Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 232 (2024) 358–367

Procedia Computer Science

www.elsevier.com/locate/procedia

5th International Conference on Industry 4.0 and Smart Manufacturing

Promoting Safety, Security, Awareness and Productivity in Port Plants

Agostino G. Bruzzone[1,2*], Marina Massei[2], Kirill Sinelshichikov[3], Alberto De Paoli[2], Antonio Giovannetti[2], Francesco Longo[4], Gianfranco Fancello[5], Tommaso Vairo[1], Claudia Giliberti[6], Raffaele Mariconte[6]

[1]*University of Genova, Via Opera Pia 15, Genova, 16145, Italy*
[2]*Simulation Team, Via Magliotto 2, Savona, 17100, Italy*
[3]*Sim4Future, Via Trento 43, Genova, 16145, Italy*
[4]*Simulation Team, MSC-LES Università della Calabria, via Pietro Bucci, Arcavacata di Rende, 87036, Italy*
[5]*University of Cagliari DICAAR, Via Marengo 2,Cagliari,09121, Italy*
[6]*INAIL DIT, Piazzale Pastore 6 , Roma, 0144, Italy*

Abstract

This paper focuses on the combined use of eXtended Reality and Simulation to improve awareness and confidence in Container Terminal Operations by tailoring a Simulation Systems. Experimentation is proposed as example of the benefits achievable by training virtually operators in this context. The complexity of Port Operations creates a quite dangerous environment where the highly competitive business sector push to increase speed of operations and flows. In additions Port Terminals involve many actors that have to work and interoperate within a multi domain environment, outdoor all around the clock along the year in an almost all- weather context. Ports are growing getting encapsulated within major city that over time turn to be megacities creating additional challenges especially in terms of Safety and Security that require to operate with high performance in a safe framework. The automation obviously is crucial to further increase operations, therefore up to know the human component is still quite critical for many ancillary activities as well as often on main and secondary ones due to the flexibility and reliability required. This aspect could suggest a big potential for Industry 4.0 and its future evolution in this field as well as a continuous struggling with the very conservative mentality of Shipping and Maritime Operations relying in Systems able to operate in the previous mentioned conditions. Indeed, Training and Education are crucial to face these challenges and make it possible to introduce new technologies, policies and approaches in the very strategic field of Port Activities. The authors propose an experimentation carried out to demonstrate the potential to move training and education on virtual interactive solutions based on MS2G paradigm (Modeling, interoperable Simulation and Serious Games) by tailoring a Simulation System on specific criticalities

Keywords: Modeling & Simulation; IoT; Serious Games; Safety & Security; Port operations

* Corresponding author.
E-mail address: agostino@itim.unige.it

10.1016/j.procs.2024.01.035

1. Introduction

The operations in Ports are multiple and very different, therefore based on previous studies [1, 2] it resulted that respect on-shore activities some specific kinds of accidents result critical and could drastically affect the competitiveness of the different harbors. Due to these reasons the Simulation Team as Genoa, Cagliari & Calabria Universities jointly with Italian National Authorities (i.e. INAIL and ASL) developed an experimentation using Modeling and Simulation as well as Extended Reality to check effectiveness of MS2G in improving safety, security and productivity at ports. The goal was to quickly adapt a Simulation Solution for conducting experiments with operators not only in terms of training, but also in raising their awareness on risks, preventing exposure to dangerous conditions and even introduce them on the impact of new threats such as Cyber Security

Indeed, the digital transformation is the main automation providing major benefits in Port Logistics and Operation, up-to-now, but it introduces and increase also new vulnerabilities in terms of cyber security that along the years and considering geopolitical conditions are further evolving to higher level of criticality. These critical aspects are addon on existing risks dealing with the many interactions, high volume, heavy loads, dangerous material and extreme working conditions (outdoor, day/night, fog, rain, ice, wind, salty atmosphere, etc). In recent years, the maritime sector has witnessed an increase in cyber-attacks, targeting various components of port infrastructure. These attacks range from disrupting logistical operations to compromising sensitive data, thereby causing significant operational and financial losses. Furthermore, the rise of STRATCOM and Media Attacks has introduced a new dimension to the threat landscape. These attacks aim to manipulate information and public perception, thereby undermining trust and stability in port operations. This evolution of threats necessitates a paradigm shift in how port security is conceptualized and implemented. The concept of Hybrid Threats has become increasingly relevant in this context. Hybrid Threats encompass a blend of conventional and unconventional tactics, including cyber warfare, misinformation campaigns, and other non-kinetic forms of aggression. They represent a sophisticated strategy employed by state and non-state actors to exploit vulnerabilities in critical infrastructure, including ports. Addressing these Hybrid Threats requires an integrated approach that combines technological prowess with strategic insight.

