XLab-UUV – A Virtual Testbed for Extra-Large Uncrewed Underwater Vehicles

Konrad Wolsing[•°], Antoine Saillard[•°], Elmar Padilla[•], and Jan Bauer[•]

[•]Fraunhofer FKIE
Cyber Analysis & Defense
Wachtberg, Germany

[°]RWTH Aachen University
Communication and Distributed Systems
Aachen, Germany

{<firstname>.<lastname>}@fkie.fraunhofer.de

***Abstract*—Roughly two-thirds of our planet is covered with water, and so far, the oceans have predominantly been used at their surface for the global transport of our goods and commodities. Today, there is a rising trend toward subsea infrastructures such as pipelines, telecommunication cables, or wind farms which demands potent vehicles for underwater work. To this end, a new generation of vehicles, large and Extra-Large Unmanned Underwater Vehicles (XLUUVs), is currently being engineered that allow for long-range, remotely controlled, and semi-autonomous missions in the deep sea. However, although these vehicles are already heavily developed and demand state-of-the-art communication technologies to realize their autonomy, no dedicated test and development environments exist for research, e.g., to assess the implications on cybersecurity. Therefore, in this paper, we present XLab-UUV, a virtual testbed for XLUUVs that allows researchers to identify novel challenges, possible bottlenecks, or vulnerabilities, as well as to develop effective technologies, protocols, and procedures.**

***Index Terms*—Maritime Simulation Environment; XLUUV; Cyber Range; Autonomous Shipping; Operational Technology**

I. Introduction

The exploitation of new areas within oceans, especially underwater, is a major driver of innovation in the maritime domain for very different actors and applications [7]. These encompass, for example, the monitoring of nutrients, pollution, or water temperatures for ecology and climate research. Furthermore, exploring natural resources such as oil and gas deposits or deep-sea mining production plays an essential role in the maritime industry to secure national energy supplies. Consequently, already today, a substantial amount of underwater infrastructures, such as intercontinental communication lines, gas pipelines, and oil production facilities, as well as offshore wind farms, are deployed within oceans requiring constant Inspection, Maintenance, and Repair (IMR).

To perform underwater IMR, smaller Remotely Operated Vehicles (ROVs), Unmanned Underwater Vehicles (UUVs), and Autonomous Underwater Vehicles (AUVs) offer initial solutions for targeted applications in shallow water depths, with limited operational ranges, durations, and close monitoring by crews, e.g., in tender vessels. But with the growing explorations of deep seas and rapid installation of underwater infrastructure, these vehicles reach inherent limitations [7], [8], [25] since mobile, long-term, and long-range solutions that are also suitable for deep-sea applications do not yet exist. Hence, the development of a new vehicle class is inevitable.

In that regard, Extra-Large Unmanned Underwater Vehicles (XLUUVs) are seen as an enabler to overcome the current limitations of previous vehicles [7], [26]. Due to their overall larger size, they promise to be capable of conducting autonomous, uncrewed, multipurpose, and long-range missions. This technology shift is made possible through drastic digitalization, which in return raises interesting engineering challenges w.r.t. (i) near real-time communication systems for supervision and remote monitoring of XLUUVs, (ii) control systems obeying maritime International Regulations for Preventing Collisions at Sea (COLREGs), as well as, (iii) ensuring operational safety, and (iv) cybersecurity for complex autonomous systems. While several XLUUVs are already being engineered [27], they are still in an early development stage.

Solving these challenges requires active research, fine-granular pre-development, and iterative testing. In this context, simulation is a key technology to tackle development challenges in a lab. In the specific scope of XLUUVs, simulations can involve many different disciplines ranging from hydrodynamics [8] to control systems for Operation Technology (OT) components [25], i.e., vehicle automation, Information Technology (IT), and navigation. Especially for such remotely controlled vehicles, cybersecurity issues and cyber risk assessments [17], even *during* development, become crucial due to the growing threats from the cyber-electromagnetic space [4]. However, while simulations are well established in research and engineering where versatile environments usually exist [5], there are no testbeds specific to maritime IT/OT of XLUUVs that are publicly available and scientifically usable as of now.

