Proc. of MARESEC 2024
DOI: 10.5281/zenodo.14214969

Threat Analysis for Novel Underwater Vehicles: Insights from the Perspective of Cyber Security

Alexander Nies°, Konrad Wolsing°•, Jan Bauer°

°Fraunhofer FKIE
Cyber Analysis & Defense
Wachtberg, Germany

•RWTH Aachen University
Communication and Distributed Systems
Aachen, Germany

{alexander.nies, konrad.wolsing, jan.bauer}@fkie.fraunhofer.de

***Abstract*—In complex underwater operations, the offshore subsea industry can benefit greatly from a novel class of extra-large uncrewed underwater vehicles due to their increasing autonomy and adaptability. However, their reliance on IT, reliable communication, and sensor information poses significant cyber security challenges exacerbated by rising maritime incidents. This study systematically analyzes the cyber attack surface of those underwater vehicles, assessing and ranking potential threats, and identifying critical system components. The research contributes by design to the definition of tailored security requirements. Our threat analysis creates the basis for simulation and test environments that foster the development of appropriate security measures in order to defend against the growing threats from cyberspace and the electromagnetic spectrum.**

***Index Terms*—Maritime Cyber Security, Unmanned Underwater Vehicle (UUV), Security Analysis, Threat Modeling.**

I. Introduction

Offshore underwater industry operations such as infrastructure installations, as well as inspection, maintenance, and repair (IMR), require a lot of underwater work [1]. This sector also involves deep sea exploration, exploitation of natural resources, and progressing maritime science. While crewed missions involving so-called remotely operated vehicles at the respective location are complex and costly, this challenging work can be mastered by a new class of underwater vehicles designed as extra-large uncrewed underwater vehicles (XLUUVs) [2]. These vehicles promise to be operated both in remotely controlled and autonomous modes without accompanying surface vessels and are suitable for transporting heavy payloads and energy-intensive missions. Furthermore, they may have a highly modular structure that is adaptable to various applications, such as the envisioned Modifiable Underwater Mothership (MUM) [3], cf. Fig. 1.

However, due to the high degree of autonomy and complete dependence on intact Information Communication Technology (ICT), uncrewed vehicles face a variety of cyber threats, ranging from cyber attacks against telecommunication [4] over sensor systems [5], [6] to malware insertion [7]. The threats' relevance arises not only from the observed increase in maritime cyber incidents [8], [9] but also from additional interference and manipulation activities, also within the electromagnetic spectrum [10], which are presumably related to the Russian attack on Ukraine [11]. Moreover, XLUUVs are valuable assets and comprise a lot of novel know-how, which makes them a particularly desirable target for cybercriminals. Therefore, sufficient robustness against a wide range of cyber attacks of all categories is essential to protect an XLUUV against hijacking, theft, blackmailing, and sabotage.

To this end, we systematically investigated the potential cyber attack surface in a dedicated threat analysis as an essential step towards a comprehensive cyber risk analysis of the new class of uncrewed underwater vehicles. Although the first security analyses of uncrewed surface vessels have already been conducted recently, cf. [12]–[15], to the best of our knowledge, a threat analysis of an XLUUV has not been presented in scientific literature yet. The main contributions of this paper thus comprise:

- a systematic XLUUV system analysis based on the representative MUM, particularly examining the XLUUV-specific challenges,
- a comprehensive threat analysis considering the identification of priority threats and identifying and reviewing critical system components.

Finally, while there is a lack of XLUUV security regulations, our work also contributes to their development and, moreover, creates the basis for suitable simulation and test environments.

II. Background

The growing need for underwater work in industry, environmental protection, and the maritime sciences goes along with two trends in developing suitable vessels [16]: A shift to submarine and uncrewed vehicles. Both trends are realized in uncrewed underwater vehicles (UUVs) and autonomous

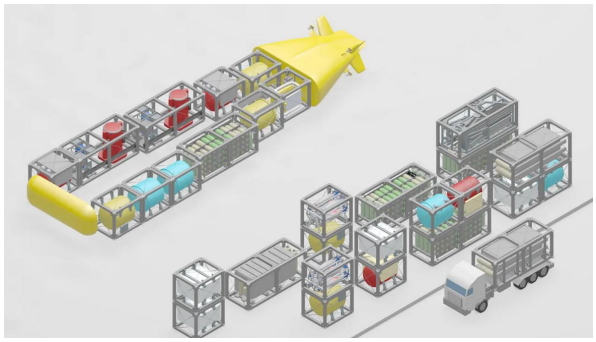

Fig. 1. Modular concept of the modifiable XLUUV MUM (source [3]).

underwater vehicles (AUVs), the latter being a subgroup of the former. UUVs do not need, and in fact are not designed to, accommodate a human operator onboard. While these vehicles are typically small and targeted to special purposes [16], larger vessels, i.e., XLUUVs, are needed for a multitude of different underwater tasks, including the transport, placing of heavy payloads in the deep sea, and IMR work in ocean regions challenging to access. Furthermore, precise positioning of XLUUVs without accompanying vessels is necessary for sensitive tasks like seafloor measurements.

