone. Cylindrical in shape, it is equipped with many sensors and is used to probe the seabed and to patrol sensitive areas. Still many experiments are carried out on it and on possible alternative uses.

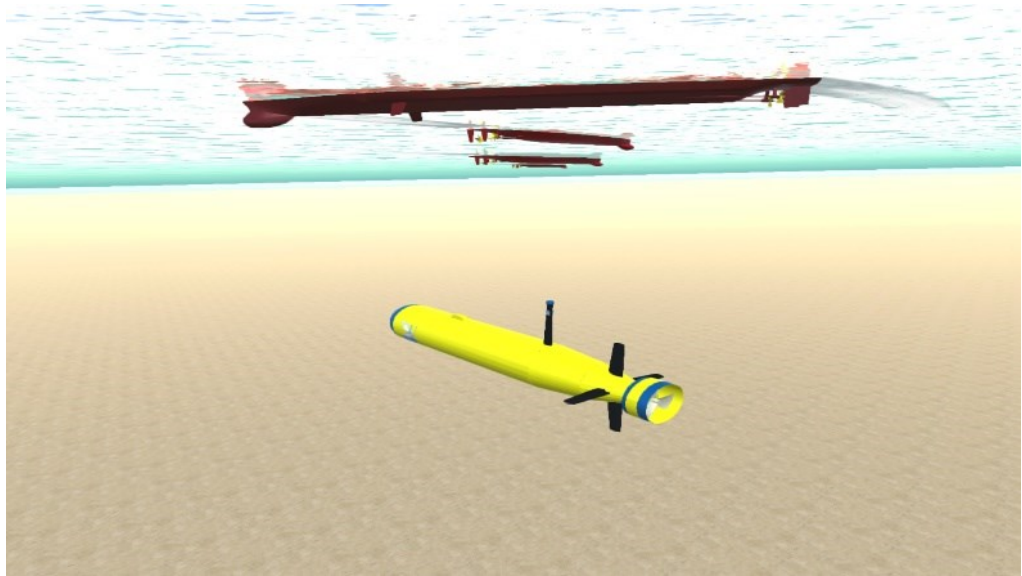


Figure 3.2: 3D representation of AUV MUSCLE

- **Communication link:** these are imaginary links that are displayed to represent communications between the vehicles in the scenario. They have different colours, sizes, and speeds depending on the type of communication, to make it clear at a glance the difference between communications in terms of packet speed and quantity of information exchanged.

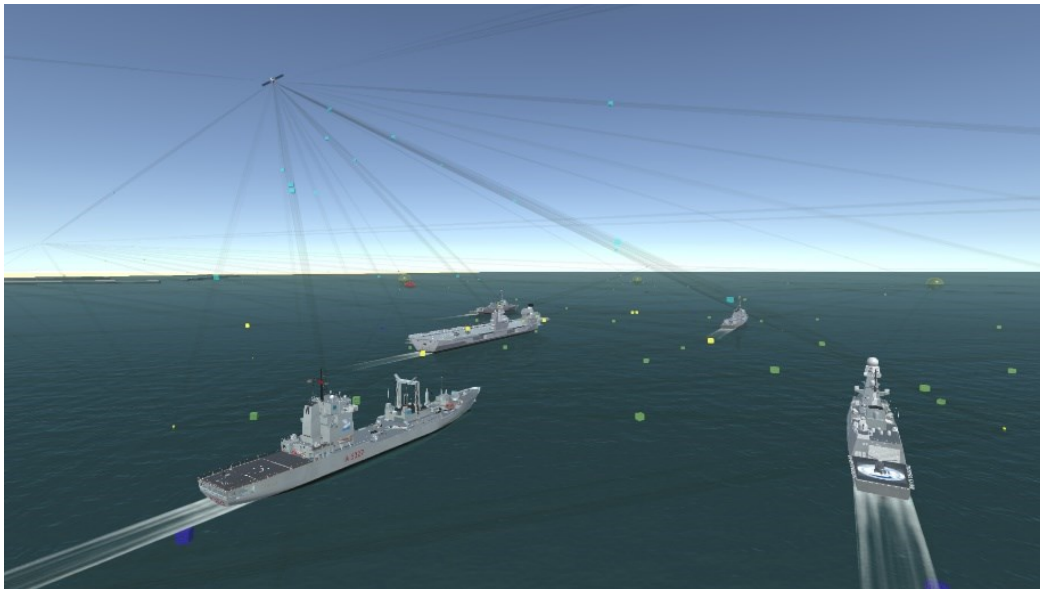


Figure 3.3: 3D representation of Communication Link

- **Cyber Elements:** these are the virtual representation in the cyber space of each asset that has an IP in the physical world. Each Elements have its indicator of his CIA triad (Confidentiality, integrity and availability).

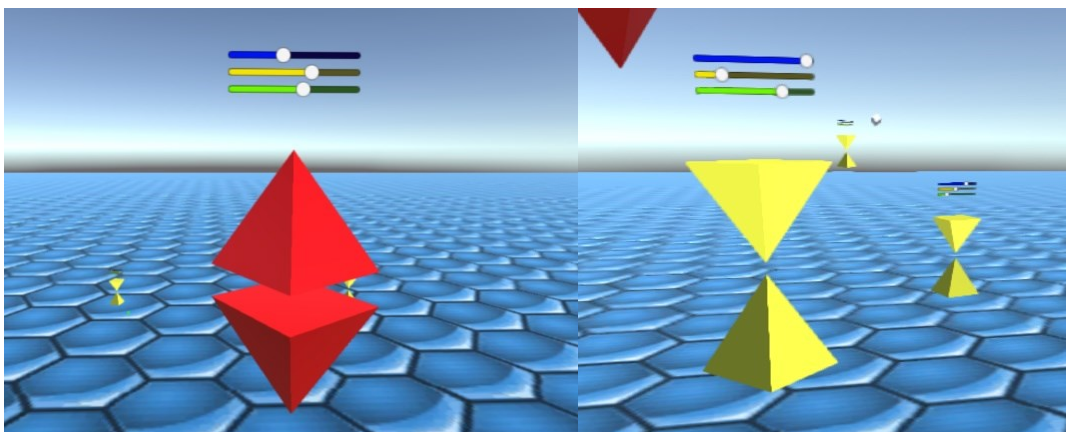


Figure 3. 4:3D Representation of IP Address in Cyber Space

- **Cyber Space:** schematic representation of the cyber space. Here are represented each IP address that is in the scenario and the exchange of data between them.

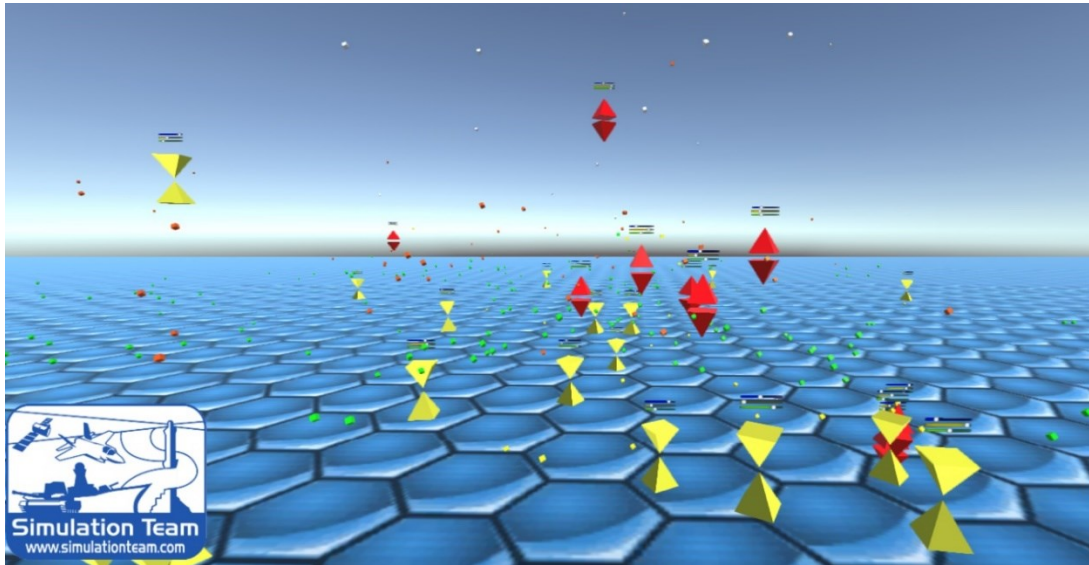


Figure 3.5:-3d Representation of Cyber Space

- **DDG:** it is a destroyer used by the US Navy.



Figure 3.6: 3D representation of DDG

- **Fishing Boat:** it is typical boat used for fishing.



Figure 3.7: 3d representation of Fishing Boat

- **FREMM:** it is a frigate used by the Italian and French navy. It is used for a variety of purposes including anti-air defence and anti-submarine missions.



Figure 3.8: 3D representation of FREMM

- **Global Hawk:** it is a remotely piloted aircraft like the Predator used by the US Air Force. The turbo-fan propulsion allows it to travel at a higher speed than the latter. It has a 36-hour battery life and is equipped with a high-resolution synthetic aperture radar and long-range infrared sensors. It can monitor almost 100,000 square kilometres a day.

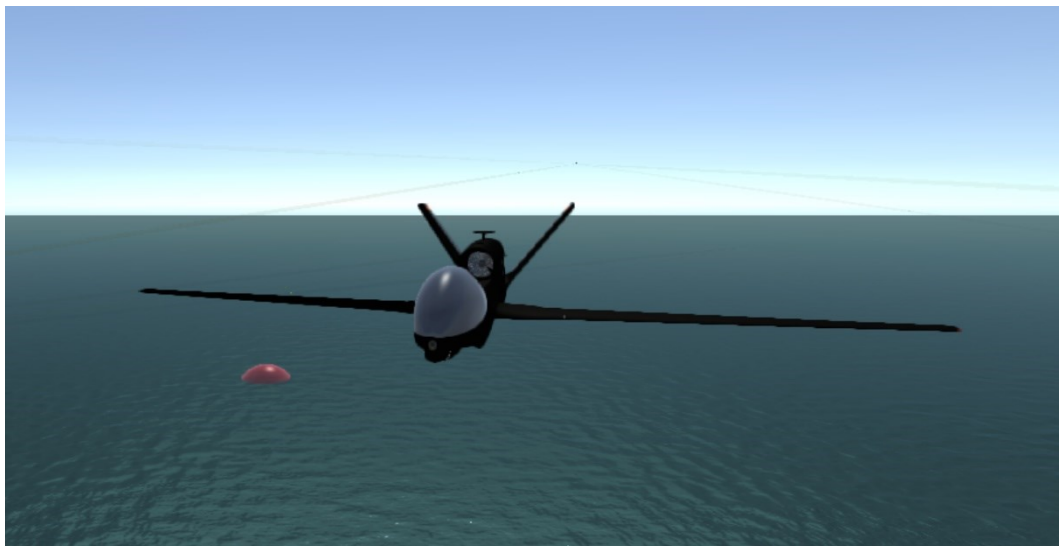


Figure 3.9: 3D representation of Global Hawk

- **IED:** they are Ordinary of Circumstance (Improvised Explosive Device). They have no peculiar shape and size due to their nature. They may have a variable explosive content and therefore it is very difficult to establish their power and range in a possible detonation. These are the devices that, in our simulation, are identified and reported by the AUV.

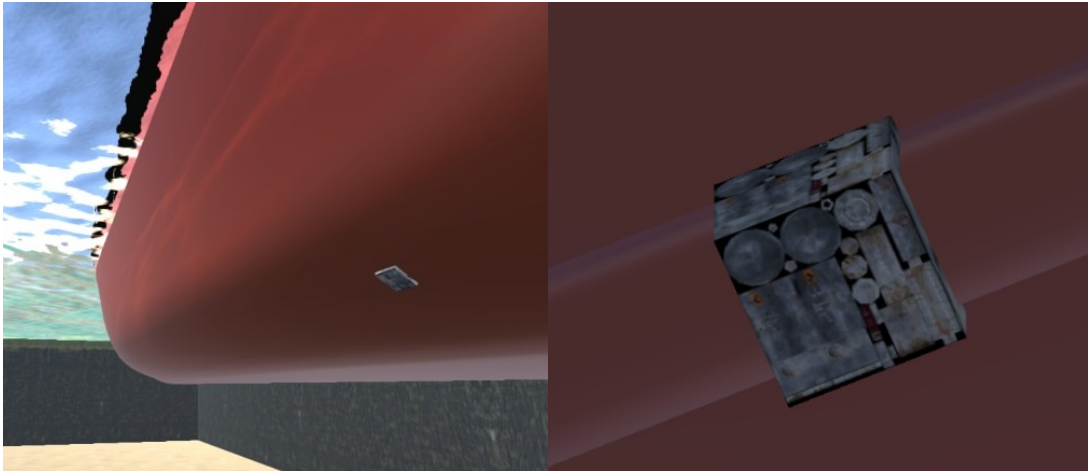


Figure 3.10: 3D representation of IED

- **KILO:** Diesel-electric submarine used by the Russian Navy.



Figure 3.11: 3D representation of a Kilo submarine

- **Offshore Tugboat:** a ship similar to a normal but larger tugboat, used to tow vessels in the open sea.



Figure 3.12: 3D representation of an Offshore Tugboat

- **Oil Platform:** in the virtual environment there is a semi-submersible offshore oil platform, intent in extracting oil from an underwater reservoir.

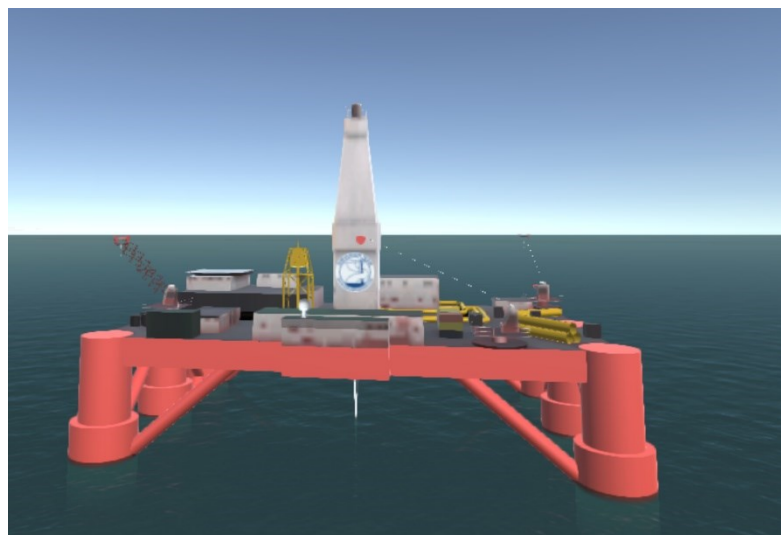


Figure 3.13: 3D representation of an Oil Platform

- **Patrol:** small military ship for coastal patrolling.



Figure 3.14: 3D representation of a Patrol

- **Pilot Ship:** in the port there are always present pilots ship used to pilot other boats in port or to carry the pilot on board those ships to command until their mooring.



Figure 3.15: 3D representation of a Pilot Ship

- **Port:** in the scenario there is a port composed of three piers plus another special act for the unloading/loading of tanker vessels. The port in the virtual environment is partly military and partly civil.

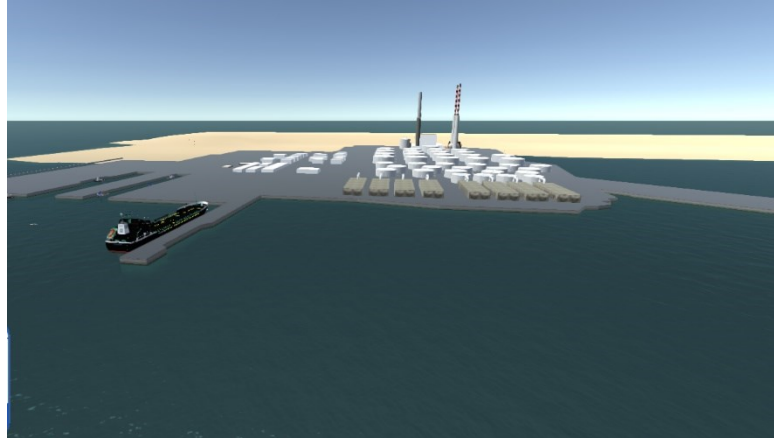


Figure 3.16: 3D representation of a Port

- **Predator:** it is a remotely piloted aircraft (RPA). It is equipped with wide-ranging cameras, infrared sensors and a synthetic aperture radar. It is used for reconnaissance and patrolling flights by many armed forces. In more modern versions it can be armed with two missiles. It is propelled to a pushing propeller.

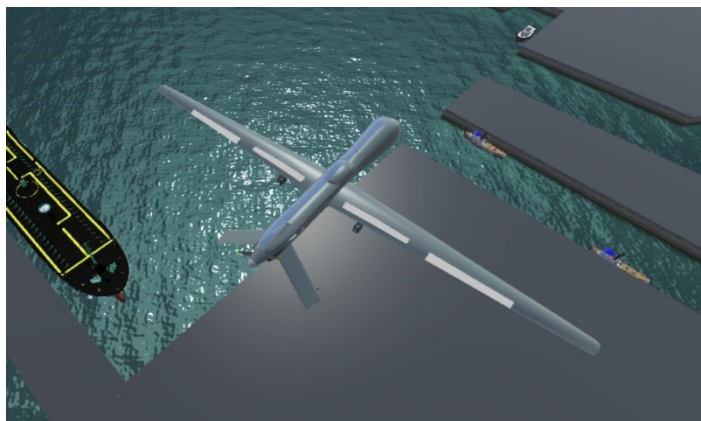


Figure 3.17: 3D representation of a Predator

- **Quadcopter:** air drone with four electrical propellers. Usually it is equipped with a camera but could have other sensors. It used for inspection in zone difficult to reach or for the surveillance of critical infrastructure. Still many experiments are carried out on it and on possible alternative uses.

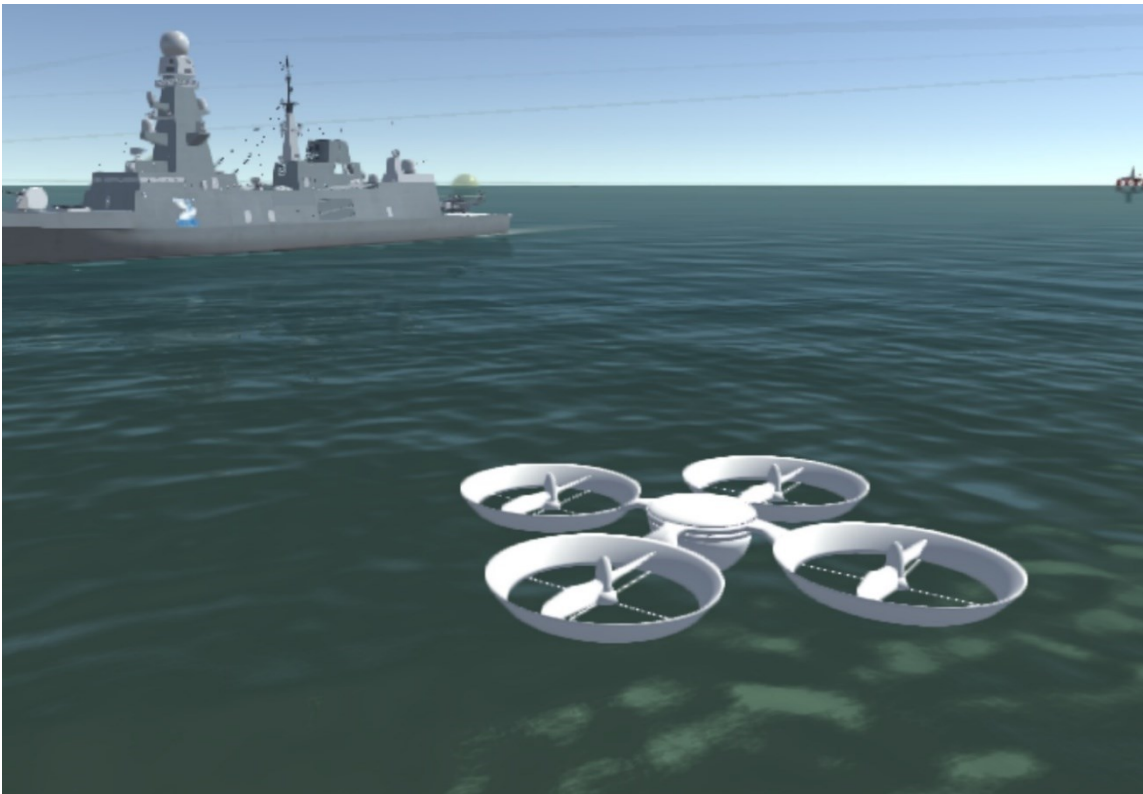


Figure 3.18: 3D Representation of Quadcopter

- **Satellite:** essential for communication and remote drone piloting, it was right to include a representation of it to better identify the route and the flow of transmissions between the various vehicles.

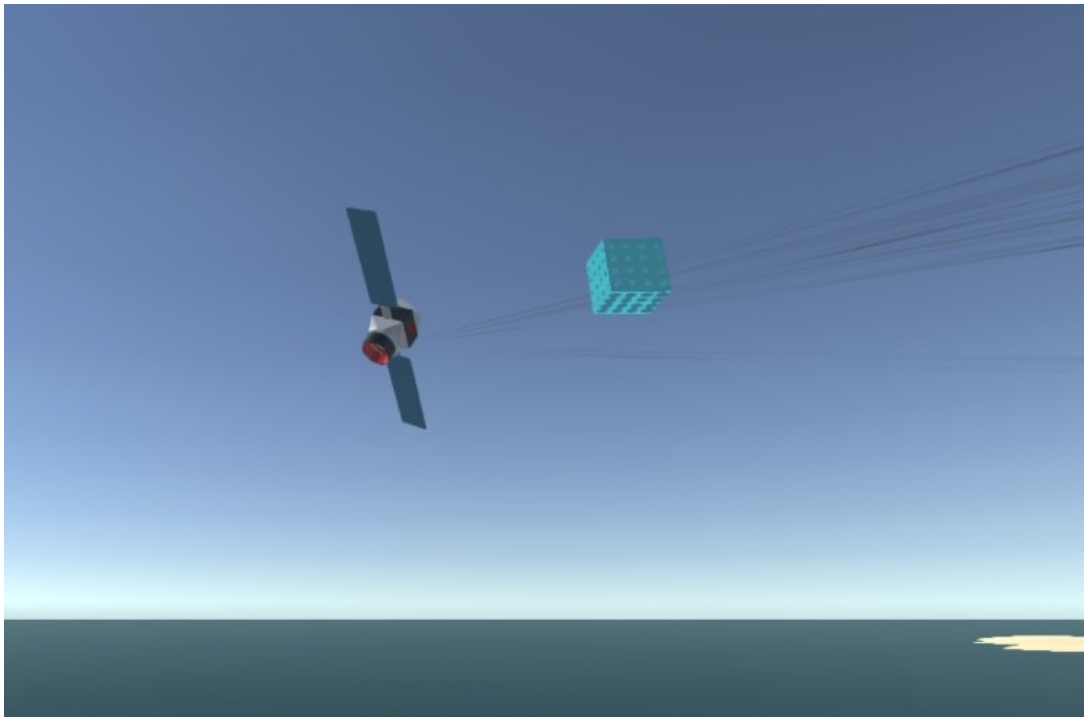


Figure 3.19: 3D representation of a Satellite

- **Sea Glider:** very advanced underwater drone. It is not equipped with propellers but moves using the currents and moving the position of its centre of gravity through a piston that longitudinally displaces a concentrated mass. The wings of the Glider behave similarly to those of an airplane generating lift in the direction of motion. This strategy makes it possible to considerably limit the use of electric power for propulsion, thus conferring an autonomy of about one month, which is enormously greater than helical propelled systems. At the moment it is being tested but it is thought to be used in all current uses of normal AUV but with more range of action.

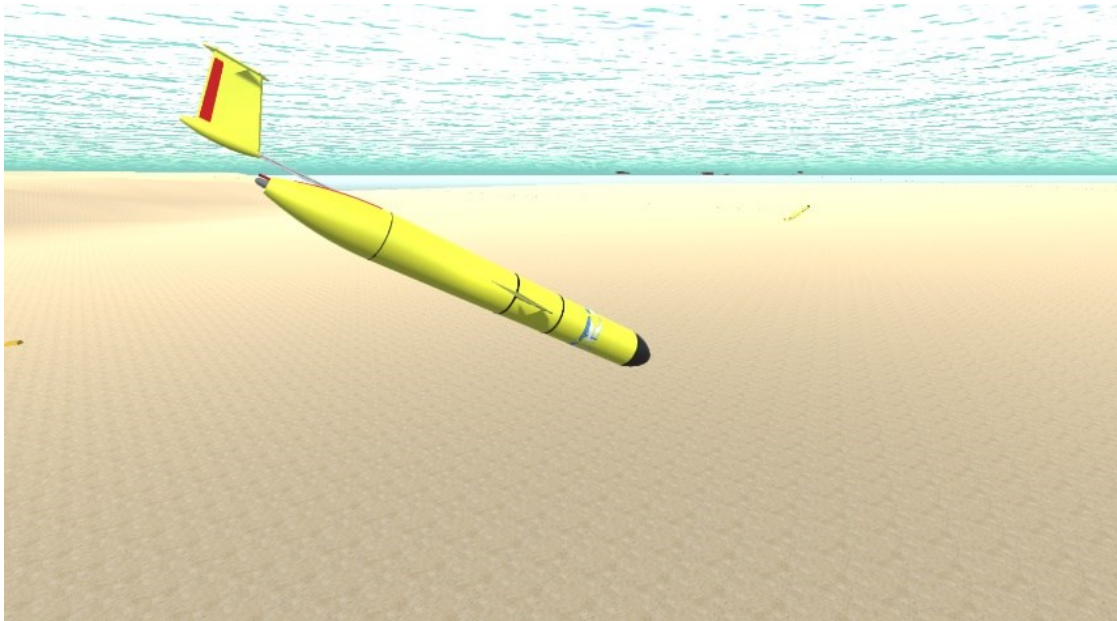


Figure 3.20: 3D representation of a Sea Glider

- **Sikorsky SH-60 Seahawk:** it is a multipurpose helicopter used by the US Navy. It is commonly boarded on aircraft carriers and frigates, very used in the marine environment.