In this paper, we present XLab-UUV, a novel simulation-based testbed for XLUUVs, holistically comprising not only the actual vehicle with its IT/OT systems, but also remote control components, on-shore IT, and possible mission payloads. To this end, the testbed particularly considers the possible modularity of XLUUV components, which is addressed through a modular structure and a flexible system architecture, as well as the mutual interaction of IT and OT. XLab-UUV is grounded on the design of a real vehicle, thus making it a realistic simulation environment for research.

Author manuscript.

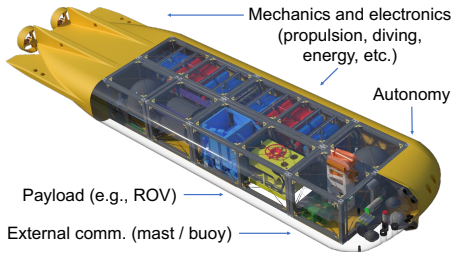


Fig. 1. Representative XLUUV: The planned Large Modifiable Underwater Mothership (MUM) [7] demonstrator (25 m length) and its subcomponents.

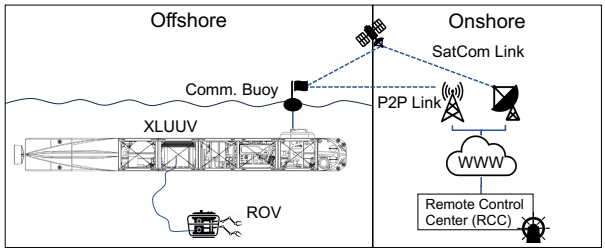


Fig. 2. A high-level overview of the entire communication system, including the onshore infrastructure (RCC), the remote communication (established via a buoy), and the XLUUV itself with an ROV as mission payload.

Starting with brief background information on XLUUVs in Sec. II, including some representatives, their commonalities, and peculiarities, the related work in Sec. III motivates the need for our virtual testbed XLab-UUV, presented in detail in Sec. IV. Afterward, Sec. V discusses the potential of this novel environment concerning possible use cases from a perspective of communication, operational safety, and cybersecurity, where we identify current shortcomings and engineering challenges to be solved with XLab-UUV in the future.

II. XLUUVs: A New Class of Underwater Vehicles

A. Application and Use-cases of XLUUVs

Large and XLUUVs represent a new generation of UUVs that aim to operate semi-autonomously, unattended for months at a time, far from land, at deep ocean depths, and even under ice surfaces [7], [26]. Due to novel fuel cell powering systems, operation ranges of thousands of kilometers enable port-to-port missions without the need for risky and weather-restricted launch and recovery maneuvers [26]. At the same time, advances in control systems and mobile Internet technology give XLUUVs increased autonomy to a point where they are merely supervised from an on-shore Remote Control Center (RCC), which is in stark contrast to current UUVs that are usually controlled (and powered) by cable.

XLUUVs can also carry much larger payloads and thus serve as transport and launch platforms to perform versatile missions, ranging from persistent surveillance over deep sea exploration to IMR of offshore assets. These payloads include, e.g., seismic meters, IMR equipment, AUVs, or ROVs. In that regard, IMR represents an interesting use case: The XLUUV navigates autonomously to a mission site, and, leveraging its communication capabilities, a remote (land-based) operator can perform work with the payload, an ROV, without requiring physical presence. This scenario is especially relevant from an Information and Communications Technology (ICT) perspective, as it requires reliable and secure communication and will therefore serve as a reference scenario in this paper. Further potential XLUUV applications are summarized in [7].

B. XLUUV Architecture

In support of submarine operations, XLUUVs are being developed worldwide. Popular representatives of this class of vehicles are the Hugin Endurance (Kongsberg), the Echo Voyager (Boeing), Solus XR (Cellula Robotics), and the Large Modifiable Underwater Mothership (MUM) (thyssenkrupp Marine Systems). Among them, MUM (Fig. 1), with a length of 25 m and ranges of thousands of kilometers [26], follows a modular design to accommodate different payloads and is drafted for multiple applications. A first demonstrator is currently under development within the research project MUM2 [30] and will be ready for sea trials in 2024. Therefore, MUM serves as the reference model in this work.

