



Development of an open source vessel – Guidelines how to set up a conceptual approach of an open source fleet

Within the framework of the Interreg NSR project AVATAR work package 6

AVATAR is a project co-funded by the
Interreg North Sea Region programme 2014-2020



Colophon

- “Development of an open source vessel – Guidelines how to set up a conceptual approach of an open source fleet” within the framework of the Interreg NSR project AVATAR work package 6.
- Interreg VB: AVATAR
- This document is published within [the AVATAR project](#), an INTERREG project of the North Sea Region programme 2014-2020 as one of the reports for WP6.
- It is allowed to distribute this publication.
- The publication may be cited as: Kia, G. and T. Pauwels (2023): Development of an open source vessel – Guidelines how to set up a conceptual approach of an open source fleet, publication in the framework of AVATAR, a project co-funded by the INTERREG North Sea Region programme 2014-2020 (ERDF).
- Source of the photo(s) on the cover: POM Oost-Vlaanderen

Contributors of this report:

Name	Organization	Website	Email
Ghazaleh Kia	SEAFAR	www.seafar.eu	Ghazaleh.kia@seafar.eu
Tom Pauwels	POM Oost-Vlaanderen	www.pomov.be	Tom.pauwels@pomov.be

Document version:

Version	Date
V1.0	30.06.2023

See also: [AVATAR website](#) and [Linkedin](#)

Project partners AVATAR:



AVATAR: Autonomous vessels, cost-effective transshipment, waste return
<https://northsearegion.eu/avatar>



1. Introduction

The massive under-exploitation of inland waterways (IWW) in the North Sea Region (NSR), especially in and around urban environments, provides opportunities for technological innovations. The AVATAR project aims to deploy (highly) zero-emission automated vessels that can do regular trips between the urban consolidation centers outside of a city and inner city hubs.

The AVATAR project aims to tackle challenges of city freight distribution by developing, testing and assessing adequate technologies and business models for urban (highly) autonomous zero-emission Inland waterway transport (IWT) solutions. Through this, the project unlocks the economic potential of urban vessels and corresponding waterways, increases available solutions for full-cycle automation and sets up a sustainable supply chain model for urban goods distribution and waste return.

An open source vessel is defined as one vessel that is being operated by different operators. The current AVATAR business case focuses on eliminating labour costs and the assumption that 1 vessel will be operated by 1 operator. In order to increase the capacity use of a vessel, it might be interesting to assign a vessel to several operators (different companies). For example, in months 1-6, the vessel is operated by company X, and in months 7-12 by company Y. It is not the purpose of this activity in the project AVATAR to test an open source vessel. Focus is on a conceptual approach by investigating why this “open source vessel” is not possible today and how can this be made possible in the future (or not?). This report contains guidelines about how an open source vessel concept can be set up and what are the current bottlenecks to deal with this.

This work should be seen in the framework of defining the necessary conditions that lead to a long-term (sustainable) uptake of the developed concepts in the AVATAR project.

Research question in this report is whether the SEAFAR controlled AVATAR vessel can be controlled by other operators.

In chapter 2 the challenges of an open source fleet are described from the point of view of SEAFAR. Security concerns and financial implications of open access for remotely operated vessels is included in chapter 3.



2. Challenges of an open source fleet

Based on discussions and brainstorming with AVATAR project partners, SEAFAR concluded that an open source vessel is not applicable at this stage, because of:

- Legislation. Current legislation does not allow fully autonomous operations. A human override is still needed, leading also to the question where the human override should be located. SEAFAR can provide the human in the loop, even if the ship is operating fully autonomously.
- Seafar considers security aspects and by transferring the automated vessel to another company Seafar cannot guarantee the security on vessel communication.
- Seafar takes care of the maintenance and upgrading of the technologies utilized on a vessel and this cannot be transferred to other companies.
- The data collection is mainly done on Seafar clouds, which cannot be transferred to other owners.
- Seafar securely shares its network interface to customers and filters the vessels which can connect to the network.
- The technologies utilized by Seafar include the scopes which have been developed within years and are unique for Seafar. For instance, the control center messaging services are cloud hosted and have more than 100 message types to handle with Seafar API's and data structure. This explains the reasons for this service to be uniquely operational by Seafar.
- The vessel data including the configuration and runtime as well as the team data are also cloud hosted and require Seafar API's and data structures.

