Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 274 (2025) 973–982

Procedia Computer Science

www.elsevier.com/locate/procedia

15th International Defense and Homeland Security Simulation Workshop (DHSS 2025), held within the 22nd International Multidisciplinary Modeling & Simulation Multiconference (I3M 2025)

Evaluating European Maritime Infrastructure Resilience through Constructive Simulation and Infrastructure Models

Arto Niemi*, Niklas Rosseck, Niklas Stockfisch, Jan Stockbrügger, Carl Wrede, Frank Sill Torres

DLR Institute for the Protection of Maritime Infrastructures, German Aerospace Centre (DLR), Fischkai 1, 27572 Bremerhaven, Germany

Abstract

The European maritime security is challenged by geopolitical tensions. This development necessitates robust protection strategies for critical infrastructure. Recent events, including suspected attacks on subsea cables and drone sightings near energy terminals, underscore the infrastructure vulnerability. We propose the application of constructive simulation models to evaluate the protection and resilience of maritime infrastructures. Constructive simulation offers an analytical tool for assessing the effectiveness of security measures. These simulations are today used in the defense field, e.g. for informing procurement decisions, optimizing ways on how well these systems are used for countering such threats, and for training practitioners. We see advantages in using this approach also in the civil security field. A simulation to replicate potential threat scenarios enables the evaluation of system capabilities and the development of effective countermeasures. This paper describes a variety of frameworks for the creation of constructive simulations. Each framework offers different advantages. A single simulation often proves insufficient in addressing the complexity of such scenarios. Thus, the use of co-simulations has become a prevalent approach. This concept requires diverse distribution standards, which in turn can be employed to establish a connection between potential simulations and infrastructure models. These standards are further described in this paper. Moreover, integrating detailed infrastructure models, exemplified by a recently developed offshore wind farm model, allows the simulation of infrastructure failures and the assessment of repair logistics. We discuss how this approach allows testing of infrastructure resilience against attacks, in terms of preventing and recovering from them.

Keywords: Maritime Security; Constructive Simulations; Infrastructure Models

* Corresponding author.
E-mail address: arto.niemi@dlr.de

10.1016/j.procs.2025.12.095

1. Introduction

European maritime security has been challenged by side effects of Russia's military aggression against Ukraine. There have been a number of suspected attacks on European submarine cables and pipes [1]. Notable, plans for green energy transition have envisioned a significant increase of offshore renewable energy [2]. These offshore assets are connected to the shore through underwater cables. So, they are vulnerable to these types of hybrid threats. Suspected spy ships have been detected near these maritime infrastructures [3]. Germany's gas supply now relies more on LNG terminals. This vulnerability is known and unidentified drones have been detected around a German gas terminal [4]. All types of uncrewed vehicles have rapidly evolved during the last few years. As a result, they have become a widely available technology with proven capabilities against maritime targets [5]. The threat is not only related to security. Russia further operates a shadow fleet to circumvent sanctions set up by the EU [6]. This fleet poses a maritime safety and environmental risk as the vessels are often old and underinsured. All these developments create an urgent need to protect European maritime infrastructures.

This paper presents how constructive simulation models [7] may assist in addressing these protection needs. Section 2 discusses on relevant threats against maritime infrastructures and challenges in protecting them. Section 3.1 introduces the advantages of constructive simulations and Section 3.2 presents different frameworks for constructive simulation. Section 4 outlines standards for distributed simulations. They are needed when combining different simulations. Section 5 discusses issues that need consideration when attempting to connect an infrastructure model to a constructive simulation. We use an offshore wind farm model as an example [8]. The advantage is that this allows modeling recovery in case of a failed protection. In the EU context, the protection is relevant in terms of new legislation focusing on critical infrastructure resilience [9]. Lastly, Section 6 concludes this paper.

2. Maritime Infrastructure Protection

2.1. Threats Against Maritime Infrastructures

Threats against maritime and offshore infrastructure have proliferated in recent years. Pirate and terrorist attacks against shipping transportation infrastructures remain a major concern. These threats are demonstrated by the ongoing Houthi threat in the Red Sea, pirate activity in the Gulf of Guinea, and warfare operations in the Black Sea [6]. However, the major focus today is on hybrid or grey zone attacks. A special interest is threats against newer infrastructures such as offshore wind farms, subsea data and electricity cables, as well as underwater gas pipelines [10]. Offshore energy and communication infrastructures are expanding rapidly, as they are crucial for the creation of digital and sustainable societies. Wind farms, for example, are a major source of domestic clean energy supplies to ensure the green energy transition. Many countries also rely on maritime gas pipelines and offshore terminals for their Liquified Natural Gas (LNG) imports, while underwater power cables help maintain efficient energy markets and transfer systems. Global internet connectivity, meanwhile, depends on a global network of submarine fiber optic cables [11].