Taking a closer look at MUM's design, Fig. 1 depicts its typical subcomponents, which can be grouped into four essential categories: (i) *Mechanics and electronics* encompass the thrusters, rudders, trim, and diving systems, as well as the hydrogen fuel cells, reactants, and batteries for energy supply. (ii) The *autonomy* component includes all IT-related components, i.e., the central intelligence for control and navigation, on-board networks, and IT-OT gateways. (iii) *External communication* to the RCC via the Internet is either provided with a mast while surfaced or a floating buoy in the submerged state. (iv) Finally, depending on the mission, different *payloads* can be incorporated into a MUM, such as an ROV to conduct IMR. These components are similarly found in other XLUUVs.

C. Specifics of XLUUVs from an ICT Perspective

From an ICT perspective, it is not the physical size that makes large and extra-large UUVs unique but rather their complexity and interactions with external applications.

Even though the actual XLUUV is uncrewed and (partially) autonomous, it is closely remotely monitored and controlled by operators in an (onshore) RCC all the time, cf. Fig. 2. To this end, regulatory requirements mandate that operators be able to maintain permanent situational awareness, cf. [9], e.g., with adequate video streams. Given these technical requirements and the increased operational range, there is a need for suitable communication solutions between XLUUV and RCC. As outlined in Fig. 2, this can be a direct Point-to-Point (P2P) connection (e.g., WLAN or 5G) or a satellite-based connection during operations further away from the coast. Thus, the remote connection of an XLUUV has a high criticality for reliability and security. Additionally, many human-related security requirements mandatory in crewed shipping are not applicable for XLUUVs or must be implemented in the RCC.

The envisioned multi-purpose applications, in conjunction with a modular and convertible concept, pose additional challenges for ICT's cybersecurity [26]. First, due to the inherent

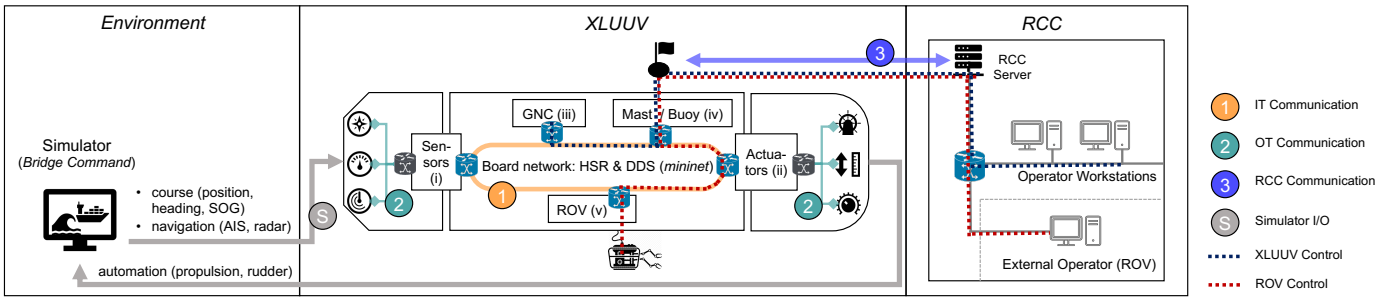


Fig. 3. The testbed's architecture includes an environmental simulator interacting with the XLUUV's OT, its connected IT systems, and the RCC with its communication link. Instructions from RCC workstations to the GNC pass through the different communication links of the testbed (dashed blue line). Furthermore, an ROV is modeled as the mission payload to include end-to-end communication between this device and its external operator (dashed red line).

modularity and limitations in space, it becomes difficult to implement physical network segmentation and separation of zones with different security levels as demanded by security standards [13]. At the same time, mission payloads potentially originating from third-party entities must be able to be integrated into the vehicle system flexibly and accessible from the RCC without causing security risks on the entire XLUUV.

As a result, solutions, i.e., automatic switching between satellite and P2P links for stable Internet connectivity and network segmentation schemes to separate third-party modules, have to be tested and adapted for XLUUVs. In that regard, a testbed, as presented in this paper, can offer a valuable platform to test such new concepts prior to their deployment.

III. Related Work

Within related domains, such as cyber-physical systems and industrial control systems, the benefits of testbeds for research, development, testing, and optimization are long known [5]. Likewise, more testbeds emerged recently in the maritime domain, with their focus strongly driven by the urgent need for maritime cybersecurity. Existing testbeds can be divided into hardware-supported and simulator-based testbeds.