Figure 3.21: 3D representation of an SH-60 Seahawk

- **SONOBUOY:** it is a special buoy equipped with sonar, used both in underwater monitoring to intercept possible threats such as submarines and hostile drones, and as a support and communication point for those allies. It is launched by a helicopter and once it reaches the water, a pentagonal structure, that constitutes the real sonar, is released, remaining afloat exploiting the floatation of the main body that contains devices for air communication. It is used in maritime operations both in the open sea and in the port area.

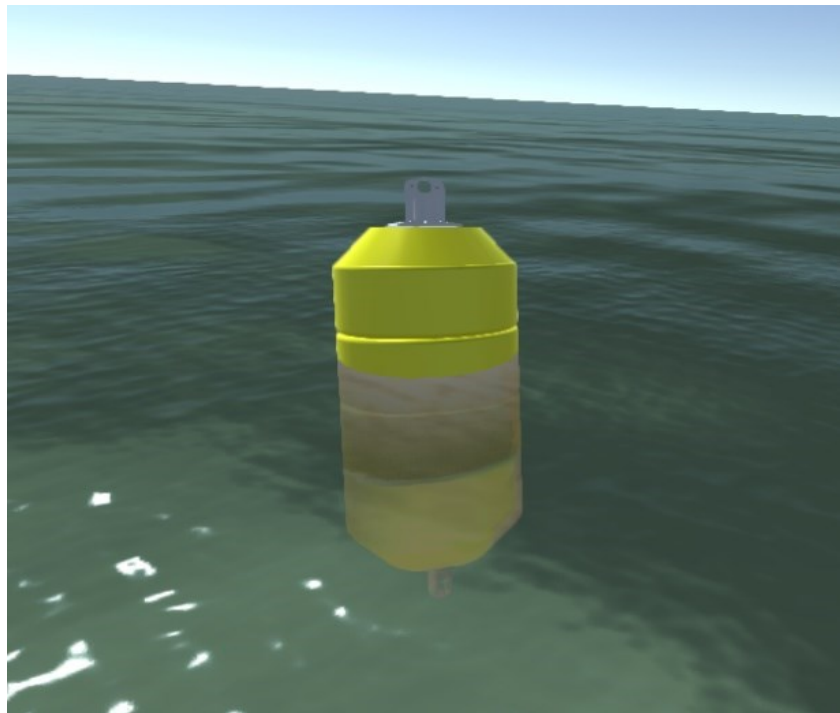


Figure 3. 22: 3D representation of a Sonobuoy

- **Sphere:** it is a semi-transparent colour sphere that is used to have a visual representation of the range of action of an IED.

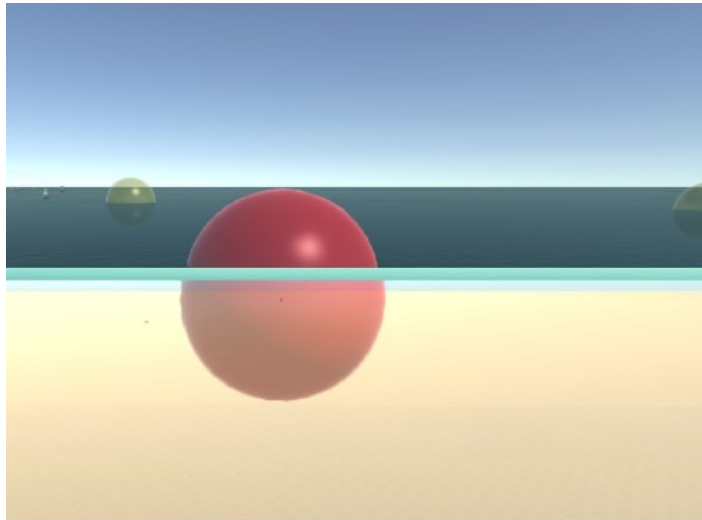


Figure 3.23: 3D representation of an Indicator Sphere

- **Supply ship:** the Italian supply ship Stromboli is reproduced. This ship has the aim to refuel the other vessels.



Figure 3.24: 3D Representation of Stromboli

- **Submarine Sensors:** they are sensors located on the seabed for the collection of oceanographic data. They are used in the prevention of seismic events but also to control the temperature, salinity, pollution and oxygenation of the water; they are also used as a network node for underwater communications or for the detection of possible threats.

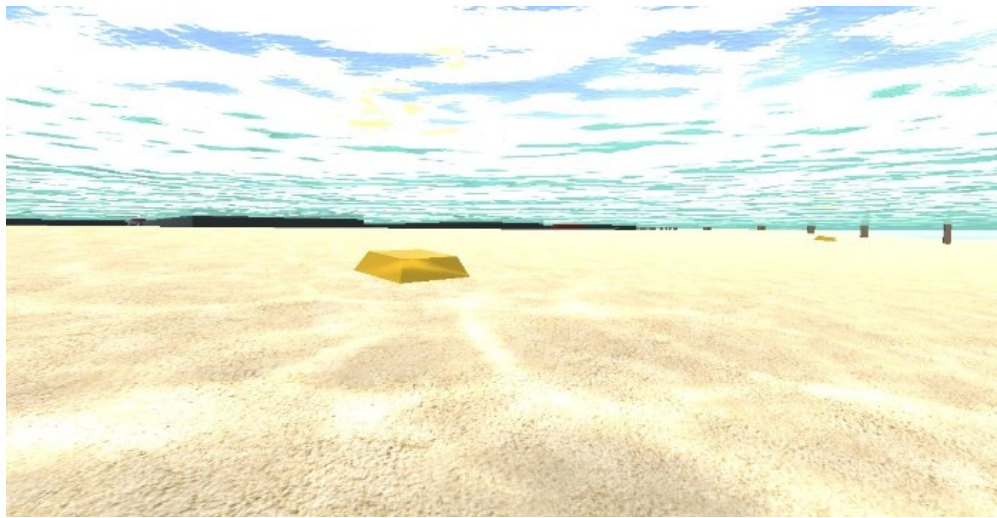


Figure 3. 25: 3D representation of a Submarine Sensor

- **Suimono:** it is the representation of the 3D sea. The model was purchased on the online store of Unity and then appropriately modified to meet the needs of the project. In this model the forces acting on the hull are not considered. The distribution of hydrostatic pressure is interpreted as a force acting at the centre of the vessel equal to the buoyancy of the volume of the immersed hull. This thrust is provided as an input parameter.

- **Tanker:** there is a VLCC (Very Large Crude Carrier) oil tanker stationary in port, intent on refuelling.



Figure 3.26: 3D representation of an Oil Tanker

- **TODARO:** Diesel-electric submarine of German design used by the Italian Navy.

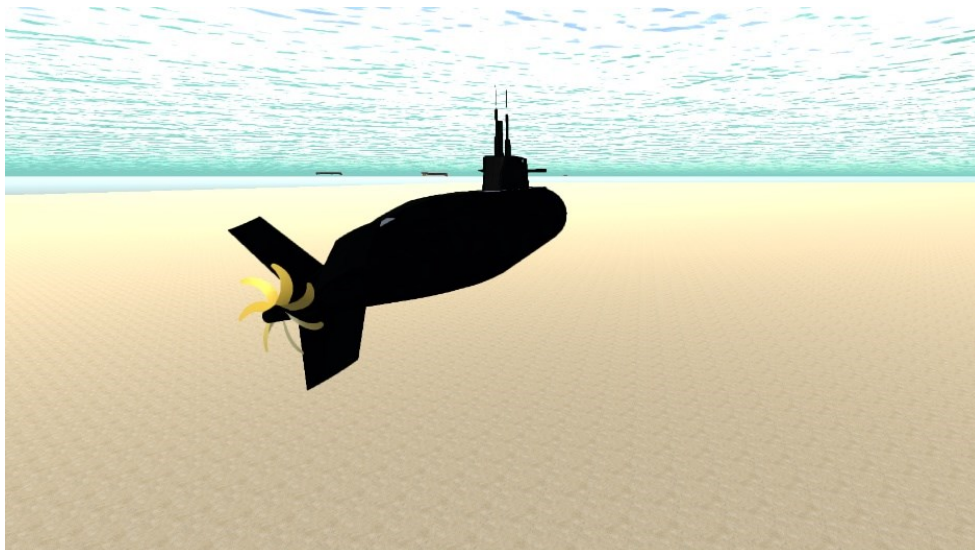


Figure 3.27: 3D representation of TODARO

- **Tugboat:** vessel with the task of towing larger ships entering and leaving the port or service for any damaged craft.



Figure 3.28: 3D representation of Tugboat

- **UGV:** it is a ground drone equipped with a series of sensors and cameras used for patrolling.



Figure 3.29: 3D representation of UGV

- **USV:** it is an unmanned surface vehicle. It is used for patrolling marine areas and for communicating with underwater drones.

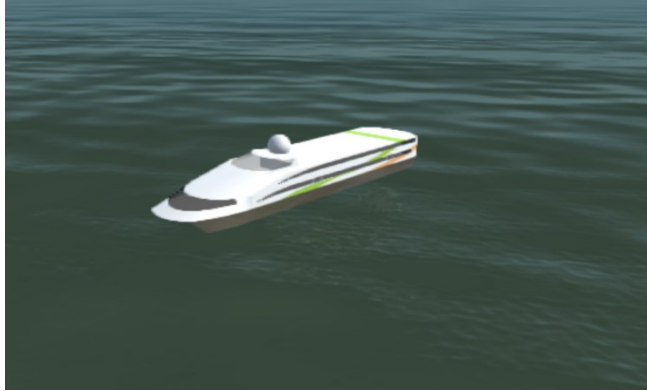


Figure 3.30: 3D representation of USV

- **Various Indicators:** these are imaginary three-dimensional geometric shapes that are used to indicate various things, such as the position on the surface of the underwater drones or the destination of an autonomous drone, the machine telegraph of the surface units and the position of the bar.

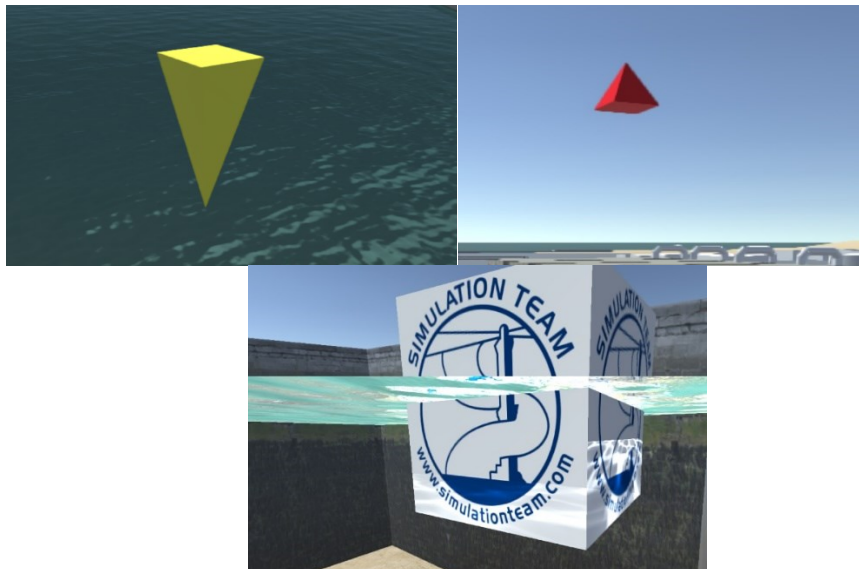


Figure 3.31: 3D representation of Various Indicators

X-47: it is a turbo-fan unmanned combat aircraft. It is used as a demonstrator and currently has never been used in any real combat.

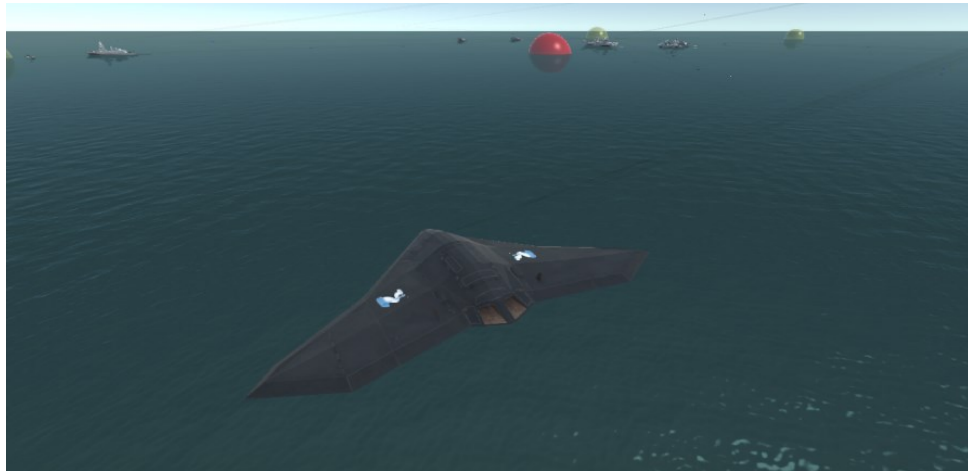


Figure 3. 32: 3D representation of X-47

- **YASEN:** Russian nuclear missile submarine. It can carry up to 24 units between missiles and torpedoes and has 8 torpedo tubes.



Figure 3. 33: 3D representation of YASEN

As can be seen from this classification, the simulator is rich in models and includes all types of vehicles currently existing, in order to provide an overall view of a marine landscape in all its aspects and be able to thoroughly investigate possible solutions to the problems that existed up to now.

3.2 Scenarios

The environment is divided into four different scenarios, designed to investigate the use of drones in possible safety procedures for critical infrastructures and for their possible use for defensive purposes.

It's possible to pass from a scenario to another switching between the camera that are in the 3D environment. Below are reported all the cameras present in JESSI

- Free Camera: it is free to move in the environment without constraints and therefore also underwater where the undersea vision is simulated. This, if you do not want, you can safely disable using keyboard commands
- AUV: camera external to the underwater drone that follows its movements. Located slightly further back and higher than it is, the AUV is centred in the frame. You can change the angle of view by moving the mouse, so you can see the surrounding environment. With this camera you can monitor the behaviour of the drone more closely to see its behaviour during patrolling.
- AUV Hostile: it is a camera like the previous one but attached to an enemy AUV.
- Predator: camera that follows the movements of the Predator and behaves similarly to the AUV Camera.
- FREMM: the camera which is integral with the frigate, is placed outside the ship and moved further behind it to have the vessel centred in the objective. You can change the angle of this camera so that you can also observe the surrounding environment.

- DDG Bridge: the camera is integral with the ship and reproduces the point of view of the commander.
- Todaro: the camera is positioned outside and behind the submarine so as to have the vehicle in the centre of the frame.
- Global Hawk: the camera is placed above the drone and follows its movements.
- Aircraft carrier: the camera attached to the ship is placed externally, in a raised and backward position, so as to have the vision of the whole ship centred in the screen. You have the possibility to change the angle of the frame, so you can observe the surrounding environment.
- DDG 1: integral to the ship, the same statements made for the camera of the carrier are valid.
- DDG 2: identical to the previous one but centred on the second DDG present in the scenario.
- FREMM 1: this has the same characteristics as the previous four.
- FREMM 2: equivalent to the previous one but centred on the second FREMM in the fleet.
- Stromboli: identical to the previous one but centred on supply ship.
- Global Hawk: the camera is placed above the drone and follows its movements.
- Missile: the camera is in solidarity with one of the missiles that are launched. It is located outside of it, in a raised and backward position. The camera is active only after the launch and there is one for each missile.

- Submarine Hostile: the camera frames the enemy submarine and follows its movements.
- Helicopter: the camera is placed above the helicopter and follows its movements.
- X-47 Drone: the camera is placed above the drone and follows its movements
- Satellite: the camera is placed above the satellite
- Buoy Camera: the camera is placed above the buoy

Below there are the descriptions of the various scenarios and their purposes and possible uses.

3.2.1 Port Scenario: Port Protection

In this scenario there is a port including four piers: two civilians, one military and the fourth act for the unloading and loading of tanker vessels. In the docks, there are moored several ships, both civil and military, and an oil tanker being unloaded. On the ground there are several buildings and a fuel depot to represent a critical security infrastructure. A UGV is in charge of patrolling the ground and a Predator flies over the area to identify possible threats to the safety of the plant and the military base.

As for the sea, an AUV MUSCLE patrols the coast under the sea surface, looking for possible IEDs hidden by a terrorist cell, while a USV follows him at a distance to receive the signals transmitted by the patrol boat.

Randomly, an IED is generated that the AUV must find to complete its mission. The MUSCLE has a predetermined path along which it scours the bottom, the coast and the

bottom of the ships in search of possible suspicious objects. When it is close to a suspicious object and identifies it as such, the drone autonomously decreases its speed and changes the route to be flown in order to investigate the alleged threat. If the latter is real, it communicates it to the USD and signals the area of action of a possible detonation. The surface vehicle, in turn, received the communication by sound waves from the AUV, immediately sends the alert via radio waves to the satellite that rebounds it to the competent authorities. Once the threat is detected and reported, the AUV takes the route to follow and continues to search for other possible threats.

By changing the AUV patrol route, you can check the find of the IED and how long it takes to complete a fly over. In this way, you can find the best route to follow to monitor the area and check if the times used are compatible with the autonomy of a single AUV. Otherwise, it is possible to evaluate the occurrence of using more than one drone, dividing the patrolling zones to monitor the entire port. The alternative to using an AUV for this task, however, remains only the man, but it is considerably slower and more expensive. So, the use of drones in this field would increase security and decrease costs.

The scenario described was created to verify the feasibility of this strategy, to test it, analyse the behaviour and performances of the various drones and highlight the problems that can be found.

3.2.2 Oil Platform Monitoring

In this scenario there is a semi-submersible oil platform operating in the open sea. To prevent any terrorist attacks, two AUVs patrol the area surrounding this infrastructure following a

predetermined route, while a third AUV follows a dynamically generated route through the control logic implemented in the code, predisposed to generate the optimal routes for patrolling. In the area there is also a FREMM that can be driven from the keyboard or from a dashboard simulator.

If the AUV is about to reach the limit of its autonomy or if the frigate sends a signal to the drone when it is close enough to be able to receive it, the automated vehicle begins the boarding operation to the ship to perform a shelter. The AUV changes its route to reach the stern area of the FREMM where there is equipment to retrieve it from the sea. The logic of the drone foresees that the manoeuvre for the shelter is constantly updated in order to avoid collision with the FREMM in case the ship cuts the route of the drone. Once the ship is reached, the drone is recovered and taken on board where the batteries are recharged. At this point, by means of a keypad command, the pilot of the ship may decide to put the drone back into the sea, making it return to the previously interrupted course. For greater clarity, it is possible to display in the virtual scenario of the AUV signals to indicate their position, on the destination points of the planned route in order to know the future route.

Changing the logic of the route generation from the AUV, in this scenario, one can understand and study, how to make the drones to be used in patrolling dynamic and autonomous. Furthermore, comparisons can be made between the dynamically self-generated routes and the pre-set ones, in order to investigate which are the most effective according to the logic used.

This scenario was also realized to study the drone recovery manoeuvres at sea, and to search for new and faster ones in the future.

3.2.3 **Glider Fleet**

In this scenario is reproduced a patrol operation of the sea floor conducted by a fleet of Glider, escorted by two ships and a submarine. The boats in question are the Air carrier Queen Elysabeth, a DDG and a small class Todaro cruise submarine. The number of underwater drones is variable (up to 100 units) and is selected before starting the simulation. On the seabed there are underwater sensors to analyse water (temperature, pollution, salinity, oxygenation and seismic activity) that can be exploited as a communication node. A Global Hawk, flying over the fleet in a circular trajectory, ensures security over airspace, while a satellite handles long-range communications.

The Gliders perform more tasks: they patrol the seabed in search of possible hostile vehicles, mines or IEDs to damage ships and underwater pipelines; during this operation, they collect data about sea conditions.

Every three or four rounds of climb and dive, the Gliders reach the surface of the sea to communicate their position and the data collected.

Since all types of media and communications are present, this scenario is used to understand the complexity of a maritime operation and the difficulty in managing the communication network. By changing the logic of generating Glider routes, it is also possible to test and study all the various patrol strategies to be able to understand which are the most convenient and useful in such a scenario.

3.2.4 **Military defence from a missile attack**

In this scenario is represented a military fleet, consisting of an aircraft carrier, two FREMM, two DDG and a Todaro, that is found targeted by a missile attack by an enemy submarine located a great distance from it. The fleet enjoys the help of several drones: a dozen divers between Glider, AUV and a Global Hawk.

The fleet is at sea during a reconnaissance mission and is sighted by an enemy submarine. The latter, after determining the position of the ships, launches a battery of supersonic missiles with the intent to sink as many ships as possible. Once these missiles are close to the target, communicating with each other, they assign themselves to the various targets.

The objective of the fleet is to be able to identify the attack in time to activate countermeasures and reduce/cancel damage to the fleet under attack. The use of drones can be fundamental in identifying this danger.

This scenario was created to investigate if in the event of enemy attacks, the use of drones could be useful and if it were, what are the best strategies to use.

3.2.5 **AUV Fleet**

Similar to the Glider Fleet Scenario is reproduced a patrol operation of the sea floor conducted by a fleet of Glider and one of AUV, escorted by six ships and a submarine. The boats in question are the Air carrier Queen Elisabeth, two DDG, two FREMM, a supply ship and a small class Todaro cruise submarine. The number of underwater drones is variable (up to 100 units) and is selected before starting the simulation. In the sea there are enemy AUV that are trying to spy the fleet.

The Gliders and AUV patrol the scenario searching the enemy drones. If they detect them informed the fleet of their presence.

Since all types of media and communications are present, also this scenario is used to understand the complexity of a maritime operation and the difficulty in managing the communication network. By changing the logic of generating Glider and AUV routes, it is also possible to test and study all the various patrol strategies to be able to understand which are the most convenient and useful in such a scenario.

3.3 Sea Glider

In the simulator proposed in this paper, there is a fleet of Glider, managed by an artificial intelligence and therefore not controlled by the user, which performs the task of sampling the marine environment. This in order to collect data aimed at deepening the propagation of sound in water according to the state variables such as density, salinity, etc. In addition, the sampling of the data is aimed at analysing the state of sea health to monitor the production of off-shore facilities while they patrol the surrounding areas in search of possible threats.

The computer implementation of the behaviour model of the Glider drones, made in JESSI, is described below. This model is a cinematic type, because this solution has a high versatility and it is the first step towards the definition of the dynamic model more coherent with reality. This model was developed and successfully tested in Unity 3D.

The programming language used is C # chosen for its affinity with the JAVA language and compatible with the development platform.

The code reproduces n-clones of an existing object (called 'father') and, calculating for each of them the positions in each instant, gives them realistic movements. In this way, with a single script executed, it is possible to simulate all the 'children' objects independently but subject to the same behavioural laws. This translates into a lightening of the computational load required by the simulator. Furthermore, with this cloning technique, it is easier to vary the number of drones to be recreated in the scenario to investigate the best strategy of use of these autonomous vehicles.

The script calculates all the 6 degrees of freedom of the objects, i.e. 3 translations (along the x, y and z axes), and 3 rotations (around the x, y and z axes). The three rotations are called with the respective naval terms Roll, Pitch and Yaw. These are all applied in the centre of gravity (G) of the model.

As already mentioned, the Sea Gliders are a 'special' type of underwater drones, which do not have a propulsion system but, to move, they exploit the force of gravity, the thrust of Archimedes and the movements of marine currents. For this reason, their motion is not straight in the vertical plane, but it is a succession of climbs and dives at pre-established odds. The horizontal motion is generated by the lift developed by the wings placed at the sides of the drone when it moves vertically.

Climbs and dives are made when the drone's centre of gravity reaches certain depths that are calculated specifically to avoid the impact of the vehicle with the seabed and to prevent it from leaving the free surface of the water. These depths are calculated as a function of the forward speed and the attitude angle of the vehicle, considering a conservative circular trajectory and using appropriate safety factors.

The glider interrupts its rotation along the y axis when the pre-set attitude angle is reached. The time derivative depending on the pitch angle (angular acceleration) is given as input parameter of the modelled system.

By way of example, the calculations carried out to obtain the safety distance 'd' in which to start the climb or the dive are shown:

$$R = v / \omega_2 * 180 / \pi$$

Where:

R = Bending radius [m]

v = Speed of model progress [m / s]

ω_2 = angular velocity y-axis [deg / sec]

$$d = k_1 * R * \left(k_2 - \cos \left(\left| \frac{a_2}{180} * \pi \right| \right) \right) + k_3$$

Where:

d = safety distance where to start the climb or the dive [m]

R = Curve radius previously calculated [m]

a_2 = pitch angle of the model [deg]

k_1, k_2, k_3 = safety factors

At present, the progress speed is the parameter that governs the simulation and it is influenced by the vertical motion of the vehicle which in turn depends on the pitch angle. It follows that the speed is minimal when the drone is close to being horizontal and maximum when it reaches the attitude angle.

At the development platform, the script can provide both speeds and positions, depending on whether you want to give more or less control to your physical engine. At the moment it is preferred to leave the total monitoring to the programmer through code, passing to the software only positions; furthermore, we are thinking of using Unity's physical engine by

passing the forces directly on it, because it guarantees a more practical management of collisions between the various objects.

If you choose to provide the development platform with the speed, the script also calculates the positions and uses them to control both the correct functioning of the Unity physical engine and the calculation of the variables to be used within the architecture.

Gliders move aiming at checkpoints generated and destroyed from time to time. The pointing logic follows certain rules that will be explained below.

First of all, the yaw angle must be obtained on the horizontal plane (a_t) which must be covered so that it goes in the direction of the target:

$$a_t = a_1 - a_n$$

Where:

a_1 = angle between the North and the direction of progress.

a_n = angle between the North and the vector pointing to the target.

Through appropriate constraints, if the module of the angle a_t is greater than 180 degrees, its complement is chosen, so as to make the vehicle always turn from the side where the angle (between the direction of advancement and the vector oriented towards the check point) is less.

Once determined a_t as the most convenient turning angle, the vehicle undergoes an angular acceleration on the y-axis which represents the lift generated by the rudder blade.

