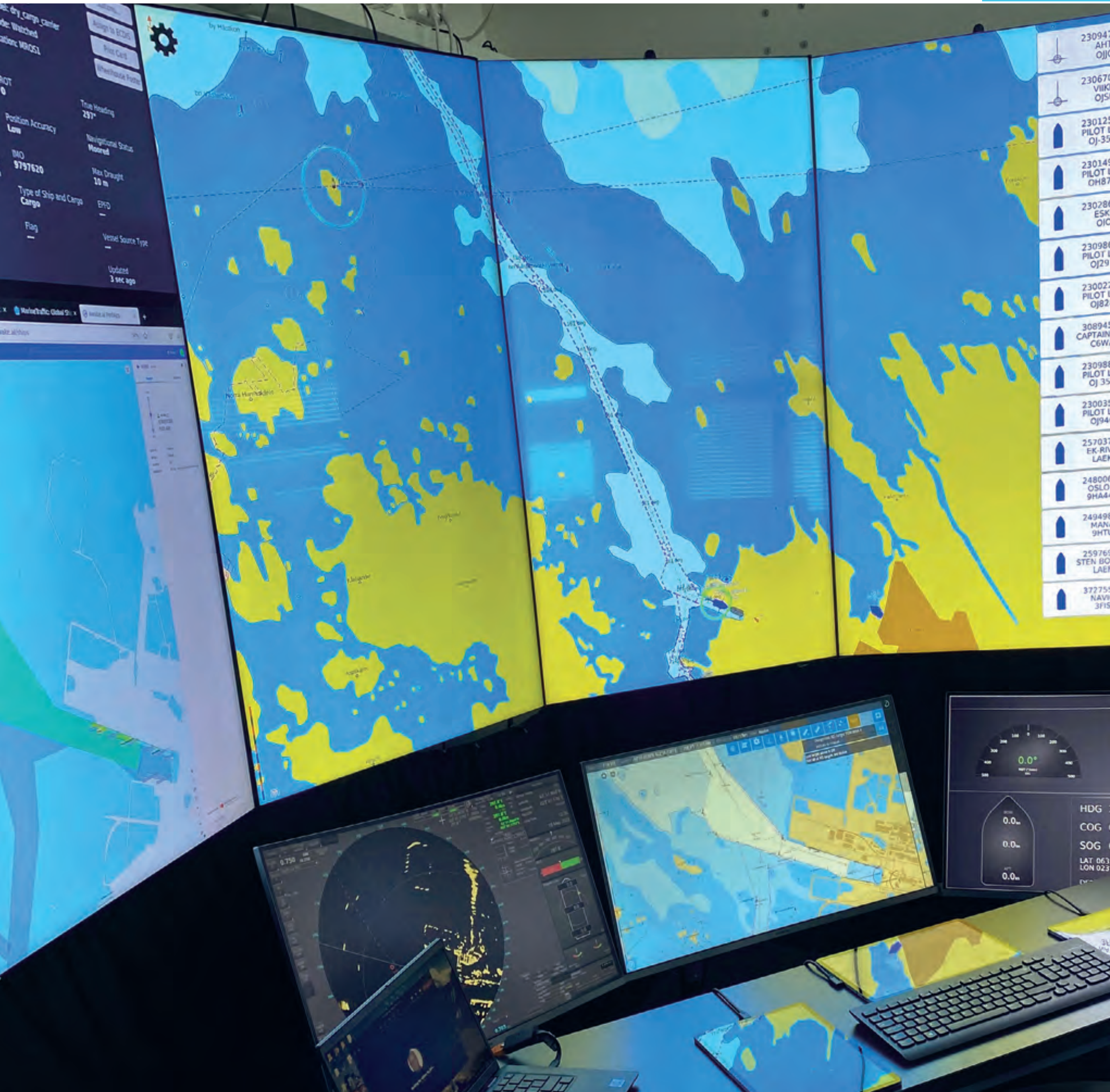
DIMECC

FINAL REPORT 2/2022

DIMECC PUBLICATIONS
SERIES NO.25

Sea4Value – Future Fairway Navigation

2020 – 2022



DIMECC
FINAL REPORT 2/2022

Sea4Value – Future Fairway Navigation

DIMECC
PUBLICATIONS
SERIES NO. 25
2020 – 2022

Publisher DIMECC Oy

Åkerlundinkatu 8, 33100 Tampere, Finland

Eteläranta 10, 00130 Helsinki, Finland

Citykulma, Yliopistonkatu 31, 20100 Turku, Finland

www.dimecc.com

ISBN 978-952-238-298-6
ISBN 978-952-238-299-3 (pdf)