Among the former is the Cyber-SHIP Lab [29], which includes physical and digital assets of Integrated Bridge Systems (IBSs), and offers multiple configurations of the IT and OT equipment to imitate differently equipped ships, thus, enabling a valuable cybersecurity research and education platform. Fathom5 follows a similar approach with their Grace Maritime Cyber Testbed System [6]. Although being close to the real system, such hardware-supported testbeds are expensive and usually offer less flexibility than simulation-based testbeds.

Simulative testbeds provide a remedy. Even though they usually depend on the quality of the respective simulation, a certain abstraction level is tolerable for many use cases. For example, in ICT and security research, accurate physical modeling of the vehicle and the environment is subordinate.

In the context of simulative testbeds, Visky et al. [31] present a cyber environment for research and training purposes based on a commercial navigational simulator (provided by Transas). In contrast, the MaCySTe testbed [20], [21] relies on open-source software, similar to the bridge and radar attack tools BRAT [10] and RAT [33]. These approaches use *Bridge Command* [3], a free interactive ship simulator, to simulate the vessel and its environment, as well as *OpenCPN* [23] as an open chart plotter. As a result, portable virtualization of testbeds is enabled, allowing flexible research and experimentation with offensive and defensive cybersecurity methods.

However, all existing maritime testbeds are designed for surface vessels and their IT/OT systems. Thus, they are of limited applicability for underwater vehicles, particularly ignoring the specifics of XLUUVs, cf. Sec. II-C.

IV. Virtual XLUUV Testbed

The goal of the envisioned XLab-UUV is to create a virtualized implementation of XLUUVs' IT/OT and their peripherals, enabling the development and analysis of novel technologies and protocols. For this purpose, we pursue a holistic approach. On the one hand, this means that viewed *horizontally*, not only is the XLUUV modeled, but also its possible mission payload and RCC. On the other hand, seen *vertically*, the entire ISO/OSI stack should be considered through exemplary protocols and applications. The design decisions and architecture created for this purpose, inspired by related work, are presented in Sec. IV-A before Sec. IV-B sheds light on the implementation details of XLab-UUV. Finally, Sec. IV-C provides a brief outlook on future enhancements.

A. Design & Architecture

The design of XLab-UUV is centered around an actual XLUUV MUM (cf. Sec. II-B). Thus, the architecture comprises three main components, as visualized in Fig. 3. First, the XLUUV's on-board network to which different vehicle modules are connected, and second, an RCC. Lastly, a simulation environment implements the physical model and interactions.

Starting with the XLUUV, our lab models five essential modules similar to those of MUM: (i) a module that combines all of the vehicle's sensors, such as course, position, heading, Speed Over Ground (SOG), or sea depth, as well as means to sense surrounding vessels via radar and Automatic Identification System (AIS); (ii) an actuator module, which models the drive system, i.e., propulsion and rudder; (iii) the Guidance, Navigation, and Control (GNC) module, implementing the central intelligence, including an autopilot, which is responsible for the semi-autonomous navigation along pre-defined waypoints

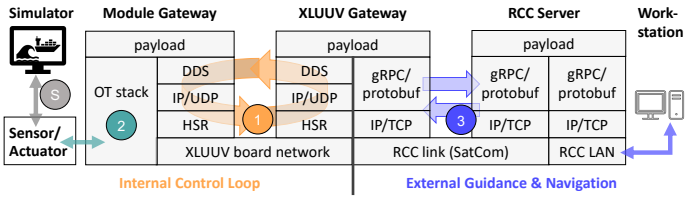


Fig. 4. A simplified representation of the testbed's protocol stacks. The control loop inside the vehicle comprises the DDS-based data exchange between GNC, sensors, and actuators. The latter are each connected to their own OT gateways, cf. Fig.3. External guidance and navigation from the RCC is implemented through gRPC-based communication via the RCC control link.

and the control loop between the sensor and actuator module; (iv) the communication module (mast/buoy) for the RCC link, to which a mission plan can be transmitted and which in turn informs the operators about the vehicle status, i.e., position, speed, and engine status; and last but not least, (v) a mission module, representing an ROV payload for IMR.

One central component of the XLab-UUV connecting all modules is the on-board network which exhibits a multi-layer topology. The core is an Ethernet ring topology (①), as frequently used in the field of automation industry. This topology, together with the High-availability Seamless Redundancy (HSR) [12] protocol, provides physical redundancy in case of a single link failure. Each of the five modules is then connected to the ring via switches acting as gateways.