The angle a_s in which to start to decrease the angular velocity with a contrary acceleration, in order to stop the drone on the route that leads to the target, is calculated as follows:

$$a_s = \left| \frac{\omega_1^2}{\dot{\omega}_1} \right| * k_1$$

Where:

ω_1 = rotational speed along the y-axis.

$\dot{\omega}_1$ = angular acceleration of the y-axis.

k_1 = safety factor

The target is considered as reached when the vehicle reaches a certain distance from it in the horizontal plane: after this, the check point is cancelled, and another is created in a different position, that can be random or determined by the developer depending on how you want.

The model also introduced the influence on the motion of the drones of marine currents. This has been implemented as an additional component to the speed of the body in water, under the hypothesis that a body immersed in a fluid in motion is dragged by it.

Moreover, in the behavioural model of underwater vehicles a rolling motion has been introduced when they turn so as to realistically reproduce the movement carried out.

In the case that the velocities of the simulated objects are supplied directly to the Unity's physical engine, instead of the positions, the collisions are detected, and the interpenetration

of the models is avoided. This setting is still rough, and the effect obtained is the blocking of vehicles in the position in which they are located, if they impact against other objects. This is due to the fact that the implemented behavioural model is kinetic and not yet dynamic. In fact, in this way, despite being the most practical and versatile architecture, it is difficult in Unity to detect the masses, the inertias, the accelerations and the speed of the elements with which it impacts without making the simulation too heavy. With the lack of these data, therefore, it is not possible to calculate the impact forces acting on the subjects of the collision and therefore reproduce a realistic behaviour.

For the same reasons, it has not yet been possible to implement a sophisticated model that allows simulated vehicles to avoid the moving obstacles they might encounter along their journey. In fact, if the speed and the accelerations of the other objects are not known, it is impossible to predict the positions that they will have in the immediate future.

Currently, therefore, a function is implemented that controls only if, up to a certain distance along its own trajectory, another entity is encountered. If this is the case, the vehicle changes its forward direction until it no longer detects the obstacle in front of it. After a suitable period of time, the model begins the manoeuvre, to return to follow its own route before the deviation and iteratively performs the verification of the presence of any obstacles. If this happened, it would repeat the previous calculations, vice versa would continue on the route calculated before the interaction with the obstacle.

The behavioural models of vehicles, other than Sea Gliders, have a logic quite similar to that described in this chapter, differentiating only in some aspects. For example, if we consider

the AUV, the control logic is similar to that of the Sea Gliders with the only difference that its motion is straight in vertical plan.

Currently we are working to recreate a dynamic behavioural model in order to reproduce the movements of simulated vehicles even more realistically and to be able to implement sophisticated models to manage collisions and / or avoid obstacles.

3.4 Validation and validation

The VV & A (Verification, Validation and Accreditation) is a fundamental phase in the development of simulators and follows the whole process from the definition of the objectives to the statistical analysis of the results of the models.

In our case, we work closely with SME (Subject Matter Experts) interacting with experts on different issues (e.g. anti-terrorism, autonomous systems and explosives experts) during the development of simulators and in order to define what aspects to go to act. Informal and static analyses were carried out during the first phases, helped by the virtual nature of the simulators, which allowed to complete a face validation on some aspects. The simulator has been integrated with other models allowing to conduct evaluations through the application of ANOVA techniques (Analysis of Variance) and Design of Experiments to verify the consistency of the data obtained. Some examples of the curves obtained in the verification of the experimental error convergence process have been attached, highlighting the convergence of the results with respect to objective functions linked to the reduction of the vulnerability of critical infrastructures with the introduction of autonomous systems.

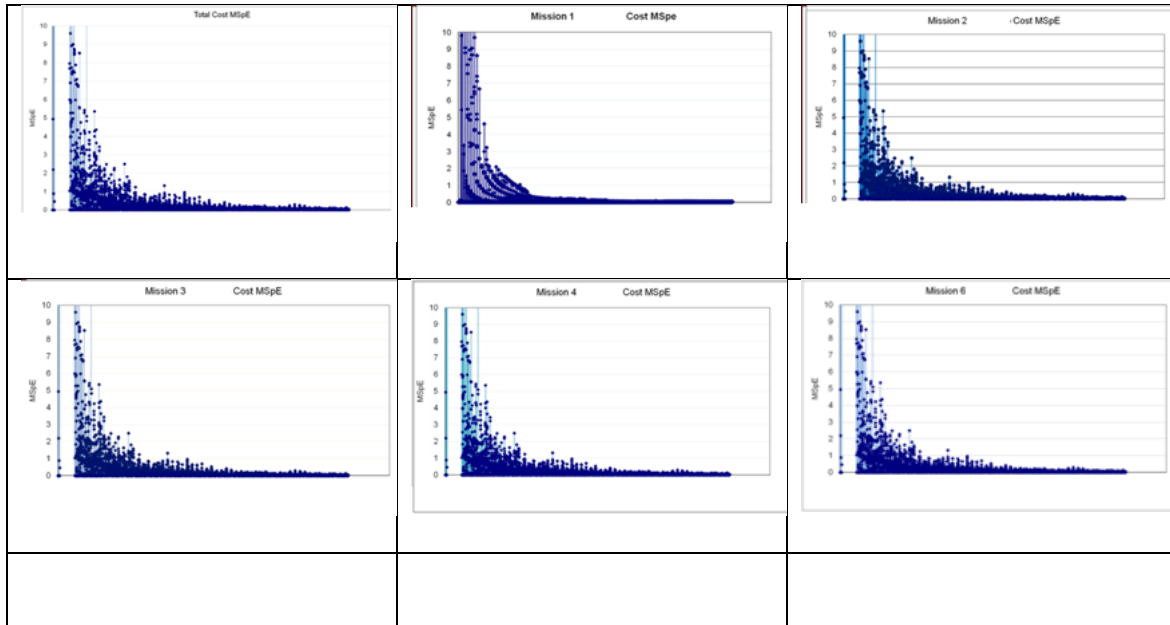


Figure 3.34: Graphs obtained from VV & A (obscured specifically for reasons of confidentiality)

Currently, tests are underway to verify the computational efficiency of the models when integrated within HLA federations and scientific publications have been made to which I actively collaborated (Bruzzone et al. 2015).

4 Other Experiences

During the research study, the author participated to several and different projects. These experiences allowed to acquire the knowledge, skills and competences needed to the development of the simulation environment subject of this thesis. The most important projects are listed below.

4.1 SEE

The Simulation Exploration Experience (SEE) event, organized every year starting in 2011 by the SISO (Simulation Interoperability Standards Organization) and other leading companies in the field of Simulation and Modelling under the coordination of NASA (National Aeronautics and Space Administration). Initially with the name of Smackdown, SEE is the project of a federation of operations simulators of a possible lunar base. The event, attended by many universities of different nationalities, is held every year in a different location of the USA and Europe, i.e. this year took place in Sofia, last year in Cape Canaveral (Florida). The objectives of this event are to familiarize students or graduates with the HLA Standard, and to provide university teams from all over the world with the opportunity to work in an international context. For this reason, the development of simulators is more focused on the interaction between the various federates than on 3D or advanced physics. Indeed, the graphic representation is entrusted to a single federated called

DON (Distributed Observer Network) to which the other simulators communicate the objects they publish and their spatial coordinates (including rotations). The University of Genoa has been participating in the event since 2012, with different projects.

The NASA Team creates the scenario composed mainly of the Sun, the Earth, the Moon and Mars; in this environment there are more reference systems and the objects published by the federates, must necessarily refer to one of the. Reference system means a set of orthogonal axes that can be used as basis for the identification of the position and the orientation in the space of the various objects and vectors. Communicating and interacting with objects that refer to different reference systems, is one of the major problems for the federates due to the complexity of the rototranslations that the different coordinate systems have among them. A list and brief explanation of the different reference systems are reported in the following:

- Inertial Barycentre of the Solar System (SolarSystemBarycentricInertial): it is the origin of the environment recreated, it is therefore the absolute zero and it has no movements or rotations.
- Centre of the Inertial Sun (SunCentricInertial): it is the position of the Sun in relation to the Inertial Barycentre of the Solar System.
- Earth-Moon Inertial Barycentre (EarthMoonBarycentricInertial): it is positioned in the Earth-Moon barycentre and is expressed in relation to the Inertial Barycentre of the Solar System.

- Rotating Earth-Moon Barycentre (EarthMoonBarycentricRotating): this reference system is placed at the same point as the previous one, but it is non-inertial, it rotates with the Earth-Moon system and is expressed in relation to it.
- Inertial Earth Centre (EarthCentricInertial): it is positioned at the centre of the Earth and it is expressed in relation to the Earth-Moon Inertial Barycentre.
- Centre of the Earth Fixed (EarthCentricFixed): expressed in relation to the previous reference system, it is positioned in its same position but rotates with the terrestrial rotation and it is non-inertial.
- Centre of the Inertial Moon (MoonCentricInertial): it is positioned at the centre of the Moon and it is expressed in relation to the Earth-Moon Inertial Barycentre.
- Centre of the Moon Fixed (MoonCentricFixed): expressed in relation to the previous reference system, it is positioned in its same position but rotates with the lunar rotation and it is non-inertial.
- L2 Rotating Earth-Moon (EarthMoonL2Rotating): this reference is non-inertial and positioned at the L2 Lagrangian point of the Earth-Moon system, rotates with it and it is expressed in relation to the Earth-Moon Inertial Barycentre.
- Inertial Mars Centre (MarsCentricInertial): it is positioned in the centre of Mars and it is expressed in relation to the Inertial Barycentre of the Solar System.
- Centre of Mars Fixed (MarsCentricFixed): expressed in relation to the previous reference system, it is positioned in its same position but rotates with the rotation of Mars and it is non-inertial.

- Base Aitken (AitkenBasin): it is positioned on the Lunar surface where the base is located and is expressed in relation to the Centre of the Fixed Moon. (Figure 4.1)
(SEE 2014)

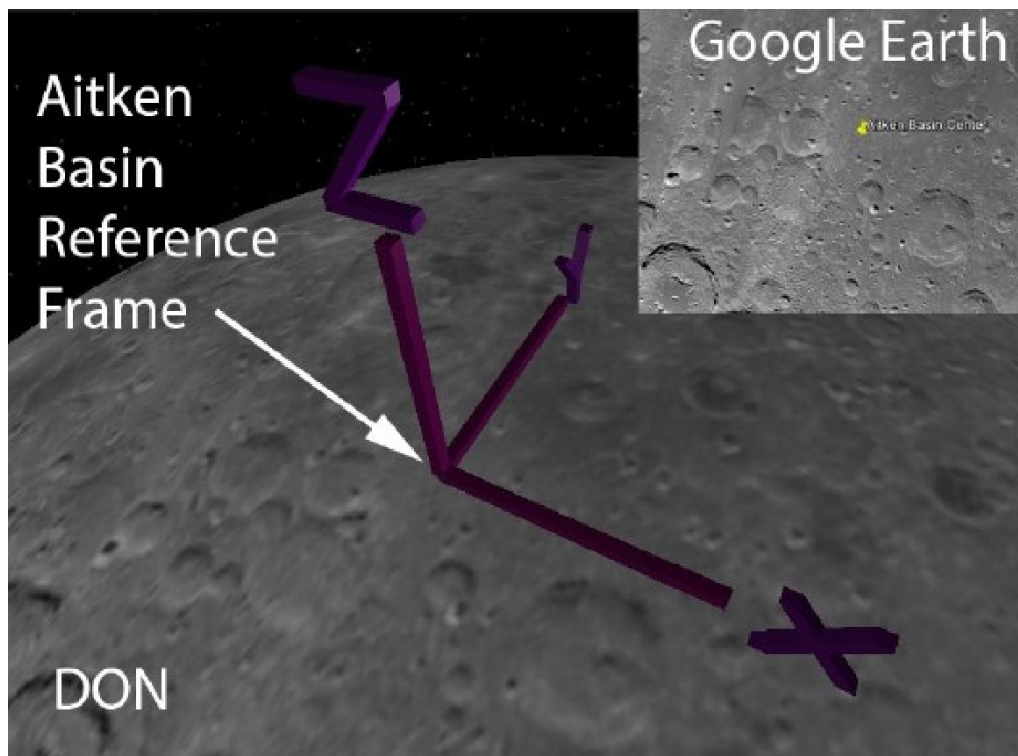


Figure 4.1: Aitken Basin reference system

A schematic representation of the reference systems structure is reported in following Figure 4.2.

The orientation of objects in space is given through a special vector of four elements: the Quaternion. The latter, like the coordinates, it must necessarily be given in relation to a precise reference system. This vector is widely used in 3D graphics and representation

programs because it is very easy to use and allows only four numbers to represent any rotation in space.

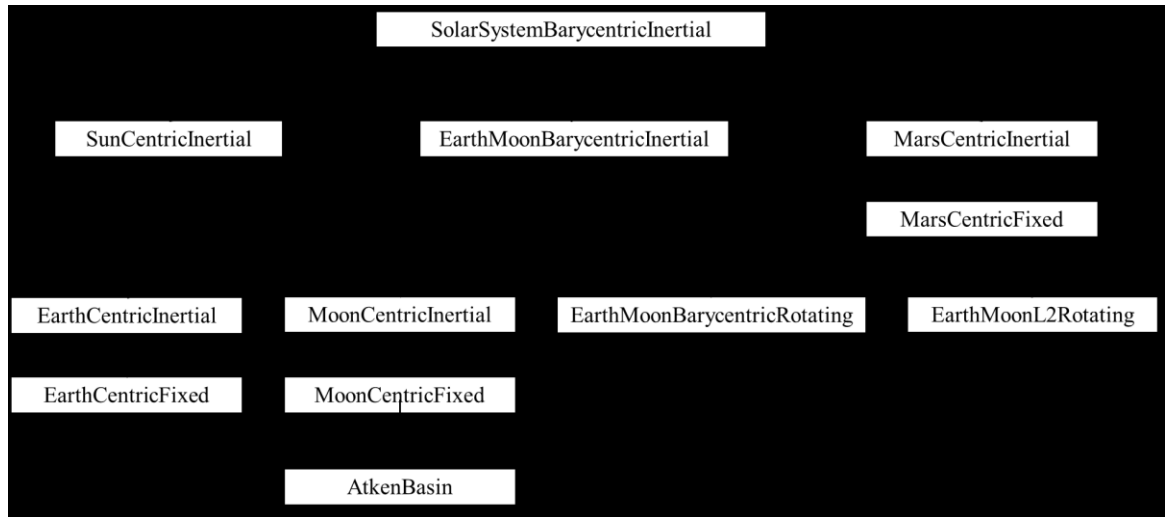


Figure 4.2: schematic representation of the reference systems

The objects published by the various federates can be fixed or moving and can change the reference system during the simulation, amplifying the problem mentioned above. Most of the objects published by the federates use the reference system of the Aitken Basin of which the vector of the translations and the quaternion of the rotations are known.

Table 4. 1: Vector translation and quaternion rotation of the base reference system Aitken

	x	y	z	w
Translation	-817582.93	-296194.93	-1504977.52	
Rotation	-0.79	0.55	0.14	0.21

Despite this there are also objects referred to the other reference system.

The federates have the task to publish the objects that they manage and to get them to carry out the tasks they have designate. These entities can be vehicles and space bases, satellites, astronauts and even asteroids from the open space in order to reproduce possible realistic critical situations. Since one of the goals is to become familiar with HLA standards, it is highly recommended that objects published by different federates interact with each other in such a way that they perform functions together or actions as a result of events created by another federate.

In order for the federates to interact appropriately with each other, managing time is a key element. The NASA Team has decided that the federates must be "Time constrained" and "Time Regulating", which means that all the federates follow the time of the federation and until it gives them the command to go to the next frame they stop and wait. This ensures that all the federates are synchronized with each other and that, given that the federation is set to real-time, one second of the simulation corresponds to a real second. In addition to this, all the federates produce output data identified by the HLA time, useful for reconstructing the sequence of events that occurred during the simulation and any repercussions on the other federates. The time is represented by a `HLAinteger64BE` (a 64-bit big endian integer) that measures the microseconds from the creation of the federation; this means that one second in the simulation corresponds to the value 1.000.000 of the time. However, this time is not to be confused with the "timetag" present between the attributes of the object class present in the FOMs, in fact the latter corresponds to the ephemeris time.

The HLA standard used is IEEE-1516.2010. The Federation Object Model (FOM) was provided by NASA. In order to be able to represent any object and possible interaction in the scenario, they have defined four models:

- Core: defines many common data such as the position vector, the quaternion or the mass, which are also used in the other FOMs.
- Environment: defines all the previously mentioned reference systems, defining the origin and orientation of the axes in such a way as not to leave ambiguity when some federate move objects, modify objects velocities and accelerations, apply forces and torques to the objects or use any another element that has sign and verse of propagation.
- Entity: defines the physical objects that you want to federate. The class described in this FOM contains a subclass that must necessarily be customized by each team, due to the considerable diversity of the federable objects. The file is used as an "agreement" between the various federates if one of them wants to receive information about an object published by another federate: if, for example, a federate would like to receive information on the position and velocity of the asteroid published by another federate it must necessarily possess the custom FOMs that defines the celestial object.
- Chat: defines the interactions and exchanges of data or messages possible between the various federates.

4 Other Experiences

As already mentioned, in the Simulation Exploration Experience event great attention is given to the use of HLA and therefore to the interoperability of the simulators. Interactions between the federates play an important role because the more they grow, the more complex and organic scenarios can be reproduced. Over the years, the number of them has increased significantly both due to the number of participants has increased and due to they have more and more refined their own federate in order to make it interact more and more with the other simulators.

Due to the complexity of the scenario, many tests were required to ensure that everything worked correctly, especially to verify that the federates actually communicated and interacted with each other. To perform these tests, all participants were assigned a Virtual Private Network (VPN) connection and an IP address for the SonicWall NetExtender VPN software provided by NASA.

The author participated to SEE each year of the PhD with three different projects, one for every year, in order to refine the knowledge about HLA needed for the research project.

The first project is IPHITOS (Interoperable simulation of a solution based on light Interceptor Tackler operating in Outer Space) and it was presented in 2016. It is a simulator of a defence system against possible meteorite impacts. The system is located on a lunar base, it is equipped with long-range radar and interceptor missiles with the aim to detect, observe and eventually destroy asteroids from outer space. IPHITOS project is the result of five years of studies, reviews, tests and field experiences.

IPHITOS publishes three objects in the federation: a lunar base, an interceptor and an asteroid that cannot all be referred to the Aitken Base. In fact, the latter reference system, located on the lunar surface, changes its position with respect to the Inertial Barycentre of the Solar System due to it moves following the rotation and revolution motion of the Moon around the Earth, which revolves around the Sun. The base of the Aitken Base is excellent for positioning the moon base and the missile when it is stationary, whereas for the asteroid it cannot be used because the space rock comes from the open space and does not rotate like the Moon. Therefore, the asteroid and the missile, once launched, refer to the reference system of the Inertial Barycentre of the Solar System.

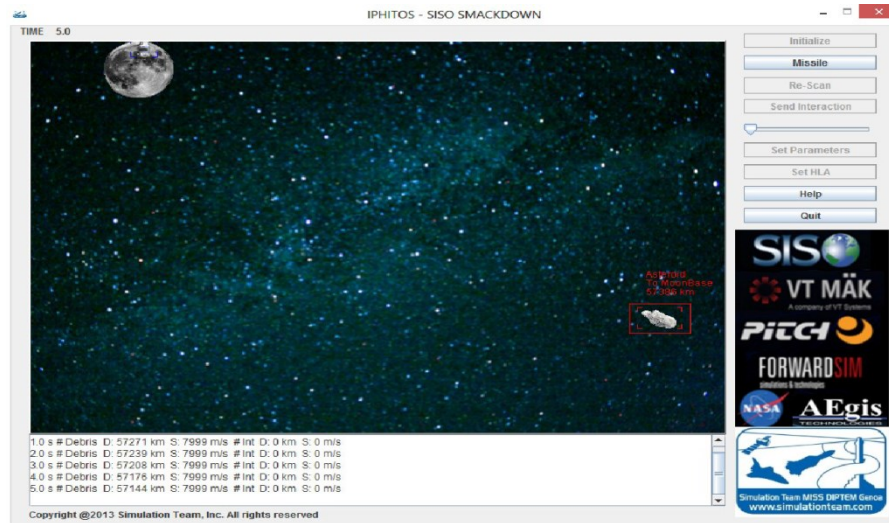


Figure 4.3: IPHITOS 2D interface

To calculate the distances between the lunar base and the asteroid or the missile, it was necessary to obtain the quaternion relative to the motion of the asteroid's triad and then

reconstruct the rototranslation matrix. Thanks to this, it was possible to calculate the distance of the asteroid from the base and the missile in order to be able to inform the federation about the development of the scenario, as we will see later.

IPHITOS has a simplified 2D interface, which goes beyond the 3D representation entrusted to the DON, designed to show to the software user what is happening during the simulation. In this way, the simulator can be launched both in stand-alone and federated.

As already mentioned, IPHITOS simulates a defensive system with long-range radar (Fig. 4.4) which, during the simulation, identify an asteroid (Fig. 4.5) on a collision course with the lunar base.



Figure 4.4: Representation of the IPHITOS defensive system on DON

Therefore, the primary tasks of the base are to identify and try to destroy or divert the meteorite with an interceptor in such a way as to preserve the structure. Furthermore, since

the moon, unlike the Earth, does not have the atmosphere that protects it from asteroids, the defence system must also limit the possible dangerous debris created by the explosion and eventually estimate their direction, their place of impact and approximately the extent of the damage they would cause.



Figure 4.5: Depiction of DON on the asteroid

The equations of the trajectories of both the moon and the meteorite objects are very complex: we must take into account the gravitational fields of the Moon, the Earth and the Sun moving with its period of revolution, and even the rotation period of the Moon that is fundamental to understand if the asteroid will impact near the moon base. The study of these trajectories was performed in 2012 in collaboration with the MBDA team, very competent in this field. Thanks to them it was possible to define that the light interceptors are the missiles that have the best characteristics to prevent the asteroid collision with the Moon.

Once IPHITOS is run, it immediately publishes its three objects, and the defence system begins to scour the space within its range of action to detect possible approaching threats. When the asteroid created enters this zone and the radar detects it, the base launches an alert message (Fig. 4.6) to all the federates and communicates the distance at which it is located and the speed with which it is approaching.

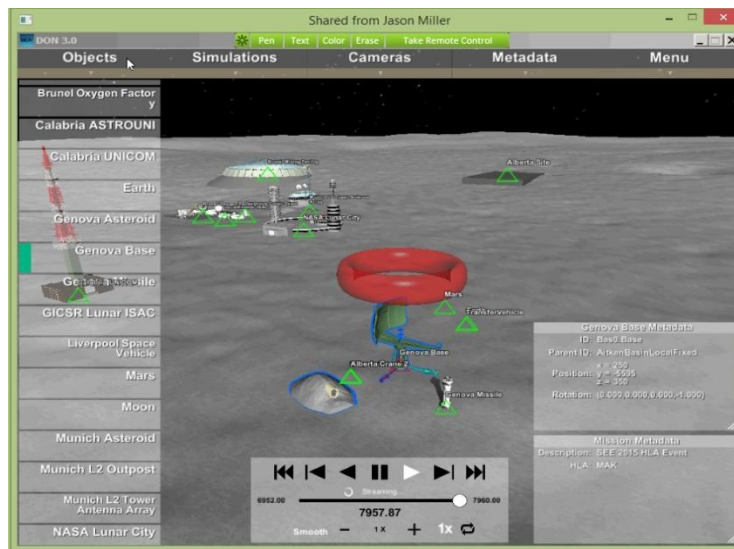


Figure 4. 6: Don representation of the sending of the defence system message

From this moment forward, the simulator does not stop observing the meteorite and at each cycle updates the federation communicating its position and speed. When the asteroid reaches a specified safety distance it sends another warning message to the federation, in which it communicates that it takes countermeasures for the detected threat and launches the interceptor (Fig. 4.7) to the asteroid.



Figure 4. 7: Representation of the Missile of IPHITOS on DON

As before, each frame IPHITOS continues to monitor the state of the situation and to update the whole federation, controlling the trajectories and the velocities of the two objects and even the remaining fuel of the missile. When the missile finally reaches the asteroid (Fig. 4.7) the simulator warns the federation of the collision but waits a few seconds before sending the last communication that warns the success of the operation: destruction or deviation of the asteroid. This interaction is sent because in reality the medium-range sensors would be affected by the interference due to the explosion shock waves and the possible residual radiations emitted.

IPHITOS is written in Java language and the bulk of the project focuses on the use of HLA. As RTI (Runtime Infrastructure) software to manage all communications, data transfers and interactions, two software have been used: PITCH and VT MAK which have released their licenses and Java libraries indispensable for the individual federates to work as well as for create the whole federation.

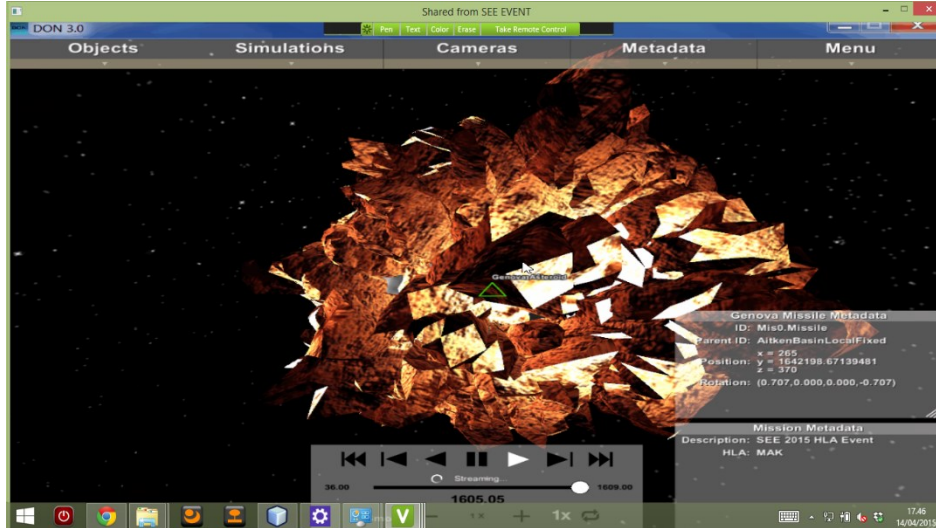


Figure 4. 8: Representation on DON of the asteroid explosion

IPHITOS, interacts a lot with UNICOM of the Italian team of the University of Calabria; as already mentioned, the defensive system publishes three interactions to the whole federation, in reality these are not immediately sent to all the federates but only to UNICOM which, by simulating a communication form, communicates to all the messages that IPHITOS sends. In addition, the simulator of the Calabrian team, publishes an astronaut in exploration on the lunar surface that once received the asteroid alert, quickly returns to its base in the hope of finding shelter, and once IPHITOS communicates the all-clear it returns to his job.

