Proc. of MARESEC 2024
DOI: 10.5281/zenodo.14214260

By-Design Risk Mitigation for Large Uncrewed Underwater Vehicles (UUVs)

Sebastian Ritz[1], Anna Loewe[2], Jan Bauer[3], and Martin Kurowski[4]
[1]TU Berlin, Design and Operation of Maritime Systems, Berlin, Germany. ORCID: 0009-0004-5136-4290
[2] Consultant, Roskow, Germany. ORCID: 0009-0004-2635-6176
[3]Fraunhofer FKIE, Cyber Analysis & Defense, Wachtberg, Germany. jan.bauer@fkie.fraunhofer.de
[4]University of Rostock, Institute of Automation, Rostock, Germany. martin.kurowski@uni-rostock.de

***Abstract*—In the age of technological advancement and the constant evolution of Uncrewed Underwater Vehicles (UUVs) with ever-increasing scopes, applications, and autonomy, it is crucial to identify and manage potential risks at the design stage to ensure their safety and efficiency. Such risk management is more important, in particular, given the increasing demand for monitoring and securing critical maritime infrastructure.This paper presents a generic set of ideas of how risks can be mitigated for large and extra-large UUVs. A risk ranking matrix, a result of a Hazard Identification Study (HAZID) study for those UUVs, forms the basis for developing methodologies and systems to mitigate the identified risks and hazards. This is done for the three main systems, i.e., mechanical system, energy system, and autonomy, as well as for the orthogonal topic of cyber security. Each system and its subsystems have their risk classification and need specialized techniques to mitigate the risks to a tolerable level considering costs and probability.**

***Index Terms*—UUV, HAZID, Risk Mitigation, Failure Mode and Effect Analysis (FMEA)**

I. Introduction

The market of large and extra-large Uncrewed Underwater Vehicles (XLUUVs) is growing as well as the physical size of the vehicles themselves. A selection of large and XLUUVs are e.g., Dive-LD (5.8 m) [1], SOLUS LR (8.5 m) and XR (12 m) [2], Hugin Endurance (10 m) [3], Ghost Shark (est. 12 m) by Anduril, Orca (26 m) by Boeing and Huntington Ingalls Industries.Already last year, four of those vehicles were proofed in sea trails. The large Modifiable Underwater Mothership (MUM) (25-50 m) [4] with multiple potential applications [5] will prove its performance by the end of 2025. The US Navy expects the delivery of five more Orca vehicles in the second half of 2024 [6] and Anduril announced to open large-scale production facility in the US with a capability of up to 200 vehicles per year [7].

The risks associated with these large maritime systems are much higher than smaller vehicles. Hence, a Hazard Identification Study (HAZID) study was performed in [8]. The severity and probability of all identified risks were rated within this study. This rating, although done by multiple experts, is a subjective estimation of these experts. Therefore, all known risks have to be reduced to an acceptable level. The accident of the German submarine U27 collided with the offshore platform Oseberg B. in 1988 e.g. demonstrated, that there is more than a potential risk and that severity is also not negligible. The repair had a final cost of about 80 million NOK (1988 value, est. 16.5 million € today) [9] and could be classified as low, as no person was injured or killed, no environmental impact was caused, and the production of the Oseberg oil field was not interrupted significantly.

An approach to develope methodologies, strategies, and systems to mitigate the identified risks and hazards is the focus of this paper. As this work is based on the recent HAZID study, it is also performed for a large generic UUV to ensure its transferability to other systems. Furthermore, it focuses on the bridge-related functions of voyage, control & monitoring, and abnormal situations, related to the SafeMASS-Report from Det Norske Veritas (DNV) [10], and neglects all deck-related functions as well as all functions in docked conditions. Despite the focus on generic UUVs, the system structure of this study is based on own work within the projects MUM2 [11] and CIAM. Fig. 1 shows a 25 m configuration of the MUM system as an XLUUV example.

This paper will give a short overview of the methods and an application scenario (Sec. II) used to identify the mitigation measures. For the analysis, the UUV was divided into four main systems and their subsystems that are assessed in individual sections. The main systems are the mechanical and electrical systems (Sec. III); the autonomy system (Sec. IV); and the cyber security as a non-physical orthogonal system (Sec. V). Finally, Section VI concludes the paper.

II. Background

A. Methodology

Based on a HAZID study for large UUVs [8], risk mitigation measures are defined to increase the safety and reliability of the system. This is done for each of the four main systems a large UUV consists of. With the help of a risk assessment, both existing and potential hazards are identified and prevented or reduced by taking protective measures that also include occupational safety and environmental protection.In the case of uncrewed vehicles, the inherently safe design and subsequently technical protective equipment are the main scope.