Inside the sensor and actuator modules, an industrial PC interfaces between the IT (on-board network) and the vehicle's OT (②). Since these components would interact with the external world of the vehicle, they are connected to the real-time ship simulator (Ⓢ). The simulator generates the vehicle's sensor data and, vice versa, receives the instructions regarding the actuator settings demanded by the GNC. The simulation includes a maritime environment model with different scenarios, maritime traffic, as well as the driving physics of the vessel, which we adapted accordingly for the specifics of MUM.

Lastly, a network bridge models the multi-link connection between XLab-UUV and the RCC, emulating the properties of P2P and satellite connections (③). In the RCC, a main server acts as a central unit between the XLUUV and the operators' workstations which are connected by a traditional Ethernet LAN. Thereby, operator instructions (and status information in the opposite direction) can be sent on multi-hop connections from the workstations to the RCC server and via the XLUUV gateway (in the communication module) to the respective vehicle's modules (cf. blue and red dashed lines in Fig. 3).

B. Implementation Details

This section gives an overview of the implementation of our testbed: technical details on the network (Sec. IV-B1), the protocol stack (Sec. IV-B2), as well as the simulator, the OT's cyber-physical interface, and the testbed's HMIs (Sec. IV-B3).

1) Multi-Topology Network: Because the testbed focuses on a realistic representation of the IT/OT systems of an XLUUV, the tool *mininet* [16] is used along with industry-standard technology and well-established protocols. Mininet is a widely-used research tool that leverages the virtualization capabilities of the Linux kernel to build virtual networks of different components running on a host system. With mininet, existing technologies and protocols in Linux can be used and, like the network topologies, these can be exchanged flexibly.

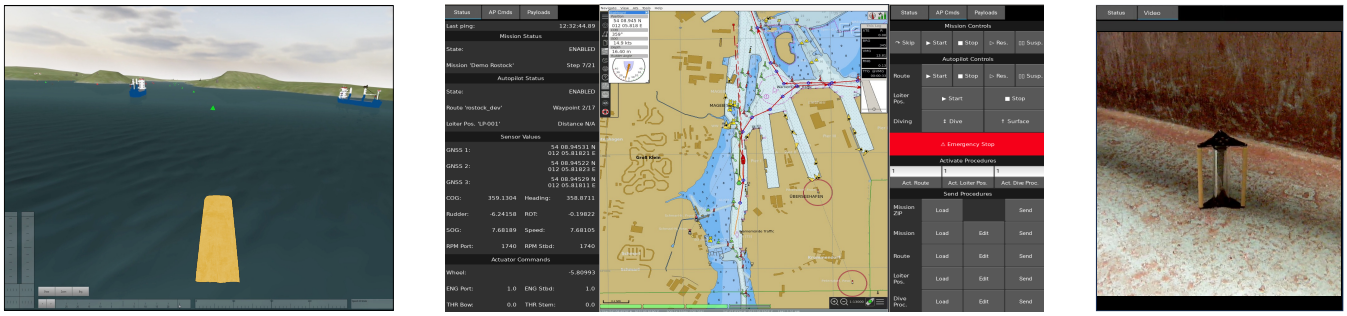
Mininet establishes a multi-topology (cf. Fig. 3) comprising the board network (①) with ring topology based on Linux's HSR [12] implementation, the external communication link (③) modeling a satellite communication with configurable link qualities by using the network emulator *netem* [15], and the Ethernet-based RCC LAN using mininet. The testbed's OT components (②) are based on a virtual automation environment from the manufacturer *Beckhoff*, provided as a Virtual Machine (VM) [2] and connected to mininet's HSR network, representing the XLUUV's sensor or actuator module.

2) Protocol Stack: In these subnetworks, different protocol stacks are built, as shown in Fig. 4. The board network (①) relies on DDS [24], an IP/UDP-based standard specified by the Object Management Group, which provides a middleware for data-centric communication between XLUUV modules. DDS implements a publisher-subscriber concept. For all sensor/actuator data, control and navigation data, as well as data of the deployed mission payloads, so-called topics are defined in XLab-UUV. These topics are grouped into domains to which devices or processes can subscribe or publish. To this end, the open-source implementation *openDDS* is used.