Due to these reasons the authors propose in this paper a project, I4D3A2 (Immersive, Interoperable, Intuitive, Interactive virtual environment for Developing and Delivering training by simulation to operators in Dangerous Areas & Activities) devoted to combine Simulation and Extended Reality to address Safety and Productivity in Port Terminal. The I4D3A2 project, recognizing these evolving challenges, has been designed to leverage Simulation and Extended Reality to effectively train port personnel. By simulating realistic scenarios, the project aims to prepare operators for a range of eventualities, including cyber attacks and the complexities of Hybrid Warfare. The initiative, backed by leading academic institutions and national safety authorities, focuses on customizing the COYOTE simulator to cater to the specific needs and challenges of port operations. The Initiative has been co-sponsored by Genoa University, UNICAL and University of Cagliari and INAIL (The Italian National Authority for Safety and for Insurance Against Injuries at Work) and included tailoring COYOTE (Container terminal & Yard Operator simulator for Training & Education) developed by Simulation Team for this purpose and conducting an extensive experimentation with several port operators aiming to evaluate the capability to improve productivity, risk awareness and safety at work on specific kinds of operations that resulted based on historical data specifically critical where they tailored version. In the forthcoming sections, we delve into the methodology employed in the I4D3A2 project, the nuances of the tailored COYOTE simulator, and the insights gleaned from the experimentation with port operators. Through this exploration, we aim to demonstrate the transformative potential of integrating advanced simulation technologies in the realm of port operations, a sector pivotal to the global economy yet fraught with inherent risks.

Fig. 1: Yard of the Terminal Container in COYOTE Simulator

1.1. State of the Art

The multidisciplinary approach's advantages are best illustrated by the design of vital infrastructure. It is crucial in these situations to ensure that the system will function properly and that it will be resilient enough to withstand changes in its surroundings and to function even in the event of a variety of potential issues. To preserve productivity, safety, and competitiveness in the face of a high volume of concurrent operations, ports must adhere to strict quality standards and procedures. These analyses typically concentrate on particular nations or important ports [3]. These studies frequently concentrate on ship accidents brought on by collisions and other shipboard incidents, even when the ships are in ports [4, 5]. Severe weather conditions are a major safety concern as well, requiring very high standards and procedures to maintain productivity, safety, and competitiveness [6]. To develop more accurate and dependable prevention and mitigation countermeasures against maritime and port accidents, field data collection and processing through the creation of a globally structured database are essential [7].

Moreover, in addition to catastrophes and natural disasters, it's imperative to ensure adequate defense against hostile acts [8]. In fact, from ancient times, one of the most alluring targets for wars have been vital facilities like seaports. Although this component used to be mostly tied to physical interference and needed controls over people and vehicle access, it is now more frequent to be the target of numerous cyber-threats [9].

Since a decade ago, cyberattacks that cause disruptions to various services have become more frequent. Specifically, since the start of the conflict in Ukraine, the nation has seen blackouts brought on by cyberattacks [10]. Attacks on IT (Information Technologies) systems used in infrastructures have been common in recent years. One of the many well-known examples is the Stuxnet virus, which was employed in many forms to compromise Iran's nuclear program and other SCADA (Supervisory Control and Data Acquisition) systems [11]. The fact that cyberattacks are now frequently employed in military, political, and commercial conflicts is another significant factor. It can be quite challenging to identify the perpetrator of this kind of aggression, and it can be even more challenging to gather enough evidence to support a legal claim. In light of this, cyberattacks have emerged as a prevalent tactic in the context of hybrid warfare, wherein causing harm while concealing one's true identity is frequently the desired outcome [12].