Yet these infrastructures – and the societies that they sustain – are increasingly threatened by grey zone or hybrid attacks. These are attacks and sabotage acts that fall below the threshold of war and armed conflict. This includes threats such as cyberattacks, the cutting of subsea cables, or sabotage and spying operations against windfarms and subsea communication and pipeline infrastructures [11]. Hybrid attacks are often difficult to attribute to a specific government or state actor. For example, who attacked the Nord Stream pipelines in September 2022 is still unknown. Moreover, hybrid attacks are sometimes intentionally obscured and camouflaged as accidents or as civilian shipping and research operations. This includes Russia's use of research vessels for spying operations or the deployment of vessels from the global "shadow" fleet to cut subsea communication cables with their anchors [12]. Moreover, states may limit their involvement in grey zone practices by outsourcing such activities to non-state actors such as criminals or terrorist groups. Iran, for example, has supported Houthi attacks against Red Sea shipping operations [13].

2.2. Challenges for Maritime Infrastructure Protection

The maritime environment poses significant challenges for infrastructure protection due to large distances and extreme weather conditions. Wind farms are getting bigger and bigger and are built at ever greater distances off the coast. The Hornsea 2 wind farm is located nearly 90 km off the United Kingdom. It is one of the largest offshore wind farms in the world (as of 2024) with over 165 turbines spanning 462 km^2 [14]. Hundreds of kilometers of electricity cables connect regional seas such as the Baltic or the Mediterranean. The network of subsea data cables is thousands of kilometers long and extends across the world's oceans [15].

The strong winds and high waves can make offshore infrastructures at times nearly inaccessible for operators and security forces. The subsea dimension, with poor visibility and limited access, adds to complexity. Maritime operations thus require specialized sensor and vehicle platforms to monitor infrastructures and respond to incidents. These equipment include radars, helicopters, patrol vessels, and unmanned underwater vehicles and cameras.

3. Constructive Simulations

3.1. Advantages of Constructive Simulations

Constructive simulation is a simulation involving simulated people operating simulated systems [7]. They can be used for analytical assessment of system capabilities against certain threats. This information is used in the defense field, e.g. to evaluate which system one should purchase, as well as optimizing ways on how well these systems are used for countering such threats. In these cases, a system could be e.g. a stationary sensor monitoring its environment [16] or a patrol vessel [17].

The simulations can further be used for training specific mission expanding experience of practitioners [7]. The advantages of simulations are reduced cost compared to live exercises, which further allows generating scenarios that would not be feasible in live exercises due to costs or safety concerns. Conducting simulations may also reduce the training time. Moreover, simulations allow practitioners to model security events and train for complex scenarios that have not yet happened, thus increasing overall readiness and preparedness.

Constructive simulations also allow the teacher or instructor of a course to start, stop, examine, or restart a simulation at any time, which is not feasible with live or virtual simulations [18]. Furthermore, these simulations allow the replication of a simulation with the exact same parameters and conditions. Training people under the same conditions allows for a better comparison. Repeatability further enables the use of reinforcement learning algorithms for improvement, as these simulations can be used to generate a large amount of data to train machine learning algorithms [19, 20].

3.2. Frameworks for Constructive Simulation

There exists a variety of options for such frameworks, which could be used for constructive simulations for maritime infrastructure resilience. This section introduces typical frameworks for this purpose, with examples. The advantages and disadvantages of these frameworks are discussed.

3.2.1. Purpose Build Software

Purpose build software (PBS) and military simulations are simulating geopolitical scenarios. They are capable of simulating multiple agents interacting with each other and reacting to specific events. Notable examples would be MAK Technologies VR Forces [21], Ternion Corporations Flames Engine [22], and Matrix Pro Sims Command Professional Edition [23]. The objective of PBS is to provide education and training for military staff. Moreover, they can be utilised in the context of simulating potential threats, thereby assisting in the planning of defensive mechanisms. One significant advantage of utilising PBS as a simulator for maritime infrastructure resilience is the integration of typically military sensor systems, and the military behaviour models of the simulations [24, 25]. A significant disadvantage associated with PBS is their military focus, which frequently results in the exclusion of natural threats, like hurricanes, earthquakes, or tsunamis. An interesting example would be the work from Boron and Darken [19]. They used a PBS for reinforcement learning training of a machine learning model for optimal offensive behavior in small tactical engagements.