Since transmission errors must be assumed for the satellite communication link (③), Google's open-source Remote Procedure Call framework gRPC is used here, as well as within the RCC. The framework provides a client-server communication and is based on HTTP/2 and the traditional IP/TCP stack, cf. Fig. 4. Internally, it uses Protocol Buffers (*protobuf*), a data format for serializing, storing, and exchanging structured data in inter-machine communication. Note that for the fault-tolerant transmission of status information from the vehicle to the RCC, we refrain from using gRPC with its transmission guarantees (i.e., TCP retransmissions). To reduce the communication overhead, pure protobuf messages are instead transmitted via UDP in this direction.

3) Simulator & Human-Machine Interfaces: Inspired by related work, for the vehicle's simulation, its environment, and vessel traffic, we use the interactive simulator *BridgeCommand* (Fig. 5(a)), which is integrated as a VM into the testbed. Besides extensions like a 3D model of the XLUUV and its driving physics, the interfaces for the integration of the simulator were created (Ⓢ), i.e., for the exchange of vehicle data between the simulator and the Beckhoff OT VMs (Fig.4). Thereby, the payload is generated for sensor data (e.g., geo-position, heading, SOG, depth, AIS, and radar) and actuator data (i.e., data from control system). Note that NMEA is used for AIS, while BR24 is used for radar payload. This payload is transferred via the OT network (②) over the module gateways to the board network, and vice versa, cf. Fig. 3.

Furthermore, we implemented a basic GNC, including an autopilot as an XLUUV module, which, in addition to following



(a) *Bridge Command* with an XLUUV model of MUM provides the interface between simulated driving physics, the environment, vessel traffic, and the actual testbed.

(b) The control terminal in the RCC is based on *OpenCPN* with a sidebar extension to transfer direct commands and mission maps to the vehicle's GNC.

(c) An RCC third-party terminal allows, e.g., to display video streams received from ROVs.

Fig. 5. Visualization of the testbed's Human-Machine Interfaces (HMIs) displayed to operators in the RCC.

a waypoint list, also has a loitering mode to dynamically hold the position, e.g., during a mission at the operation site. The GNC is instructed by the human operator in RCC. To this end, we use the chart plotter *OpenCPN*, which we extended with additional XLUUV-specific control bars, cf. Fig. 5(b).

Finally, the simulation of the ROV is kept very simple. Network data recorded in field trials (i.e., control and video data in MAVLink format) are replayed to produce realistic traffic between ROV and its RCC terminal, cf. Fig. 5(c).

C. Future XLab-UUV Extensions

The previously presented design of XLab-UUV naturally leaves room for future enhancements. One planned extension is a diving mode during which radio-based communications, AIS, and radar are interrupted. In that regard, it is also planned to extend the external communication link to a true multi-link with parallel WLAN, 5G, and satellite connectivity for redundancy. In the future, it would also be possible to enhance the ROV logic as well as to add modules for underwater acoustic communication [14] and underwater positioning systems [19].

Overall, our unique XLab-UUV provides an essential cornerstone for a virtual testbed in which XLUUVs can be examined digitally for the first time.

V. Use Cases & Outlook

To highlight the benefits of the proposed testbed, possible use cases from the perspectives of communication (Sec. V-A), safety (Sec. V-B), and cybersecurity (Sec. V-C) are discussed in the following, identifying current shortcomings of XLUUV development and the potentials for future improvements.

A. Communication Systems

Regarding communication, common use cases of comparable testbeds are protocol development, performance evaluation, and optimizations, which XLab-UUV likewise enables. For instance, one crucial aspect of the control loop steering an XLUUV is the delay introduced by the communication network towards sensors and actuators, i.e., the DDS layer in the onboard network. XLab-UUV enables performance studies on such a design decision regarding the delay, jitter, and their impact on the vehicle's control system. Similar analyses can be conducted for the external communication link. For instance, in case of connection losses between XLUUV and the RCC or link failure, fast recovery is essential. To this end, multi-path routing, transport protocols, as well as optimal handshaking strategies for switching between the different transmission technologies could be investigated and further developed.

Our holistic environment also tackles new use cases, such as mission payload integrations. For example, the testbed can be used to develop robust and flexible video compression for ROV streams and parameterize them appropriately for satellite links with inherent delay and bandwidth limitations. These can ultimately be evaluated in Quality of Experience (QoE) studies w.r.t. to long-range remote control of ROVs.