It is crucial to first gain a better understanding of the nature of attacks in order to analyze what and how needs to be protected.

From the attacker's perspective, it is obvious that the best outcomes come from causing the enemy as much trouble as possible for an extended period of time. Given this, the ideal target should have an impact on the greatest number of people and be either easily damaged or difficult and costly to repair. Given that it is very difficult to inflict physical harm when dealing with cyber threats, it is far more common to interrupt services and prevent specific infrastructures from operating, whenever feasible. It is therefore essential to study real cases in depth, understand their causes and create methods of prevention and training and education [13, 14]. Not just protection software but tools that enable personnel to understand the complexity of a crisis.

1.2. Scenario

The scenario obviously concerns a port terminal and the activities carried out in this context with particular attention to human activities in the pipeline and along the docks near the containers. Thanks to the advice of port security experts, it was possible to identify two of the major port terminals of Genoa as the main environment for simulation: PSA terminal and Bettolo terminal. In this context, the attention is paid, following the analyses previously carried out, on the accidents in the pipeline due to collisions and load problems, varying the extent of the risk according to the danger of the goods transported. I4D3A2 designs and develops the models and the virtual world through the reproduction of the operations in the port terminal and in particular in the Yard, therefore reproduces thanks to the control given by the IA the movement and actions of the means of the square. The IAs also check the staff on the ground and the operations they lead, both the standard ones (E.G. Customs inspections, service to the refrigerated containers, maintenance to the vehicles and the square, handling support, refueling checks, changes, periodic inspections) that Those linked to particular cases (e.g. investigate a problem or a suspected situation). The scenario i4d3a2 involves people, cranes, vehicles, containers on the square and docks in compared to safety problems and takes into consideration realities corresponding to the port observers involved easily extensible to others. Particular attention is dedicated to those areas where operators' movements, often due to lack of experience or paradoxically for excessive security, are carried out near dangerous means, in which excessive noise and the lack of a clear view make the task difficult to execute. Of great importance are also those areas in which the movement and storage of dangerous goods takes place, where operations must be sequentially carried out according to a pre-established and clear process in order to reduce damage to people and objects due to human errors.

Building on the established scenario of port operations in the I4D3A2 project, the integration of IoT (Internet of Things) sensors and other cutting-edge technologies was a natural progression. This addition to the virtual environment not only enriched the simulation but also set the stage for a seamless transition into the world of cyber-threats. The virtual Container Terminal was augmented with a network of IoT sensors, replicating real-world scenarios where ports increasingly rely on these technologies for efficient operations. These sensors were embedded within the infrastructure to monitor various operational parameters like container movements, environmental conditions, and equipment status. This technological enhancement provided users with a more immersive and realistic experience in managing port operations. The integration of IoT technologies in the simulation presented an opportunity to explore the vulnerability of port operations to cyber-threats. As the reliance on networked technologies and automated systems grows in real-world ports, so does the risk of cyber-attacks. This aspect of the simulation allowed users to understand and experience the interplay between physical operations and cyber-security. With the virtual environment now equipped with IoT technologies, the training extended to encompass not just the physical aspects of port operations but also the cyber-security challenges. Users engaged in scenarios where they had to identify and respond to cyber-threats targeting the IoT infrastructure. This included dealing with issues like data breaches, system hacking, and the disruption of automated processes.

In the context of enhancing port security, especially against cyber threats, a well-defined scenario is crucial. This scenario must encompass several key characteristics to effectively address the challenges unique to port operations and their critical infrastructure:

- Targeting Critical Infrastructure: The scenario must focus on critical components of port infrastructure. This includes cargo handling systems, navigational aids, communication networks, and logistical support systems. These elements are vital for the smooth functioning of port operations and, if compromised, can lead to significant disruptions.