The second project that author participated is MMALT presented 2017. The federate act as Command and Control (C2) for SEE event based on GIS (Geographic Information System) applications, providing visual representation on Google Earth of the federates assets information and position both on the Moon and Mars.

MMALT receive all the objects published in the scenario with their different attributes. The latter are divided into Static and Dynamic attributes: the first ones remain constant over federation execution; the second ones are updated every given time step.

The Static Attributes are:

- Name (e.g. Excavator1, Excavator2, Radio Station 2, Jack)
- Source (e.g. Calabria Team, Liverpool)
- Type (e.g. Ground Vehicle, Flying Asset, Radio Station, ROVER)
- Autonomy (e.g. Remotely Operated, Autonomous, Manned, Not Applicable)
- Reference System (either Moon, Mars or Earth)
- Brief Description (e.g. The vehicle extracts minerals from moon ground)
- Transportable Capacity (e.g. 78 m³)
- Max Speed (e.g. 10 m/s)
- Antenna Height (for communication systems)
- Signal Frequency (for communication systems)
- Transmitter Rated Power (for communication systems)
- Directional Characteristic (for communication systems)

The Dynamic Attributes are:

- Coordinates (Latitude, Longitude, Height, e.g. 56,5832°; 92,9588°; 37)
- Orientation (Azimuth, Roll angle, Pitch Angle)

- Status (e.g. active, inactive, recharging, waiting, in operations, wandering outside, sampling, building, loading, patrolling, listening, receiving, transmitting) depending on assets goal
- Current Speed (e.g. 7 m/s)

In the following are reported the attributes table:

Table 4. 2: Static Attribute received by MMALT

Static Attribute	Value	Unit Measure	HLA Data Type
Name			String
Ownership			String
Type			String
Autonomy			String
Reference Position			String
Brief Description			String
Transportable Capacity		[m ³]	Real64
Max Speed		[m/s]	Real64
Antenna Height		[m]	Real64
Signal Frequency		[Hz]	Real64
Transmitter Rated Power		[W]	Real64
Directional Characteristic		[°]	Real64

Table 4.3: Dynamic Attributed Showed by MMALT

Dynamic Attribute	Value	Unit Measure	HLA Data Type
Latitude		[decimal degrees]	Real64
Longitude		[decimal degrees]	Real64
Height		[m]	Real64
Azimuth		[decimal degrees]	Real64
Roll		[decimal degrees]	Real64
Pitch		[decimal degrees]	Real64
Status			String
Current Speed		[m/s]	Real64

In this way, MMALT (Moon and Mars Assets Location Tool) gives a clear picture of the situation of the environment simulated. MMALT is written in Java language and use HLA. As RTI (Runtime Infrastructure) software to manage all communications, data transfers and interactions have been used: PITCH.

The third project that author participated presented in the SEE 2018 Event is DACTYL (Dynamic simulator of Autonomous robotic Carrier, Transporter, with hand for handling, Yanking and Loading).

The DACTYL federate is devoted to simulating Autonomous Ground Vehicle able to operate inside and outside of extra-terrestrial planetary bases. DACTYL units move autonomously on rough surface of celestial bodies. These autonomous systems are driven and controlled by Artificial Intelligence that allow to carry out individual and/or collective missions. The DACTYL unit is equipped with a robotic arm for material handling and use of tools and equipment. In facts, the Dactyls autonomous systems are pretty compact vehicles with capability to use different tools and devices by operating their robotic arm with 6 Degrees of Freedom.



Figure 4.9: Dactyl running in the SPIDER Immersive Cave

DACTYL Operations have been tested in terms of sample collection, drilling and conducting measures as well as assembling, welding and constructions tasks to erect the base or other structures. In facts each unit could operate stand alone or in a swarm for missions such as supervision, inspections, welding/assembling, material handling, sample collection, coring. DACTYL Federate simulates a single Dactyl and could be federated with other DACTYLS units or with different models for dealing with complex tasks autonomously in individual or collaborative way. DACTYL was implemented to operate on workstation using regular screen head mounted display and the SPIDER, an interoperable immersive cave.

The development of DACTYL federate was carried out by a mixed team involving different kind of scientists, Engineering Students and High School students.

The best way for learn HLA is, without doubt, the practice. For this reason, participating in these projects has helped me a lot. In fact, thanks to these experiences I improve my knowledge about HLA indispensable for the development of the simulation environment described in this thesis.

4.2 SIMCJOH

SIMCJOH (Simulation of Multi-Coalition Joint Operations involving Human Modelling) is a research and development project aimed at understanding the extent to which interoperable simulators can be used in a multiple coalition context, involving both the master and all his staff to address and solve strategic problems where human factors are relevant. Modelling and simulation make possible to recreate complex scenarios and perform "what-if" analysis with the aim of evaluating the effectiveness of the various alternatives (Course Of Actions, COA) and then preparing the master and his staff to deal with unusual situations.

The scenario used in this simulator is a United Nations Mission in a complex context: the software user plays the role of the Commander of an Italian contingent in mission in a foreign country called "Eblanon", in the Middle East, which presents own territory, different religions and political groups; it needs an active support to keep the situation under control and the United Nations must therefore pay particular attention to protecting the population and avoiding possible causes that could trigger armed conflicts.

The simulator logic of this scenario is:

- The Commander (and his staff) is guided through a multi-step process in which he has to make decisions about how and when to intervene.
- Depending on the MEL/MIL (Master Event List/Master Incident List) chosen, SIMCJOH generates events dependent on stochastic variables, so whenever the simulator is restarted, there is a scenario that starts and evolves in a different way. The Commander must therefore evaluate the situation, obtain information on what is

happening and on the current state religious politics. In this way he can acquire the knowledge to make informed decisions about how to move and choose the COA (Course Of Action) suggested by his staff that he considers most suitable.

- As happens in reality, the Commander can ask his staff for additional information on each COA with the aim of testing the feasibility of each of them, collecting other data, assessing the legal consequences and also the secondary effects, such as the effects it could have on the population.

As mentioned above, the commander interacts with his staff and there are two different ways to do this:

- Synchronous Activities: structured actions linked to the analysis of COAs.
- Asynchronous Activities: actions such as asking staff to provide additional data, assessments, information, etc. which can be done at any time during the simulation.

After choosing the COA to be used, the discrete event simulation evolves stochastically following the selected MEL/MIL and the selected Course of Actions. It is able to perform multiple fast-time replications of the same simulation and to assess the military secondary effects on the population and the risks, in order to provide an indication of the Commander's performances (Bruzzzone & Massei 2017a).

The Staff that the commander has available is composed of 15 characters covering 15 different roles:

- JCoS: Joint Chiefs of Staff
- G1: Staff

- G2: Intelligence
- G3: Operations
- G4: Logistics
- G5: Operations Plans
- G6: Command, Control, Communications and Computers / Cyber
- G7: Preparation and training of forces.
- G8: Structure of Forces, Resources, and Assignments
- G9: CIMIC (Military Civil Cooperation)
- Legad: Legal Counsellor
- Polad Counsellor: Political Counsellor
- PAO: Public Relations Officer
- Culad: Cultural Counsellor
- Squad: The team in the territory to whom a report can be requested on current situation.

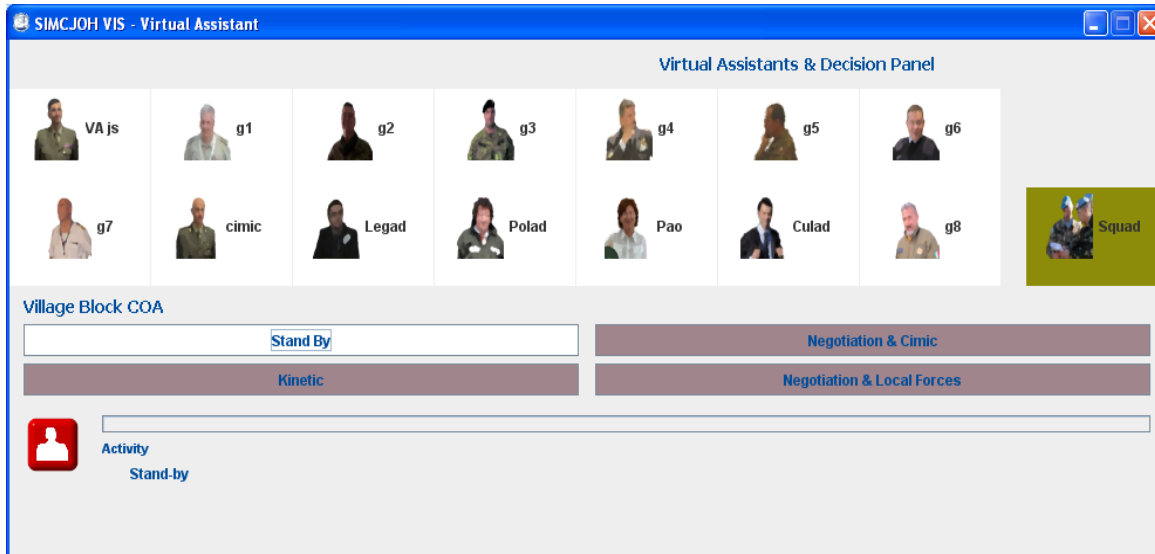


Figure 4. 10: Staff of the Commander

The staff, also called virtual assistant, allows the Commander to make decisions to request reports and details on what is happening in the scenario considering different aspects.

The scenario MEL/MIL 1 which deals with an Italian team of a platoon of UNIFLI (United Nation Force for Large Improvement of Eblanon) composed of 12 soldiers who is surrounded by a crowd of protesters in a foreign village during a task force. The number of people around them continues to increase and the team commander warns that he is no longer able to move and resolve the situation. The procedures for deploying units around the village are then activated. Three COAs are suggested by the Commander's Staff and are called CIMIC, KINETIC, LOCAL FORCES (they are included in MEL/MIL). Their descriptions include military effects, secondary effects on the population, risks derived from suggested actions and possible mitigation actions.

Table 4. 4: Example of a COA: CIMIC COA

COA	Military effect	Effects on population	Risks	Mitigations
<u>CIMIC</u> <ul style="list-style-type: none"> - Introduction of a CIMIC operator for direct Face to Face (F2F) negotiation. - 2 Teams for protecting the CIMIC operator - Availability of food kits to be distributed on-site (100 food kits) - Local Policies and Forces have not been contacted - Two helicopters are available for surveillance operations - Preparation of an official press to support the counterpropaganda (info-ops) 	<ul style="list-style-type: none"> - Reduction of the brigade reserve - Insertion of a vehicle for the food kits transportation - Reduced Helicopter transportation capability for the time of the operations - Concentration of military forces in the village area / reduction of military forces in surrounding areas - The presence of the 2 Squads supporting the CIMIC operator will saturate (in terms of military presence) the area of the event 	<ul style="list-style-type: none"> - The presence of helicopters scares the local population - The distribution of food kits will increase the number of people in the area of the event - General increase of social tension - The F2F negotiation activity could enhance the importance of the local person involved in negotiation (he can be recognized as the leader by the local population) - The massive presence of armed soldiers could induce the local male population to arm themselves - Any flash news broadcasted on the national radio network could negatively affect the population of the village 	<ul style="list-style-type: none"> - Reduction in the capability to satisfy further requests for additional military operations - Reduction of 30% of the helicopter transportation capability - Possible reduction of movement capabilities (e.g. the vehicle for food kit transportation is blocked) - Possible exploitation of hostile forces in other areas due to the reduced military presence - Possible loss of credibility at the local level - Negative Media effects 	<ul style="list-style-type: none"> - Immediate reconstitution of the reserve with retired staff - Use of trailers for security team transportation - Temporary enlargement of the AOO (Area Of Operations) of minor units (company + special assets)

The COA suggested by the staff follow a certain flow chart that handles action to be undertaken according to the possibilities the situations with which the scenario can evolve.

An example of a Flow Chart is shown in figure 4.11.

4 Other Experiences

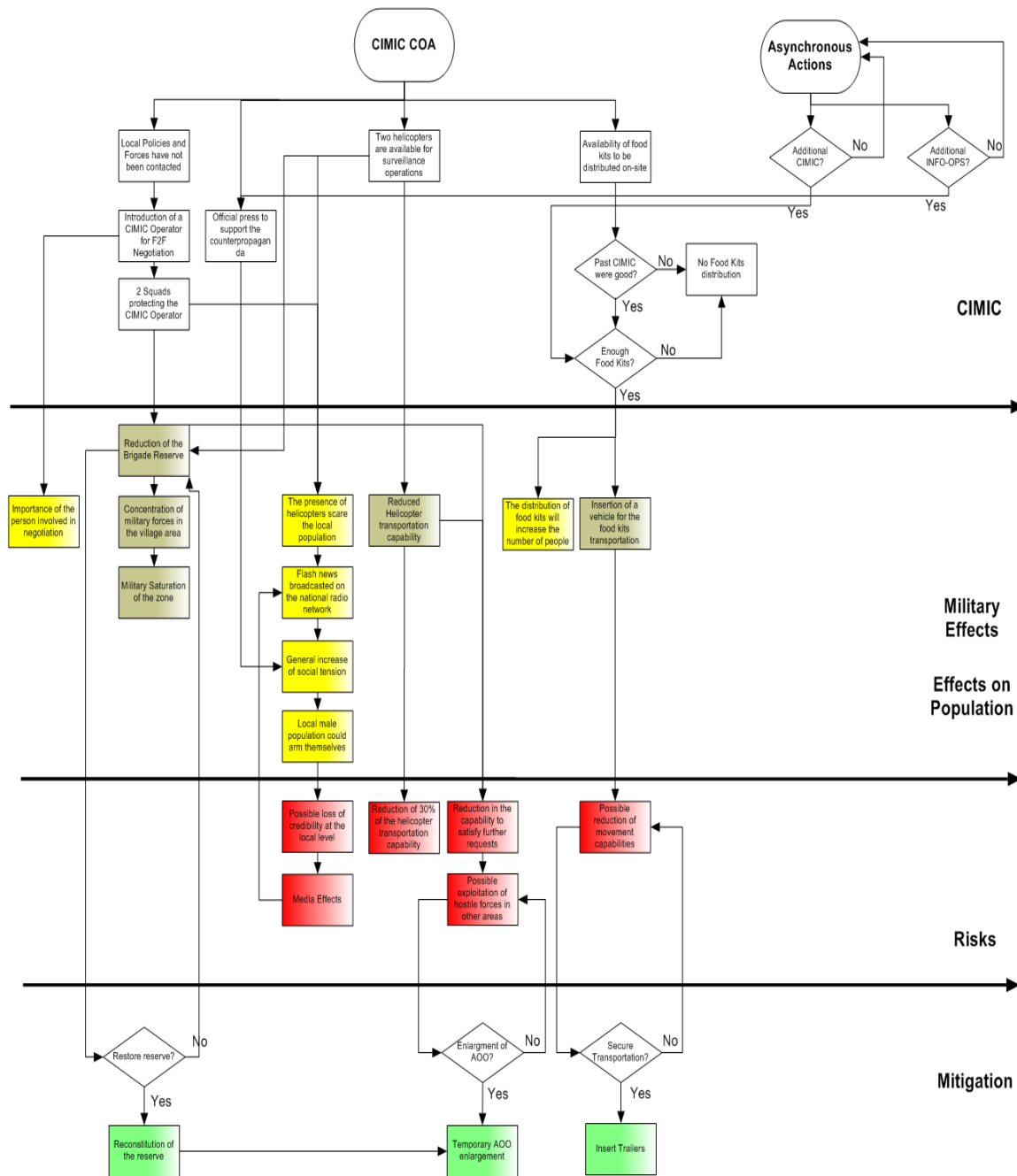


Figure 4.11: Example of a Flow Chart. COA CIMIC

The SIMCJOH simulator automatically generates updated dynamic reports based on the events and decisions taken by the commander. These reports can be requested by the user whenever he wishes and are displayed as a Power Point file. In order to simulate real reports, they do not always contain true information: they are written from the point of view of the blocked team, which may have incorrect information. The information contained in these reports, however, can be improved and verified by requesting reconnaissance or confirmation from the Intelligence.

SIMCJOH is currently composed of 4 different simulators federated with each other through the HLA: SIMCJOH VIS (Virtual Interoperable Simulator), SIMCJOH VIC (Virtual Interoperable Commander), GESI and SGA. The first is the real "thinking head", contains within it the AI-CGF (Intelligent Computer Generated Forces in Conventional Framework) that simulates human behaviour, and then manages the possible reactions of the crowd that blocks the team to the decisions and actions taken and undertaken by the Commander. So the simulation is made almost entirely from it and is the only one of the four federates that can work alone, the other three simulators in fact serve to add more functionality, to give more immersion or to take the place of staff characters to real physics people instead of being just the entities created by the simulator; the goal of this project would be that every staff member would take care of a real physical person as it would really happen, so as to be able to train all the staff members and not just the commander

The second simulator, SIMCJOH VIC, is a 3D viewer that has the purpose to represent what is happening during the simulation in such a way as to make the simulator much more

immersive to give the illusion of being really in that particular condition so as to identify more in the criticality of the scenario and to understand at a glance how the situation is evolving. In its VIC architecture it includes analytical models that are used to recreate realistic scenarios such as the real-time movement of the helicopter with its 6 degrees of freedom or the model of the movement in real time of military vehicles. In VIC, again to make the scenario as realistic as possible, there are also many animations that reproduce human movements for both citizens and the military. SIMCJOH VIC was realized with the Unity 3D software and therefore, as already mentioned, presents problems in using the HLA, so it was necessary to realize here also a program that acts as a bridge in the communications between the various simulators. The other two simulators, SGA and GESI, instead are in order a scenario generator and communications manager, and a tactical viewer.

SIMCJOH can have three different configurations depending on the federated simulators and the people who use them:

- Stand Alone (fig.4.12): in this configuration we only have SIMCJOH VIS or SIMCLOH VIS federated with SIMCJOH VIC for a clearer view and greater immersion. This architecture is used for training only the commander or one of his staff.

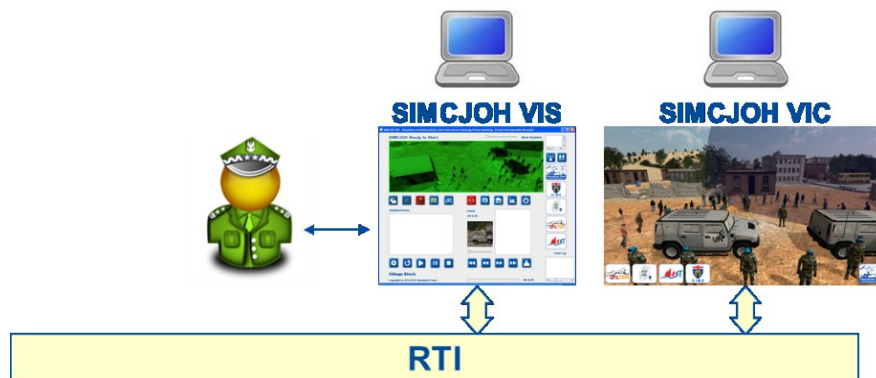


Figure 4. 12: SIMCJOH Stand Alone

- Fully Federate (Fig. 4.13): in this mode we have SIMCJOH VIS federated with all the other construction simulators created up to now. In this way, we will have the commander struggling with a very immersive environment and can also take advantage of a tactical view.

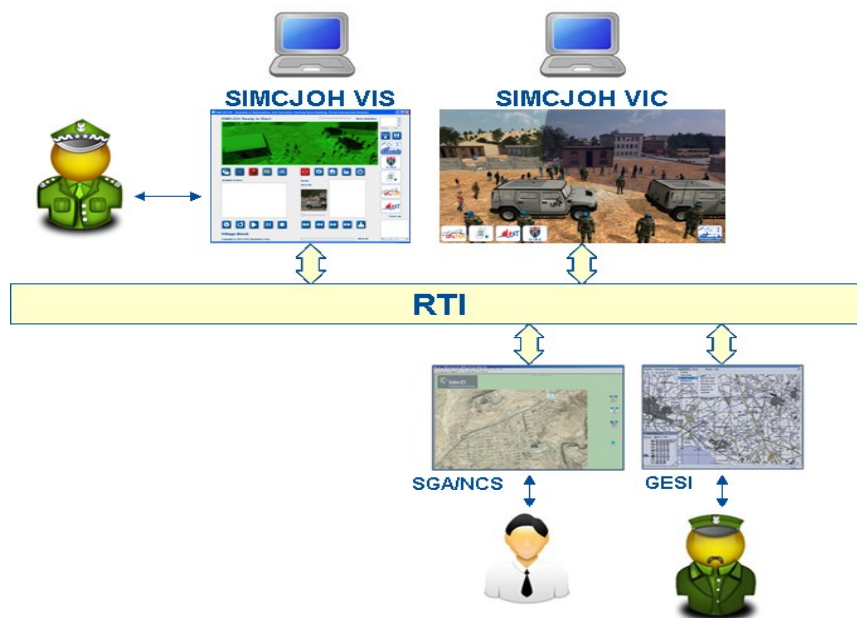


Figure 4. 13: SIMCJOH Fully Federate

- SIMCJOH within CAX (Figure 4.14): this configuration is the one that trains multiple people at the same time. With the help of the CAX the whole brigade can perform the exercise and train to the possible situations simulated by SIMCJOH VIS.

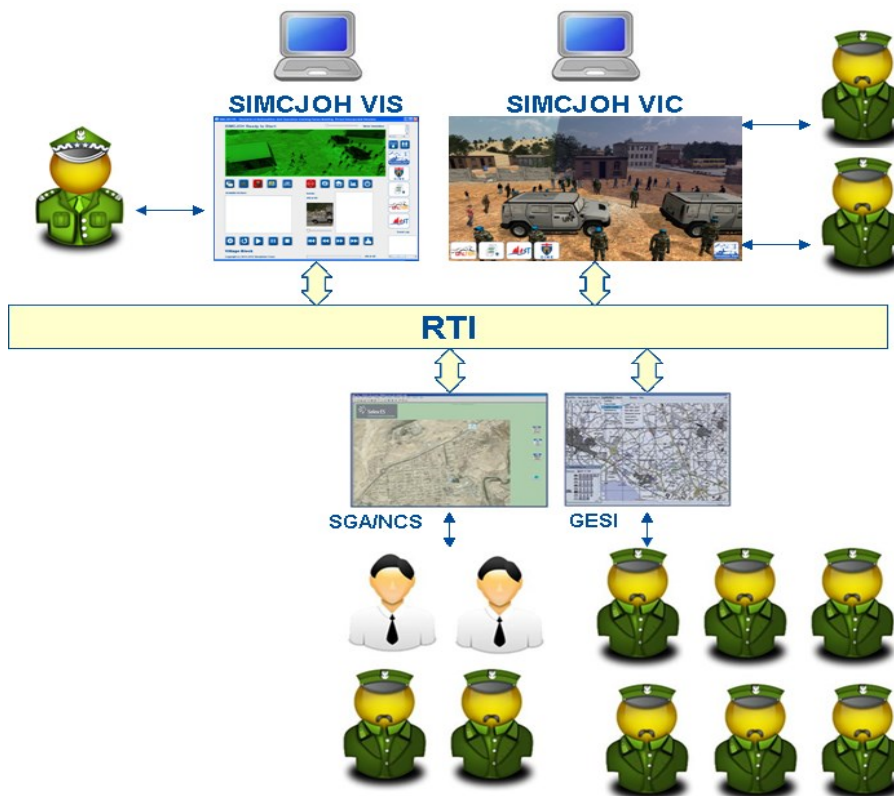


Figure 4. 14: SIMCJOH within a CAX

As we have seen, therefore, SIMCJOH is an interoperable simulator through HLA. A big problem encountered was the difference between the two SIMCJOH VIS and VIC

simulators: the first one is a discrete element simulator, while the second one is in real time. So, for VIS an action takes place in an instant, in a fraction of a second, while in VIC this action takes some time to be finalized. This difference caused discrepancies in what was happening in VIS and what VIS was representing, so a good way to solve this problem was to stop the progress of the VIS simulation when the instruction to show a particular animation arrives at the 3D viewer until the latter does not come to an end, and then resumes when VIC announces that it is over.

The HLA standard used is the IEEE 1516. The FOM which, as already mentioned, includes the definition of the object classes, the attributes, the interactions, the parameters and any other information pertinent to the federation, was written, at the request of the partners they contributed to the realization of SIMCJOH, as similar as possible to the FOM already existing in other simulators (such as the RPR-FOM version 2.0) in such a way as to be easily federable with other possible existing simulators.

Class	Definition
Asset	Every asset on which sensors or weapons are mounted in the scenario e.g. aircraft, drone, ground unit, demonstration...