3.2.2. Robotic simulators

Robotic simulators such as Gazebo [26], Simulink [27], and Webots [28] are widely known for their use in the simulation of robots and autonomous vehicles. These simulators usually provide features like a physics engine and different sensors. The primary objective of these simulators is to replicate robotic systems. Consequently, most of them are equipped with standard sensors and the Robot Operating System (ROS) [29] to provide data transfer outside of the simulation. A significant benefit of robotic simulators is that the majority of them are open source, which prevents vendor lock-in. Furthermore, robotic simulators are potentially easy to use because their main audience is engineers. Therefore, they do not require a high level of knowledge about computer science.

The development of robotic simulations has been highly purpose-driven. Consequently, these simulations are typically deficient in terms of providing realistic rendering and useful world-building tools, such as features like OpenStreetMap [30] integration [31]. In addition, a number of robotic simulation programs are computationally intensive. One such example is Gazebo, which has an internal limitation of the number of robots that can be simulated simultaneously. Thus, it is not a suitable simulation for scenarios involving a high number of agents [32]. Another example of a robotic simulation would be the UUV Simulator [33]. The UUV Simulator is an extension of Gazebo, which is capable of simulating multiple underwater robots and models, as well as underwater effects, sensors, and disturbances.

3.2.3. Game Engines

Game engines such as Unity [34] and Unreal Engine [35] are commonly used for simulations [36, 37, 38, 39, 40, 41]. Game engines have built-in physics engines, high-resolution graphics, word-building tools, and collision systems. These features make them well-suited for simulations. However, they generally lack physical-based sensors or other useful models, meaning that researchers must construct everything from scratch. A further advantage of game engines is the existence of a large community that provides useful information for potential projects and the fact that most engines are expendable. A notable disadvantage of game engines is that certain features are not essential for simulations, thereby increasing the overall computational demands of the system. One example of this is HoloOcean [37], an underwater robotics simulator built with Unreal Engine 4. Multiple sensors, including sonar, depth sensors, Doppler velocity log (DVL), and inertial measurement unit (IMU), were implemented for an autonomous underwater vehicle.

3.2.4. Custom build engines

Another possibility to consider would be the creation of a custom engine for a specific simulation. The advantage of this option would be that the researcher would be able to adapt everything as he wishes. Therefore, the advantage would be that he would be required to start from the beginning, but since he is not bound to any other tool, his limits would be only his own. Some notable examples would be SO2UCI, a simulation that supports training for critical infrastructures from threats and can simulate autonomous systems [42]. Another noteworthy example is the ALACER2 Port simulator, which is related to safety and security in the marine environment [43].

4. Standards for Distributed Simulations

In the context of simulating complex systems, it is often necessary to divide the entire simulation into smaller sub-simulations, Figure 1 illustrates this type of division. This approach is used to reduce the overall complexity of the simulation and ensure its manageability. This leads to the need for a standard for distributed simulations. In addition, it is necessary to establish a connection between the infrastructure models and the simulations. We see utilizing distributed simulation as a way to connect an infrastructure model, like the one presented in section 5, to a constructive simulation framework. For this it is essential to establish a standard that enables the integration of various tools, allowing individual researchers to implement their models in their chosen environment while maintaining connectivity with the primary simulation. This section presents three of these standards and discusses their advantages and disadvantages. Furthermore, ways for interconnecting different standards are shown.