B. Safety & Functional Reliability

Temporary disruptions of remote connection undoubtedly have safety implications but are not the only aspects regarding the operational safety of autonomous ships [18].

The safety of a system is usually evaluated by Hazard Identifications (HAZIDs) and Failure Mode and Effect Analyses (FMEAs), which accompany the technical development and engineering of the system [26]. In this context, failure probabilities are often based on statistics of other applications or subcomponents, as they still need to be created for XLUUVs. XLab-UUV offers a substitute for this deficit with laboratory experience and can support safety assessments this way.

Similarly, when developing the central intelligence of XLUUVs, especially the COLREGs, it is essential to validate their correctness and consider potential failures of subcomponents to mitigate accidents at sea. An early analysis, as possible with XLab-UUV, reduces development costs and enables experiments in controlled environments before conducting costly and lengthy sea trials, e.g., by examining scenarios where the system deliberately receives erroneous input data.

C. Cybersecurity & Analysis

Finally, due to XLUUVs' enlarged operational radius and higher monetary or intellectual value, there is a substantially higher risk for cyberattacks. Currently, the the International

Association of Classification Societies (IACS) pushes towards establishing cybersecurity standards, e.g., based on widely-used IEC 62443 [13] standards for industries, to establish unified requirements for cyber resilience of ships (E26) and on-board systems and equipment (E27) with mandatory implementation by January 2024 [11]. As these requirements become mandatory in the near future, the need for testbeds to perform risk assessments or develop security solutions grows.

Like safety-related HAZIDs, cyber risk assessments [1], [17], [28] can benefit from experimentation in XLab-UUV. This includes practical analyses, such as penetration tests with the help of specific attack tools like BRAT [10] and RAT [33], to reveal attack vectors against novel XLUUV designs.

To mitigate vulnerabilities identified, well-established solutions, e.g., from other domains, must be adopted or newly invented. These involve security measures such as network segmentation into critical and less-critical zones via VLANs, as already supported by XLab-UUV, to isolate control and payload traffic in the shared board network. These can be complemented with network encryption, e.g., on the data link layer via MACsec (IEEE 802.1AE) [22] or on the application layer through DDS [24]. Lastly, the ability to detect malicious actions with the help of intrusion detection systems [32] can be evaluated or models pre-trained within the testbed.

In summary, XLab-UUV meets the needs for such testbeds, contributes the benefits that have long been recognized in the industry [5], and thus fills the gap for maritime XLUUVs.

VI. Conclusion

In this paper, we presented XLab-UUV, a novel virtualized testbed for an upcoming class of underwater vehicles called Extra-Large Unmanned Underwater Vehicles, to advance their technical development concerning Information and Communications Technology and cyber resiliency. The testbed's design and architecture were modeled on a representative vehicle, the Large Modifiable Underwater Mothership (MUM) currently being engineered. Inspired by related maritime and industrial environments, established open-source software was adopted for this purpose, such as a maritime simulator and a network visualization tool, combined with widespread industrial IT/OT protocol suites. Based on selected use cases, we have identified the research needs for safety and security, highlighting the testbed's benefits, and provided an outlook on the future potential for enhancing this new vehicle class.

Availability Statement. The source code of XLab-UUV is available at: https://github.com/fkie-cad/XLab-UUV.

Acknowledgments

This work is part of the project MUM2 [30]. It was funded by the German Federal Ministry of Economic Affairs and Climate Action (BMWK) with contract number 03SX543B managed by the Project Management Jülich (PTJ). The authors would like to thank Merlin von Rechenberg and Lucca Ruhland for their technical contribution and all project partners, especially the German Aerospace Center (DLR) for the provision of real-world ROV video/network data. The authors are responsible for the contents of this publication.