Attribute Definition table

Class	Attribute	Definition
Asset	Position	Latitude, [degrees decimal], Longitude, [degrees decimal], Height/Depth [m]
	Angles	Course, Pitch, Roll [radians]
	Speed	Speed [m/s]
	ID	Code to uniquely identify the platform: e.g. AW129_71_xxxx

Figure 4. 15: FOM extract of SIMCJOH

The variables present in SIMCJOH are innumerable, demonstrating that the scenario is very complex. The following is a list of the main ones:

- Duration of Simulation (time spent by troops in the village)
- Final Result (success or failure)
- Number of Protesters (Medium, Min., Max.)
- Situation of the Final Conditions of Protesters
- Injured Italian
- Wounded of Coalition
- Wounded Civilians
- Wounded OPFOR FOE_KIA
- Friendly Forces Present in the Area of the Fallout
- Enemy Forces Present in the Area of the Fallout
- Friendly Deterrence Exercised in the Fallout Area
- Enemy Deterrence Exercised in the Fallout Area
- WIA Italian Simulation
- Team State
- MEDEVAC Result
- Evacuation Result
- Italian Impact on Domestic Media
- Italian Impact on Local Media
- Speed in Press Release

- Stress Level in the Village
- Fear Level in the Village
- Fatigue Level in the Village
- Aggression Level in the Village
- Respect of UNIFIL conditions on the Fire
- Respect of UNIFIL conditions on arrests
- Respect of UNIFIL conditions on the use of the EW Bubble
- Closing of the Communications given by the EW
- Situation of the Village where the Fact happened
- Final Results of the Team
- State of the CIMIC
- State of the CIMIC after the Actions
- State of the PSYOPS Radio
- Status of the PSYOPS leaflets
- State of the PSYOPS Speakers
- Combat Status in the Village
- List of All Decision Taken

All the variables listed above are influenced by the decisions that can be made by the commander (such as the selection of the COA, Intelligence Operations, CIMIC Planning,

etc.) and from the boundary conditions such as time, hostile forces, the history of events that occurred in the area of the event etc.

Analysis of the simulator parameters was also carried out regarding the MEL/MIL of the team blocked in the village in the Middle East described above, in order to estimate the impact of the stochastic variables in the functions sought. The decision of the Commander was considered as the main independent variable in the COA present in the scenario.

Furthermore, in order to establish a confidence interval for the main variables sought, the mean square deviation was calculated. In the following figures (Figure 4.16, 4.17, 4.18) you can see some graphs of some variables analysed.

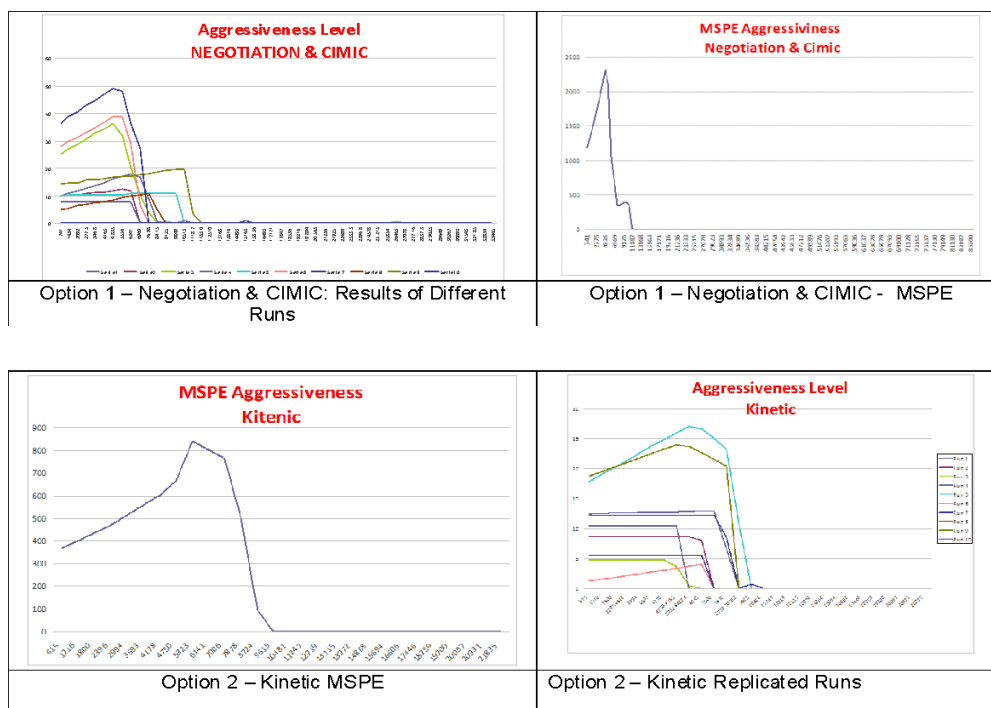


Figure 4.16: Graph of the average square deviation of Aggressiveness in two different COAs.

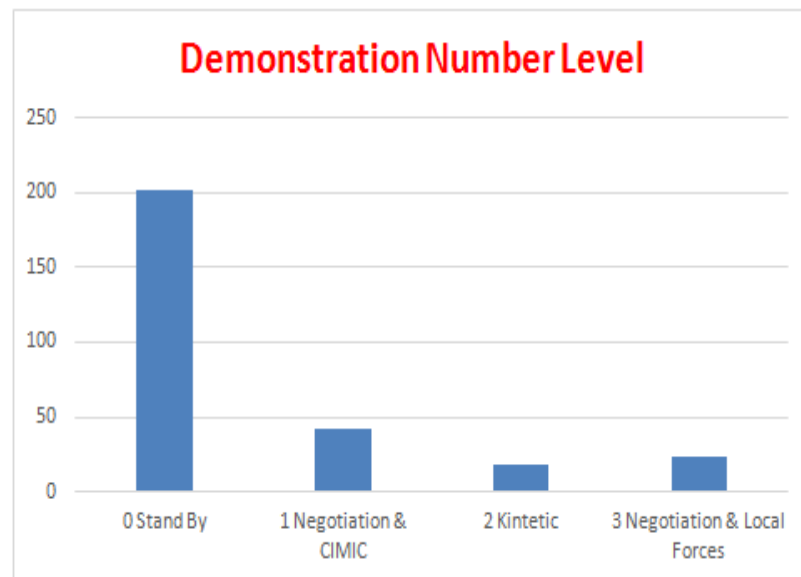


Figure 4.17: Demonstrators Number in the different COAs

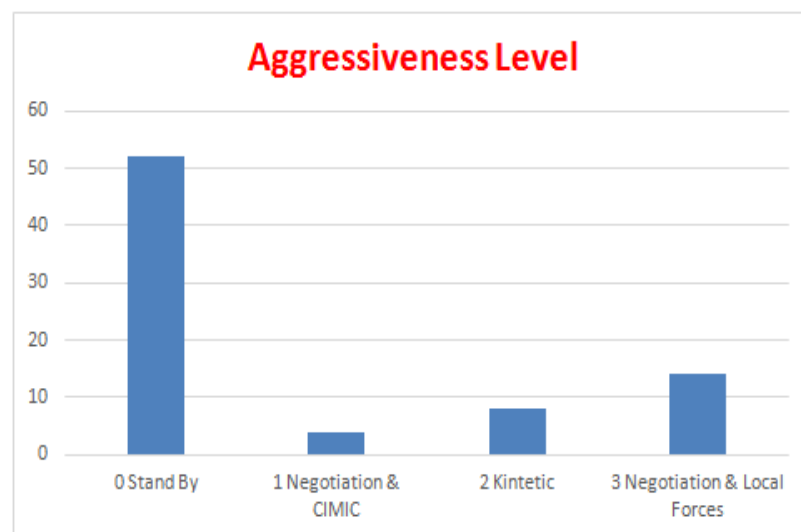


Figure 4.18: Level of Aggressiveness in the different COAs

So, the SIMCJOH project interfaces with new and laborious aspects, and allows the study and development of new simulation models to support the Commanders and their staff in

making decisions. The architecture, the way of use and all the conceptual models have been successfully completed and the federation, with all the federates described above, are operational and in demonstration.

4.3 MALICIA

MALICIA (Model of Advanced pLanner for Interoperable Computer Interactive simulAtion) is a stochastic discrete event simulator for maritime interdiction (Bruzzone et al. 2011e) and derived from a previous project called PANOPEA (Piracy Asymmetric Naval Operation Patterns modelling for Education & Analysis). MALICIA is focusing on Maritime Interdiction Scenarios and could be applied to different cases from piracy to illegal immigration or anti-smuggling missions. The simulator simulates the maritime interdiction by modelling the general framework, platforms, C2 and even the specific anti-piracy operations or illegal immigration interdiction procedures. MALICIA reproduces weather conditions over wide area considering influence on sensor and platforms; the model cover fog, rain, wind, current, waves. In addition, the simulator includes models of multiple assets such as MPA (Maritime Patrolling Aircraft), Vessel, AUV, Helicopters, Submarines, Cargo, Yachts, Fishermen Boat, etc.; these entities are driven and operated by IA-CGF that reproduce their behaviour and their interaction dynamics (Bruzzone et al. 2013c). In facts the assets simulated by intelligent agents interact dynamically each other in to recreate the dynamic simulation needed to those kind of scenarios (Bruzzone 2013a).

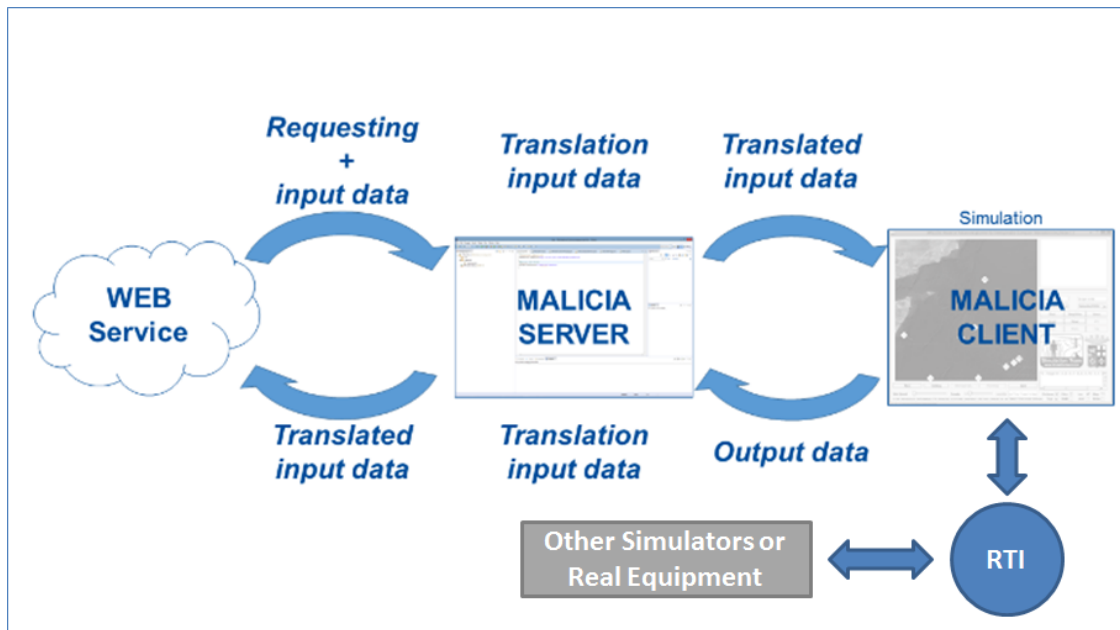


Figure 4.19: MALICIA Architecture

The model receives the data input from web services and interacts with Tactical Naval Situation; the model includes commercial traffic, threats and false alarms. MALICIA evaluates the measures of merit as individual factors as well as overall performance covering Efficiency, Risk and Costs of the whole planning proposed by the user or generated by an intelligent decision support system (Bruzzzone et al. 2006). For these reasons, MALICIA represents a useful instrument for supporting dynamic Operation Planning and Optimization. In fact the proposed approach supports both the automated use in connection with optimizers as well as interactive use with decision makers refining interactively the planning based on the result of the simulator.

MALICIA GUI (Graphic user interface) is proposed in Figure 4.20, while the overall structure is presented in figure 4.19 and described in the following. The simulator is divided into two components: MALICIA Server and Client.

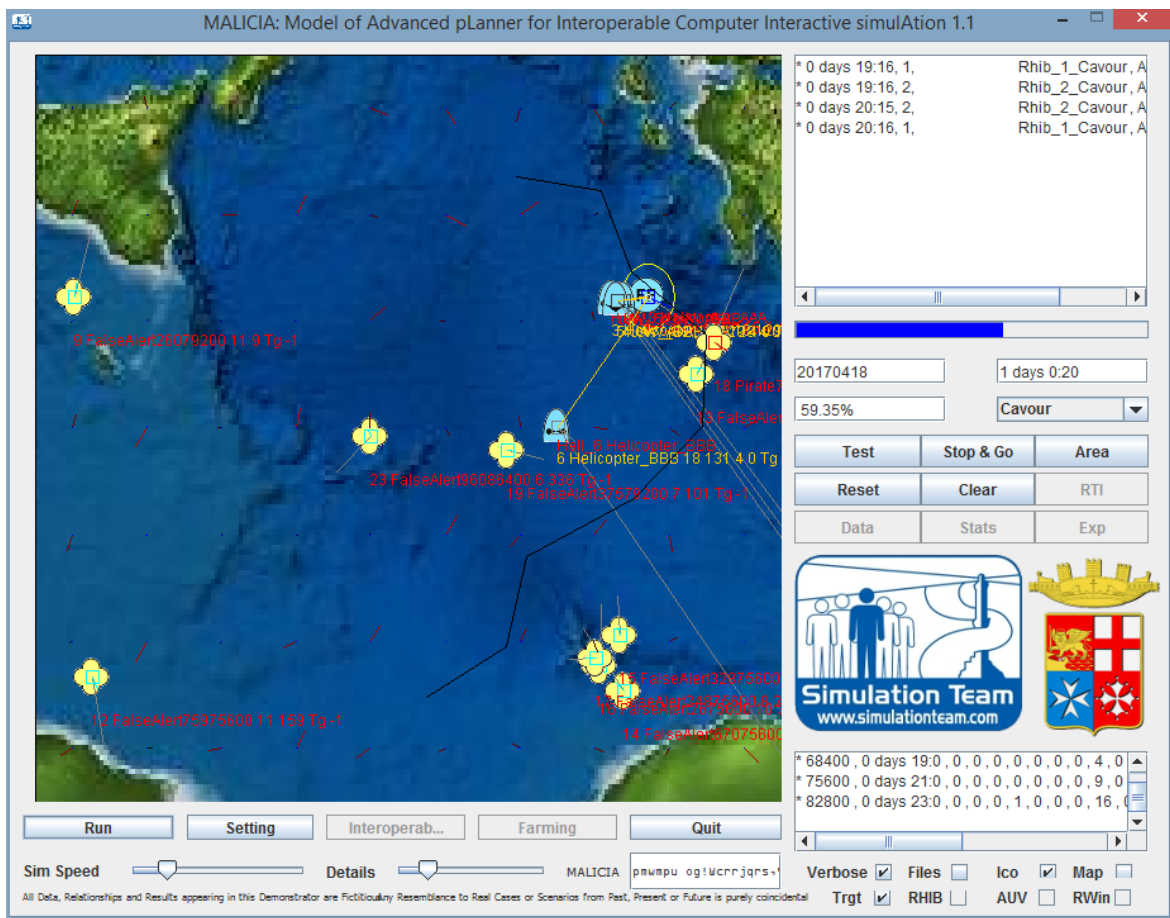


Figure 4.20: MALICIA GUI

The Server is the component developed to establish the communications with the web services and MALICIA Client and it operates as dBase server. The Server main tasks are receiving requests and data input from web applications especially related to the up-to-date

situation of the vessels and the weather conditions; the server takes care of acquiring the input data in the correct way and to propose them to MALICIA Client and send back the results of the simulation to web services connecting MALICIA with the planning framework that uses touch screen technologies over wide board for supporting decision makers in their planning..

The Client is the real simulator elaborating input data simulating the scenario and providing the output to the Server; MALICIA is designed to be federated within a High Level Architecture interoperable federation with other models in case it should be used as part of a distributed simulation.

Indeed, MALICIA is ready to be used both stand-alone and federated, as well as connected with dBase by web services or operating on local data sets. In stand-alone mode the input data should be pre-compiled, instead when is connecting with web services the Requesting application should send the data input continuously to keep the simulator on-line with the real situation (Bruzzzone et al. 2002a).

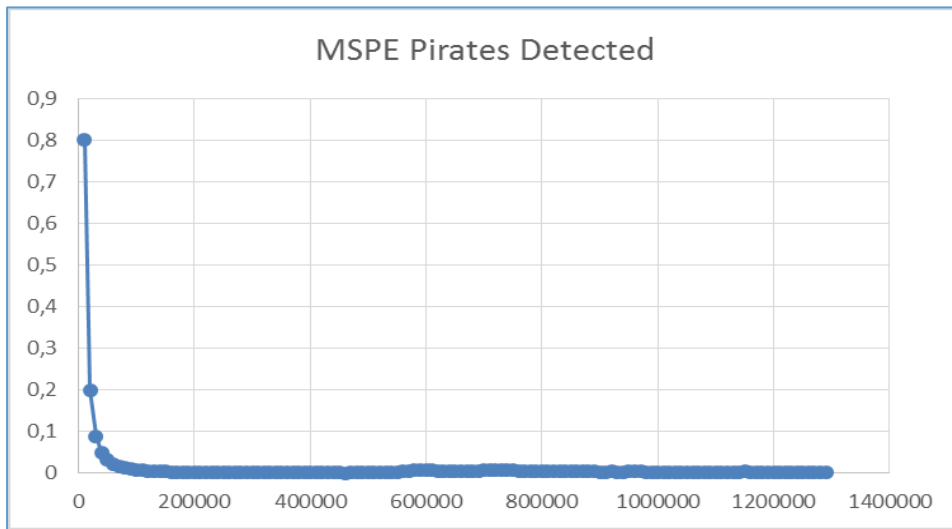


Figure 4.21: MSPE of Prates Detected Target Function

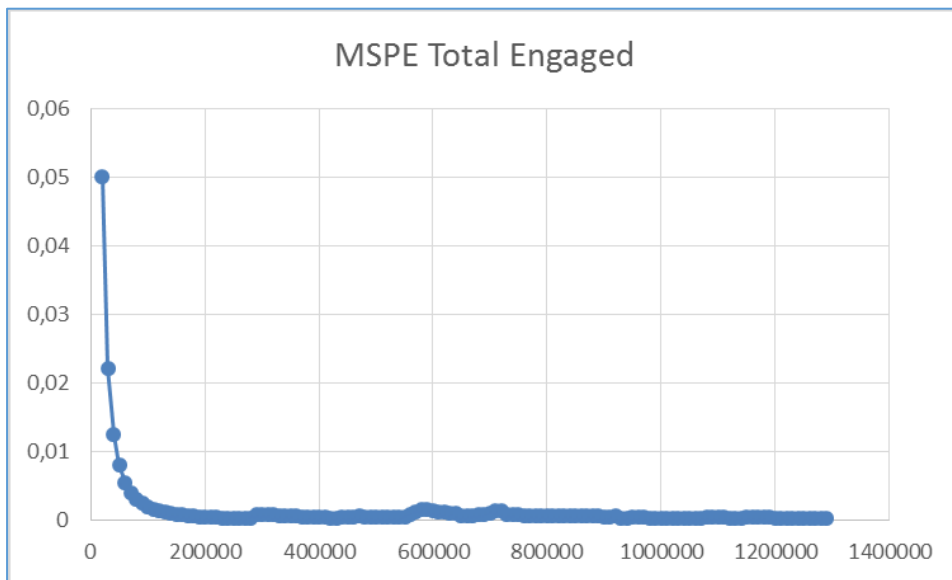


Figure 4.22: MSPE of Total Small Boat Engaged Target Function

Due to the quantity and the complex nature of input data it proposed a specific set of variables that could be also partially incomplete.

This particular solution has been adopted in order to run the simulation even in case of missing data. In this case users feeds the simulation with his available data and for the

missing ones it is assumed to use the standard value from a reference dbase developed and implemented by the authors based on historical data.

MALICIA Client receives as input from dBase manager:

- Weather Conditions: actual and provided during the period of the simulation (given by a web service when is possible)
- The assets used in the simulation with a defined set of technical characteristics (e.g. name, speed, autonomy) and rules of engagement.
- Patrolling routes associated to the assets.
- A probability map of possible presence of pirate threats or illegal immigrants.
- General data about number of interactions, duration of the simulation, resolution of output data, the scenario size.

The model reproduces assets behaviour during the period of simulation, taking into account their interactions and the influence of the boundary conditions. Simulation is able to run real time or fast time based on user preferences; in a complex scenario involved a dozen of assets with their resources (i.e. on-board helicopters, UAV, RHIB) the simulator at fastest speed is able to cover 3 days of activity in few minutes.

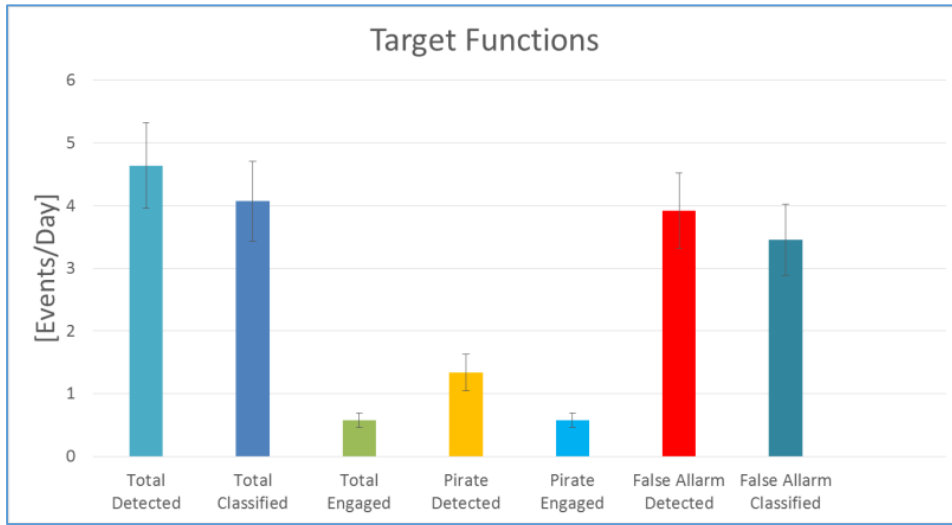


Figure 4.23: Events per Day for each Target Function

The simulator reproduces small-medium size boat representing commercial traffic and pirates. The assets employed in patrolling and block operations are capable to Detect (boat enters asset sensor range), Classify (distinguishes pirates from false alarms) and Engage (performs actions to intercept or neutralize menaces). Succeeding in the actions depends on onboard systems availability and reliability, influenced by the stochastic evolution of the simulation (e.g. drones not available because in maintenance, sensor failure) and by weather condition. The simulator provides detailed log about the operations such as:

- Patrolled area by the assets employed
- The tracking and operations of all the different assets and their technical-operational conditions
- A scenario general overview including the cumulative temporal distribution of the following target functions: number of false alarms, number of piracy threats, number

of detections, classifications and engagements performed for each category (False Alarms, Pirates, Overall) during the time period simulated and differentiated for the different types (i.e. successfully classified, unsuccessfully classified)

The experimental campaign is focusing on a specific set of the target functions covered by the simulator and specifically on the following ones:

- Total Small Boat Detected by the assets
- Total Small Boat Classified by the assets
- Total Small Boat Engaged by the assets
- Pirates Detected by the assets
- Pirates Boat Classified by the assets
- Pirates Engaged by the assets
- False Alarms Detected by the assets
- False Alarms Boat Classified by the assets
- False Alarms Engaged by the assets

Replicated simulations with the same initial boundary conditions, but different random seeds for the statistical distributions of the simulator have been performed. The Data have been collected every 10'000 simulated seconds for a total simulated time of 15 days (1'296'000 seconds).

In figure 4.21 and 4.22 it is proposed the analysis of the experimental error due to the pure influence of stochastic component for Pirates Detected and Total Small Boat Engaged Target Function (Balci 1998, Montgomery 2000, Kleijnen 2007, Telford 2012).

ANOVA technique have been applied and it was possible to verify and validate the target functions stabilization based on Mean Square pure Error Temporal Evolution analysis. So, Figure 4.23 shows the average number of events per day for each target function and the amplitude of the confidence band due to the stochastic nature of the simulation. Obviously, the variance is pretty large, therefore the values and results result consistent with the fidelity requirements for being applied to maritime interdiction planning.

4.4 DIES IRAE

DIES IRAE (Disasters, Incidents and Emergencies Simulation Interoperable Relief Advanced Evaluator) is a simulator about the Disaster Relief.

In disaster relief is crucial to develop methodologies and techniques to support planning of operations and to evaluate impact of decisions (Bruzzone et al 2016c). The areas to be addressed, in most of the cases, in the above-mentioned examples are related to several aspects including among others:

- Logistics
- Health Care
- Food Distribution

- Engineering
- Services Activation
- Infrastructure & Equipment Deployment
- Security & Defence

Therefore, in these contexts the situation is usually very complex due to infrastructure collapse (e.g. economic, transportations, food chains, etc) and to the presence of multiple actors (e.g. refugees/IDPs Internally Displaced Persons, local population, conflict actors, supporting coalitions, NGO Non-Governmental Organization). Often these actors have conflicting interests, sometimes they are even fighting at level of organizations (e.g. war or civil war) or socially (e.g. ethnic tensions, social tensions). It is evident that due to these reasons the scenarios are very complex and require the use of simulation to be properly studied and to support the decision-making process (Anderson et al. 2007; Werker 2007; Bruzzone & Sokolowski 2012c; Latek 2013, Bruzzone et al. 2017b).

The complexity of these scenarios is further reinforced by the heavy impact of human factors affecting social, ethnics, tribal, religious and political issues. These elements are often the main factors to be considered such as in recent conflicts ongoing in Africa and Asia (Johnson & Mason 2008, Bellamy et al. 2011; Dewachi et al. 2014). In facts the HBMs (Human Behaviour Modifiers) include psychological factors (e.g. fear, stress, aggressiveness, etc.) as well as primary needs (e.g. food, security, health care) based on the local hierarchical

priorities (Maslow 1943; Møller & Schlemmer 1983; Longo et al. 2005; Saati et al. 2011, Bruzzone et al. 2018a).

In general, it emerged that the use of Human Behavior Models could be pretty effective to reproduce the people reactions and to measure the effectiveness of the disaster relief actions (Uno & Kashiyaama 2008; Bruzzone et al 2014d). These elements strongly affect the behaviour of conflict actors, humanitarian supports and population as well as local and domestic public opinion (Gartner & Segura 2008). The Simulation Team of University of Genoa acquired good expertise in modelling critical situations such as country reconstructions, disasters and emergencies (Bruzzone & Massei 2010). Simulation Team has conducted several experimental cases in this sector including Haiti Simulation based on use of interoperable IA-CGF and CAPRICORN Project (CIMIC And Planning Research In Complex Operational Realistic Network) on CIMIC (Civil Military Cooperation) carried out in Afghanistan. These are a valuable base to further develop innovative models (Bruzzone 2013b).