A variety of XLUUV prototypes is available or under development. The military sector is particularly active in the field [17]. Prominent projects in the civilian sector are the Hugin Endurance developed by Kongsberg Maritime [18] and MUM, which is presently under development, and the authors of this paper are responsible for the cyber security aspects within the project [1]–[3], [19]. A demonstrator of MUM is planned to be operable in 2025. The overall goals of both projects are similar and include autonomy, modularity, long endurance and corresponding energy supply, heavy payloads, navigation quality, underwater and surface communication, and remote control. Many of these goals pose significant and partially new challenges in terms of cyber security.

Threat analysis has become a key component of modern-day cyber security analysis and cyber risk management. It has its background in software development, where it is an integral part of its Security Development Lifecycle [20]. Since then, the methods have been extended to threat analysis of general complex systems to increase the system's security and engineering and deliver more resilient and hardened products. Note, however, that threat analysis is an integral part of a full cyber security analysis and further steps are necessary to eventually judge the cyber security of an XLUUV, which are beyond the scope of this paper: Adequate security measures must be derived which prevent main threats or effectively mitigate their impact to an acceptable level as a residual risk.

Security requirements have the same direction of impact as security measures: if they are fulfilled, attacks become more difficult or even impossible. Various standards and guidelines for cyber security have been proposed, and Table I contains a selection of prominent examples, along with a brief description and information on their areas of application and technical depth. Of particular importance are the publications of the International Electrotechnical Commission (IEC) [21]–[23], which provide a risk-based approach to prevent and mitigate security risks. The standards have been transferred to the maritime domain by the classification societies [24], [25], serving to approve maritime systems. Among these, however, there are no cyber security requirements for UUVs, let alone XLUUVs. Therefore, an adaptation of available requirements is necessary to counter important threats effectively and hence make provisions for later international approval.

TABLE I
OVERVIEW OF A SELECTION OF RELEVANT SECURITY STANDARDS AND GUIDELINES USED TO DEVELOP NEW REQUIREMENTS FOR XLUUVS.

Document	Description	Appl.
NIST SP800-160 [26]	Cyber resiliency engineering framework	ICT ○
IT-Grundschutz [27]	IT baseline protection (and profiles [28])	ICT, Maritime ●
MITRE [29]–[31]	Cyber attack and defend frameworks	ICT, Industry ●
IEC-62443 [22, 23]	Technical and procedural cyber security	Industry ●
DNV-RP-G108 [32]	Security in the oil and gas industry	Maritime ○
DNV-RU-SHIP [25]	Security rules for ship classification	Maritime ●
BIMCO [33]	Risk management and security guidelines	Maritime ◐
IEC-61162-460 [34]	Security extension of IEC-61162-450	Maritime ◐
IACS E26/27 [35, 36]	Minimum set of security requirements	Maritime ◐

Domain: ICT, Industry/CPS, Maritime; Technical depth: ○ low – ● high

III. RELATED WORK

With the emergence of uncrewed, remote-controlled vehicles in a wide variety of domains and the associated total dependence on a reliable and fail-safe ICT, there is an inevitable need to also incorporate cyber risk assessment into established traditional risk analysis and drive forward research in this area. The first scientific work in this area can be found in the aviation sector, where unmanned aerial vehicles (UAVs) have existed for decades and are used particularly in the context of military operations. Based on current cyber attacks and their likelihood and impact, Javaid et al. [37], for example, present a goal-oriented approach to cyber security threat analysis that uses visual models, including architectures and threat trees, to explicitly address threat-related concepts.

In the maritime sector, Tam and Jones have made great strides in assessing cyber risk in traditional shipping with their holistic model-based MaCRA [38] framework. Driven by the development of uncrewed water-borne systems and pushed in particular by the recent realization of the first prototypes of large uncrewed cargo vessels, such as the YARA Birkeland, publications on cyber risk assessment of uncrewed and near-future autonomous ships are gradually appearing in the literature. With [12], the authors thus apply their framework to such autonomous vessels and describe a comprehensive threat analysis as a basis for risk assessment, which includes threats against navigation and sensor systems and a plurality of technologies onboard autonomous vessels.

Other related work from maritime cyber security research includes threat analyses from Kavallieratos et al., who, on the one hand, focus more on cyber attacks against autonomous ships as a basis for a well-founded threat analysis [39] and, on the other hand, carry out a qualitative risk analysis on this basis [13]. In contrast, the authors of [14] and [15] focus more on the methodology required for the actual threat analysis, which is also applied to the context of autonomous surface vessels and will be discussed in the following Section IV.

Despite the growing body of work in this area in recent years, there is still a lack of dedicated threat analyses for UUVs, particularly for novel XLUUVs, which represent an extraordinary value due to their size, versatility, capabilities, and specific purposes. This value and technological advantage alone increase the attraction of the asset for malicious actors and thus impacts threat modeling. In addition, however, there are other special properties that distinguish them from surface vehicles, such as significantly longer offline phases while on submerged voyages, during which no remote monitoring is possible for human operators on shore.