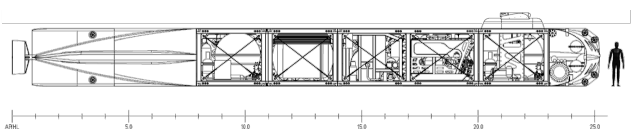

Fig. 1. Modular concept of the modifiable XLUUV mothership MUM (source thyssenkrupp Marine Systems).

Organizational protective measures have to be implemented to the autonomy, especially for untethered vehicles. Personal protective equipment plays a minor role, especially in this case, when neglecting all deck-related functions. The safe design aims to reduce or replace risks, hazardous materials, and processes within a system. In maritime vehicle design, this is done by selection of reliable components with known failure performance.

The protective measures can be divided into prevention and detection measures. Prevention measures reduce or prevent the occurrence of a cause of failure. For detection, measures are used to detect the causes of faults early so they can be counteracted. With the defined protective measures, the risks are reassessed and repeated until an acceptable risk is reached.

In this study, the potential causes for the identified risks and hazards from the HAZID study [8] are taken. For this, all components involved in a failure are tagged and their types of malfunction are figured out by the guide words of the HAZID. Subsequently, the measures for each component are defined. Multiple measures for one risk are assessed, regarding Space, Weight And Power and Cost (SWAP-C) with priority to production cost. Of course, the main requirement is to decrease the risk to an acceptable level.

B. Showcase Application

As the variety of risks and mitigation measures are too extensive for this paper, it is focused on the inspection phase of the scenario "Inspection & Maintenance of offshore wind turbines", related to [5]. This phase is visualized in Fig. 2. The UUV mothership is submerged in the wind farm and navigates to the next inspection site. After arriving, it does dynamic positioning and launches a midsize work class Remotely Operated Vehicle (ROV) to perform the inspection. Subsequently, the ROV will be recovered and the UUV will head for the next inspection site. This mission is performed under the supervised autonomy of an operator in a Remote Control Center (RCC). For stable communication with the mothership, it launches a communication buoy, which enables satellite communication, radio link, or Wi-Fi depending on the distance to the RCC. This application is chosen as wind parks are part of the maritime critical infrastructure [12] and are rapidly growing for the energy transition with an equally growing demand for inspection, maintenance, and repair. Furthermore, this application represents periodic tests over years on homogeneous structures, which facilitate mission automation, both make it economically beneficial.

The considered risks are colliding with the turbine or converter platform, grounding causing damage to cables, unwanted emerging and collision, e.g., with a crew transfer vessel, and the own operational risks from a mission aboard to total loss. Reasons for these risks, neglecting their cause, could be a fault in navigation or position determination, a malfunctioning diving or propulsion system, a leak, or a malfunction of operational procedures. The causes of these reasons and especially their mitigation are the subject of the presented study.

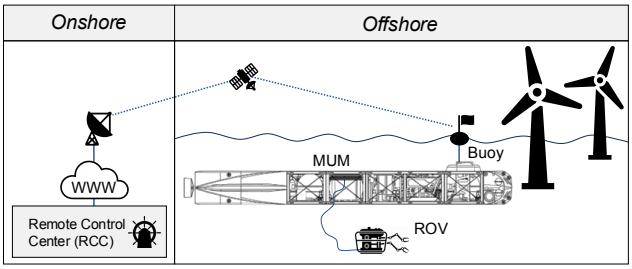

Fig. 2. MUM during a stationary wind park inspection mission.

III. Mechanic System and Energy System

The mechanic system consists of the vehicle structure and outfitting, but also of propulsion, actuators, and sensing as well as auxiliary systems. Whereas all energy sources, commonly used battery and fuel cells, and the power distribution belong to the energy system. These systems are handled in this context together, as their mitigation measures are in general on top level the same. They incorporate a robust design and construction/dimensioning, redundant components & functions, and fail-safe strategies.

A. State-of-the-Art Design Rules

A result of the HAZID study [8] is that the mechanical and energy system had already an acceptable risk or could reach it with minor measures. The main reason is that engineers have handled structural integrity, electrical installations, and mechatronics for a long time and have a corresponding range of experience. These include, in particular, mechanical and electrical workloads and extreme load conditions with their probability.

All these and additional requirements are also defined in the rules and guidelines of the class societies, e.g., in DNV's "Rules for Classification" for underwater technology Part 1–7 [13], of which the latest edition (July 2024) has a particular section "additional requirements for XLUUV" [13, Pt. 5, Ch. 7]. Compliance with the mentioned rules does not lead necessarily to heavy, costly, or complex systems, as also innovative solutions, that fulfill the requirements could be approved. Also, especially for XLUUVs, the approval of a class society is mandatory to get legal authorization to take part in marine traffic.