DIES-IRAE has a general architecture similar to SIMCJOH structure as presented in Figure 4.24 (Bruzzone et al. 2015d).

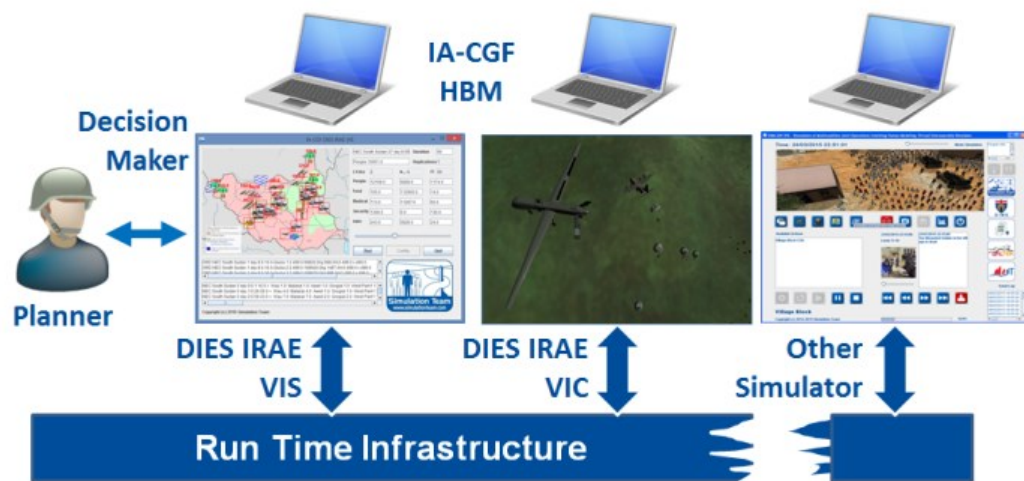


Figure 4.24: DIES IRAE Architecture

). Indeed, DIES IRAE adopts MS2G (Modelling, Interoperable Simulation and Serious Game) Paradigm (Raybourn 2012; Bruzzone et al.2014e) and it is composed by two main simulators federated by using HLA:

- DIES IRAE VIS (Virtual Interoperable Simulator): is a stochastic discrete event agent driven simulation using the IA-CGF for reproducing HBM; it simulates the actions of components, equipment, units and population. This module supports operation planning, commander training, policy analysis and review of procedures and processes.
- DIES IRAE VIC (Virtual Interoperable Commander) is a Virtual Simulator using Serious Game approach that provide the Synthetic Environment to reproduce the events and takes care of the detailed dynamics (e.g. air drops, landing, etc) such module allows to provide support for tactical training and education.

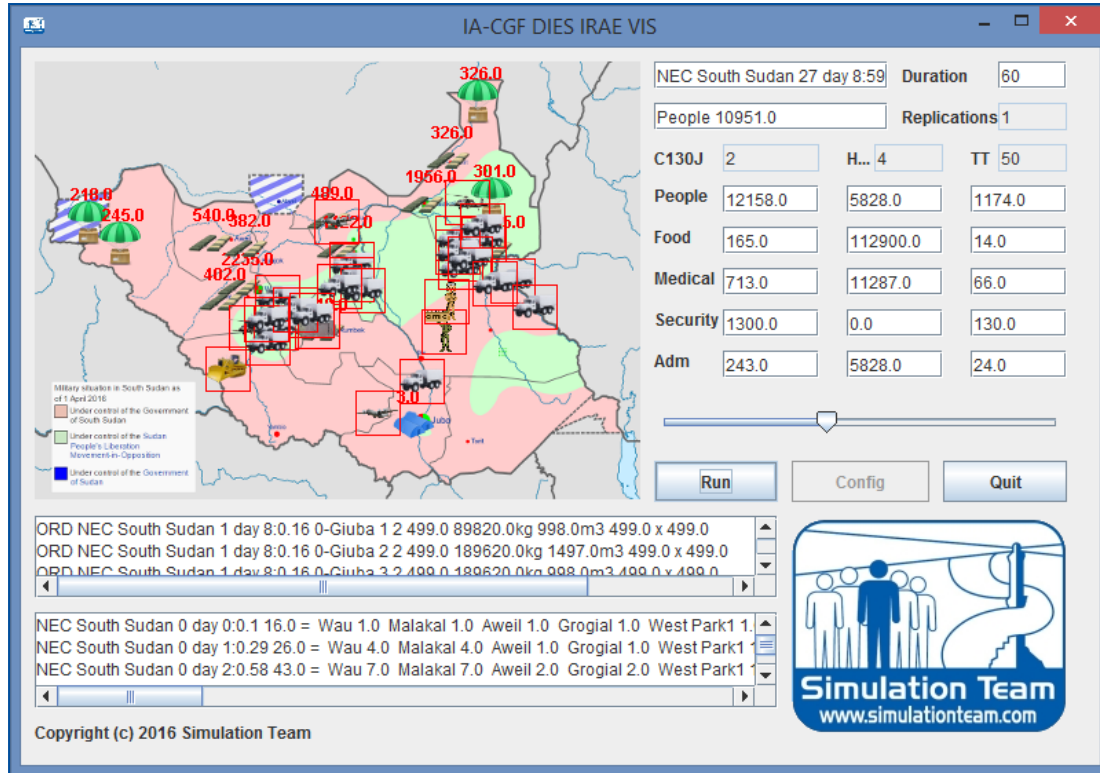


Figure 4.25: DIES IRAE VIS: The Discrete Event Stochastic Simulator

Indeed, the solution guarantees maximal flexibility by adopting interoperable HLA: in this way it becomes possible to combine the proposed simulators also with other models. This approach enables the stand-alone use of DIES IRAE VIS without Virtual representation or to combine it with DIES IRAE VIC and other models addressing specific aspects (e.g. economics, war gaming, CIMIC, etc.) in a distributed simulation. In addition, this simulation might be combined with other ones in order to be active part of a complex CAX.

DIES IRAE VIS (see figure 4.25) allows to simulate the operations and phenomena evolution in order to evaluate efficiency and effectiveness of the disaster relief plan. In facts, the Discrete Event Stochastic Simulator provides estimation of times, costs and availability of resources respect the demand. The model reproduces the flow of IDPs and refugees and their needs in terms of:

- Accommodation
- Food & Water
- Health Care
- Security
- Administrative Procedures

Each of these issues requires, potentially, to establish infrastructures to be deployed on site (e.g. camps, airstrips), consumables to support the operation (e.g. food packages) and resources (e.g. soldiers and medical doctors). The simulator reproduces the logistics of the operations from major hubs, to local Hub and HQs establishment, force deployment, transportations and material handling. The simulator considers using both naval cargos, aerial solutions including helicopters and planes as well as ground vehicles (Bruzzone et al. 2002b, 2017c). The delivery and deployment could be carried out by conventional deliveries and/or air drops. Entities simulated include military units, NGO, paramilitary, civilians, IDPs, Refugees, Local Authorities, etc.

The Intelligent Agents drive the entities and the people on the scenario based on their perception and considering human factors (e.g. stress, fatigue, fear, hunger, etc)

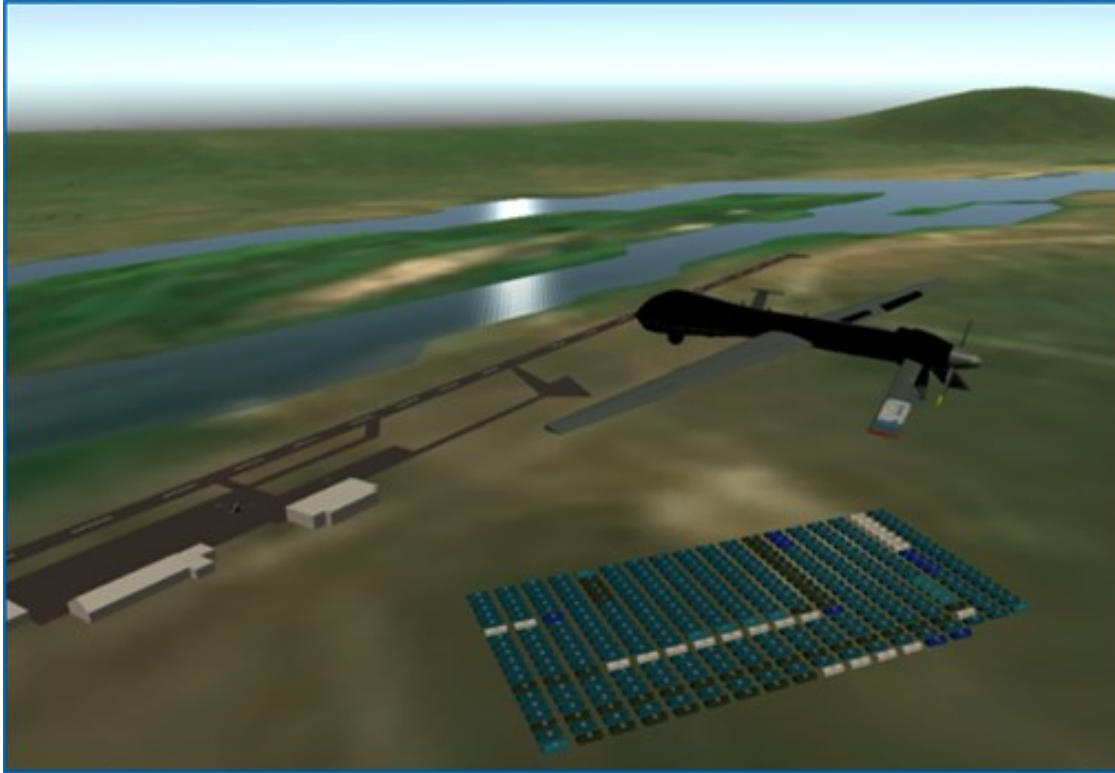


Figure 4.26: DIES IRAE VIC: Synthetic Environment and Virtual Simulation

In DIES IRAE VIC the IA are in charge of applying the disaster relief plan based on logic sequence, available resources and dynamic evolution of the boundary conditions (e.g. security, weather, availability of resources). The population model considers the Interest Groups and People Objects (Bruzzzone 2013b). Indeed, the Interest Groups represent the different entities on the area and are interconnected by relationships identifying the intensity and type of their mutual attitude through multiple parameters.

Vice versa, each People Object reproduces a small group and its basic characterization including, among others:

- Gender
- Age
- Health Status
- Education
- Social Status
- Religion
- Ethnicity
- Tribe
- Political Orientation
- Stress
- Fear
- Fatigue
- Aggressiveness
- Resilience
- Trustiness

The People Objects are interconnected by their social network through compatibility algorithms and are connected with the Interest Groups as well. They are also associated with the terrain, if appropriate, respecting geosocial characteristics of the area.



Figure 4. 27: South Sudan Localization

The DIES IRAE VIS allows to virtually reproduce these operations both in terms of observation of scenario evolution within the virtual simulator or interactive control of specific equipment as a Serious Game (e.g. conducting an Air Drop, Delivery on an Air Strip, Reorganizing a Camp). An example of the interface is proposed in figure 4.26.

In order to evaluate the capabilities of DIES IRAE Simulation the authors decided to identify a scenario that could be used for the VV&A.

Based on a preliminary analysis of the existing situation, it resulted that the current South Sudan situation could be an inspiring scenario. Indeed, this reality represent a good example of modern crisis of the African continent after colonialism (Chatterjee 1993).

All African countries became independent in the second half of the 20th century. Although some countries became independent in the 1950s, most of Africa was decolonized during the 1960s.

However, after independence, some of these states found themselves powerless against armed conflicts requiring trained, combat seasoned forces and quality equipment (Ciekawy 1998).

Some turned to UN requesting intervention to support local forces in internal or inter-state conflicts to ensure regional stability. In this context, International Coalitions started to conduct overseas operations (Murphy 1996).

During the 2000s, the European Union became a full-scale actor for peace and security in Africa, developing the African component of the European security and defence policy from 2005 (Smith 2015).

Humanitarian assistance provided in recent years by non-governmental organizations (NGOs) in Africa has saved hundreds of thousands of lives; moreover, NGOs now collaborate with military forces in the delivery of humanitarian supplies.

The above-mentioned elements raise questions about the diverse range of operations and their capacity to address various needs (Pettit et al 2005).

Indeed, the use of military forces to support humanitarian operations has grown along last decades to be almost commonplace in today's world.

A key objective must be to define workable doctrines for this involvement and to make commanding officers aware of the social, political and economic impact they may have with different modalities of commitment (Caunhye et al.2012).

Some of the questions to be addressed are proposed hereafter:

- How are military forces and their assets deployed in humanitarian operations?
- Which deployment models are commonly used, and which doctrines need to be developed for each?
- Are the current roles effective and, if not, which roles are effective?
- How can military units be committed to peacekeeping or humanitarian operations without violating their neutrality?
- How can foreign military commanders best coordinate with civil relief authorities?

Based on the previous consideration, the proposed scenario proposed is South Sudan and its currently acute humanitarian crisis. In this country, emergency level of food insecurity is evident due to the on-going conflict (Pantuliano et al. 2008; Rai et al. 2012; Johnson 2014; UNHCR 2015; Kegley et al. 2015; Zambakari 2015).

Despite progress in the political situation following the formation of the Transitional Government of National Unity, the economic decline, depreciation of the South Sudanese

pound and the sporadic violence continue to have a significant impact on the humanitarian needs within the country.

Clashes between government forces and an armed group are reported all around the country. The rapid decline in the food security situation and distribution raises fears an escalation of the crisis.

In this chaotic situation United Nations Security Council is:

1. Expressing its deep concern about the ongoing escalation of insecurity and the continued rise in violence in South Sudan as well as the persisting political impasse in the country,
2. Condemning strongly the increased cases of human rights violations and abuses and underscoring its deep concerns on further decline in the food security and nutritional status of the population,
3. Welcoming the decision of the Secretary-General to deploy a military contingent in Western Bahr el Ghazal (WBeG) region to support population and NGOs in the area.

South Sudan, with a surface area of 93,900 square km is one of the largest among the other regions; according to the last population census has an estimated 333,431 inhabitants, with Christians and Muslims being the largest groups.

The source of livelihood for its inhabitants was subsistence farming, supplemented by small-scale cattle rearing and petty trading.

There were tensions triggered by boundary disputes now escalated into conflict due to rivalries over grazing land and ethnic/religious reasons. The situation is presently evolved in

a humanitarian crisis, in particularly in Wau and Jur River counties refugees continue to arrive spontaneously.

The Contingent planned for testing the simulator is based on the organization proposed in Figure 4.28 and requires the deployment of 1,450 people.

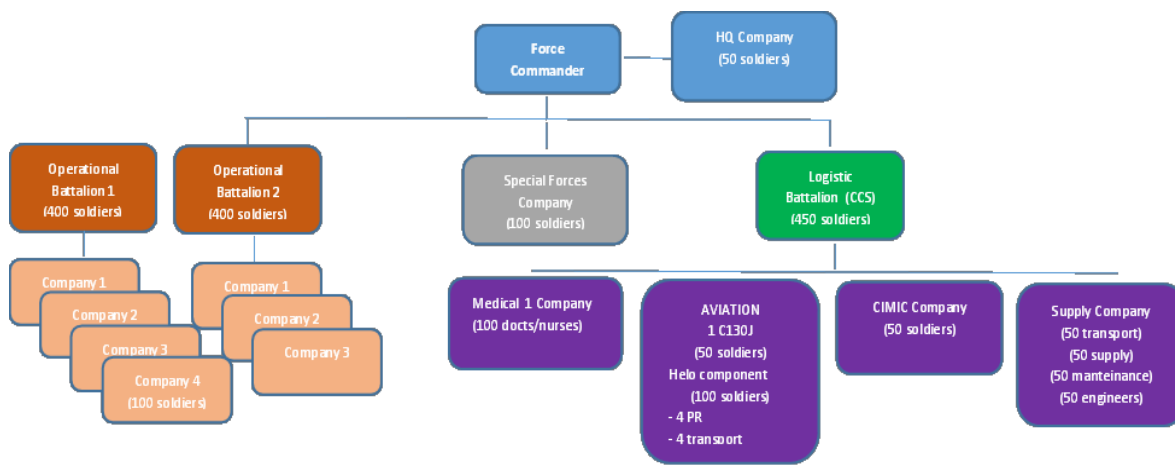


Figure 4.28: Contingency Structure

The organization includes C130J Planes and UH-60 Helicopters as well as UAV (Unmanned Aerial Vehicle) and ground vehicles.

With the population suffering from a humanitarian crisis that caused several thousand and to support the U.N.'s Food and Agriculture Organization (FAO), a multinational military contingent is planned to be deployed under UN mandate aims in a humanitarian operation to establish protected zones in South Sudan. The aim is also to interpose between two warring parties and to control areas.

4 Other Experiences

The mission core is to perform a stability operation to restore a peaceful situation in order to supply, maintenance operations, deployment and distribution, health service support (HSS), engineering and logistic services.

The following phases have been planned in the simulator:

1. Deployment: Port Operations is Djibouti; Airport of operation is Djibouti. Port and airport capacity determine the flow of materiel into area of operations.
2. Transports: Air transport permits the rapid deployment and movement of personnel and cargo to, from and within area of operations and provides tactical mobility for all mission elements.
3. Mission: support to enable access for humanitarian personnel and relief goods, followed by medical operations and the provision of material relief goods (such as tents, clean water and food supplies).

The Multinational Logistic Planning is expected to follow the following schedule, the simulator checks the feasibility to respect the timelines.

Day X	contingent arrive in Djibouti
X+1	SF, 1 and 2 Company (1 BTG) and Engineers Company in OA (operation area): secure area and prepare logistic (1 flight C1230J – 1 flight transport Helo);

4 Other Experiences

X+2	3 and 4 Company (1 BTG) and HQ troops in OA: complete secure area and establish C2 capability (1 flight C1230J – 1 flight transport Helo);
X+3	CIMIC Company
X+5	Medical Company
X+7	FOC (full operational capability)
X+30	Sustainability

In this context, the following MEL/MIL are proposed to be considered and evaluated by using simulation:

MEL/MIL 1: Transport

In a deteriorated road network, military supply (Class I subsistence/food) convoys, the greatest logistics challenge depends on the number of transportation nodes and conveyance modes involved:

- Scarcity of vehicles (especially those capable of carrying refrigerated cargo)
- Limited space container area

Increase in fuel consumption (Class III petroleum, oils, and lubricants):

- Difficulties to maintain scheduled transport
- Self-sustainment just vouched for a reduced time

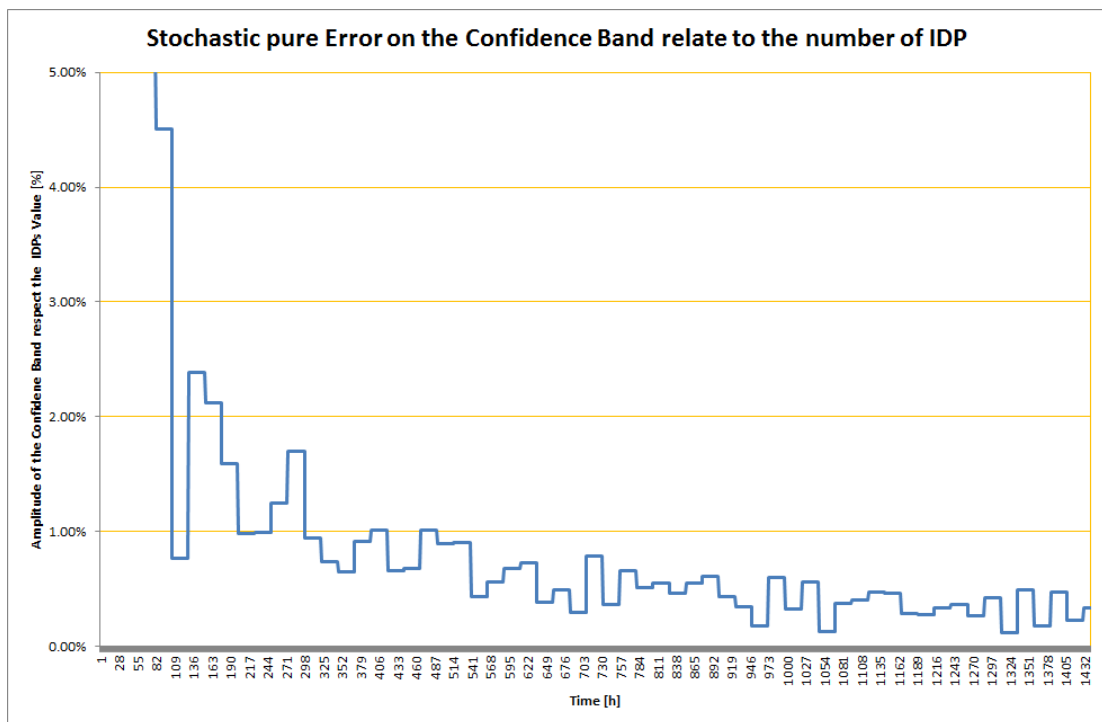


Figure 4.29: Experimental Error

MEL/MIL 2: Hospital

Theatre Hospitalization Capability delivers health support required to medically sustain forces in the JOA. Hospitalization capabilities in the JOA deploy as modules:

- Lack of full modules capabilities reduce role 2 availability and operational readiness of critical equipment (Class VIII major end item)
- According to medical plan, three technicians and one laboratory assistant must perform mass inoculation and provide logistical support for the local authorities
-

MEL/MIL 3: Helo

The theatre logistic picture suffered lack of critical information about the logistic situation, sustainability and availability of key equipment:

- Joint Force Logistic Component Headquarters must coordinate a range of logistic support activities to support helo component (UH60 Helicopters)
- Lack of sustainability and availability of key equipment impact scheduled mission

MEL/MIL 3: Evacuation

Local situation is volatile, unstable and likely to deteriorate rapidly:

- Must be able to achieve crowd control without jeopardizing the logistic support and make it easier to carry out the operation,
- A back-and-forth organization reducing the operation's logistical constraints is necessary to plan helicopter rotations in the space of 1 day.

The formal and static Verification and Validation of the Models has been conducted with Subject Matter Experts applying different techniques (e.g. face validation, flow charts). The use of DIES IRAE Simulation allowed to present dynamic results and graphics to the SME to proceed in the validation of the conceptual models and experimental results. The authors are currently implementing the MEL/MIL and preliminary experimental results have been carried out in order to support the VV&A based on Design of Experiments (Montgomery 2008). In figure CVC it is proposed the analysis of the experimental error due to the pure

influence of stochastic component (Longo et al. 2008). The graph proposes the amplitude of the confidence band respect the number of the IDPs.

4.5 Scuba Diver

Scuba Diver is a project created in collaboration with the company Dark Energy Software s.r.l. regarding a possible scenario of attack on a port. The idea of developing the software was conceived after the realization of a Serious Game called Platform Defend developed by the same company and based on the procedural training in the defence of off-shore platforms.



Figure 4.30: Platform Defend software scenario

Scuba Diver is a Serious Game that recreates a port scenario in which a diver tries to reach the moored boats to install an explosive device. Man, to reach his destination, must cross a stretch of sea equipped with surveillance sensors.



Figure 4. 31: Representation on the Scuba Diver of the sub

Two different versions of the software have been created: in one the user plays the role of the defender, in the other of the attacker.

In the first variant the user initially has to choose the place and the number of detecting sensors to be put in the scenario, through a tactical map.

Once the detection systems are in place, you can start the simulation and move freely in the scenario. The goal is to be able to identify the diver that starting from a random point far from the coast, approaching the coast.

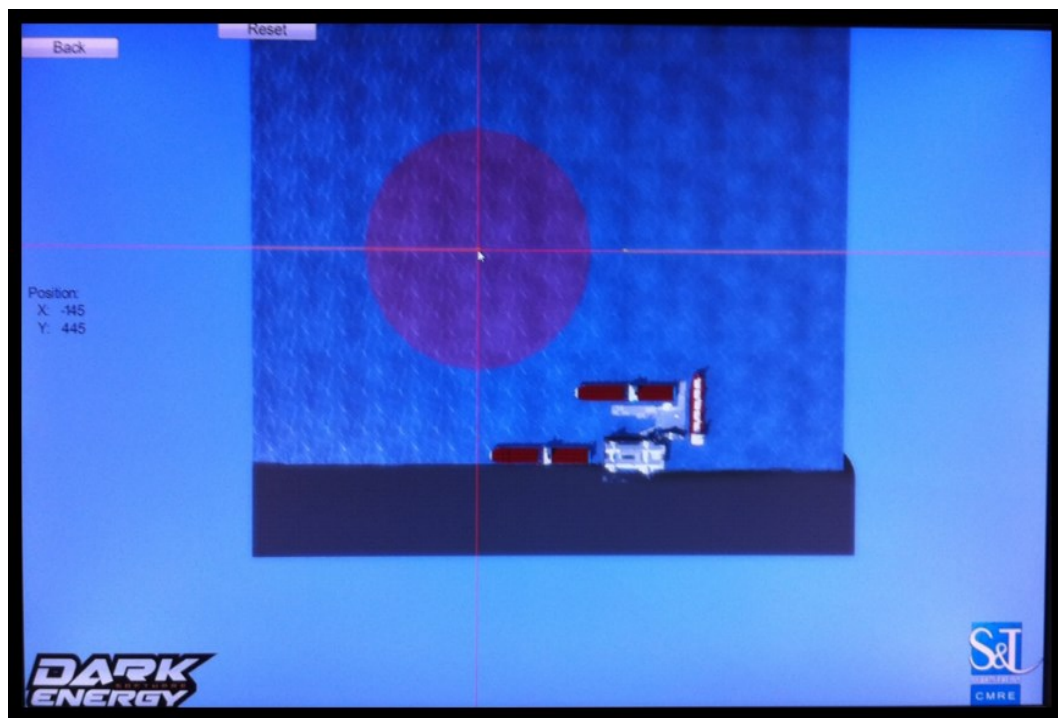


Figure 4. 32: Tactical map of the scenario in Scuba Diver

The positioned sensors have a decisive role in the search for man because, if the latter were to pass in an area guarded by them, they would indicate the direction in which the threat is located with respect to them.