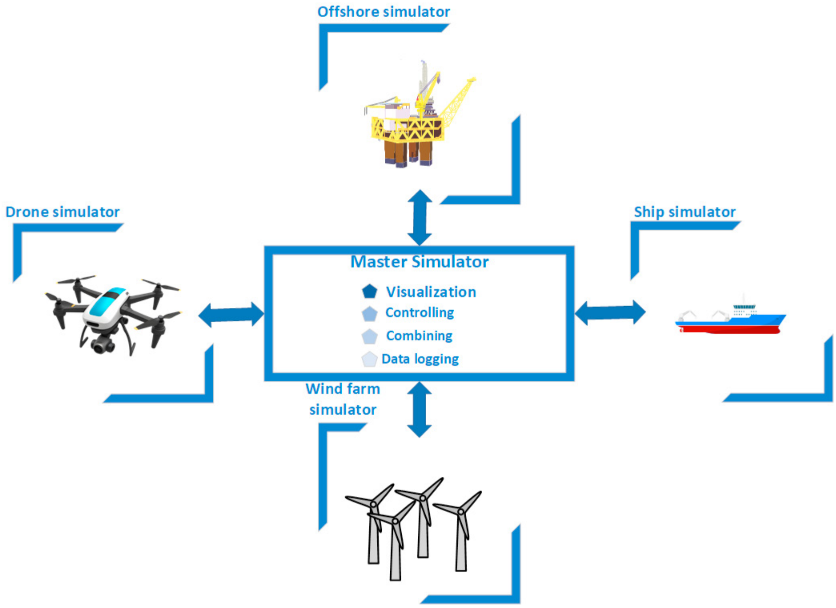

Fig. 1. Example of Co-Simulation with the context of maritime resilience

4.1. High Level Architecture

The High Level Architecture (HLA), illustrated in figure 2, was developed by the US Department of Defense (DoD) in 1995 [44]. It was designed for military purposes, but today it is widely used also in civilian fields. HLA is a framework for distributed simulations and provides a platform for interconnecting interacting simulations [45]. The HLA standard defines a distributed simulation as a federation and each simulation entity is called a federate. These federates interact over the Run-Time Infrastructure (RTI). The RTI manages the communication and data exchange between federates and provides standard protocols. The federation has a federation object model (FOM), which is created in accordance with the Object Model Template (OMT) defined by the standard [46]. The FOM contains the common specification of data communication that all federates share, which is based on a publish/subscribe model. HLA also defines a set of rules, which federates must follow to be HLA compliant.

Some of the advantages of HLA, according to [47], are:

- better simulation time management with the ability to synchronize time-stepped and event-based models;
- faster data exchange rates when modeling large-scale systems using multiple simulators; and
- improved interoperability between heterogeneous simulators by providing an object model template (OMT) to set the exchanged data formats.

The main drawback when using HLA is its complexity and the steep learning curve [48].

4.2. Data Distribution Service

The data distribution service (DDS), illustrated in figure 3, is an open standard by the object management group (OMG) and the latest version 1.4 was published in 2015. The standard defines a data-centric publish-subscribe model for distributed application communication and integration [50]. It builds on a ”global data space” that all interested applications can access. Applications intending to contribute data to this data space have to declare their intent to become publishers. Those wishing to access data must also declare their intent to become subscribers. Applications can be publishers and subscribers at the same time. When a publisher shares data, the middleware distributes this data to all subscribers. One famous framework that utilizes DDS as middleware is ROS.

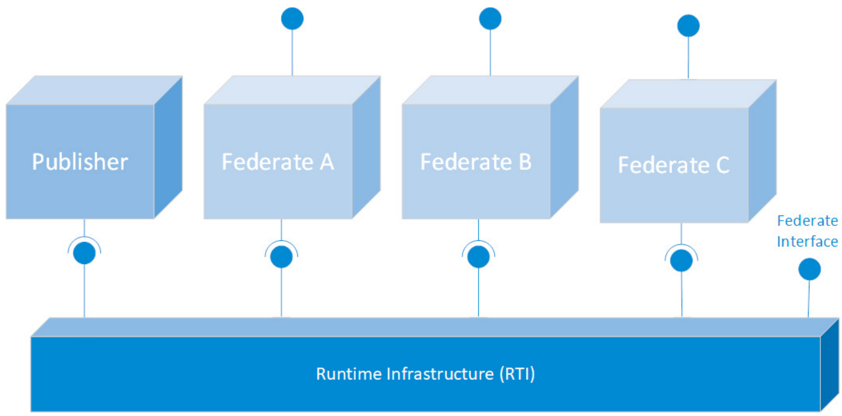

Fig. 2. HLA-Architecture according to [49]

There have been a few approaches to connect DDS with HLA. These approaches fit into three main categories: the fusion model, the transport layer replacement model, and the gateway model [51]. In the fusion model, a simulation middleware is used which combines HLA and DDS by utilizing the concept of a HLA federation but using DDS as the standard for messaging. An example that utilizes this concept would be SimWare [52]. The transport layer replacement model uses an HLA-based system but replaces the transport layer with DDS. This approach keeps the main architecture of HLA and it complies with HLA standard APIs [53]. The gateway model uses a two-way gateway between both middlewares. The gateway appears to the HLA middleware as an HLA federate and to the DDS middleware as a participant. The last part of the gateway is a data converter which contains the functions used for converting the communication of both systems. This approach supports the integration with HLA based systems as well as the integration with DDS based systems.