B. Redundancy

Redundancy is frequently used to mitigate risks caused by malfunctions or failure of components or system functions. Redundancy, in a technical context, means the additional presence of functional equal or comparable resources within a system to avoid a single point of failure and thereby the failure of the complete system.

Component redundancy means the same component is present at least twice in the system. An example is two main propulsion, as used in the MUM vehicle [14]. As they are usually used in parallel and a failure in one component could be compensated by the others without interruption, it is called hot-spare or active redundancy.

Functional redundancy describes the takeover of the function of a downed component by another different component. The diving depth, for instance, will be controlled by the thruster when the ballast system fails. Or in the case that both main propulsion fail, the maneuvering thrusters could be used. For the MUM vehicle, this would be two pump jets and vectorized thruster could be used for other vehicles.

Dissimilar redundancy is an important requirement in component redundancy, since the probability of a failure due to the operating period will be the same if the same component from the same supplier is used for redundancy. Furthermore, failures caused e.g. by faulty firmware, utilized parts, or production faults will lead to component failure within a short period of time. The requirement of dissimilarity is not just related to hardware, but also to software. A full implementation means that, e.g., a redundant vehicle motion controller should be designed and implemented, in the best case, by another development team, with another programming language and on another execution hardware.

Multiple redundancy and voting logic come into play when two active redundant components behave differently, e.g., two pressure sensors sending different values. In this case, triple redundancy and a voting logic could help, which means, the voting logic gets a value from each of the three sensors and identifies and ignores the faulty one. For this fault detection, model systems could also serve as a redundant system for voting comparison, cf. Sec. IV. The redundant implementation of a simple sensor seems easy, but it gets much more complex with more advanced sensors like obstacle avoidance sonars or even the vehicle controller. For all systems, it is important how the system should behave in the event of a fault.

- Fail-Passive: The system gets, if possible, controlled and shut down, with the result that a slightly positive buoyant UUV will surface slowly and float around with all risks from collision to total loss.
- Fail-Safe: The UUV gets a safe mode, which could be the return on a known track back to a safe starting point, where it could be maintained or an anchoring maneuver to wait for help.
- Fail-Operational: The system stays operational despite the occurrence of a failure, which is the best option.

From stage to stage, the implementation will get more complex and costly. Furthermore, the type of behavior could not be chosen freely, as it depends mainly on the faulty component and their relevance for the vehicle and the mission and its phase during the fault occurs.

An effective implementation to reach a fail-safe mode for the control hardware could be the use of a flight controller from the Uncrewed Arial Vehicle (UAV) market. Usually, these have already an integrated inertial measurement unit (IMU) for basic dead reckoning, multiple interfaces like CAN and Ethernet and a small SWAP-C footprint. Basic operational procedures could be implemented and the activation could be done by a watchdog of the main controller.

Disadvantages are mainly the impact of redundancy on SWAP-C, as additional components add weight to the system, need space, and consume power as well as their acquisition costs money. All this has to be considered in the vehicle design, whereby the importance of early consideration of redundancy in the design process is emphasized. Moreover, redundancy in software has to be taken into account in an early stage as it does not need space or add weight as long as the execution hardware stays the same. It may require a little more power and for certain more costs and development time for implementation.

Furthermore, all these measures could lead to less reliability of the system caused by the higher complexity and the linked probability of design and development faults. Therefore, another risk assessment should be conducted for the development of these more complex implementations.

IV. Fault tolerance for autonomous operations

When talking about the operation of uncrewed vehicles, automated functions for vehicle guidance play a key role. In the context of small underwater vehicles, the term autonomy is often used when operations are limited in time and area. For extra-large UUVs described here, significantly differing requirements for autonomy have to be addressed, which are comparable to aspects of the development of autonomous functions in maritime shipping [15]. Especially for the maritime sector, different institutions have defined comparable automation levels from manual to autonomous operation, e.g., [16] refers to safety-critical maneuvering situations.

In times of increasing complexity and strong interaction between technical systems, faults often have a significant impact on the safety and availability of the mission. As a result, various procedures are combined with the focus on fault-tolerant mission execution. These are designed to ensure the stability and quality of missions even under the influence of faults. This requires the classification of faults and malfunctions according to their effect and possible countermeasures.

A. Operational Fault Detection

To avoid hazardous situations, it is necessary to be able to detect faults that occur during operation. For this purpose, fault diagnosis algorithms are used that can be divided into tasks

- fault detection, i.e., the detection of a faulty system status,
- fault isolation, i.e., determining the faulty component (fault location), and
- fault identification, i.e., determining the type and extent of the fault,

with increasing complexity, where Fault Detection and Isolation (FDI) is used as a common abbreviation. The FDI algorithms are categorized into model-based, signal-based, knowledge-based, and hybrid/active approaches [17]. Model-based algorithms can be used if the motion behavior of the vehicle is represented by a dynamical model, as it applies for the MUM system concept [18].