References

[1] A. Amro *et al.*, "Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework," *ACM Trans. Priv. Secur.*, vol. 26, no. 2, 2023.
[2] Beckhoff, "TwinCAT/BSD Hypervisor," https://www.beckhoff.com/en-us/products/automation/twincat-bsd-hypervisor/ (accessed 2023-06-06).
[3] Bridge Command, "An interactive 3d ship & radar simulator," https://www.bridgecommand.co.uk (accessed 2023-06-06).
[4] M. Caprolu *et al.*, "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead," *IEEE Commun. Mag.*, vol. 58, no. 6, 2020.
[5] M. Conti *et al.*, "A Survey on Industrial Control System Testbeds and Datasets for Security Research," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, 2021.
[6] Fathom5, "Grace Maritime Cyber Testbed System," https://www.fathom5.co/grace (accessed 2023-06-06).
[7] M. Golz *et al.*, "MUM – Large Modifiable Underwater Mother Ship: Requirements and Application Scenarios," in *Proc. of OCEANS*, 2018.
[8] M. Greve *et al.*, "Design of the Propulsion System for the Autonomous XLUUV MUM," in *Proc. of OMAE*, 2022.
[9] J. T. Halog *et al.*, "Legal challenges for the law of the sea in the light of disruptive technologies: Modular and autonomous submarines," in *MARESEC*, 2022.
[10] C. Hemminghaus *et al.*, "BRAT: A BRidge Attack Tool for cyber security assessments of maritime systems," *TransNav*, vol. 15, 2021.
[11] IACS, "UR-E26 – Cyber resilience of ships; UR-E27 – Cyber resilience of on-board systems and equipment," 2022.
[12] IEC 62439-3, "Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundanc (HSR)," 2016.
[13] IEC 62443-4-2, "Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components," 2019.
[14] S. Jiang, "On Securing Underwater Acoustic Networks: A Survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, 2019.
[15] A. Jurgelionis *et al.*, "An Empirical Study of NetEm Network Emulation Functionalities," in *Proc. of ICCCN*, 2011.
[16] K. Kaur *et al.*, "Mininet as Software Defined Networking Testing Platform," in *Proc. of ICCCS*, 2014.
[17] G. Kavallieratos *et al.*, "Managing Cyber Security Risks of the Cyber-Enabled Ship," *JMSE*, vol. 8, no. 10, 2020.
[18] T.-e. Kim *et al.*, "Safety challenges related to autonomous ships in mixed navigational environments," *JOMA*, vol. 21, 2022.
[19] Z. Liu *et al.*, "Underwater acoustic positioning with a single beacon and a varied baseline for a multi-jointed AUV in the deep ocean," *IET Radar, Sonar & Navigation*, vol. 14, no. 5, 2020.
[20] G. Longo *et al.*, "Electronic Attacks as a Cyber False Flag Against Maritime Radars Systems," in *Proc. of MarCaS*, 2023.
[21] ——, "MaCySTe: A virtual testbed for maritime cybersecurity," *SoftwareX*, vol. 23, 2023.
[22] J. Lázaro *et al.*, "MACsec Layer 2 Security in HSR Rings in Substation Automation Systems," *Energies*, vol. 10, no. 2, 2017.
[23] OpenCPN.org, "OpenCPN Chart Plotter Navigation," https://opencpn.org (accessed 2023-06-06).
[24] G. Pardo-Castellote, "OMG Data-Distribution Service: Architectural Overview," in *Proc. of Distributed Computing Systems Workshops*, 2003.
[25] E. Rentzow *et al.*, "Modeling and Control of a Highly Modular Underwater Vehicle with Experimental Results," in *Proc. of ECC*, 2021.
[26] S. Ritz *et al.*, "Specialties of HAZID-Study for Large Unmanned Underwater Vehicles," in *Proc. of OCEANS*, 2023.
[27] H. I. Sutton, "Naval Group Reveal XLUUV Demonstrator," http://www.hisutton.com/Naval-Group-XLUUV.html (accessed 2023-06-06).
[28] K. Tam *et al.*, "Cyber-Risk Assessment for Autonomous Ships," in *Proc. of Cyber Security*, 2018.
[29] K. Tam *et al.*, "Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities," in *Proc. of ICMET*, 2019.
[30] The MUM-Project, "Large Modifiable Underwater Mothership," https://www.mum-project.com (accessed 2023-06-06).
[31] G. Visky *et al.*, "Multi-Purpose Cyber Environment for Maritime Sector," in *Proc. of ICCWS*, 2022.
[32] J. Wang, "The Art of Intrusion Detection," in *Computer Network Security: Theory and Practice*, 2009, pp. 317–347.
[33] K. Wolsing *et al.*, "Network Attacks Against Marine Radar Systems: A Taxonomy, Simulation Environment, and Dataset," in *Proc. of LCN*, 2022.