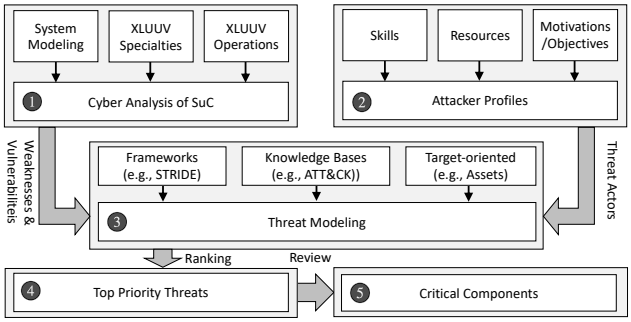

Fig. 2. Schematic representation of our procedure to threat analysis of an extra-large uncrewed underwater vehicle (XLUUV).

IV. Methodology

The essence of threat analysis is identifying all relevant threats and not to overlook important ones. A systematic implementation of threat modeling is supported by frameworks like STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privileges) and DREAD (Damage, Reproducibility, Exploitability, Affected users/systems, and Discoverability), cf. [13], [15], [20], as well as attack trees [40] and the focus on systems' assets [20]. Knowledge bases like MITRE ATT&CK [29], [41], [42] and the Common Vulnerabilities and Exposure (CVE) program, as well as the OWASP [43], can serve as a foundation for the development of specific threat models.

In this paper, these systematics were combined with our own experience in threat analysis in various technological fields and used in a holistic approach to model threats to an XLUUV in a structured and effective way. Figure 2 outlines the procedure, which comprises five main steps. The focus of the first step is an initial cyber analysis of the system under consideration (SuC) [21] ❶ (Section V), which is the overall XLUUV system with the land-side control station and necessary Internet infrastructures. Based on a systematic gathering of knowledge about the SuC, the specific characteristics of the vehicle, and the consideration of its operation, an abstracted model of the SuC is successively created. This model allows an initial cyber analysis revealing a first insight into the SuC's weaknesses and vulnerabilities. The latter are, however, only relevant for the cyber security of the SuC if they represent a realistic threat. To judge whether they may be exploited, it is necessary to know the potential attackers' profiles ❷ (Section VI), i.e., which skills, resources, and motivations the adversaries possess.

Threat modeling ❸ (Section VII) must combine the findings about the SuC's vulnerabilities with the attackers' assumed capabilities and objectives. In accordance with [20], we have also included assets of the SuC in our threat modeling, as, due to their outstanding value, they may particularly attract potential attackers. The outcome of threat modeling is a comprehensive set of threats to the SuC.

Ranking these threats, based on their likelihood and impact, leads to top-priority threats ❹ (Section VIII) posing security challenges. Participation in the MUM research project [3] allows us, in line with the security-by-design principle, to address these challenges during the early conception of the novel vehicle class and, hence, to effectively counter corresponding cyber threats. As in [44], the price of this early involvement is that the attack vectors and techniques remain on a high level as detailed design decisions for MUM are still pending.

The threat analysis is terminated by reviewing the SuC's components and identifying critical ones that need higher protection ❺ (Section IX). This is based on our experience in other fields and general knowledge about attack surfaces. In an iterative process, criticalities and preliminary assumptions of individual components are reviewed to determine whether they are particularly vulnerable to the identified priority threats.

V. Cyber Analysis of the System and Its Operation

This and the following Sections VI to IX present the results of our five-step threat analysis, as depicted in Figure 2. The SuC, on the highest structural level, consists of three components, as shown in Figure 3:

- the *XLUUV*, including its peripherals, e.g., a communication buoy and facilities for underwater positioning and communication (Section V-A),
- a *command and control center (C&CC)* to remotely control the XLUUV and to supervise it during autonomous operations as far as possible (Section V-B),
- and a *communication* system typically involving diverse communication technologies (Section V-C).

In Figure 3, the XLUUV, typically some tens of meters long, is depicted in a submerged state during a mission that involves a small remotely operated vehicle (ROV). Communication with the C&CC is provided by a communication buoy and a satellite-based communication (SatCom) link. The C&CC is usually located onshore. The XLUUV exchanges all necessary data with the C&CC via the communication links. Supervision is also provided by institutions like vessel traffic service (VTS), informing about marine traffic. The following paragraphs contain more security-relevant details of the three main components of the SuC.