Faults are usually divided into actuator, component, and sensor faults according to where they occur. In this context, model-based FDI methods are mainly used to detect mission-influencing faults such as actuator faults (e.g., thruster failure or reduced drive power of a thruster), component faults that change the dynamic properties of the system or sensor faults (e.g., a Doppler Velocity Log (DVL) when measuring

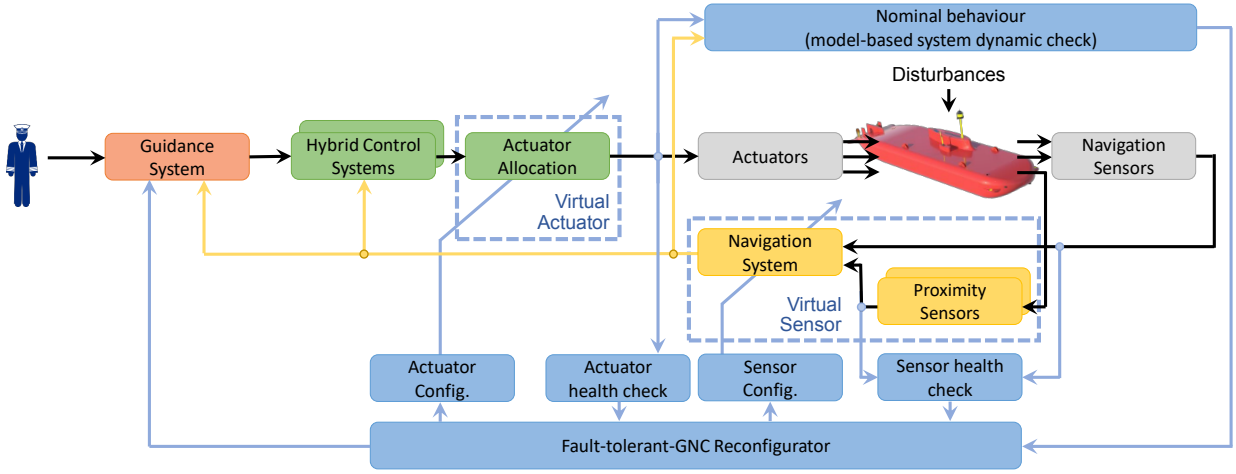

Fig. 3. Vehicle guidance system extended by components for Fault Detection and Isolation (FDI) and Fault-Tolerant Control (FTC) (colored in blue).

the speed over ground/speed through water or the orientation sensors). From [18], it can be seen that the motion behavior of the vehicle itself and the corresponding dynamical model are non-linear. In order to deal with that, the multi-model approach is used [19]. In principle, the procedure linearizes the non-linear system behavior locally. Finally, the deviations are calculated between the modeled and measured signals, which are referred to as residuals.

Based on the generated residuals, the faults that occur can be estimated using a fault model matrix. Setting up such a matrix requires an analysis of the effects of potential faults on the residual. This can result in under- or over-defined systems of equations with the usual consequences for solvability.

B. Multi-Layer Concept

After the FDI, the fault information must be used to influence the automated vehicle operation and minimize the effects. Therefore, a multi-layer concept has been developed. For the implementation of the multi-layer structure, the basic Guidance, Navigation, and Control (GNC) loop shown with the inner blocks in Fig. 3 serves as the basis. The following individual components are essential for automated operations and can be realized in different levels of complexity [20]:

- Guidance (red), which provides the reference values and serves as a human-machine interface (HMI),
- Navigation (yellow), which calculates the state vector of the vehicle motion from measurements, and
- Control (green), which processes the reference values and compares them with the actual states to calculate the manipulating variables.

The multi-layer concept extends this loop by the components for fault handling (blue) in order to generate a specific fault tolerance. As can be seen from Fig. 3, the *control system* processes the reference values of the *guidance system* and compares them with the actual state vector given by the *navigation system*. The forces and torques, which are necessary to follow set state trajectories or to compensate for disturbances, are generated by specific controllers and given to the *actuator allocation*. The allocation converts the forces and torques to the installed and available actuators like propulsions, thrusters, rudders, etc. For Fault-Tolerant Control (FTC) purposes, a *virtual actuator* approach is used, where the *actuator configuration* can be changed in operation. In the event of a faulty actuator, the required forces and torques can be distributed very efficiently to the remaining actuators. This procedure is possible as long as there is a redundant drive configuration.