Focus in this chapter was on writing why an open source vessel is not possible from the point of view of SEAFAR. In chapter 3, focus is on the implications of an open access for remotely operated vessels. In other words, what are the bottlenecks that should be addressed to make an open source vessel realistic.



3. Security concerns and financial implications of open access for remotely operated vessels

In the rapidly evolving landscape of maritime and inland navigation technology, remotely operated vessels/ semi-autonomous vessels have emerged as a promising innovation with the potential to transform various industries including ship management, remote operation, network applications, etc. . However, alongside the numerous advantages they offer, there are critical considerations that must be addressed to ensure the safe and efficient operation of these vessels. One significant concern is the practice of granting open access to other companies beyond the designated operators, as this could expose the vessels to cyber attacks and compromise their integrity.

The notion of allowing remote access to remotely operated vessels (ROV's) by entities other than the operators raises a series of security red flags. Cyber attacks targeting maritime assets have become increasingly sophisticated, and the potential consequences of an attack could be catastrophic. Unauthorized access to an ROV's control systems could lead to loss of control over the vessel, manipulation of its operations, or even the possibility of using it as a tool for malicious activities. By limiting access solely to authorized operators, the risk of these vulnerabilities is significantly mitigated.

Furthermore, the security concerns extend beyond potential attacks. The act of granting open access necessitates the development and implementation of complex software systems to manage permissions and communication protocols. These software systems require continuous updates and patches to defend against new cyber threats, resulting in ongoing costs for maintenance and security. Additionally, acquiring licenses for the necessary equipment and software components involves substantial upfront expenses, followed by recurring payments for updates and improvements.

The financial implications associated with open access for semi-autonomous vessels are substantial and multifaceted. Initial costs encompass the procurement of specialized software, licensing fees for proprietary technology, and the hardware required for secure remote operation. However, the expenses do not conclude there. As technology rapidly evolves, maintaining compatibility with other systems and addressing emerging security concerns demands ongoing investments. These recurring costs, including software updates, equipment upgrades, maintenance, and license renewals, can strain budgets and affect the economic viability for the operations of these vessels.

While the financial considerations hold significance, they represent merely one aspect within the broader spectrum of concerns encircling the concept of open access for remotely operated vessels. Other pivotal factors encompass the potential operational disruptions, the intricate web of legal and regulatory frameworks that oversee remote access, and the complexities surrounding liability in instances of unauthorized access or system malfunctions.

Given the current absence of comprehensive regulations governing autonomous or semi-autonomous navigation, obtaining authorization for remote voyages through waterways is highly challenging. Substantial documentation is imperative to substantiate the safety of such navigation methodologies. Ultimately, this effort culminates in the acquisition of permissions



tailored to specific time frames and trajectories. Any deviation from the predefined zone or designated timeframe mandates the submission of a new application. This new application can only be submitted by the developers of the semi-autonomous technology for that specific vessel.

Expanding on the realm of liability and insurance, two primary insurance domains come into play: one tied to the vessel owner and the other intricately linked with the remote control system. The orchestration of these elements necessitates the presence of a dedicated party responsible for remote operations, vested with the authority to pursue permissions and secure insurance coverage for the intricate systems. The role of this party consolidates as the central figure in navigating the intricate landscape of permissions and insurance in the realm of remote operations when it has the ownership of the devices and remote operation technology,

4. Conclusion

Research question in this report was whether the SEAFAR controlled AVATAR vessel can be controlled by other operators. In conclusion, while the idea of providing open access to remotely operated vessels for external entities may hold certain benefits, it introduces a plethora of security risks and financial implications that must not be underestimated. To ensure the safe, secure, and sustainable utilization of these innovative maritime technologies, stakeholders must carefully weigh the advantages against the potential drawbacks. Prioritizing robust cybersecurity measures, staying alongside of evolving threats, and building long-term financial strategies are imperative for the successful integration of remotely operated vessels into modern industry practices.

It turns out that, from a commercial and regulatory point of view, risks will occur when a SEAFAR controlled AVATAR vessel would be controlled by other operators. On the other hand, that doesn't mean it is not possible. During the AVATAR project, it has been shown that the KUL Maverick vessel and the TUD vessels (each with their own remote control system) has been integrated with another UOL remote control system. This has been demonstrated in AVATAR WP3 and WP5-activities.



AVATAR is a project co-funded by the
Interreg North Sea Region programme 2014-2020

Project partners AVATAR:



AVATAR: Autonomous vessels, cost-effective transshipment, waste return
<https://northsearegion.eu/avatar>