A. Extra-Large Uncrewed Underwater Vehicle (XLUUV)

The *XLUUV* has a modular structure that makes it adaptable to a variety of use cases and corresponding missions [1], [2]. In particular, it comprises basic modules and mission modules. Basic modules like a guidance and control system (GCS) module and an energy supply module are needed in every

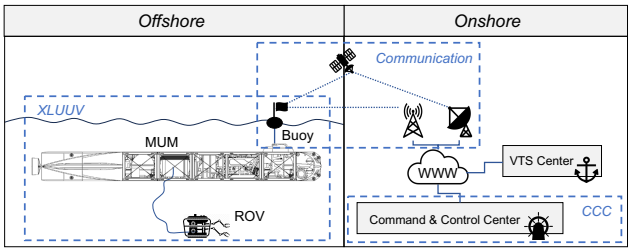

Fig. 3. The system under consideration (SuC) with its main components during an exemplary stationary IMR mission.

application. Mission modules are specific for a certain application of the XLUUV and may include heavy payloads or exploration equipment [44]. The discrimination between the two is important from a security point of view as basic modules are produced and hence under the control of the manufacturer, whereas mission modules are contributed by users or customers who are beyond the producer's control.

The paramount component of basic modules in an XLUUV is the GCS module, which navigates the XLUUV, regulates and monitors its position, and maneuvers. The GCS receives information about the XLUUV's environment through sensors and can initiate action through its actuators. The GCS is connected with the trim and diving system and the thrusters.

B. Command & Control Center (C&CC)

An XLUUV needs a *C&CC* entity outside itself where its regulation, control, and monitoring are executed. The C&CC may be located onshore or on an accompanying vessel and provides the traffic situation, radar, video data, and other information regarding the XLUUV's position and movements to operators. The XLUUV must be able to receive data and commands from the C&CC during its operation. Vice versa, the C&CC must be able to download data that were gained during the XLUUV's mission.

The C&CC is needed for both remotely controlled and autonomous operation of an XLUUV. If the XLUUV is operated under remote control, the C&CC will be permanently in charge during the entire mission. If the XLUUV is in autonomous operation, the role of the C&CC is reduced to monitoring and backup actions in case of operational failures. Mission plans must have been loaded into the XLUUV's GCS beforehand, and the C&CC observes their correct execution. The spectrum of processable information ranges from simple waypoint plans to complex maneuvering for reactive autonomy.

C. Communication

Communication and reliable data exchange between the XLUUV and the C&CC are indispensable for the XLUUV's safe operation. Diverse communication technologies may be used to provide redundancy in this safety-critical component of the system. In the case of MUM, redundancy is foreseen by a multi-link connection between the XLUUV and the C&CC. MUM must be able to autonomously establish a communication connection with the C&CC.

The diverse communication technologies can be grouped depending on the distance between the XLUUV and its C&CC: In the short range, WiFi 802.11 may be used, whereas public land mobile networks, e.g., LTE, may be suitable for mid-range and SatCom, e.g., Starlink, is appropriate for long range. In a submerged state, a communication buoy may be deployed to establish a reliable connection to the C&CC.

MUM's XLUUV-internal communication has a ring structure with switches connected to all modules. While this topology offers redundant routes for each connection, it also may be a potential threat as it provides a direct connection between trustworthy basic and non-trustworthy mission modules.

D. Synthesis

Altogether and beyond a mere system description, the cyber analysis of the SuC, as part of a threat analysis, reveals already in the early stadium of system modeling weaknesses, vulnerabilities, and potential attack surfaces. Obviously, the system is vulnerable in all three main components discussed above, making parts of the XLUUV, like the GCS, the communication with the C&CC, and the C&CC itself candidates for critical components of the SuC from the very beginning. Furthermore, cyber attacks may remain undetected for extended time spans since XLUUVs are uncrewed and designed to be underway for longer mission durations and far from direct human control. The aspired high modularity makes physical access easier, and mission-specific modules may be included in an XLUUV as "black boxes" offering backdoors for malicious entry attempts. The internal communication within the XLUUV is endangered by the fact that it must establish connections between third party modules and the GCS.

VI. Attacker Profiles

While Section V extracted SuC features relevant from a cyber security perspective, this section is devoted to the potential attackers' side and their conceptions. Attackers or, in the context of threat analysis, *threat actors* use weaknesses in systems to achieve their individual attack objectives. Generally, their profiles vary enormously. We, therefore, focus on those profiles that are particularly relevant for XLUUVs.

There exist catalogs of attacker types available in the scientific literature (e.g., [38]) and also in dedicated maritime guidelines (e.g., [33]), displaying a vast diversity of potential attackers. It ranges from playing "script kiddies" over professional criminals to state organizations. However, not all threat actors are equally relevant or relevant at all in the context of an XLUUV. We have carefully examined attacker groups regarding their technical skills, available resources, motivations, and objectives pursued.

As a result of our deliberations, Table II enumerates those threat actors considered as most relevant in the XLUUV context. The list includes "accidental actors" who damage the system accidentally or without malicious intentions. Cybercriminals must be taken into account as an XLUUV comprises a lot of novel know-how and smart high-tech solutions. For the same reasons, competitors could have a corporate interest in spying on an XLUUV. Internals may seek revenge for perceived unjust treatment and usually need fewer resources than external actors as they have professional access to the system. Eventually, hacktivists have been included in the list since the missions of an XLUUV often pursue objectives that engaged environmentalists may combat.