DIMECC Publications series

Graphic design and layout: Public Design Oy

Images: Väylävirasto, Shutterstock and participating organizations

Cover photo: Seppo Tikkanen/DIMECC

English language editor: Semantix Oy

Printed in Finland: Grano Oy, Tampere, 2023

CONTENTS

FOREWORDS

Digitalization and the development of autonomous vessels is transforming marine industry. In the near future, vessels with different levels of autonomy will sail the seas. These vessels will continue to need services, such as pilotage, fairways etc. to sail safely in the coastal waters. The development of vessels challenges fairway services to meet their future needs and requirements. To speed up the development of future fairways and their services, One Sea, the autonomous maritime ecosystem, supported the realisation of a research program Sea for Value Future Fairway.

According to One Sea, operational efficiency comes with more optimized operations, where decisions for the combination of routes, weather conditions and traffic are made entirely by artificial intelligence, resulting in the most economical, safe, and ecological combination. Already during the development phase towards this scenario, digitalization will bring a much-needed update to marine transportation, which has yet to adopt intelligent solutions on a large scale. According to the vision of the One Sea, in the autonomous shipping ecosystem old ships are improved by retrofitting them with new technologies to make them smarter and able to communicate with other devices in the ecosystem. A fleet of smart ships underlines the possibilities to optimize, streamline and economize the whole business. However, the full benefits of digitalization on maritime transportation can only be achieved when future ships are able to utilize the full potential of digitalization also during the most challenging parts of their journeys, the navigation on the last mile.

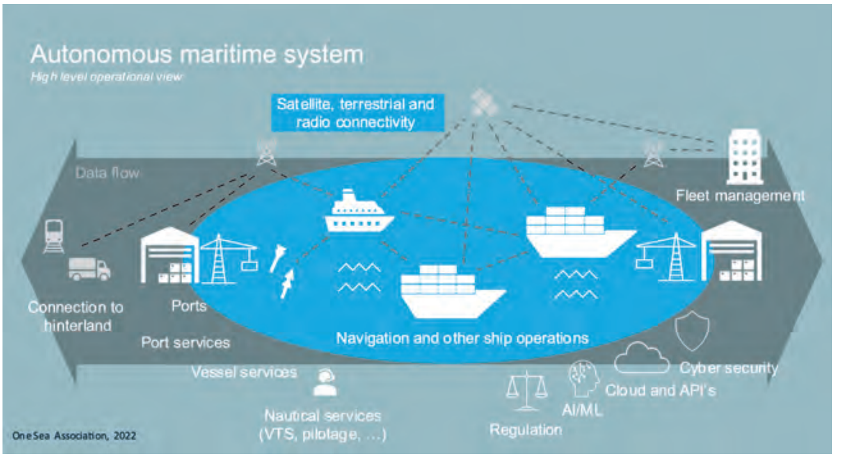


Figure 1. Autonomous Maritime System (One Sea Association, 2022).

The mission of the Sea4Value Future Fairway Navigation program was to provide blueprints towards digitalization, service innovation and information flows in maritime transport. Its longer-term mission was to prepare for advanced autonomous operations and navigation. A key step towards an autonomous transport system is to ensure safe, sustainable, and efficient channel for ships to enter and leave harbors.

The Future Fairway Navigation program was created to find solutions for the safe last-mile navigation on the challenging fairways in the Finnish coastal areas and archipelagos using new knowledge in human-machine interaction. The main topics were remote pilotage and the future fairway, its elements and services. The program aimed to combine suitable technologies, practices and operations to enable future fairway services such as increased situational awareness and remote pilotage and to ensure the safety and security of these fairway services.