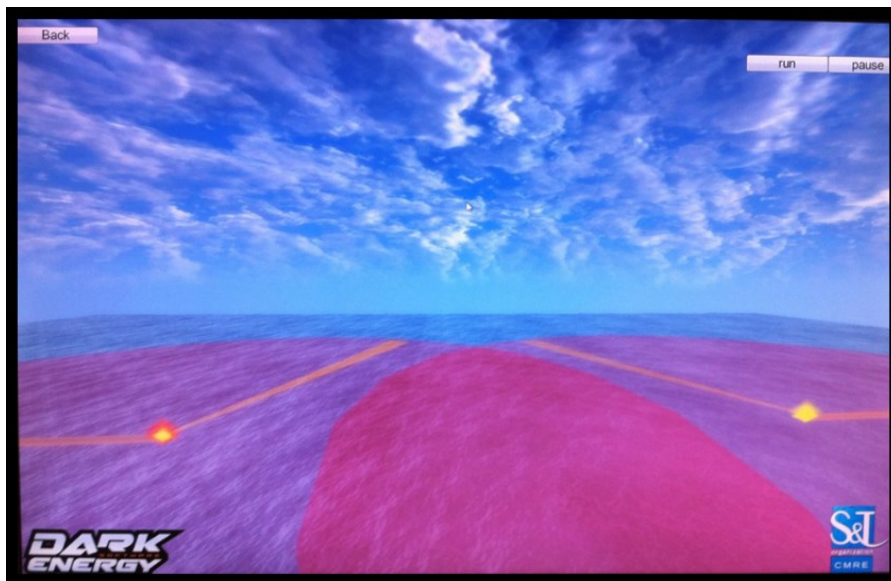


Figure 4.33: Detection of the sub by sensors in Scuba Diver

In the second version, the scenario is slightly different: the user controls the sub and must arrive at a pre-set point in the port. Along the way there are scattered buoys that detect the presence of possible threats.



Figure 4.34: Scenario of the second version of Scuba Diver.

If the player is detected by such devices, an AUV is activated and goes in pursuit of the threat. If the drone reaches the sub, the simulation is interrupted, and a failed mission message is displayed.



Figure 4. 35: Scuba Diver unsuccessful mission message

So, Scuba Diver is a Serious Game designed to support personnel training on a tactical-strategic level

5 Conclusions

The project presented in this thesis work is the result of the researches performed by the author within the Simulation Team during the Ph.D. period at Genoa University.

The main objective of the study carried out during the Ph.D. was the develop of an innovative interoperable environment that includes many different models to simulate complex heterogeneous networks and entities with their interactions & operations involving all the Extended Maritime Framework (Sea Surface, Air, Coast & Land, Underwater, Space and Cyber Space).

In order to obtain all the needed competences to achieve the objective, the author performed several researches focused on the use of Interoperable Simulation in different applications and he was involved several parallel projects within Simulation Team. The obtained results underline the importance of M&S in the investigation of the news problem such us Hybrid Warfare, possible uses of drones, integration of autonomous systems with the actual technology etc.

The Intelligent Agents developed by Simulation Team was a fundamental point of start for the develop of the simulator JESSI. Indeed, IA were used to reproduce social networks, human factors, vehicles & autonomous system behaviour in the virtual environment. JESSI addresses industrial, defence and homeland security complex Scenarios over multiple domains and running on multiple platforms (e.g. IoT, cloud, computers) being ready to be federated with other models & simulators. JESSI studies, by virtual experimentation,

strategies, policies & technological alternatives for improving overall efficiency, effectiveness and reliability. It is very interesting for its versatility and for its ability to investigate complex scenarios in the marine environment.

The interoperability of JESSI is guaranteed by the use of HLA that, as previously explained, is an international standard. Fundamental for integration of this technology with the simulator, were the experiences carried out with the Simulation Team in the SEE events and SIMCJOH project. Indeed, during these activities the author had the possibility to learn, understand and use intensively the HLA and he obtained the best capabilities to achieve this important objective. With the HLA, JESSI can be federate with other simulators in order to further extend the possible applications of the virtual environment and further increase the detail level of the simulation federating with more specific and sophisticated simulators.

The Simulation Team is currently studying possible extensions to employ JESSI in its research works. Undoubtedly, it could be used to define innovative technological solutions that involve training and use of drones. In fact, with adequate modifications, it could become an excellent Serious Game to train personnel in emergency critical scenarios both operationally and tactically. Moreover, as already seen, it is useful for training in drone driving and could be integrated with real unmanned vehicles used in operational missions reproducing the real scenario in which they are found. In this way, it could help the guide if they are in remote control, as well as the ability to better monitor the behaviour of these new technologies and help in decision making.

5 Conclusions

JESSI finally resulted a valid tool to study the problem of the vulnerability of on-shore and offshore critical infrastructures; these could seriously consider the use of new technologies to greatly decrease their vulnerabilities and protect themselves against possible economic and social disasters. The developed project would then be able to estimate the positive contribution of the autonomous vehicles that would lead to such facilities, and also help to devise the best strategies in order to use them successfully. They could also use this software to connect it to the drones used in their security plan and then monitor them constantly knowing their position and their movements.

In conclusion, the proposed environment was completed and experimented confirming the validity of the proposed approach; the scenario developed include pretty advanced scenarios as confirmation of the flexibility achieved. The key of success was based on availability of previous researches used for creating a new multiple advanced maritime architecture environment and the approach based on multi resolution meta-models to be integrated based on specific simulation need.

There is no doubt that this project may have additional future developments, some of which would lead to be used in areas not yet identified at the time of conception.

Currently the Simulation Team of University of Genoa is working on the improvement and the development of further extensions of these simulators.

Bibliography

- AA. VV., “I terrorismi contemporanei”, *Stratetique*, n.ri 2-3, 1997.
- Abrahams A., Boisot M., Bharathy Gnana (2005) “Simulating the Knowledge Transfer Dilemma: Lessons for Security and Counter-Terrorism”, *Proceedings of SCSC*, CherryHills, NJ, July
- Altawy, R., & Youssef, A. M. (2016) "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey" *ACM Transactions on Cyber-Physical Systems*, 1(2), 7
- American Institute of Steel Construction [AISC], Inc., Chicago, Illinois, USA.
- American Petroleum Institute [API], 1996. (RP-2A 20th edition, and Supplement 1, dated December 1996.
- Amico Vince, Guha R., Bruzzone A.G. (2000) "Critical Issues in Simulation", *Proceedings of Summer Computer Simulation Conference*, Vancouver, July
- Anagnostou, A., Nouman, A., Taylor, S.J.E., 2013. Distributed hybrid agent-based discrete event emergency medical services simulation, in: *2013 Winter Simulations Conference (WSC)*. IEEE, pp. 1625–1636. doi:10.1109/WSC.2013.6721545
- Anderson, J., Chaturvedi, A., & Cibulskis, M. (2007) “Simulation Tools for Developing Policies for Complex Systems: Modeling the Health and Safety of Refugee Communities”, *Health Care Management Science*, 10(4), 331-339.
- Apvrille, L., Roudier, Y., & Tanzi, T. J. (2015) "Autonomous drones for disasters management: Safety and security verifications", *Proc. 1st IEEE URSI Atlantic*, May

- A Valle, L., Bruzzone, A. G., Copello, F., Guerci, A., & Bartoletti, P. (1999) "Epidemic diffusion simulation relative to movements of a population that acts on the territory: bio-dynamic comments and evaluations" Proc. of WMC99.
- A Valle, L., Bruzzone, A. G., Copello, F., & Guerci, A. (1996) "Determination and Quantification of Functional Parameters Relative to Contamination Vector Logic in an Epidemic Simulation" Proceedings of ESS, Vol. 96, pp. 24-26
- B. Mller, THE HLA TUTORIAL v1.0, Pitch Technologies, Sweden, 2013.
- Bachmann, S. D. O. V., & Gunneriusson, H. (2014) "Terrorism and cyber attacks as hybrid threats: defining a comprehensive approach for countering 21st century threats to global risk and security", The Journal on Terrorism and Security Analysis.
- Baker B.D. (2015) "Hybrid Warfare With Chinese Characteristics", The Diplomat, September
- 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", Defence Modelling and Simulation Office, Alexandria, VA, November
- Balci, O. (1998). Verification, Validation and Testing. in Handbook of Simulation: Principles, Advances,
- Banks J. (1998) "Handbook of Simulation: Principles, Methodology, Advances, Applications, and Practice", John Wiley and Sons, NYC
- Banks, J., Carson, J.S., Nelson, B.L., Nicol, D.M., 2010. Discrete-Event System Simulation. Pearson.

- Been, R., Hughes, D.T., Potter, J.R., Strode, C., (2010). Cooperative Anti-Submarine Warfare at NURC Moving Towards a Net-Centric Capability, in: Proceedings of Oceans. Sidney NSW Australia.
- Been, R., Hughes, D. T., & Vermeij, A. (2008). Heterogeneous underwater networks for ASW: technology and techniques. Proc. UDT-Europe.
- Been, R., Jespers, S., Coraluppi, S., Carthel, C., Wathelet, A., Strode, C., Vermeij, A., 2007. Multistatic Sonar: A Road to a Maritime Network Enabled Capability, in: Proceedings of UDT. Naples, Italy.
- Bellamy, A. J., & Williams, P. D. (2011) “The New Politics of Protection? Côte d'Ivoire, Libya and the Responsibility to Protect”, *International Affairs*, 87(4), 825-850
- Benney R., Henry M., Lafond K., Meloni A., Patel S. (2009). "DoD New JPADS Programs & NATO Activities", Proceedings of 20th AIAA Aerodynamic Decelerator Systems Technology Conf. and Seminar, Seattle, WA, May 4-7
- Boer, C.A., de Bruin, A., Verbraeck, A., 2008. Distributed simulation in industry - a survey Part 3 - the HLA standard in industry, in: 2008 Winter Simulation Conference. IEEE, pp. 1094–1102.
- Bonante L., “Le sfide e i misteri del terrorismo”, *Relazioni Internazionali*, n.ro 1, Giugno 1986
- Bonante L., “Terrorismo internazionale”, *XX Secolo*, Prato (PO), Giunti, September 1994.

- Bossomaier T, A.G. Bruzzone, M. Massei, D. Newth, J. Rosen (2009) “Pandemic dynamic object and reactive agents”, Int. Workshop on Modelling and Applied Simulation, Puerto de la Cruz, Tenerife
- Bossomaier T., Green G.D. (2000) “Complex Systems”, Cambridge University Press, Cambridge
- Brauzzi A., “L’Europa ed il terrorismo mediorientale”, Rivista marittima, n.ro 1, 1987.
- Bruzzone A.G. (2018) “MS2G as Pillar for Developing Strategic Engineering as a New Discipline for Complex Problem Solving”, Keynote Speech at I3M, Budapest, September
- Bruzzone A.G., Massei M., Sinelshchikov K., Di Matteo R. (2018a) "Population behaviour, social networks, transportations, infrastructures, industrial and urban simulation", Proceedings of EMSS, Budapest, September
- Bruzzone A.G., Di Matteo R., Sinelshchikov K. (2018b) "Strategic Engineering and Innovative Modelling Paradigms", Proc.of WAMS, Praha, October
- Bruzzone A.G., Massei M., Di Matteo R., Agresta M. (2018c) "Simulation of crisis affecting critical Infrastructures and industrial plants", Proc. of DHSS, Budapest, September
- Bruzzone, A. G., Massei, M., Cianci, R., de Gloria, A., & Sciomachen (2018d) A New Educational Programs based on M&S for Strategic Engineering. In Workshop on Applied Modelling & Simulation, Praha, October

- Bruzzone A.G., (2017) "Smart Simulation: Intelligent Agents, Simulation and Serious Games as enablers for Creating New Solutions in Engineering, Industry and Service of the Society. Keynote Speech at International Top-level Forum on Engineering Science and Technology Development Strategy- Artificial intelligence and simulation, Hangzhou, China
- Bruzzone A.G., Massei, M. (2017a) "Simulation-Based Military Training", in Guide to Simulation-Based Disciplines, Springer, pp. 315-361
- Bruzzone, A. G., Massei, M., Bella, P. D., Giorgi, M., & Cardelli, M. (2017b). Modelling within a synthetic environment the complex reality of mass migration. In Proceedings of the Agent-Directed Simulation Symposium, Society for Computer Simulation International, April
- Bruzzone A.G., Massei M., Agresta M., Sinelshchikov K., Di Matteo R. (2017c) "Agile Solutions & Data Analytics for Logistics Providers Based on Simulation", Proc. of I3M, Barcelona, September
- Bruzzone A.G., Cayirci E. (2016a) "T-REX About Hybrid Warfare" Invited speech, CAX Forum, Munich, Germany, September
- Bruzzone, A.G., Massei, M., Di Matteo, R., Maglione, G.L., (2016b) "Model Of An Advanced Planner For Interoperable Computer Interactive Simulation" proceedings of the 13th International Multidisciplinary Modelling & Simulation Multi-Conference - I3M 2016, Cyprus, September 26-28

- Bruzzone, A.G., Massei, M., Di Matteo. R., Agresta, M., Franzinetti, G., Porro, P. (2016c), “Modelling, Interoperable Simulation And Serious Games As An Innovative Approach For Disaster Relief”, proceedings of the 13th International Multidisciplinary Modelling & Simulation Multi-Conference - I3M 2016, Cyprus, September 26-28
- Bruzzone A.G., Massei M., Maglione G.L., Di Matteo R., Franzinetti G. (2016d) “Simulation of Manned & Autonomous Systems for Critical Infrastructure Protection”, Proc. of I3M, Larnaca, Cyprus, September
- Bruzzone A.G., Longo F., Massei M., Nicoletti L., Agresta M., Di Matteo R., Maglione G.L., Murino G., Antonio Padovano A. (2016e) “Disasters and Emergency Management in Chemical and Industrial Plants: Drones simulation for education & training”, Proc. of MESAS, Rome, June 15-16
- Bruzzone A.G., Massei M., Longo F., Cayirci E., di Bella P., Maglione G.L., Di Matteo R. (2016f) “Simulation Models for Hybrid Warfare and Population Simulation”, Proc. of NATO Symposium on Ready for the Predictable, Prepared for the Unexpected, M&S for Collective Defence in Hybrid Environments and Hybrid Conflicts, Bucharest, Romania, October 17-21
- Bruzzone A.G. (2015a) “Simulation of Autonomous Systems to Augment scenario Awareness and Capabilities in joint Cooperation within traditional assets to protect Marine, Littoral & Coastal Critical Infrastructure”, Maritime Security Initiative Project Proposal, CMRE, La Spezia, Italy

- Bruzzone A.G. (2015b) “Cyber Warfare Simulation”, Invited Speech and Demonstration, NATO CAX Forum, Vicenza, September-October
- Bruzzone A. G., Massei M., Tremori A., Camponeschi M., Nicoletti L., Di Matteo R., Franzinetti G. (2015a) “Distributed Virtual Simulation Supporting Defence Against Terrorism”, Proceedings of Harbour Maritime Modelling and Simulation Conference, Bergeggi Italy, 21-23 September.
- Bruzzone A. G., Massei M., Tremori A., Longo F., Crespo P. D., Franzinetti G., Oddone M., Carrera A., Camponeschi F., Dato L.,(2015b) “Autonomous System Simulation to Improve Scenario Awareness and Capabilities to Protect Marine, Off-Shore and Coastal Critical Infrastructure”, Proceedings of Harbour Maritime Modelling and Simulation Conference, Bergeggi Italy, 21-23 September.
- Bruzzone A.G., Crespo P.D., Tremori A., Massei M., Scapparone M., (2015c) “Interoperability and Performance Analysis of a Complex Marine Multidomain Simulation Based on High Level Architecture”, Proceedings of Harbour Maritime Modelling and Simulation Conference, Bergeggi Italy, 21-23 September.
- Bruzzone, A.G., Massei, M., Tremori A., Di Matteo R., Maglione G. L., (2015d) “Synthetic environment for interoperable advanced advanced marine simulation”, Proceedings of Harbour Maritime Modelling and Simulation Conference, Bergeggi Italy, 21-23 September.
- Bruzzone A.G., Massei M., Longo F., Nicoletti L., Di Matteo R., Maglione G.L., Agresta M. (2015e) “Intelligent agents & interoperable simulation for strategic

- decision making on multicoalition joint Operations”, Proc. Of DHSS2015, Bergeggi, Italy, September
- Bruzzone A.G. (2014) “Modelling and Simulation of Autonomous ASW capable vehicles to Augment surface and maritime air Capabilities”, CMRE ET Proposal, SP
 - Bruzzone A.G., Massei M., Agresta M., Poggi, S., Camponeschi F., Camponeschi M. (2014a) “Addressing Strategic Challenges on Mega Cities through MS2G”, Proc.of I3M2014, Bordeaux, France, September
 - Bruzzone A.G., Tremori A. (2014b) “Modelling and Simulation and Serious Games for Anti-Terrorism: Crowdsourcing within the SMEs Community”, CMRE Report, La Spezia, December
 - Bruzzone A.G., Frascio M., Longo F., Chiurco A., Zaroni L., Zavanella L., Fadda P., Fancello G., Falcone D., De Felice F., Carotenuto P. (2014c) “Disaster And Emergency Management Simulation In Industrial Plants” Proc. of EMSS, Bordeaux, France, September
 - Bruzzone, A., Massei, M., Longo, F., Poggi, S., Agresta, M., Bartolucci, C., & Nicoletti, L. (2014d) “Human behaviour simulation for complex scenarios based on intelligent agents”, Proceedings of the Annual Simulation Symposium, Tampa, FL, April
 - Bruzzone, A., Massei, M., Longo, F., Tremori, A., Nicoletti, L., Poggi, S., Bartolucci, C., Picco, E., Poggio, G., (2014e) “MS2G: Simulation as a Service for Data Mining

and Crowd Sourcing in Vulnerability Reduction” Proc. of WAMS, Istanbul, September

- Bruzzone A.G. (2013a) “New Challenges for Modelling & Simulation in Maritime Domain”, Keynote Speech at SpringSim2013, San Diego, CA, April
- Bruzzone, A. G. (2013b) “Intelligent agent-based simulation for supporting operational planning in country reconstruction”, International Journal of Simulation and Process Modelling, 8(2-3), 145-159.
- Bruzzone A.G., Fontaine J., Berni A., Brizzolara, S., Longo F., Dato L., Poggi S., Dallorto M. (2013c) "Simulating the marine domain as an extended framework for joint collaboration and completion among autonomous systems", Proc. of DHSS, Athens, Greece, September
- Bruzzone, A. G., & Longo, F. (2013b). 3D simulation as training tool in container terminals: The TRAINPORTS simulator. Journal of Manufacturing Systems, 32(1), 85-98.
- Bruzzone, A., Longo, F., & Tremori, A. (2013c). An interoperable simulation framework for protecting port as critical infrastructures. International Journal of System of Systems Engineering, 4(3-4), 243-260.
- Bruzzone, A.G., Berni, A., Fontaine, J.G., Cignoni, A., Massei, M., Tremori, A., Dallorto, M., Ferrando, A., (2013d) Virtual Framework for Testing/Experiencing Potential of Collaborative Autonomous Systems, in: Proceedings of I/ITSEC, Orlando. FL USA.

- Bruzzone, A.G., Merani, D., Massei, M., Tremori, A., Bartolucci, C., Ferrando, A., (2013e). Modelling cyber warfare in heterogeneous networks for protection of infrastructures and Operations, in: Proceedings of I3M. Athens, Greece.
- Bruzzone A.G., Marques H.C., Cantice G., Turi M. (2012a) "Innovative C2 and Simulation for Crowdsourcing as Force Multiplier", Proceedings of EMSS2012, Wien, September
- Bruzzone, A., Longo, F., Nicoletti, L., & Diaz, R. (2012b). 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 (p. 16) , March. Society for Computer Simulation International.
- Bruzzone A., Sokolowski J. (2012c) "Internally Displaced Persons (IDPs), Refugees & Immigrants as Agents and Models for Simulation Scenarios", Proc. of 7th NATO CAX Forum, Rome, Italy
- 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 Modelling and Simulation Symposium, EMSS2011 (Rome, Italy, September 12-14, pp.775-781

- Bruzzone, A.G., Tremori, A., Massei, M., (2011d), “Adding Smart to the Mix,” Modelling, Simulation & Training: the International Defence Training Journal, 3, 25-27.
- Bruzzone A.G., Tremori A., Merkurjev Y. (2011e) “Asymmetric Marine Warfare: Panopea A Piracy Simulator For Investigating New C2 Solutions”, Proc. of SCM MEMTS, pp. 32-49.
- Bruzzone, A. G., & Massei, M. (2010) “Intelligent agents for modelling country reconstruction operation”, Proceedings of the Third IASTED African Conference, Vol. 685, No. 052
- Bruzzone, A., Cunha, G., Elfrey, P., & Tremori, A. (2009a). Simulation for education in resource management in homeland security. In Proceedings of the Summer Computer Simulation Conference (pp. 231-238), Istanbul, Turkey, July
- Bruzzone, A. G., Cunha, G., & Tremori, A. (2009b). Intelligence and Security as a Framework for Applying Serious Games. Proceedings of Serixgame, Civitavecchia, November.
- Bruzzone, A. G. (2008). Net-centric supply chain management based on interoperable simulation. In Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on (pp. 708-715) , May. IEEE.

- Bruzzone A.G., Massei M. (2006) “Modelling for Estimating Impact on Road Transportation of Regional Emergencies & Disasters”, Proc.of HMS, Barcelona, Spain
- Bruzzone A.G., Sietta S. (2002a) "LESNEX: Lean Simulation Network of Excellence", Proceedings of Harbour Maritime Modelling and Simulation Conference, Bergeggi Italy, October 3-5, pp. 179-186
- Bruzzone, A.G., Orsoni, A., Mosca, R., Revetria, R. AI-based optimization for fleet management in maritime logistics (2002b) Winter Simulation Conference Proceedings, 2, pp. 1174-1182
- Bruzzone, A.G., (2002) “Simulation based VV&A methodology for HLA federations: an example from the Aerospace Industry” Proc. of Annual Simulation Symposium. pp. 80–85.
- Bürkle, A., Segor, F., Kollmann, M. (2011). "Towards autonomous micro uav swarms". Journal of intelligent & robotic systems, 61(1-4), pp. 339-353.
- Cai, L., Yang, Z., Yang, S. X., & Qu, H. (2013) “Modelling and Simulating of Risk Behaviours in Virtual Environments Based on Multi-Agent and Fuzzy Logic” International Journal of Advanced Robotic Systems”, 10.
- Calvi G., Martini M., “L’estremismo politico. Ricerche psicologiche sul terrorismo e sugli attentati radicali”, Milan, Franco Angeli Editore, 1982.
- Castelfranchi, C., & Conte, R. (1996) “The Dynamics of Dependence Networks And Power Relations In Open Multiagent Systems”, Proc. of COOP, June, pp. 12-14

- Cayirci, E., & Ghergherehchi, R. (2011) “Modelling Cyber Attacks and their Effects on Decision Process”, Proceedings of the Winter Simulation Conference, December, pp. 2632-2641
- Chailand G., “Il terrorismo è uno strumento di liberazione?”, Terrorism and Political Violence, vol. 1, january 1989, n.ro 1.
- Chatterjee, P. (1993) "The nation and its fragments: Colonial and postcolonial histories", Princeton University Press, NJ, USA
- Christman, W. L., Di Giovanni, F. C., & Wells II, L. (2015) “Global Knowledge Networking: Smart Strategies for Promoting Innovative Learning and Leader Development”, Defence Horizons, (80), 1
- Ciekawy, D., & Geschiere, P. (1998) "Containing Witchcraft: Conflicting Scenarios in Postcolonial Africa", African studies review, 41(03), 1-14
- Clarke, R., & Moses, L. B. (2014) “The Regulation of Civilian Drones' Impacts on Public Safety” Computer Law & Security Review, 30(3), 263-285
- Cline S. R., Yonah A., “Terrorismo la pista sovietica”, il mosaic, Trento, Reverdito Editore, September 1985, Traduzione di Addetti A.
- Cohen, J. E., Small, C., Mellinger, A., Gallup, J., Sachs, J., Vitousek, P. M., & Mooney, H. A. (1997). Estimates of coastal populations. Science, 278, 1209.
- Commissione delle Comunità Europee, “La protezione delle infrastrutture critiche nella lotta contro il terrorismo”, Comunicazione della Commissione al Consiglio e al Parlamento Europeo, Com (2004) 702 definitivo, Bruxelles, 20 Ottobre 2004.