- Realistic IT Infrastructure Representation: A detailed and accurate representation of the port's IT infrastructure is essential. This includes network architectures, data storage systems, operational technology (OT) systems like SCADA (Supervisory Control and Data Acquisition), and IoT (Internet of Things) devices prevalent in modern ports. The simulation should mirror real-world complexities and interdependencies.
- Simulation of Hypothetical Threats and Tactics: The scenario must be capable of simulating a range of cyber-threats, from common malware attacks to sophisticated state-sponsored cyber-attacks. This includes phishing, ransomware attacks, DDoS (Distributed Denial of Service) attacks, and more covert tactics like APTs (Advanced Persistent Threats). The scenario should also account for the evolving nature of cyber threats in the maritime context.
- Countermeasure Deployment: It is critical to include the ability to test and deploy various countermeasures within the simulation. This ranges from basic cybersecurity hygiene practices to advanced defensive measures like intrusion detection systems, network segmentation, and incident response protocols. The scenario should allow for the evaluation of these countermeasures in real-time.
- Integration of Real-World and Cyber-Space Events: The scenario must address the mutual influence of events occurring in the physical realm of the port and in cyberspace. This includes understanding how a cyber-attack can have physical repercussions (such as disabling a crane or leaking sensitive location data of shipments) and how physical events (like natural disasters) can exacerbate cyber vulnerabilities.
- Adaptability and Extensibility: The developed model should be adaptable and easily modifiable to fit different port environments and emerging threats. This flexibility ensures that the simulation remains relevant and effective as new technologies and threat vectors emerge.

2. The Proposed Model

COYOTE architecture was designed to create a dynamic and interactive virtual environment that closely mimics real-world port operations. This architecture integrates various components, including Intelligent Agents (IA), IoT sensors, and simulation models, to provide a comprehensive training and research tool.

Intelligent Agents (IA)

- Functionality: In the virtual port environment, Intelligent Agents (IA) act as the primary drivers of activities. They control entities and characters, simulating realistic behaviors and responses in the port operations scenario.
- Roles: These agents perform a range of functions, from operating virtual machinery to managing logistical tasks and responding to environmental changes.
- Adaptability: IAs are programmed to adapt to changing scenarios, including reacting to user actions, environmental changes, and unexpected events within the simulation.

IoT Integration

- Sensor Network: The virtual environment incorporates a network of IoT sensors, providing real-time data on various operational aspects like container movement, equipment status, and environmental conditions.
- Data Utilization: This data is used by IAs to make decisions and respond to the simulation's evolving dynamics, enhancing the realism of the scenario.

Cyber-Threat Simulation

- Scenario Development: The model extends to include cyber-threat scenarios, where the virtual port's IoT infrastructure becomes vulnerable to cyber-attacks.
- Attack Types: These threats can range from data breaches, unauthorized access, to disruptions in automated processes.

Response Mechanisms

- Detection and Response: IAs are programmed to detect anomalies indicative of cyber-threats and execute predefined response protocols.

- Training Focus: Users interact with these scenarios to understand and learn how to identify, mitigate, and respond to cyber threats effectively.

Realism and Complexity

- Dynamic Threat Landscape: The model presents a constantly evolving threat landscape, challenging users to adapt their strategies and responses.
- Layered Challenges: Users face layered challenges, balancing the physical operational tasks with the need to maintain cyber-security.

In Figure 2 is depicted the General Architecture.