The questions Future Fairway Navigation program aimed to answer were:

- What are the future teams that will ensure safe navigation?
- How to build the necessary situational awareness to enable decision-making to assist the navigation work in the future?
- Which part of the intelligence should be built on the fairway and surrounding infrastructure and which on the ship?
- What are the changes to be done in fairways and existing navigational and communication equipment within short and medium term?

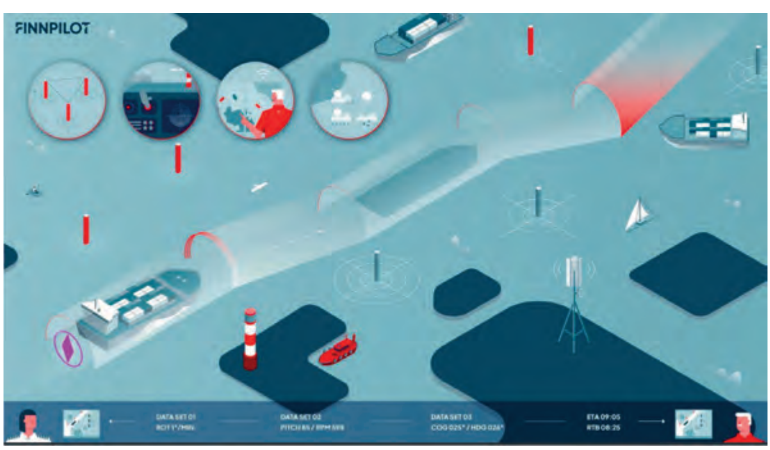


Figure 2. Finnpilot's visualization of the safe navigational tube created for future fairway users with increased navigational information (Finnpilot Pilotage Ltd., 2022).

The Future Fairway Navigation program results include a comprehensive description on the future fairway elements and a working concept for the remote pilotage. The remote pilotage concept was tested in real conditions successfully. Although the demonstration was a success, there are still work ahead before remote pilotage can be implemented. The experiment showed that remote pilotage is possible from a technology point of view but many open questions and issues are still to be resolved before a safe and commercially viable service can be implemented.

The definitions of the elements of future fairway is a success and will be a significant framework for authorities and various fairway ecosystem stakeholders. The fairway elements were identified and defined by program partners together with relevant authorities. The elements of the future fairway offer new insight into essential fairway services for both traditional and autonomous vessels.

The program started in spring 2020 and ended in fall 2022. The program faced the restrictions caused by COVID-19, but they did not have significant effects on program outcomes. The collaboration worked extreme well, and the partners showed great flexibility in the remote pilotage demonstration as the demonstration was realized in different fairway, at a different time and with different a vessel from those originally planned.

This report gives insights into the outcomes of the Future Fairway Navigation program partners' work. We wish you an enjoyable read!

Sanna Sonninen
Chair of the program

Seppo Tikkanen
Program manager

awake.ai

BRIGHTHOUSE INTELLIGENCE

ERICSSON

FINNPILOT

Haltian

MEYER TURKU SHIPYARD 1737

ESL Shipping

A! Aalto University

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

NOVIA UNIVERSITY OF APPLIED SCIENCES

Tampere University

UNIVERSITY OF TURKU

TRAFICOM

Väylävirasto
Trafikledsverket

Fintraffic

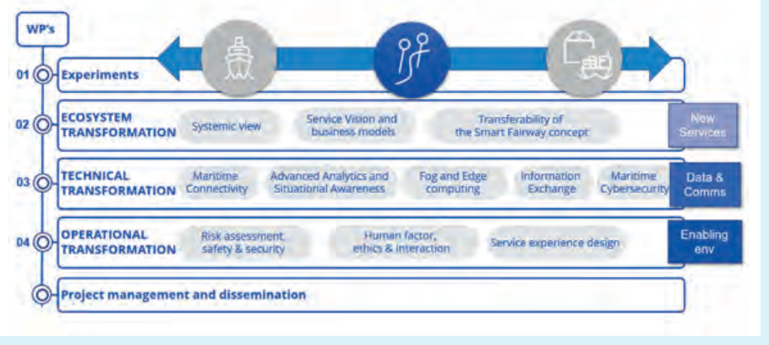
ILMATIETEEN LAITOS
METEOROLOGISKA INSTITUTET
FINNISH METEOROLOGICAL INSTITUTE

BUSINESS FINLAND

DIMECC

PROGRAM IN A NUTSHELL

TheSea4Value Future Fairway Navigation program concentrated on developing the remote pilotage concept and defining the future fairway, its elements, and services. Within the program, partners searched for and implemented combinations of suitable technologies, practices and operations to enable future fairway services, such as increased situational awareness and enabling remote pilotage. The figure below shows the structure and research topics of the Sea4Value Future Fairway Navigation program.