Fig. 3. DDS-Architecture according to [54]

4.3. *Functional Mock-up Interface*

The Functional Mock-up interface (FMI), illustrated in figure 4, is a free standard for the exchange of dynamic models and for co-simulation [55]. The FMI defines a ZIP archive and an API to exchange dynamic models. A model implementing the FMI standard is called a Functional Mock-up Unit (FMU) and it is distributed as one ZIP file. This file contains an XML file, with the model description that includes the definition of all exposed variables and their interdependencies. Moreover, the ZIP file comprises a C-code that implements a set of functions as defined by the standard. FMI defines three types of interfaces: co-simulation (CS), model exchange (ME), and scheduled execution (SE). In this work only the interface for CS is relevant. The CS interface contains its own scheduler and solver and is designed for the coupling of simulation tools as well as the coupling of subsystem models.

There exist a few drawbacks regarding the usage of FMI. Despite the fact that it is a free, standard, open-source initiative, there is a lack of available implementations for a significant number of programming languages [56]. Moreover, in order to execute a co-simulation that comprises multiple FMUs, it is necessary to use a master algorithm [57].

The standard does not provide such a master algorithm, but there are some free and commercial ones available. One possible master for multiple FMUs could be the RTI from HLA. To act like an HLA federate the program which loads the FMU only needs to obey the HLA rules [58].

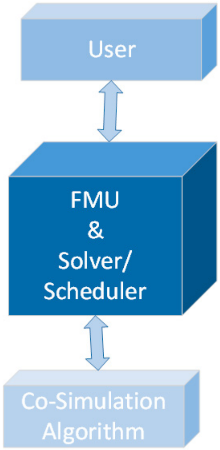

Fig. 4. FMI-Architecture according to [55]

5. Infrastructure Models

Combining an infrastructure model with a constructive simulation allows testing cases where the protection of the infrastructure fails. In these cases, an attacker manages to damage the infrastructure and this damage has to be repaired for the infrastructure to regain its functionality. Several examples of these models exist in risk and reliability engineering fields.

We use a recently published model of an offshore wind farm [8] as an example of how failures and maintenance processes are modeled in infrastructures. Figure 5 shows the main components of this model, which are:

1. Fault trees are used for modeling the system functionality. A system may have a number of subsystems, which may be in a functional or fault state. The logic on how subsystem states affect the state of the overall system is defined with fault trees.
2. A maintenance model handles failure events. It keeps track of maintenance resources, such as vessels and personnel to conduct the maintenance. The model initiates a maintenance action when required assets are in place and the weather is suitable. Weather conditions are a critical aspect when considering offshore infrastructures. Conducting maintenance requires a sufficiently long "weather window" during which weather conditions are tolerable.
3. The model has a stochastic weather generator to create varying weather conditions.

Integrating this kind of infrastructure model with a constructive simulation has the advantage of being able to accurately simulate the effects of damage to the infrastructure. But, there are certain challenges that need to be addressed while connecting the models.

1. Damage sources in the constructive simulation must be connected to system failures in the infrastructure model.
2. Assets for infrastructure repairs need to be included in the constructive simulation. These assets could be valid targets for an aggressor who tries to stop the infrastructure from regaining functionality. Accordingly, damage to the maintenance assets must also be included in the infrastructure model.
3. Models must share the weather conditions, i.e. both models must get the weather information from the same source.

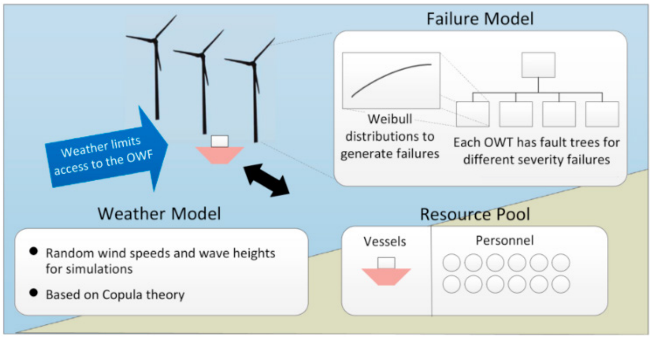

Fig. 5. Illustration of the components of an offshore wind farm failure and maintenance model [8]. (Re-use in accordance with the Elsevier's authors' rights)