The FDI components include monitoring functions for the actuators and sensors as well as a model-based part for comparing the movement behavior with the model behavior (*model-based system dynamics check*). The *actuator* and *sensor health checks* evaluate the integrity information of the propulsions and maneuvering drives as well as the sensors. Simultaneously, commanded actuator values are compared with the actual values, where faulty actuators can be detected and identified by processing the deviations. The nominal system behavior is continuously evaluated using the dynamical motion model applied with the model-based system dynamics check. The simulated vehicle motion is compared with the actual navigation data. Increasing residuals indicate a faulty system and are evaluated using the fault model matrix.

The *Fault-tolerant-GNC Reconfigurator* processes information about faulty actuators and sensors as well as deviations in the system behavior and decides automatically to reconfigure the components of the GNC system. Information about the health status of the system is also forwarded to the guidance and thus to a potential (human) supervisor. In particular, the data contain information about the actuator configuration that is currently in use. Based on the diagnostic functionalities, the FTC components are added to the structure. A reconfigurator changes the sensor or actuator configuration depending on the specific faults, e.g., re-configuration of the actuator allocation to weight the actuators differently or to exclude them. Similarly, the sensor configuration can be adapted by the virtual sensor structure to replace faulty sensors with redundant sensor values or by using model-based predictions of the motion states, provided by common model-based filtering [21].

V. Cyber Security

With the increasing digitization, automation, and interconnection of maritime platforms, cyber threats are also rising significantly [22]. The number of cyber incidents is hence growing worldwide, also fueled by geopolitical conflicts [23]. As cyber threats are highly rated risks, particularly for uncrewed and autonomous vehicles [8, 24, 25], adequate mitigation measures play a key role in an effective cyber defense. Cyber security is moreover of particular importance as it is orthogonal to the three conventional main systems, i.e., mechanical and energy systems (cf. Section III) as well as autonomy (cf. Section IV). For holistic cyber security, a sound defense-in-depth strategy is essential, i.e., multi-level mitigation measures that do not rely solely on the external protection of the "water"-gapped system and which are ideally already developed and incorporated by design.

A. Methodology

Similar to the HAZID for conventional main systems, the general procedure for the identification, specification, and implementation of protection and mitigation measures initially involves a so-called *threat analysis* in order to determine and evaluate all possible threats and potential risks to the system under consideration (SuC) [26]. The procedure shown in Fig. 4 covers a *cyber analysis* ① with *threat analysis* ②, including the development of attacker profiles. Based on the likelihood and impact of possible attacks on the SuC, top-priority threats are identified and, finally, critical SuC components are determined, cf. [24, 25, 27]. It is not unimportant to consider the global situation provided by cyber threat intelligence (CTI) regarding current cyber attacks, but also attacks from the electromagnetic spectrum, such as increased interference with GNSS in the Baltic Sea [28] or other malicious activities in association with the Russian attack on Ukraine [23]. Methodologically, the popular STRIDE [26] approach is often used, with the help of which *security requirements* ③ for the SuC can ultimately be derived, taking into account an initial rough risk assessment.

However, the security requirements derived and customized for the SuC essentially define the objectives to be achieved by the *security measures* ④, but not the specific measures themselves, which are usually extremely diverse. Thus, those must be designed differently for individual subsystems and may not always be achievable for every subsystem. It is therefore meaningful to specify alternative, compensatory measures [29].

The realization of measures requires a multi-stage *verification & validation* ⑤ process and must be practicable. The expected benefit must justify the effort and costs of development. There is often a residual risk assessment, which in the particular case of completely novel types of UUVs is complicated by the fact that there is no history and no statistics on cyber incidents. An iterative process is, therefore, necessary, which evaluates the efficiency and effectiveness of designed measures and provides for *revisions* to the implementation or even the type of measure itself, as outlined in Fig. 4. As a bridge between the theoretical model and the real system, virtualized testbeds for verification and validation that contain the SuC or its subsystems are recommended, cf. [30].

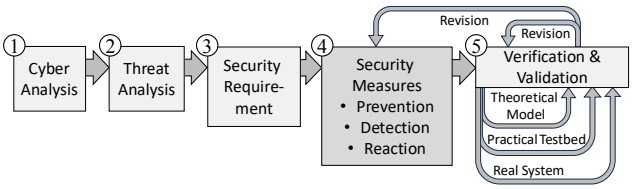

Fig. 4. Overview of the five main methodological steps for successful implementation of effective security measures and mitigation techniques.