In its last column, Table II contains a security level (SL) corresponding to the definitions given in IEC 62443 4-2 [23] where four security levels are discriminated. Starting from SL-1 to protect against casual exposure or accidental misuse, a higher SL is required to mitigate intentional misuse, where adversaries have more and more extensive resources at their disposal, specific knowledge, and possess high motivation. In summary, internals and competitors represent the most important threat actors, followed by cybercriminals and hacktivists.

TABLE II
THREAT ACTORS RELEVANT FOR XLUUVS WITH THEIR PROFILE AND ASSIGNMENT OF THE NECESSARY SECURITY LEVEL (SL).

Threat Actors	Skill	Resources	Motivation / Reason	Objectives	IEC SL [23]
Accidental	low	low	no malicious motive / lack of care	none	SL-1
Hacktivists	high	medium	political conviction	disruption of operation, publication of sensitive data	SL≥3
Cybercriminals	high	diverse	financial gain, commercial espionage	fulfill assignment	SL≥3
Internals	diverse	diverse	revenge, disgruntlement	destruction, blackmailing, reputational damage	SL-4
Competitors	high	high	corporate interests, industrial espionage	competitive advantage, reputational damage	SL-4

VII. THREAT MODELING

Threat modeling combines both the system analysis (Section V) and the capabilities of potential attackers (Section VI) to achieve the overall goal of threat analysis, i.e., to identify all relevant threats. The results are based on applying various methods (cf. Section IV) and represent a holistic approach to achieving the overall goal. From the abundance of work invested in threat modeling, two illustrating examples of specific relevance for XLUUVs are presented below.

A. Asset-focused Modeling

One way of approaching threat modeling is focusing on assets, i.e., things attackers want and things an owner aims to protect [20]. An *XLUUV as a whole* is a high-tech vehicle with a considerable value. Furthermore, it comprises a lot of novel know-how and a variety of precious components, including highly sophisticated instrumentation, *hardware*, *software*, and sensor systems. On a mission, it is equipped with additional, mission-specific modules and may collect *mission data and information* of interest e.g., from competitors. Thus, an XLUUV is a typical candidate for asset-focused modeling.

Figure 4 depicts the XLUUV's assets and relevant threat actors, their objectives, and potential actions. All types of threat actors identified as relevant for an XLUUV (cf. Table II) except accidental actors are involved when the focus is on assets. Their interaction with assets, however, is different. While cybercriminals, competitors, and corrupt internals are attracted by the assets and may want to steal them, hacktivists and disgruntled internals are not chasing the values but may have the intention to destroy them, be it by demolition or be it by hampering a mission. The latter is not only a material loss but also damages the reputation of the XLUUV owner as being unable to accomplish a mission reliably.

B. Threat Tree-focused Modeling

In the style of attack trees [40], numerous threat trees have been produced during our examinations and the second

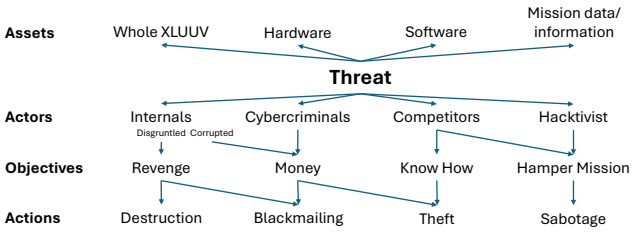

Fig. 4. Assets of an XLUUV, threat actors, and their objectives and their actions to achieve them.

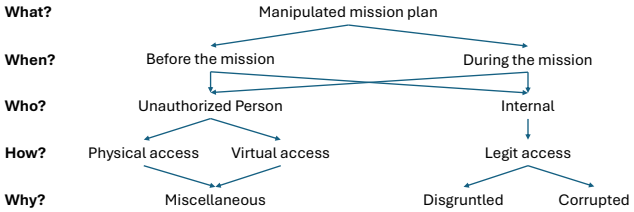

Fig. 5. Example threat tree for a manipulated mission plan.

example of threat modeling deals with one of those. The example relates to a mission that the XLUUV undertakes. The threat is that the mission plan is manipulated. The example is of particular relevance for an XLUUV because, at least in the case of MUM, it is foreseen that the mission plan could have to be altered during the mission so that such an actual change does not come as a surprise and a manipulation does not attract immediate attention as an anomaly.

A mission typically involves transferring an XLUUV from a starting point (e.g., the harbor) to a target mission site. The operational part of the mission may be carried out remotely by an expert team working in the C&CC, resulting in a third party having physical access to the C&CC. In the case of MUM, the ride to the target location shall be performed autonomously, after having left the high-traffic zone. Thus, the scenario may involve several characteristics of an XLUUV and its operation: Missions, remote and autonomous operations, and experts from third parties working in the C&CC.