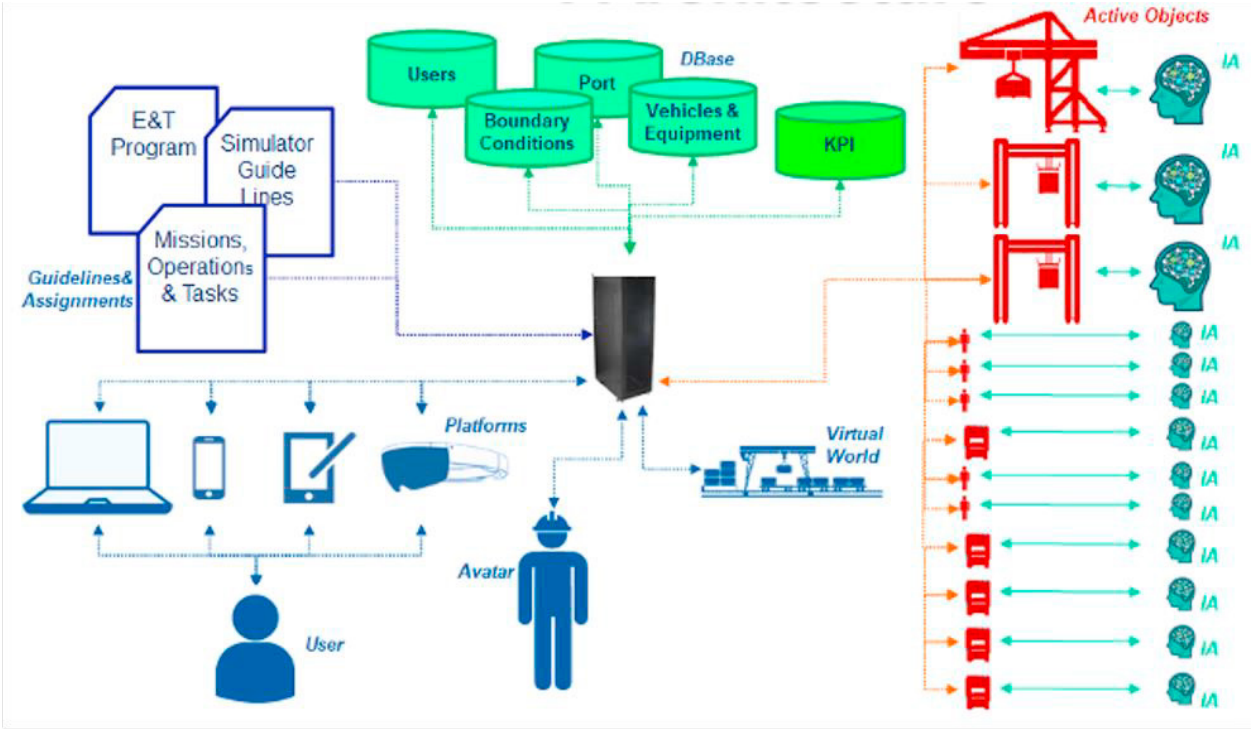


Fig. 2: General Architecture of the COYOTE

3. Users Tasks and Experimentation

Users are required to carry out typical port operations, like navigating vehicles, managing cargo, and coordinating logistics within the virtual port environment. Here are presented the measures of merit of the simulation.

Accuracy: Represents a measure of the quality of the work done by the operator and how much of the assigned work was completed correctly

Readiness: Represents a measure of how quickly the operator completed the assigned work

Correctness: Represents the ability to comply with rules and procedures and not make mistakes in performing the assigned task

Shrewdness: Represents the operator's prudence and attitude not to expose himself to risk or his ability to

reduce his exposure to risk while performing the task

Awareness: Represents a measure of the operator's awareness of the risks around him and his ability to limit them by taking appropriate actions in carrying out the assigned mission

The user must perform tasks within the port terminal while avoiding undue exposure to hazards associated with vehicle movement. Therefore, the user must move around the virtual environment looking for containers with the same code given in the list presented to him.

The Mission consists of three tasks i.e., a given check to be performed on three containers: the User has to find the three containers by searching the area based on the data received; each time he finds a container he has to indicate whether it has a small slick, medium slick, or is intact. In addition, he has to check the seal status. The KPI created for the simulation are

Response Speed: This KPI measures how quickly users can respond within different operational scenarios. It reflects the user's ability to rapidly adapt and react to changes in the simulation environment.

Accuracy: This indicator assesses the correctness of completing assigned tasks. It emphasizes the importance of performing tasks correctly and efficiently within the simulation.

Operational Safety Level: This KPI evaluates the level of safety maintained while completing tasks. It takes into account the ability to adhere to best practices and safety protocols under various conditions, such as changes in weather, traffic, and emergency situations.

Risk Perception: This indicator assesses the user's perception of risk exposure during a simulation run. It quantifies how users perceive and understand the risks they are exposed to in the virtual environment, providing insights into their awareness and ability to recognize potential hazards.