B. Background

Due to the exclusivity of the UUV domain and also due to the niche of the novel vehicle class, which is still under development, there is very little direct preliminary work in the scientific literature regarding threat and risk analyses from a cyber perspective. There is only related work for unmanned surface vehicles. Publications such as [24, 31, 32] utilize the approach described in the previous section and differ in their focus (e.g., attacks vs. risks) and specific methodologies.

In our preliminary work [4, 27], we carried out dedicated threat analyses for the class of extra-large UUVs for the first time, which was based, among others, on the related work mentioned above. Still, it was only made possible by the close cooperation with the MUM developers within the research project MUM2 [11]. Consequently, this preliminary work, which describes steps ① and ②, forms the basis for this work. Partial results were the development of attacker profiles with different skills, resources, motivations, and intentions, shown in Fig. 5 in a simplified and summarized manner (*threat actors* in the upper part). From the attackers' objectives, different cyber *attack types* were derived, which can ultimately all be grouped into three main categories, *leakage of data*, *disruption of operation*, and *hijacking of UUV*.

The situation is similar with regard to available *security requirements* ③ for UUVs. To date, there are no dedicated listings for this vehicle class. However, there are numerous established security standards across a variety of domains, ranging from traditional enterprise information technology (IT) and communication systems over industrial control systems with operation technology (OT) to the maritime sector and the oil and gas industry, cf. e.g., [27]. Particularly worth mentioning in this context are standard series IEC 62443 [29, 33] and its adaptions to the maritime domain by DNV [34] as well as the Unified Requirements of the IACS [35]. These standards define a wide range of versatile security requirements for maritime IT and OT systems of traditional, manned surface vessels and casually also focus on cyber threat mitigation measures, which comprise both *preventive* and *detective* measures as well as partially *reactive* measures to recover the SuC after cyber incidents, covering technical aspects but also organizational facets of a holistic cyber security approach.

C. By-Design Cyber Threat Mitigation

The result of our detailed conception of suitable and feasible (mainly technical) *security measures* ④ is visualized in Fig. 5. Due to space restrictions in this paper, the results can only be presented in a very essential and partly simplified manner and are therefore bundled together in the figure.

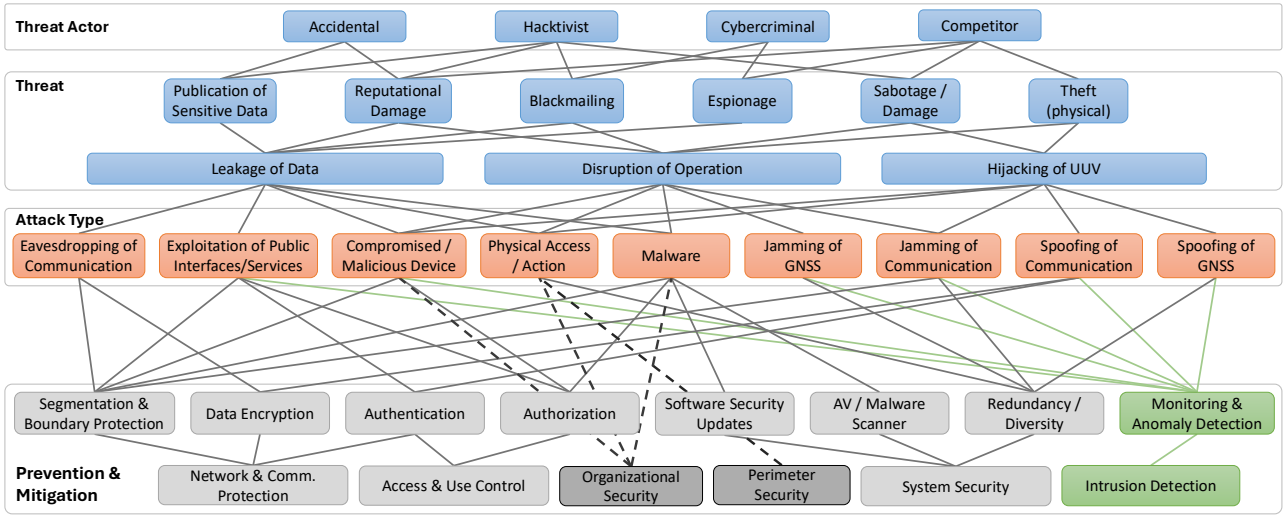

Fig. 5. High-level overview of the developed by-design cyber prevention and mitigation measures. The link between these measures (lower section) and the threat tree (upper section) shows the relationship between the respective measure and the specific type of attack and highlights the fact that effective cyber defense generally requires several preventive (gray) and/or detective (green) measures, but also that, conversely, one type of measure often provides protection against different types of attack.

The three main threat categories are ultimately countered by various preventive and mitigating measures from different main categories (bottom line), which meet the security requirements specified in preliminary work and counteract the threats. These security requirements are closely based on those of the IEC 62443 [29] standard, referenced below by § in brackets.