6. Conclusions

The escalating threats to European maritime infrastructure necessitate new scrutiny of security and resilience. This paper has highlighted the potential of constructive simulation models as a valuable tool in evaluating and enhancing the protection of these critical assets. By simulating threat scenarios one can gain critical insights into the effectiveness of existing security measures and optimize the deployment of resources. In conclusion, this paper advocates for the broader adoption of constructive simulation methodologies within the civil security domain to bolster the resilience of European maritime infrastructure. These approaches are already well established in the defense field. Future work should focus on testing if these methods are also well suited for modeling civil security scenarios.

Integrating constructive simulations with infrastructure models is interesting in terms of infrastructure resilience [9]. This integration allows assessing the infrastructure recovery in case of failed protection. This paper presented and discussed a variety of simulation frameworks that could be used for constructive simulations. The concept of co-simulation was introduced, and consequently, a variety of distribution standards were presented for use in communication between multiple simulations and models. In addition, this paper used an offshore wind farm infrastructure model example [8] to present technical issues that need to be solved when considering integrating infrastructure models with constructive simulations.

References

[1] Bueger C, Liebetrau T, Franken J, et al. Security threats to undersea communications cables and infrastructure–consequences for the EU. Report for SEDE Committee of the European Parliament, PE702. 2022;557:11-56.
[2] EC. An EU Strategy to harness the potential of offshore renewable energy for a climate neutral future; 2020. (COM(2020) 741 final) European Commission.
[3] Corera G. Ukraine war: The Russian ships accused of North Sea sabotage.; 2023. BBC, https://www.bbc.com/news/world-europe-65309687, 2023-04-19.
[4] Heine F, Laudani P. Covestro, Holcim help German investigators after drone flights over plants.; 2024. https://www.reuters.com/world/europe/covestro-holcim-help-german-investigators-after-drone-flights-over-plants-2024-08-23/,2024-08-23.
[5] Tecklenburg B, Hüfmeyer D, Majri S, Wrede CP. Preliminary lessons from current conflicts about threats on critical maritime infrastructure by unmanned systems; 2024.
[6] Bueger C, Edmunds T, Stockbruegger J. Securing the Seas: A Comprehensive Assessment of Global Maritime Security. United Nations; 2024.
[7] Neugebauer E. History and Basic Concepts of M&S.; 2007. Educational Notes, RTO-EN-MSG-067.
[8] Niemi A, Skobiej B, Kulev N, Torres FS. Modeling offshore wind farm disturbances and maintenance service responses within the scope of resilience. Reliability Engineering & System Safety. 2024;242:109719.
[9] European Union. Directive (EU) 2022/2557 on the resilience of critical entities and repealing council directive 2008/114/EC. Official Journal European Union. 2022;65:164-98.
[10] Bueger C, Edmunds T. Understanding maritime security. Oxford University Press; 2024.
[11] Bueger C, Liebetrau T. Critical maritime infrastructure protection: What's the trouble? Marine policy. 2023;155:105772.
[12] Aliyev N. The Mayhem of Russia's "Research" Fleet; 2025. War on the Rocks, https://warontherocks.com/2025/01/the-mayhem-of-russias-research-fleet/, 2025-01-07.