The experimentation conducted with port operators involved a total of 27 Port operators. They participated in a total of 355 trials using a simulator under different input and boundary conditions. Additionally, 21 engineers from universities were also involved in further comparisons, contributing to 170 trials. For each trial, user data and performance indicators were recorded to compare performance improvements across various criteria. These criteria included differences between individual players, between simulation runs per player, and between the groups of players. The platform used for these experimental trials was a PC. The tasks assigned to the simulator users involved performing a mission that required inspecting three containers located at the Port Container Terminal yard. Each container was identified by an ID code and its location on the yard, defined as Block-Row-Slot-Shot. For example, a location could be denoted as BK23-3-2-1, indicating Block 23, Row 3, Slot 2, and Shot 1 (resting on the ground).The mission's tasks included finding the three containers based on the provided data, checking for any slicks (small, medium, or intact) on the containers, and verifying the presence of a seal on the container door. The absence of a seal could imply potential malicious activities, such as the spillage of hazardous materials or compromise of the container's integrity. The experimental setup was similar preliminary case, but tests were reduced for many port subjects given the limited time available. In fact, after processing the data available in the first experiment and as a result of the results obtained, it was decided to proceed with a new experiment considering a new sequence of (2 normal trials with minimum difficulty, 1 with fog, 1 normal with maximum difficulty, and 1 normal with maximum difficulty).

4. Results

In this section we present some of the results of the Sensitivity and Trend Analysis

Target:	DurDista		
Total Tests	18		
Significant Results		10,0	56%
Improving	10,0	100%	
Imprvements	Average	57%	
	Max	75%	
Overall	Average	54%	
People	Significant	Improvement	Negative
P1			
P2			
P3			
P4			
P5	1,0	42%	
P6	1,0	53%	
P7	1,0	51%	
P8	1,0	26%	
P9	1,0	74%	
P10			
P11			
P12	1,0	75%	
P13			
P14	1,0	66%	
P15	1,0	62%	
P16	1,0	62%	
P17			
P18	1,0	28%	

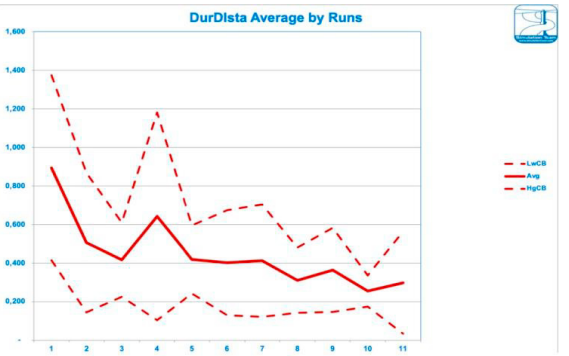


Fig. 3: Average Duration normalized by distance by runs

All users improved their performance in terms of duration relative to distance traveled, with a significance of 56 %. The average improvement is 57%.

Target:	TotRE		
Total Tests	18		
Significant Results		11,0	61%
Improving	11,0	100%	
Imprvements	Average	56%	
	Max	83%	
Overall	Average	56%	
People	Significant	Improvement	Negative
P1			
P2			
P3	1,0	31%	
P4			
P5	1,0	56%	
P6	1,0	65%	
P7	1,0	44%	
P8	1,0	36%	
P9	1,0	83%	
P10			
P11			
P12	1,0	83%	
P13	1,0	53%	
P14	1,0	35%	
P15	1,0	74%	
P16	1,0	59%	
P17			
P18			