Preventive measures include hardening the entire IT and OT subsystems in all of the main systems discussed in the previous sections, e.g., applying the principles of *least privilege*, *least functionality*, and *defense-in-depth*, and conceptionally also architectural segmentation and the possibility of isolation in the event of cyber attacks.

Essential here is *system security*, which covers system-oriented measures on the individual IT/OT systems of the SuC. The importance of up-to-date anti-virus/malware software (§3.2, §3.4) and the regular installation of security updates (§3.10) should be emphasized. Furthermore, a redundant design (§7.1) and technological diversity are not only essential for fail-safety but also raise the barrier for adversaries to degrade the capabilities and availability of the SuC.

Since remote-controlled systems are always also geographically distributed, communication and thus *network and communication protection* is inherently essential to secure (wireless) communication interfaces and, in particular, services that are publicly accessible from the Internet. Confidentiality can be ensured by cryptographic encryption (§4.1, §4.3) and integrity by authentication (§1.6, §1.11, §3.1). In addition, multi-level network segmentation (§5.1) – physical or logical via e.g., VLANs – and boundary protection (§5.2), e.g., using firewalls or DMZs, are necessary.

Access to the system via consoles in the RCC and other HMIs must also be protected against misuse and unauthorized access. To this end, measures for authentication (§1.1-5, §1.7-9) and authorization (§2.1, §2.5, §2.7) are necessary for *access & use control*. A role-based approach with staggered user privileges and accounting measures is recommended.

Besides these technical measures, there are also measures in the area of *operational security* (§5.3), which also include security awareness training, as well as *perimeter security* (§3.11) for the physical protection of facilities.

All of these measures above (gray-shaded boxes in Fig. 5) are mainly of a preventative nature. However, holistic system protection with effective defense-in-depth also requires measures to detect ongoing malicious activities so that appropriate technical and/or operational responses can be initiated. Hence, *intrusion detection* measures aim at the early detection of cyber attacks [36]. They are based on system-wide continuous monitoring (§2.8, §2.11, §3.5, §3.11, §6.1, §6.2) and analysis of processes, communication, and system behavior [36] and, thus, are closely related to methods applied in the context of FDI (cf. Section IV-A). Especially for attacks that are difficult to prevent and that can only be coped with redundancy, the detection of anomalies in the system's behavior is essential.

Overall, the possibilities for mitigation measures are as varied as the attacks that threaten the SuC. The well-founded design of cyber measures is only the first step. As mentioned in Section V-A, an iterative testing, evaluation, and development process within the framework of *verification and validation* ⑤ is necessary for the later realization of the measures in the finished system. Our future work will therefore initially use testbeds [30], followed by real systems of a demonstrator.

VI. Results & Conclusion

The results do not show a one-fits-all solution, but depict some approaches how to decrease risks, posed by large UUVs, to an acceptable risk level. The presented results are concepts for mitigation measures and need detailed development and implementation. Furthermore, operational risk mitigation measures must be considered to achieve holistic risk management for large and extra-large UUVs.

ACKNOWLEDGMENTS

This work is part of the project MUM2 [11] and CIAM (https://www.tu.berlin/ebms/forschung/aktuelle-projekte/ciam). It is funded by the German Federal Ministry of Economic Affairs and Climate Action (BMWK) within the "Maritime Research Programme" with contract number 03SX543 and 03SX540H managed by the Project Management Jülich (PTJ). The authors are responsible for the contents of this publication.

REFERENCES

[1] Anduril Industries, "Anduril - Dive-LD." [Online]. Available: https://www.anduril.com/hardware/dive-ld/

[2] Cellula Robotics Ltd., "Cellula Robotics." [Online]. Available: https://www.cellula.com/

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

[4] S. Ritz, M. Golz, F. Boeck, G. Holbach, E. Rentzow, M. Kurowski, T. Jeinsch, W. Wehner, N. Richter, and T. Voß, "Large Modifiable Underwater Mothership: A Case Study for Ocean Bottom Nodes Deployment and Recovery," in *Society of Petroleum Engineers – SPE Offshore Europe Conference and Exhibition (OE)*, Aberdeen, UK, 2019.

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

[6] Zach Abdi, "US Navy Expects More Orca Extra Large UUV Deliveries This Year ." [Online]. Available: https://www.navalnews.com/event-news/sna-2024/2024/01/us-navy-expects-more-orca-extra-large-uuv-deliveries-this-year/#prettyPhoto

[7] Anduril Industries, "Anduril - Anduril to Open Large Scale Production Facility for Autonomous Underwater Vehicles." [Online]. Available: https://www.anduril.com/article/anduril-to-open-large-scale-production-facility-for-autonomous-underwater-vehicles/

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

[9] J.-E. Vinnem and W. Røed, *Offshore Risk Assessment Vol. 1*, 4th ed., ser. Springer Series in Reliability Engineering. Springer, June 2020, vol. 1, no. 978-1-4471-7444-8.