Figure 5 displays a threat tree addressing the situation in a structured manner. The tree's root, i.e., the threat, is that the mission plan is manipulated. The mission plan could have been maliciously altered before it was included in the XLUUV's GCS or the mission plan could have been manipulated later during the mission. The mission plan may be forged by an internal or unauthorized person. The latter needs access to the system, whether virtually or physically, while an internal has legit access by its very position. The reasons why internals act as attackers may be that they are disgruntled or corrupted. In contrast, an unauthorized person can be any other threat actor with pertaining objectives (cf. Table II).

VIII. TOP-PRIORITY THREATS

The two cases exemplify how the various methodologies for threat modeling (cf. Section IV) are used to gradually identify the most important threats to the SuC. Threat modeling yields, in a first step, a large set of conceivable threats, but with very different likelihoods and impacts. To rank them according to their security importance, each was assigned a priority level

TABLE III
TOP-EIGHT ATTACK VECTORS FOR XLUUVS WITH ATTACKER-SPECIFIC AND INTEGRAL LIKELIHOOD AND OVERALL IMPACT.

Nr.	Attack	Trgt. Point	Description / Example	Accidental	Hacktivist	Cybercriminals	Competitor	Internal	Likelihood	Impact
1	Supply chain	Entire SuC	Supplied components or 3rd-party software are unknowingly integrated into the XLUUV.							
2	Malware	GCS	Infiltrated malware or manipulated software maliciously interacts with the GCS.							
3	Malware	C&C	Mission plans and XLUUV navigation may be maliciously altered.							
4	Mal. device	Basic module	Manipulated device firmwares could expose access to the internal communication network.							
5	Mal. device	Payload	Untrustworthy 3rd-party payload modules may been compromised prior to their integration.							
6	Physical access	Entire SuC	Peripherals, e.g., the communication buoy or the ROV, can serve as physical entry points.							
7	Communication	Ext. comm.	WiFi enables close-range access, while distant attackers may interact with ext. interfaces [4].							
8	Electromagnetic	Ext. sensors	Sensors the XLUUV relies on, such as GNSS [6], or AIS [5], can be jammed or spoofed.							

Color-coded risk: low mid high Probability is considered lower but not negligible.

based on two factors. The first factor represents the efforts a threat actor must undertake to conduct the corresponding attack successfully. The second factor takes the impact of each attack into account. Both factors were then combined into the overall priority level ranking, similar to, e.g., [13], [21], [39].

Based on this prioritization, eight top-priority threats were identified. Table III presents, for each of the eight priority threats and corresponding attacks, their target points together with a brief description. The subsequent actors' columns combine these threats with those actors identified as relevant for an XLUUV (cf. Table II) in a colored matrix structure, highlighting the threat probability of each attacker profile. Finally, the last two columns contain the resulting overall likelihood of a threat, weighed over the actors, along with its potential impact. Note that these quantifications are based on expert knowledge and the subjective assessment of the authors. They are to be understood relative to the top-priority threats, all of which have a higher security significance than other threats.

Altogether, the results show that cyber and electromagnetic attacks against communication and sensor systems 7 and 8, malware in the GCS 2 and malicious devices in basic modules 4 pose the most relevant threats to an XLUUV. This result would be further reinforced when state-level actors were to be taken into account.

IX. BASIC PROTECTION AND CRITICAL COMPONENTS

Based on the threat modeling (Section VII) and the identified top-priority threats (Section VIII), we have reviewed our initial ideas (Section V-D) the critical components of the SuC. The following five critical components have been identified: the GCS, the C&CC, external interfaces and communication, internal interfaces and communication, and data management.

The criticality of the first three components is intuitive since these components are directly at risk from external threats. The result of our analysis underlines that they offer attack surfaces for priority threats 1–3, 7, and 8. In addition, internal interfaces and communication are a critical component, as compromised XLUUV modules (threats 4 and 5) pose a significant threat through the internal communication network. Successful attacks of the GCS, the C&CC, and the related internal and external communication may make the SuC a complete victim of the attackers. Finally, as sensitive management data may be manipulated or mission data stolen after physical access (threat 6) has been established, data management is another critical component. Successful exploits of the weaknesses in data management may open backdoors to XLUUV manipulations and its missions.

Security-critical components should be protected at an elevated security level, i.e., level SL-2 or higher [23]. In addition, a valuable and complex system like the SuC must inevitably have a basic protection corresponding to SL-1 of [23]. It is thereby protected against common unintentional or accidental misuse (cf. Table II). Furthermore, SL-1 provides protection against many cases of untargeted attacks and forms the foundation for cyber protection as part of holistic risk mitigation [47].

X. CONCLUSION

In this paper, we briefly describe our approach and our results of a comprehensive threat analysis of a new, powerful class of future multipurpose underwater vehicles which, as being uncrewed, partly autonomously operating systems, urgently need protection against various threats from cyberspace and the electromagnetic spectrum.