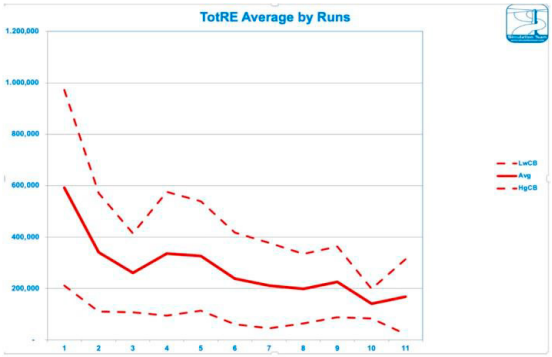
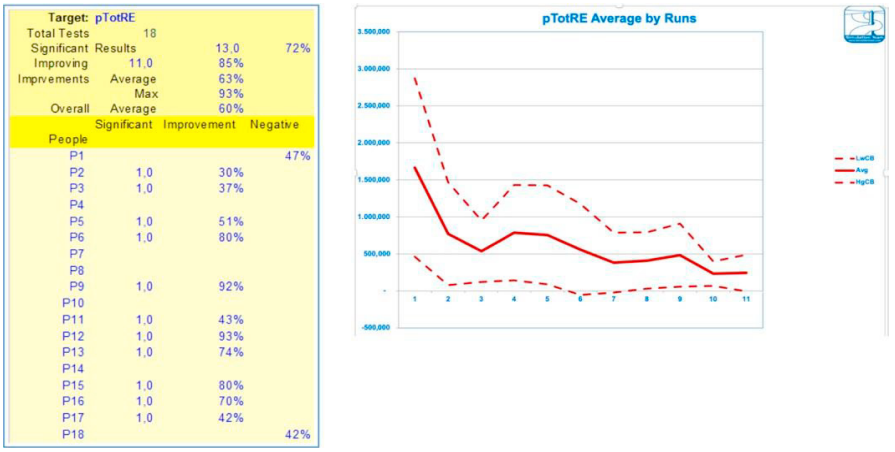


Fig. 4: Average Total Risk Exposure by Runs

All users showed an improvement to total risk exposure, with a significance of 61%. The average improvement was 56% and the maximum was 83%.



Target: pTotRE			
Total Tests	18		
Significant Results		13.0	72%
Improving	11.0	85%	
Improvements	Average	63%	
	Max	93%	
Overall	Average	60%	
	Significant	Improvement	Negative
People			
P1			47%
P2	1.0	30%	
P3	1.0	37%	
P4			
P5	1.0	51%	
P6	1.0	80%	
P7			
P8			
P9	1.0	92%	
P10			
P11	1.0	43%	
P12	1.0	93%	
P13	1.0	74%	
P14			
P15	1.0	80%	
P16	1.0	70%	
P17	1.0	42%	
P18			42%

Fig. 5: Average Total Perceived Risk Exposure by Runs

Eighty-five percent of users improved their perception of risk exposure with a significance of 72%. The average improvement was 63%, while the maximum value was 93%.

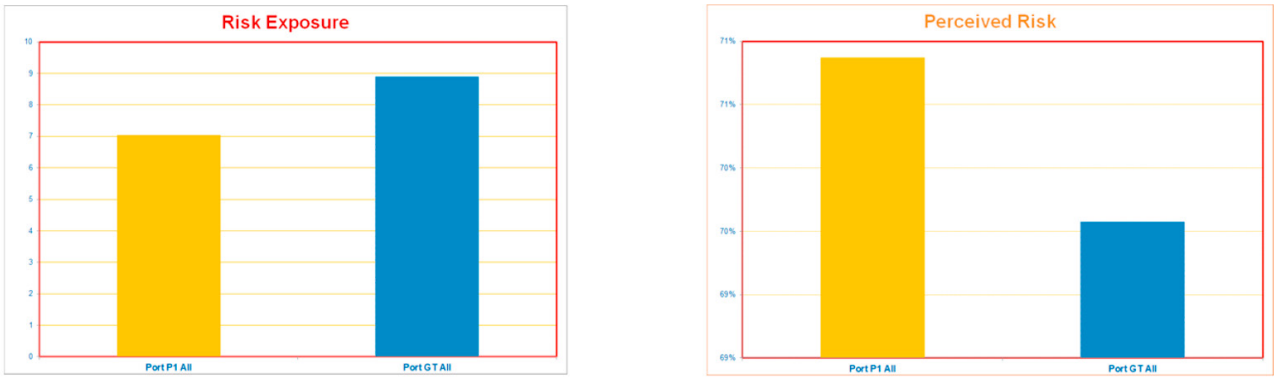


Fig. 6: Comparison between real risk exposure and perceived risk exposure

The user-perceived risk was analyzed in Fig.6, which, consistent with the previous graph, appears to have higher values for those who achieved a lower risk score during the test.

5. Conclusion

The research presented in this paper provides significant insights into the enhancement of safety and operational efficiency in port environments through advanced simulation techniques. The study involving port operators, comprising 27 individuals participating in trials, emphasized the effectiveness of simulation in improving task performance, particularly in identifying and handling potential hazards in container terminals. This enhanced operational understanding and efficiency, as evidenced by the tasks performed, demonstrate the value of simulation-based training in complex and risk-prone environments such as ports.