[10] DNV GL AS Maritime Safety, Risk & Reliability, "Study of the risks and regulatory issues of specific cases of mass-part 2 european maritime safety agency (emsa); report no.:2019-0805," DNV AS, Tech. Rep., 2020. [Online]. Available: www.dnvgl.com

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

[12] D. Voelsen, R. Bossong, M. Böttcher, O. Geden, J. M. Pepe, B. Rudloff, C. Schaller, G. Swistek, and L. Voigt, "Maritime kritische infrastrukturen: strategische bedeutung und geeignete schutzmaßnahmen," Stiftung Wissenschaft und Politik, Berlin, Tech. Rep., 2024. [Online]. Available: https://www.swp-berlin.org/10.18449/2024S03/

[13] DNV-RU-UWT, "Rules for Classification – Underwater technology – Part 1-7, Editions July 2021-July 2024," DNV, July 2024.

[14] M. Greve, M. Kurowski, S. Ritz, M. Golz, L. N. Vijayasarathi, N. Bayazit, and E. Rentzow, "Design of the Propulsion System for the Autonomous XLUUV MUM," in *Proc. of International Conference on Offshore Mechanics and Arctic Engineering (OMAE)*, vol. 5A: Ocean Engineering, 2022, p. V05AT06A035.

[15] A. U. Schubert, R. Damerius, C. Rethfeldt, M. Kurowski, T. Jeinsch, and M. Gluch, "Concepts and System Requirements for Automatic Ship Operations*," in *MTS/IEEE OCEANS 2023*, Limerick, Ireland, 2023, pp. 1–8.

[16] A. Schubert, M. Kurowski, M. Gluch, O. Simanski, and T. Jeinsch, "Manoeuvring Automation towards Autonomous Shipping," in *Proc. of the 14th Int. Naval Engineering Conference (INEC)*, Glasgow, UK, 2018, pp. 1–8.

[17] Z. Gao, C. Cecati, and S. X. Ding, "A Survey of Fault Diagnosis and Fault-Tolerant Techniques—Part I: Fault Diagnosis With Model-Based and Signal-Based Approaches," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 6, pp. 3757–3767, 2015.

[18] E. Rentzow, M. Kurowski, and T. Jeinsch, "Generalized Approach for Modeling and Control of Structurally Variable Underwater Vehicles," in *Proc. of the MTS/IEEE OCEANS 2024 - Singapore*, 2024, pp. 1–9.

[19] J. Pabst, T. Müller, and T. Jeinsch, "Modular fault diagnosis for ROVs based on a multi-model approach," in *Proc. of the MTS/IEEE Global OCEANS 2020: Singapore – U.S. Gulf Coast*, 2020, pp. 1–7.

[20] M. Kurowski, A. Haghani, P. Koschorrek, and T. Jeinsch, "Guidance, Navigation and Control of Unmanned Surface Vehicles," *at – Automatisierungstechnik*, vol. 63, no. 5, pp. 355–367, 2015.

[21] E. Rentzow, M. Kurowski, H. Korte, and T. Jeinsch, "Navigation System Integration and Evaluation for Precise Underwater Operations," in *Proc. of the 2023 DGON Inertial Sensors and Systems (ISS)*, 2023, pp. 1–14.

[22] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore, and P. Tedeschi, "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead," *IEEE Communications Magazine*, vol. 58, no. 6, 2020.

[23] R. Cichocki, "State-Sponsored and Organized Crime Threats to Maritime Transportation Systems in the Context of the Attack on Ukraine," *TransNav*, vol. 17, no. 3, 2023.

[24] 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.

[25] 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.

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

[27] A. Nies, K. Wolsing, and J. Bauer, "Threat Analysis for Novel Underwater Vehicles: Insights from the Perspective of Cyber Security," in *Proc. of the European Workshop on Maritime Systems Resilience and Security (MARESEC)*, Bremerhaven, Germany, 2024.

[28] 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/

[29] 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.

[30] 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.

[31] 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: Springer, 2019, pp. 20–36.

[32] 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.

[33] 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.

[34] 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.

[35] IACS, "UR-E26 – Cyber resilience of ships, UR-E27 – Cyber resilience of on-board systems and equipment," International Association of Classification Societies (IACS), Unified Requirements, Apr. 2022.

[36] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, Jul. 2018.