The XLUUV demonstrator of MUM is scheduled to be available by the end of 2025, and our accompanying research on the vehicle's cyber security will continue accordingly. The threat analysis will be embedded in a full security analysis, including a refined risk evaluation of the top-priority threats and the determination of further design details for MUM. Suitable intrusion detection and security measures will be identified to finally make the XLUUV sufficiently cyber-resilient. Simulation and test environments already exist for traditional surface vessels [45], [46] but are just emerging for XLUUVs, e.g., [19]. Those environments are urgently required for the targeted development and validation of tailored countermeasures and cyber defense strategies and are planned as part of the MUM project.

ACKNOWLEDGMENTS

This work is part of the project MUM2 [3]. It was partially funded by the German Federal Ministry of Economic Affairs and Climate Action (BMWK) within the "Maritime Research Programme" with contract number 03SX543B managed by the Project Management Jülich (PTJ). The authors are responsible for the contents of this publication.

REFERENCES

[1] M. Golz, F. Boeck, S. Ritz, G. Holbach, N. Richter, P.-M. Haselberger, W. H. Wehner, M. Schiemann, E. Rentzow, T. Müller, and T. Jeinsch, "MUM – Large Modifiable Underwater Mother Ship: Requirements and Application Scenarios," in *Proc. of OCEANS – MTS/IEEE Kobe/Techno-Oceans (OTO)*, Port Island, Kobe, Japan, 2018.

[2] W. H. Wehner, N. Richter, M. Schiemann, P.-M. Haselberger, S. Ritz, M. Golz, and F. Boeck, "Mastering High Product Variety of an Underwater Vehicle Class in the Concept Design Stage," in *Proc. of the International Conference on Offshore Mechanics and Arctic Engineering (OMEA)*, Madrid, Spain, 2018.

[3] The MUM-Project, "Large Modifiable Underwater Mothership." [Online]. Available: https://www.mum-project.com

[4] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "A Tale of Sea and Sky On the Security of Maritime VSAT Communications," in *Proc. of the IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2020.

[5] M. Balduzzi, A. Pasta, and K. Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proc. of the Computer Security Applications Conference (ACSAC)*, New Orleans, LA, USA, 2014.

[6] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships Via False GPS Signals: Demonstration and Detection," *Journal of the Institute of Navigation*, vol. 64, no. 1, 2017.

[7] P. H. Meland, D. A. Nesheim, K. Bernsmed, and G. Sindre, "Assessing cyber threats for storyless systems," *Journal of Information Security and Applications*, vol. 64, 2022.

[8] M. Schwarz, M. Marx, and H. Federrath, "A structured analysis of information security incidents in the maritime sector," *ArXiv*, vol. abs/2112.06545, 2021.

[9] P. H. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim, "A Retrospective Analysis of Maritime Cyber Security Incidents," *TransNav*, vol. 15, no. 3, 2021.

[10] D. Goward, "From Russia with love for Christmas: Jamming Baltic GPS," GPS World – GNSS Positioning Navigation Timing, Jan. 2024. [Online]. Available: https://www.gpsworld.com/from-russia-with-love-for-christmas-jamming-baltic-gps/

[11] R. Cichocki, "State-Sponsored and Organized Crime Threats to Maritime Transportation Systems in the Context of the Attack on Ukraine," *TransNav*, vol. 7, no. 3, 2023.

[12] K. Tam and K. Jones, "Cyber-Risk Assessment for Autonomous Ships," in *Proc. of the Internatioonal Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Glasgow, UK, 2018.

[13] G. Kavallieratos and S. Katsikas, "Managing Cyber Security Risks of the Cyber-Enabled Ship," *Journal of Marine Science and Engineering*, vol. 8, no. 10, 2020.

[14] J. Yoo and Y. Jo, "Formulating Cybersecurity Requirements for Autonomous Ships Using the SQUARE Methodology," *Sensors*, vol. 23, no. 11, 2023.

[15] R. Sahay, D. S. Estay, W. Meng, C. D. Jensen, and M. B. Barfod, "A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS," *Computers and Security*, vol. 128, no. C, may 2023.

[16] J. Neira, C. Sequeiros, R. Huamani, E. Machaca, P. Fonseca, and W. Nina, "Review on Unmanned Underwater Robotics, Structure Designs, Materials, Sensors, Actuators, and Navigation Control," *Journal of Robotics*, vol. 2021, 2021.

[17] H. I. Sutton, "Naval Group Reveal XLUUV Demonstrator," http://www.hisutton.com/Naval-Group-XLUUV.html (accessed 2023-06-06).

[18] Kongsberg Maritime, "Hugin Endurance AUV," 2024. [Online]. Available: https://www.kongsberg.com/globalassets/discovery/commerce/surveillance--monitoring/hugin-endurance/473631a_hugin_endurance_datasheet.pdf

[19] K. Wolsing, A. Saillard, E. Padilla, and J. Bauer, "XLab-UUV – A Virtual Testbed for Extra-Large Uncrewed Underwater Vehicles," in *Proc. of the 1st IEEE Workshop on Maritime Communication and Security (MarCaS)*, Daytona Beach, FL, USA, 2023.