- Dascalu M, Franti E, Stefan G: Artificial (1998) “Societies, a new paradigm for complex systems’ modelling”, Proc. Of SWISS’ 98. Sinaia, Romania, pp 62-67
- Davis J.R. Jr (2015) “Continued Evolution of Hybrid Threats”, The Three Sword Magazine, N. 28, pp.19-25
- De Grande, R.E., Almulla, M.A., Boukerche, A., (2012) Measuring and Analyzing Migration Delay for the Computational Load Balancing of Distributed Virtual Simulations. IEEE Trans. Instrum. Meas. 61, 3158–3174. doi:10.1109/TIM.2012.2205103
- De Grande, R.E., Boukerche, A., (2011) Predictive Dynamic Load Balancing for Large-Scale HLA-based Simulations, in: 2011 IEEE/ACM 15th International Symposium on Distributed Simulation and Real Time Applications. IEEE, pp. 4–11. doi:10.1109/DS-RT.2011.17
- De Grande, R.E., Boukerche, A., Ramadan, H.M.S., 2011. Measuring Communication Delay for Dynamic Balancing Strategies of Distributed Virtual Simulations. IEEE Trans. Instrum. Meas. 60, 3559–3569. doi:10.1109/TIM.2011.2161143
- Della Porta D., Pasquino G., “Terrorismo e violenza Politica”, Bologna, Società editrice il Mulino, 1983.
- Dewachi, O., Skelton, M., Nguyen, V. K., Fouad, F. M., Sitta, G. A., Maasri, Z., & Giacaman, R. (2014) “Changing Therapeutic Geographies of the Iraqi and Syrian Wars”, The Lancet, 383(9915)

- Di Bella P. (2015) “Present and Futures Scenarios and Challenges for M&S terms of Human Behaviour Modelling”, Invited Speech at I3M2015, Bergeggi, Italy, September
- Di Capua D., Di Matteo D., Trifanescu D., Buccilli G., Volpe D., Barbagiovanni M., Vella P., Fornaro C. (1998) “Il terrorismo navale. Rischi ed implicazioni nel Mediterraneo allargato”, Livorno, Italy, 13 July 1998.
- Di Donato (2017) “Intelligent Systems for Safety of Industrial Operators, the Role of Machines & Equipment Laboratories”, SISOM Workshop, Rome
- Di Matteo R. (2015) “Metodologie Innovative Basate sulla Simulazione Interoperabile e Virtuale per la Protezione di Infrastrutture Critiche e Impianti in Ambito Marino e Portuale”.
- DoD (2010) “TENA Architecture Reference Document, Version 2002 Review Edition”, DoD Technical Report
- DoD, (2009). DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A) [WWW Document]. DoDI 5000.61. URL http://www.msco.mil/documents/_1_500061p.pdf
- Doherty, P., & Rudol, P. (2007) "A UAV search and rescue scenario with human body detection and geolocalization", Proceedings of the Australian Conference on Artificial Intelligence, Vol. 4830, December, pp. 1-13
- Djellal, F., & Gallouj, F. (1999) “Services and the search for relevant innovation indicators: a review of national and international surveys”, Science and Public Policy, 26(4), pp. 218-232

- Elfrey P. R., Zacharewicz G., Ni M., Smackdown: Adventures in Simulation Standards, Eds. S. Jain, R.R. Creasey, J. Himmelspace, K.P. White, and M. Fu, Proceedings of the 2011 Winter Simulation Conference.
- Elfrey, P. (2006) “Imagine Moving Off the Planet”, Key Note Speech at Summer Computer Simulation Conference, Calgary, Alberta Canada, July
- Enders, W., & Sandler, T. (2002). Patterns of transnational terrorism, 1970–1999: alternative time-series estimates. *International Studies Quarterly*, 46(2), 145-165.
- F. Kuhl, R. Weatherly, J. Dahmann, “Creating Computer Simulation Systems: An Introduction to the High Level Architecture,” Prentice Hall, 1999.
- Ferber, J., & Gutknecht, O. (1998) “A meta-model for the analysis and design of organizations in multi-agent systems”, Proceedings of the IEEE International Conference on Multi Agent Systems, July, pp. 128-135)
- Floreano, D., & Wood, R. J. (2015) “Science, technology and the future of small autonomous drones”, *Nature*, 521(7553), 460
- Gardi, A., Sabatini, R., & Ramasamy, S. (2016) “Stand-off measurement of industrial air pollutant emissions from unmanned aircraft”, *Proc. of IEEE International Conference on Unmanned Aircraft Systems*, June , pp.1162-1171
- Gartner, S. S., & Segura, G. M. (2008) “All Politics Are still Local: The Iraq War and the 2006 Midterm Elections”, *Political Science & Politics*, 41(01)

- Gerasimov V. (2013) "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", Voenno-Promyshlennyy Kurier online, February 26
- Giribone, P., & Bruzzone, A. G. (1994, April). Man-made disasters- Chemical plant accidents. In SCS Simulation Multiconference, San Diego, CA(USA), 10-15 Apr 1994 (Vol. 1994, pp. 30-35).
- Gori U., "Una nuova forma di violenza, il terrorismo internazionale" Istrid, 401, 1996.
- Grande, R.E. De, Boukerche, A., 2010. Self-Adaptive Dynamic Load Balancing for Large-Scale HLA-Based Simulations, in: 2010 IEEE/ACM 14th International Symposium on Distributed Simulation and Real Time Applications. pp. 14–21.
- Grocholsky, B., Keller, J., Kumar, V., Pappas, G., (2006) "Cooperative air and ground surveillance", Robotics & Automation Magazine, IEEE, vol.13, no.3, September, pp.16-25
- Guo S., Bai F., Hu X (2011) "Simulation software as a service and Service-Oriented Simulation Experiment", Proceedings of IEEE International Conference on Information Reuse and Integration, August, pp.113-116
- Hill David (1996) "Object-Oriented Simulation", Addison Wesley, Reading MA
- Horst M., "Per la critica del terrorismo", Bari, De Donato, 1980.
- <http://www.irs.uji.es/uwsim/about>
- <http://www.vigilfuoco.it/asp/ReturnDocument.aspx?IdDocumento=2833>

- Hudson, R. A., & Majeska, M. (1999). The sociology and psychology of terrorism: Who becomes a terrorist and why? Washington, DC: Federal Research Division, Library of Congress, September.
- IEEE, 2015. IEEE Draft Standard for Distributed Interactive Simulation (DIS) - Communication Services and Profiles 1–42.
- IEEE, 2012. IEEE Standard for Distributed Interactive Simulation - Application Protocols.
- IEEE, 2010a. IEEE Standard for Modeling and Simulation (M\&S) High Level Architecture (HLA)-- Framework and Rules.
- IEEE, 2010b. IEEE Standard for Modeling and Simulation (M\&S) High Level Architecture (HLA)-- Object Model Template (OMT) Specification.
- IEEE Std 1516.1-2000, IEEE Standard for Modelling and Simulation (M\&S) High Level Architecture (HLA) Federate Interface Specification, September 2000.
- Ishiki, T., & Kumon, M. (2014) "A microphone array configuration for an auditory quadrotor helicopter system", Proc. IEEE International Symposium on Safety, Security, and Rescue Robotics, pp. 1-6
- James A., “Le finanze del terrorismo”, Milano, Suarco edizioni, 1984.
- Jans, W., Nissen, I., Gerdes, F., Sangfelt, E., Solberg, C. E., & van Walree, P. (2006) “UUV covert acoustic communications– preliminary results of the first sea experiment”, in Techniques and technologies for unmanned autonomous underwater

- vehicles– a dual use view”, RTO Workshop SCI-182/RWS-016, Eckernförde, Germany
- Jemkins M. B., “Terrorismo internazionale: l’altra guerra mondiale”, Il Mulino, anno XXXVI, n.ro 311, Maggio-Giugno, 1987.
 - Johnson, D. H. (2014) "Briefing: the crisis in South Sudan", African Affairs, 113(451), 300-309.
 - Johnson, T. H., & Mason, M. C. (2008). Understanding the Taliban and insurgency in Afghanistan. *Orbis*, 51(1), 71-89
 - Jones, D. (2005) “Power line inspection-a UAV concept”, Proc. of the IEE Forum on Autonomous Systems, Ref. No. 11271, November
 - Joo, J., Kim, N., Wysk, R. A., Rothrock, L., Son, Y. J., Oh, Y. G., & Lee, S. (2013) “Agent-based simulation of affordance-based human behaviours in emergency evacuation”. *Simulation Modelling Practice and Theory*, 32, 99-115.
 - K. Sadeghi, GAU J. Soc. & Appl. Sci., 2(4), 1-16, 2007 An Overview of Design, Analysis, Construction and Installation of Offshore Petroleum Platforms Suitable for Cyprus Oil/Gas Fields Kabir Sadeghi1 Girne American University, Department of Industrial Engineering, Mersin 10, Turkey
 - Kegley, C. W., & Blanton, S. L. (2015) "World Politics: Trend and Transformation, 2016-2017", Nelson Education, Scarborough, ON, Canada

- Kehoe, B., Patil, S., Abbeel, P., & Goldberg, K. (2015) "A survey of research on cloud robotics and automation", IEEE Transactions on automation science and engineering, 12(2), pp.398-409
- KEPCO Engineering Department, 2001 Work Report on data obtained from Khazar oceanography buoy and related CD electronic file, Winter of 2001.
- Kim, D. H., Kwon, S. W., Jung, S. W., Park, S., Park, J. W., & Seo, J. W. (2015) "A Study on Generation of 3D Model and Mesh Image of Excavation Work using UAV", Proceedings of the International Symposium on Automation and Robotics in Construction, Vol. 32, Vilnius, January
- Kleijnen, J. P. C. (2007). Design and Analysis of Simulation Experiments (International Series in Operations Research & Management Science).
- Knight, P., Corder, A., Liedel, R., Giddens, J., Drake, R., Jenkins, C., Agarwal, P., 2015. Evaluation of Run Time Infrastructure (RTI) Implementations, in: Huntsville Simulation Conference
- Kosarev AN, Yablonskaya EA, 1994. The Caspian Sea. Translated from Russian by Winstin AK, SPB Academic Publishing, The Hague.
- Kovacevic, M. S., Gavin, K., Oslakovic, I. S., & Bacic, M. (2016). "A new methodology for assessment of railway infrastructure condition". Transportation research procedia 14, pp. 1930-1939.
- Lacontre R., "Terrorismo e pirateria – La civiltà in piena rotta", Figaro Magazine, 10 Maggio, 1996.

- Lamb C., Stipanovich S. (2016) “Back to Basics on Hybrid Warfare in Europe A Lesson from the Balkans”, in *Joint Force Quarterly*, 81, March 29
- Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3), 49-51.
- Macal, C. M., & North, M. J. (2010) “Tutorial on agent-based modelling and simulation” *Journal of simulation*, 4(3), 151-162
- Lanman, J., Kemper, B., Rivera, J., & Krueger, C. (2011) “Employing the second generation software product-line for live training transformation”. *Proc. of I/ITSEC*, Orlando Nov.
- Laqueur W., “Riflessioni sul terrorismo”, *Foreign Affairs*, Autunno 1986.
- Łatek, M. M., Rizi, S. M. M., & Geller, A. (2013) “Verification through Calibration: an Approach and a Case Study of a Model of Conflict in Syria”, *Proceedings of the Winter Simulation Conference: Simulation*, Washington DC, USA, December
- Leão, D. T., Santos, M. B. G., Mello, M. C. A., & Morais, S. F. A. (2015) "Consideration of occupational risks in construction confined spaces in a brewery", *Occupational Safety & Hygiene III*, 343
- Lodge J., “Terrorismo e comunità europea: verso il 1992”, *Terrorism and Political Violence*, vol. 1, Gennaio, 1989, n.ro 1.
- Lojacono V. “Alto Adige Sudtirol”, *Tempo d’oggi*, Torino, Mursia, 1968.
- Longo, F., Chiurco, A., Musmanno, R., Nicoletti, L. (2014). Operative and procedural cooperative training in marine ports. *Journal of Computational Science*, DOI: 10.1016/j.jocs.2014.10.002 (in press).

- Longo F, Huerta A, Nicoletti L (2013). Performance Analysis of A Southern Mediterranean Seaport via Discrete Event Simulation. STROJNISKI VESTNIK, vol. 59, p. 517-525, ISSN: 0039-2480, doi: 10.5545/sv-jme.2013.963.
- Longo, F., Nicoletti, L., Chiurco, A. (2013). Cooperative training for ships and tugboats pilots based on interoperable simulation. Proceedings of the 25th European Modelling and Simulation Symposium, EMSS 2013, pp. 695-703.
- Longo F (2012). Supply chain security: an integrated framework for container terminal facilities. International Journal of Simulation & Process Modelling, vol. 7, p. 159-167, ISSN: 1740-2123, doi: 10.1504/IJSPM.2012.049154
- Longo F (2011). Advances of modeling and simulation in supply chain and industry. SIMULATION, vol. 87, p. 651-656, ISSN: 0037-5497, doi: 10.1177/0037549711418033.
- Longo F. (2010). Design And Integration Of The Containers Inspection Activities In The Container Terminal Operations. International Journal of Production Economics, vol. 125(2); p. 272-283, ISSN: 0925-5273, doi: 10.1016/j.ijpe.2010.01.026.
- Longo, F., Bruzzone, A.G. Modelling and simulation applied to security systems (2005) Summer Computer Simulation Conference 2005, SCSC 2005, Part of Summer Simulation Multiconference, SummerSim, pp. 183-188
- MAK, VR-Forces: The complete simulation toolkit, available from: <http://www.mak.com/products/simulate/vrforces.html>, accessed January 2014.

- Malinga, L., Le Roux, W.H., 2009. HLA RTI performance evaluation, in: Simulation Interoperability Standards Organization: 2009 SISO European Simulation Interoperability Workshop. pp. 1–6.
- Marszal A. (2013) “Syria: Putin warns West not to arm rebels who 'eat the organs' of their enemies”, The Telegraph, June 13, 16, 16:14 BST
- Maslow, A. H. (1943) “A theory of Human Motivation”, Psychological review, 50(4), 370.
- Massei, M., & Tremori, A. (2014) “Simulation of an urban environment by using intelligent agents within asymmetric scenarios for assessing alternative command and control network-centric maturity models”, The Journal of Defence Modelling and Simulation: Applications, Methodology, Technology, 11(2), 137-153.
- 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. doi:10.1504/IJSPM.2013.055206
- 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 Modelling and Simulation, St.Petersburg, Russia, May
- 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*. Los Angeles: Sage.
- McCuen, J. J. (2008). "Hybrid Wars", *Military Review*, 88 (2), 107
- McCurry Justin (2017) "Dying robots and failing hope: Fukushima clean-up falters six years after Tsunami", *The Guardian*, March 9
- McGlynn L. (1996) "In Pursuit of M&S Standards", *Proc.of ESS*, Genoa, October
- Ross, P., 2014. Comparison of High Level Architecture Run-time Infrastructure Wire Protocols – Part Two, in: *Fall Simulation Interoperability Workshop*. Orlando, United States, pp. 8–12.
- Ross, P., 2012. Comparison of High Level Architecture Run-Time Infrastructure Wire Protocols – Part One, in: *SimTecT*.
- 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 Modelling and Simulation: Principles of Good Practice", SCS, San Diego
- Merwaday, A., & Guvenc, I. (2015) "UAV assisted heterogeneous networks for public safety communications", *Proc. of IEEE Wireless Communications and Networking Conference Workshops*, March, pp. 329-334
- 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.

- Migliorino L., “La dichiarazione delle Nazioni Unite sulle misure per eliminare il terrorismo internazionale”, *Rivista di diritto internazionale*, n.ro 4, 1995.
- MIMOS (2002) “Panel on M&S” MIMOS Annual Meeting, Turin
- MMI, “Rapporto 1997”, *Supplemento a Panorama Difesa*, n.ro 152, Marzo 1998.
- Mobley, R. K. (2001) “Plant engineer's handbook”, Butterworth-Heinemann, Oxford, UK
- Møller, V., & Schlemmer, L. (1983) “Quality of Life in South Africa: Towards an Instrument for the Assessment of Quality of Life and Basic Needs”, *Social Indicators Research*, 12(3), 225-279
- Montgomery, D. C. (2000). *Design and Analysis of Experiments*, John Wiley & Sons, NYC
- Mosca, R., Bruzzone, A. G., & Costa, S. (1996). Simulation as a support for training personnel in security procedures. *SIMULATION SERIES*, 28, 251-255.
- Murphy, S. D. (1996). *Humanitarian intervention: the United Nations in an evolving world order*", University of Pennsylvania Press, Philadelphia, PA, USA
- Nano, G., & Derudi, M. (2013) "A critical analysis of techniques for the reconstruction of workers accidents", *Chemical Engineering*, 31
- NATO (2012) "NATO Modelling and Simulation Master Plan: Version 2.0", Technical Report NMSG, Document AC/323/NMSG(2012)-015

- NATO (1998) "NATO Modelling and Simulation Master Plan: Version 1.0", Technical Report, Document AC/323/(SGMS)D/2
- Naturalgas.org
- Netanyahu B., “Terorismo come l’Occidente può sconfiggerlo”, Milano, Arnaldo Mondadori Editore, 1986.
- Offshore-technology.com
- Ören T., Longo F., (2008). Emergence, anticipation and multisimulation: Bases for conflict simulation Proceedings of the 20th European Modelling and Simulation Symposium, EMSS 2008, pp. 546-555
- Palazzi, E., Caviglione, C., Reverberi, A.P., Fabiano, B. (2017) “A short-cut analytical model of hydrocarbon pool fire of different geometries, with enhanced view factor evaluation”, Process Safety and Environmental Protection, August
- Pantuliano, S., Buchanan-Smith, M., Murphy, P., & Mosel, I. (2008) "The Long Road Home: Opportunities and Obstacles to the Reintegration of IDPs and Refugees Returning to Southern Sudan and the Three Areas", Humanitarian Policy Group, Overseas Development Institute Report , London
- Parunak, H. V. D., Nielsen, P., Brueckner, S., & Alonso, R. (2006) “Hybrid multi-agent systems: integrating swarming and BDI agents”, In Engineering Self-Organising Systems, Springer Berlin Heidelberg, pp. 1-14
- Perros Y., “Le terrorisme maritime”, Defence Nationale, Novembre, 1985.

- Pettit, S. J., & Beresford, A. K. (2005) "Emergency Relief Logistics: an Evaluation of Military, Non-Military and Composite Response models", *International Journal of Logistics: Research and Applications*, 8(4), 313-331
- Pisano V., "Riflessioni sul terrorismo contemporaneo nell'area mediterranea", *Rivista Marittima*, Dicembre, 1996.
- Pitch Technologies, The simulation toolkit, available from: <http://www.pitch.se>, accessed January 2014.
- Pizzella, L. A. E. (2014) "Contributions to the Configuration of Fleets of Robots for Precision Agriculture", Thesis, Universidad Complutense, Madrid, Spain, May
- Prats, M.; Perez, J.; Fernandez, J.J.; Sanz, P.J., "An open source tool for simulation and supervision of underwater intervention missions", 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 2577-2582, 7-12 Oct. 2012
- Pulina, G., Canalis, C., Manni, C., Casula, A., Carta, L. A., & Camarda, I. (2016) "Using a GIS technology to plan an agroforestry sustainable system in Sardinia", *Journal of Agricultural Engineering*, 47(s1), 23-23.
- R.M. Fujimoto, "Time Management in the High Level Architecture." *Simulation*, Vol. 71, No. 6, pp. 388-400, 1998.
- Rai, R. K., Ramadhan, A. A., & Tulchinsky, T. H. (2012) "Prioritizing maternal and child health in independent South Sudan", *Maternal and Child Health Journal*, 16(6), 1139-1142

- Raybourn, E.M. (2012) “Beyond Serious Games: Transmedia for more Effective Training & Education”, Proc. DHSS2012, Rome, Italy
- Resnick, M. (1996) “StarLogo: An environment for decentralized modelling and decentralized thinking”, In ACM Conference Companion on Human Factors in Computing Systems, April, pp. 11-12
- Roberts A., “L’etica, il terrorismo, l’antiterrorismo”, Terrorism and Political Violence, vol. 1, Gennaio, 1989, n.ro 1.
- Rogers J. (2014) "Review of Maritime Transport 2014", Technical Report UNCTAD RMT 2014, Geneve, CH
- Ronzetti N., “Europa e il terrorismo internazionale”, Milano, Franco Angeli, 1990.
- Ronzitti N., “Un nuovo accordo contro il terrorismo internazionale: la Convenzione di Roma del 10.03.88 sulla repressione degli atti illeciti diretti contro la sicurezza della navigazione marittima”, Rivista di diritto internazionale, n.ro 2, 1988, pp. 379.
- Saaty, T. L., & Shang, J. S. (2011) “An Innovative Orders-of-Magnitude Approach to AHP-based Mutli-Criteria Decision Making: Prioritizing Divergent Intangible Humane Acts”, European Journal of Operational Research, 214(3), 703-715
- Sadeghi K, 1989. Design and Analysis of Marine Structures. Khajeh Nasirroddin Toosi University of Technology, Tehran, Iran, 456 pages [ISBN 964-93442-09].
- Sadeghi K, 2001. Coasts, Ports and Offshore Structures Engineering. Power and Water University of Technology, Tehran, Iran, 501 pages.

- Sadeghi K, 2004. An Analytical Approach to Predict Downtime in Caspian Sea for Installation Operations, 6th International Conference on Ports, Coasts and Marine Structures (ICOPMAS 2004), Tehran, Iran, Dec. 2004.
- Salvini, P. (2017) “Urban robotics: Towards responsible innovations for our cities”, Robotics and Autonomous Systems, Elsevier
- Sanchez-Lopez, J. L., Pestana, J., de la Puente, P., & Campoy, P. (2016) "A reliable open-source system architecture for the fast designing and prototyping of autonomous multi-uav systems: Simulation and experimentation", Journal of Intelligent & Robotic Systems, 84(1-4), pp.779-797
- Sapienza R., “Le risposte legali al terrorismo”, Relazioni internazionali, n.ro 11, 1990.
- Schmidt W. (2015) “Training below joint operational level - a JFTC activities insight”, Proc. of NATO CAX Forum, Vicenza, Italy, September-October
- SEE 2014 Federation Agreement
- Shafer, A.J., Benjamin, M.R., Leonard, J.J., Curcio, J., (2008) "Autonomous cooperation of heterogeneous platforms for sea-based search tasks", Oceans, , September 15-18, pp. 1-10
- Shonkwiler, R., & Thompson, M. (1986) “A validation study of a simulation model for common source epidemics” International Journal of bio-medical computing, 19(3), 175-194

- Siebert, S., & Teizer, J. (2014) "Mobile 3D mapping for surveying earthwork projects using an Unmanned Aerial Vehicle (UAV) system", *Automation in Construction*, 41, pp.1-14
- Siegfried, R., van den Berg, T. W., Cramp, A. J., & Huiskamp, W. (2014, January). M&S as a Service: Expectations and Challenges. In 2014 Fall Simulation Interoperability Workshops (SIW), 8-12 September 2014, Orlando, Florida, USA, 248-257. SISO.
- Simulation Exploration Experience, available from: <http://exploresimulation.com>, accessed May 2014.
- Smith, K. E. (2013) "European Union Foreign Policy in a Changing World" John Wiley & Sons, NYC, USA
- Smith, R. (2002, March). Counter terrorism simulation: a new breed of federation. In Proceedings of the Spring 2002 Simulation Interoperability Workshop.
- Spanu S., M. Bertolini, E. Bottani, G. Vignali, L. Di Donato, A. Ferraro, F. Longo (2016) "Feasibility study of an Augmented Reality application to enhance the operators' safety in the usage of a fruit extractor", *Proc. FoodOPS*, Larnaca, Cyprus, September 26-28
- Spillane, J. P., Oyedele, L. O., & Von Meding, J. (2012) "Confined site construction: An empirical analysis of factors impacting health and safety management", *Journal of Engineering, Design and Technology*, 10(3), pp.397-420
- Staszack C., "Terrorist attack USN Ship", *Proceedings*, Giugno 1986.

- Stilwell D. J., A. S. Gadre, C. A. Sylvester and C. J. Cannell (2004) “Design elements of a small low-cost autonomous underwater vehicle for field experiments in multi-vehicle coordination”, Proc. of the IEEE/OES Autonomous Underwater Vehicles, June, pp. 1-6
- Strode, C., Mourre, B., Rixen, M., 2012. Decision Support using MSTPA. Ocean Dyn. 62, 161–175.
- Sujit, P. B., Sousa, J., Pereira, F.L., (2009) "UAV and AUVs coordination for ocean exploration", Oceans - EUROPE, vol., no., pp.1,7, 11-14 May
- Takadama, K., Kawai, T., & Koyama, Y. (2007) “Can Agents Acquire Human-Like Behaviours in a Sequential Bargaining Game? – Comparison of Roth’s and Q-Learning Agents –”, in Multi-Agent-Based Simulation VII, Springer Berlin Heidelberg, pp. 156-171
- Takadama, K., Kawai, T., & Koyama, Y. (2008) “Micro-and macro-level validation in agent-based simulation: reproduction of human-like behaviours and thinking in a sequential bargaining game”, Journal of Artificial Societies and Social Simulation, 11(2), 9
- Tanner H. G. (2007a) “Switched UAV-UGV cooperation scheme for target detection”, IEEE International Conference on Robotics and Automation, Roma, Italy, April, pp. 3457-3462.
- Telford, B. (2012). Marine Corps Verification, VV&A Best Practices Guide.

- Tremori A., Baisini C., Enkvist T., Bruzzone A.G., Nyce J. M. (2012), "Intelligent Agents and Serious Games for the development of Contextual Sensitivity", Proceedings of AHFE 2012, San Francisco, US, July
- UNHCR (2015) "World at War: UNHCR Global Trends, Forced Displacement in 2014", UNHCR Report, Geneva, CH, June
- Uno, K., & Kashiyaama, K. (2008) "Development of Simulation System for the Disaster Evacuation based on Multi-Agent Model Using GIS", Tsinghua Science & Technology, Vol.13, October, pp.348-353.
- Valavanis, K. P., & Vachtsevanos, G. J. (2014) "Handbook of unmanned aerial vehicles", Springer Publishing Company, NYC
- Valpolini P., "Forze Speciali addestramento, compite ed armi", Supplemento a Panorama Difesa, n.ro 127, Dicembre 1995.
- Vego M., "La sicurezza del Mediterraneo", Rivista Marittima, Marzo, 1995.
- Veronese B., "Terrorismo in Mediterraneo", Rivista Marittima, Gennaio, 1986.
- Waite, Bill (2001) "M&S Professional Body-of Knowledge", Proc. of SCSC, Orlando Fl, July
- Wathelet, A., Vermeij, A., Strode, C., Justus, B., 2008. Track classification model for the Multistatic Tactical Planning Aid.
- Weitz, R. (2009) "China, Russia, and the Challenge to the Global Commons", Pacific Focus, 24(3), 271-297.

- Werker, E. (2007) “Refugee Camp Economies”, *Journal of Refugee Studies*, 20(3), 461-480
- Wilkinson P., “Le giustificazioni morali del terrorismo: un’improponibile difesa”, *Terrorism and Political Violence*, vol. 1, Gennaio, 1989, n.ro 1.
- Wintour P., Shaheen K. (2016) “Aleppo doctors appeal to US as violence continues during Russian *Pause*”, *The Guardian*, August 11, 14.24 BST
- www.nato.int
- Yonah A., “Il narcotraffico sponsorizzato d Stato e sottostato e le sue conseguenze”, *Relazione Stampa*, n.ro 2, 1996.
- Zambakari, C. (2015) "South Sudan and the Nation-building Project: Lessons and Challenges", in *National Democratic Reforms in Africa*, Springer, NYC, pp. 89-127
- Zhang M. (2016) “Large-scale Agent-based Social Simulation -A study on epidemic prediction and control”, PhD Thesis TU Delft, May