[13] Haugstvedt H. Red Sea Drones: How to Counter Houthi Maritime Tactics. War on the Rocks. 2021;3. https://warontherocks.com/2021/09/red-sea-drones-how-to-counter-houthi-maritime-tactics/.
[14] Blackridge. Top 10 Largest Offshore Wind Farms in the World 2025.; 2024. https://www.blackridgeresearch.com/blog/top-ten-offshore-wind-farms-in-the-world, 2024-12-09.
[15] Franken J, Reinhold T, Dörnfeld T, Reuter C. Hidden structures of a global infrastructure: Expansion factors of the subsea data cable network. Technological Forecasting and Social Change. 2025;215:124068.
[16] Alexopoulos M, Niemi ATO, Skobiej B, Sill Torres F. Enhancing Resilience of Critical Maritime Infrastructure through Modeling and Simulation of Sensors Configuration. Proceedings of MARESEC 2024. 2024.
[17] Skobiej B, Sill Torres F, Minssen FM. Surveillance of Offshore Installations with Patrol Routine. In: International Conference on Critical Information Infrastructures Security. Springer; 2023. p. 208-23.
[18] Šimic G. Constructive simulation as a collaborative learning tool in education and training of crisis staff. Interdisciplinary Journal of Information, Knowledge, and Management. 2012;7:221-36.
[19] Boron J, Darken C. Developing Combat Behavior through Reinforcement Learning in Wargames and Simulations. In: 2020 IEEE Conference on Games (CoG); 2020. p. 728-31.
[20] Heslinga FG, Fokkinga EP, Eker TH, Liezenga AM, den Hollander RJM, Oppeneer VO, et al. On the use of simulated data for target recognition and mission planning. In: Bouma H, Prabhu R, Yitzhaky Y, Kuijf HJ, editors. Proceedings Volume 13206, Artificial Intelligence for Security and Defence Applications II. Bellingham, WA: International Society for Optics and Photonics; 2024. p. 132060M.
[21] MAK Technologies. VR Forces; 2025. https://www.mak.com/mak-one/apps/vr-forces, Accessed 11.06.2025.
[22] Corporation T. Flames Simulation Framework; 2025. https://flamesframework.com/, Accessed 12.06.2025.
[23] Matrix Pro Sims. Command Professional edition; 2025. https://www.matrixprosims.com/game/command-professional-edition, Accessed 11.06.2025.
[24] McCreight R. Scenario development: using geopolitical wargames and strategic simulations. Environment Systems & Decisions. 2013 Mar;33(1):21-32. Available from: https://doi.org/10.1007/s10669-012-9426-1.
[25] Bruzzone AG, Giovannetti A, Cirillo L, Gotelli M, Ghisi F. An Audacious Wargame on Critical Infrastructures based on LLMs and Simulation over Physical, Cyber & Cognitive Actions. Proceedings of the 14th International Defense and Homeland Security Simulation Workshop (DHSS 2024), 007. 2024. DOI: https://doi.org/10.46354/i3m.2024.dhss.007.
[26] Koenig N, Howard A. Design and Use Paradigms for Gazebo, An Open-Source Multi-Robot Simulator. In: IEEE/RSJ International Conference on Intelligent Robots and Systems. Sendai, Japan; 2004. p. 2149-54.
[27] Documentation S. Simulation and Model-Based Design. MathWorks; 2020. Available from: https://www.mathworks.com/products/simulink.html.
[28] Michel O. Webots: Professional Mobile Robot Simulation. Journal of Advanced Robotics Systems. 2004;1(1):39-42. Available from: http://www.ars-journal.com/International-Journal-of-Advanced-Robotic-Systems/Volume-1/39-42.pdf.
[29] Macenski S, Foote T, Gerkey B, Lalancette C, Woodall W. Robot Operating System 2: Design, architecture, and uses in the wild. Science Robotics. 2022;7(66):eabm6074. Available from: https://www.science.org/doi/abs/10.1126/scirobotics.abm6074.
[30] OpenStreetMap. About OpenStreetMap; 2025. https://wiki.openstreetmap.org/wiki/About_OpenStreetMap, accessed on 11.06.2025.
[31] Collins J, Chand S, Vanderkop A, Howard D. A Review of Physics Simulators for Robotic Applications. IEEE Access. 2021;9:51416-31.
[32] Read M, Möslinger C, Dipper T, Kengyel D, Hilder J, Thenius R, et al. Profiling Underwater Swarm Robotic Shoaling Performance Using Simulation. vol. 8069; 2013. .
[33] Manhães MMM, Scherer SA, Voss M, Douat LR, Rauschenbach T. UUV Simulator: A Gazebo-based package for underwater intervention and multi-robot simulation. In: OCEANS 2016 MTS/IEEE Monterey; 2016. p. 1-8.
[34] Unity Technologies. Unity; 2025. https://unity.com/, Accessed 11.06.2025.
[35] Epic Games. Unreal Engine; 2025. https://www.unrealengine.com/, Accessed 11.06.2025.
[36] Chance G, Ghobrial A, McAreavey K, Lemaignan S, Pipe T, Eder K. On Determinism of Game Engines Used for Simulation-Based Autonomous Vehicle Verification. IEEE Transactions on Intelligent Transportation Systems. 2022;23(11):20538-52.
[37] Potokar E, Ashford S, Kaess M, Mangelson JG. HoloOcean: An Underwater Robotics Simulator. In: 2022 International Conference on Robotics and Automation (ICRA); 2022. p. 3040-6.
[38] Carpin S, Lewis M, Wang J, Balakirsky S, Scrapper C. USARSim: a robot simulator for research and education. In: Proceedings 2007 IEEE International Conference on Robotics and Automation; 2007. p. 1400-5.
[39] Wang Z, Han K, Tiwari P. Digital Twin Simulation of Connected and Automated Vehicles with the Unity Game Engine. In: 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI); 2021. p. 1-4.
[40] Katara P, Khanna M, Nagar H, Panaiyappan A. Open Source Simulator for Unmanned Underwater Vehicles using ROS and Unity3D. In: 2019 IEEE Underwater Technology (UT); 2019. p. 1-7.
[41] Stockfisch N, Meurer C, Bachmayer R. Multimodal Detection of Underwater Gas Seeps Using U-Nets Trained on Simulated Acoustic and Visual Data. In: Oceans Conference. Brest, FRA; 2025. In press.
[42] Bruzzone AG, Massei M, Maglione GL, Di Matteo R, Franzinetti G. Simulation of manned & autonomous systems for critical infrastructure protection. Proceedings of I3 M, Larnaca, Cyprus. 2016.
[43] Bruzzone A, Gotelli M, Giovannetti A, Paoli A, Ferrari R, Gadupuri B, et al. Safety and Security in the Marine and Harbor Environment; 2024. .
[44] Dahmann JS. High level architecture for simulation. In: Proceedings First International Workshop on Distributed Interactive Simulation and Real Time Applications. IEEE; 1997. p. 9-14.
[45] IEEE. IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)–Framework and Rules; 2025. https:

//standards.ieee.org/ieee/1516/6687/.
[46] Falcone A, Garro A, Anagnostou A, Taylor SJ. An introduction to developing federations with the High Level Architecture (HLA). In: 2017 Winter Simulation Conference (WSC). IEEE; 2017. p. 617-31.
[47] Wang F, Magoua JJ, Li N. Modeling cascading failure of interdependent critical infrastructure systems using HLA-based co-simulation. Automation in Construction. 2022;133:104008.
[48] Puch S, Fränzle M, Osterloh JP, Läsche C. Rapid Virtual–Human–in–the–Loop Simulation with the High Level Architecture. In: Proc. of Summer Computer Simulation Conference (SCSC 2012). The Society for Modeling & Simulation Int., Curran Associates, Inc., Genua. vol. 44; 2012. p. 44-50.
[49] Topçu O, Oğuztüzün H. Guide to distributed simulation with HLA. Springer; 2017.
[50] OMG. OMG Data Distribution Service (DDS); 2015. https://www.omg.org/spec/DDS/1.4/PDF.
[51] Kaya MC, Karamanlioglu A, Çetintaş İÇ, Çilden E, Canberi H, Oğuztüzün H. A configurable gateway for DDS-HLA interoperability. In: Proceedings of the 2019 Summer Simulation Conference; 2019. p. 1-11.
[52] Lopez-Rodriguez JM, Martin R, Jimenez P. How to develop true distributed real time simulations? Mixing IEEE HLA and OMG DDS standards. Nextel Aerospace Defense & Security (NADS), http://simware es. 2011.
[53] Park Y, Min D. Development of HLA-DDS wrapper API for network-controllable distributed simulation. In: 2013 7th International Conference on Application of Information and Communication Technologies. IEEE; 2013. p. 1-5.
[54] Friesen M, Karthikeyan G, Heiss S, Wisniewski L, Trsek H. A comparative evaluation of security mechanisms in DDS, TLS and DTLS; 2018. .
[55] Modelica. Functional mock-up interface specification; 2024. https://fmi-standard.org/docs/3.0.2/.
[56] Hatledal LI, Styve A, Hovland G, Zhang H. A language and platform independent co-simulation framework based on the functional mock-up interface. IEEE Access. 2019;7:109328-39.
[57] Reiher D, Hahn A. Ad hoc HLA simulation model derived from a model-based traffic scenario. Simulation. 2023;99(8):859-82.
[58] Awais MU, Palensky P, Elsheikh A, Widl E, Matthias S. The high level architecture RTI as a master to the functional mock-up interface components. In: 2013 International Conference on Computing, Networking and Communications (ICNC). IEEE; 2013. p. 315-20.