[20] A. Shostack, *Threat Modeling: Designing for Security*. Wiley Publishing, 1st edition, 2014.

[21] IEC 62443-3-2, "Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design, Edition 1.0," International Electrotechnical Commission (IEC), June 2020.

[22] IEC 62443-3-3, "Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels, Edition 1.0," International Electrotechnical Commission (IEC), August 2013.

[23] IEC 62443-4-2, "Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components, Edition 1.0," International Electrotechnical Commission (IEC), February 2019.

[24] DNVGL-CP-0231, "Class Programme – Type approval – Cyber security capabilities of systems and components, Edition March 2020," DNV, March 2020.

[25] DNVGL-RU-SHIP-Pt6, "Rules for Classification – Ships – Part 6 Additional class notations Chapter 5 Equipment and design features, Edition July 2020, Amended October 2020," DNV, October 2020.

[26] NIST Special Publication 800-160, "Developing Cyber Resilient Systems: A Systems Security Engineering Approach," Vol. 2 Rev. 1, National Institute of Standards and Technology (NIST), 2021.

[27] BSI, "IT-Grundschutz-Compendium," Bonn, Germany, 2022, German Federal Office for Information Security (BSI).

[28] VHT, "IT-Grundschutz-Profil für Reedereien – Mindest-Absicherung für den Schiffsbetrieb," Bremen, Germany, 2020, Verein Hanseatischer Transportversicherer e.V. (VHT).

[29] MITRE, "MITRE ATT&CK Framework," The MITRE Corporation, 2024. [Online]. Available: https://attack.mitre.org

[30] ——, "MITRE ATT&CK ICS Matrix," The MITRE Corporation, 2024. [Online]. Available: https://attack.mitre.org/matrices/ics/

[31] ——, "MITRE D3FEND Framework," The MITRE Corporation, 2024. [Online]. Available: https://d3fend.mitre.org

[32] DNVGL-RP-G108, "Recommended Practice – Cyber security in the oil and gas industry based on IEC 62443, Edition September 2017," DNV, September 2017.

[33] BIMCO, "The Guidelines on Cyber Security Onbaord Ships (Version 4)," The Baltic and International Maritime Council (BIMCO) 2020.

[34] IEC 61162-460:2018, "Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security," International Electrotechnical Commission (IEC), 2018.

[35] IACS, "UR-E26 – Cyber resilience of ships," IACS Unified Requirements, Apr. 2022.

[36] ——, "UR-E27 – Cyber resilience of on-board systems and equipment," IACS Unified Requirements, Apr. 2022.

[37] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System," in *Proc. of the Conference on Technologies for Homeland Security (HST)*, Waltham, MA, USA, 2012.

[38] K. Tam and K. Jones, "MaCRA: a Model-Based Framework for Maritime Cyber-Risk Assessment," *WMU Journal of Maritime Affairs*, vol. 18, 2019.

[39] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber-attacks against the autonomous ship," in *Proc. of the Int. Workshop on SECurity and Privacy Requirements Engineering (SECPRE 2018)*, Barcelona, Spain, 2019.

[40] J. M. Couretas, *An Introduction to Cyber Analysis and Targeting*. Springer, 2022.

[41] A. Yousaf and J. Zhou, "From sinking to saving: MITRE ATT&CK and D3FEND frameworks for maritime cybersecurity," *International Journal of Information Security*, Jan. 2024.

[42] S. Roy, E. Panaousis, C. Noakes, A. Laszka, S. Panda, and G. Loukas, "SoK: The MITRE ATT&CK Framework in Research and Practice," *ArXiv*, vol. 2304.07411, 2023.

[43] Open Web Application Security Project (OWASP), "OWASP Top Ten," website, Oct. 2021. [Online]. Available: https://owasp.org/www-project-top-ten/

[44] S. Ritz, A. Loewe, and J. Bauer, "Specialties of HAZID-Study for Large Unmanned Underwater Vehicles," in *Proc. of OCEANS 2023 – Limerick*, Limerick, Ireland, 2023.

[45] K. Tam, K. Forshaw, and K. Jones, "Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities," in *Proc. of the International Conference on Marine Engineering & Technology (ICMET)*, Oman, 2019.

[46] J. Bauer, J. Kutzner, P. Sedlmeier, A. Rizvanolli, and E. Padilla, "Phish & Ships and Other Delicacies from the Cuisine of Maritime Cyber Attacks," in *Proc. of the European Workshop on Maritime Systems Resilience and Security (MARESEC)*, Bremerhaven, Germany, 2023.

[47] S. Ritz, A. Loewe, J. Bauer, and M. Kurowski, "By-Design Risk Mitigation for Large Uncrewed Underwater Vehicles (UUVs)," in *Proc. of the European Workshop on Maritime Systems Resilience and Security (MARESEC)*, Bremerhaven, Germany, 2024.