Furthermore, the development and implementation of a sophisticated cyber simulation model, featuring a two-level architecture that encompasses both real-world and virtual counterparts of a seaport, mark a significant advancement in the field of cybersecurity. The model's comprehensive coverage, from the handling of various network connections and data exchange to the ability for users to configure and adapt to different security scenarios, underscores the critical role of simulated environments in understanding and mitigating cyber threats in critical infrastructure sectors. Overall, the research offers a compelling case for the broader adoption of advanced simulation technologies, including MS2G (Modeling interoperable Simulation and Serious Game) and XR (eXtended Reality), in enhancing safety, security, and efficiency in port operations. These technologies not only facilitate a deeper understanding of complex systems and potential threats but also enable the development of more effective strategies for risk management and operational optimization in maritime and other critical sectors.

References

[1] Bruzzone, A.G., Massei, M., Sinelshchikov, K., Gotelli, M., Giovannetti, A., De Paoli, A., Ferrari, R., Cardell,i M. (2023a) “Operations in Ports supported by Simulation, XR and AI”, Proc. of HMS, Athens, Greece, September

[2] Bruzzone, A.G., Giovannetti, A., Ferrari, R., Gadupuri, B., Karim, J., Sciomachen, A., Longo, F., Fancello, G., Martella, A., Monaci, F., Bucchianica, L., Giliberti, C. (2023b) “Data Analytics for Safety and Security within Ports based using Open Sources”, Proc. of HMS, Athens, Greece, September

[3] Chen, J., Zheng, H., Wei, L., Wan, Z., Ren, R., Li, J., & Bay, Y. (2020). Factor diagnosis and future governance of dangerous goods accidents in Chuina's ports. Environmental pollution , 257, 113582.

[7] Dominguez-Péry, C., Vuddaraju, L. N., Corbett-Etchevers, I., & Tassabehji, R. (s.d.). Reducing maritime accidents in ships by tackling human error: a bibliometric review and research agenda. Journal of Shipping and Trade, 6, 1-32

[6] Othman, A., El-gazzar, S., & Knez, M. (2022). A Framework for Adopting a Sustainable Smat Sea Port Index. Sustainability, 14(8), 4551.

[4] Park, Y., Yip, T. L., & Park, H. G. (2019). An analysis of pilotage marine accidents in Korea. The Asian Journal of Shipping and Logistics, 35(1), 49-54.

[5] Pawel, Z., & Katarzyna, P. (2021). Analysis of ship accidents based on European statistical surveys. 68 Scientific Journals of the Maritime University of Szczecin, (68).

[8] Bruzzone, A. G., Massei, M., Longo, F., Nicoletti, L., Di Matteo, R., Maglione, G. & Agresta, M. (2015). Intelligent agents & interoperable simulation for strategic decision making on multicoalition joint operations. Proc. of DHSS2015, Bergeggi, Italy, September.

[9] Bruzzone, A. G., Massei, M., Maglione, G. L., Di Matteo, R. & Franzinetti, G. (2016). Simulation of manned & autonomous systems for critical infrastructure protection. Proceedings of I3 M, Larnaca, Cyprus.

[11] Bruzzone, A. G. & Di Bella, P. (2018). Tempus Fugit: Time as the main parameter for the Strategic Engineering of MOOTW. Proceedings of WAMS.

[12] Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. In IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society (pp. 4490-4494). IEEE.

[10] Sullivan, J. E., & Kamensky, D. (2017) “How cyber-attacks in Ukraine show the vulnerability of the US power grid”, the Electricity Journal, 30(3), 30-35

[13] Bunyamin Gunes, Gizem Kayisoglu, Pelin Bolat, (2021) Cyber security risk assessment for seaports: A case study of a container port, Computers & Security, Volume 103, 102196, ISSN 0167-4048

[14] Chalermpong Senarak, (2021) Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel, The Asian Journal of Shipping and Logistics, Volume 37, Issue 4, Pages 345-360, ISSN 2092-521