The FFN resulted in a working concept for remote pilotage. The concept was successfully tested in real conditions. The second main result of the Future Fairway Navigation program was definitions of elements of the future fairway.

Partners

Awake.ai Oy, Brighthouse Intelligence Oy, Finnpilot Pilotage Oy, Haltian Oy, Oy L M Ericsson Ab, Meyer Turku Oy

ESL Shipping Oy, Neste Oyj, Port of Turku, Port of Helsinki, Port of Rauma, Suomen Varustamot ry.

Aalto University, University of Jyväskylä, Novia University of Applied Sciences, Tampere University, University of Turku

Traficom, Finnish Transport Infrastructure Agency and Finnish Meteorological Institute.

Facts

Duration: .... 2/2020 – 12/2022

Budget: .... about EUR 6 m

Funding: .... Business Finland and participating companies and universities

UNIVERSITY OF TURKU

Väylävirasto
Trafikledsverket

Tampere University

TRAFICOM

Fintraffic

awake.ai

FINNPILOT

BRIGHTHOUSE INTELLIGENCE

ILMATIETEEN LAITOS
METEOROLOGISKA INSTITUTET
FINNISH METEOROLOGICAL INSTITUTE

FUTURE FAIRWAY

Smart fairways

Contributors

- University of Turku, **Marikka Heikkilä & Jukka Heikkilä**
- Traficom, team led by **Heidi Himmanen**
- The Finnish Transport Infrastructure Agency, team led by **Tuomas Martikainen**
- Finnpilot, **Sanna Sonninen**
- Fintraffic Vessel Traffic Services, **Olli Soininen**
- Finnish meteorological institute, **Jani Poutiainen**
- **and the other consortium members**

Digitalization is taking big leaps in the maritime sector with the aim of creating more efficient and sustainable transport. So far, most interest has focused on the development of autonomous ships and digitalization in ports. While all this development toward digital and autonomous maritime operations is taking place in other areas of the maritime industry, there has not been much change in fairways.

Our collaborative research project took up this challenge of the development of future smart fairways in Finland. The first research task was to describe what a smart fairway is, and the second task was to suggest the main elements of a future fairway.

Background

Maritime transport has been a catalyst for economic development and prosperity throughout its history. It enables trade and contacts between nearly all nations. In Finland, too, sea traffic is crucial to the economy in terms of both efficiency and security of supply, as 90% of freight trade is seaborne[1]. Distinguishing factors for Finland, and the Nordic countries in general, are the territorial waters' extensive archipelago and fjords, which is why the fairways (defined by Gucma and Zalewski (2020) *as harbor approach channels, designed for safe navigation of vessels*) are of high importance.

[1] https://shipowners.fi/en/competitiveness/key-figures-of-maritime-in-finland/

Not only navigation but also the provision and maintenance of fairway infrastructure and services is challenging, with the harsh conditions of four true seasons. The conditions vary from gentle white summer nights to freezing cold, dark, stormy conditions on shallow and rocky waters with winding fairways. The current static waterway beacons, with lateral and leading marks, are designed to keep vessels in deep enough, safe waters. This basic fairway infrastructure is enhanced with vessel traffic services, pilotage, towing and ice-breaking services. VHF-radio communication is compulsory for larger vessels in territorial waters; sending and receiving vessel location information (AIS, Automated Identification Service) is common. Safe navigation is also ensured using global positioning systems and online services, and real-time weather, current, and sea-level information with forecasts.

Even though safety on the Finnish seas has improved in the past years, it is clear that fairways must be developed further, because the number of vessels, boats and other vehicles in territorial waters has grown, the traffic is denser, and other emerging uses of regional and local water areas have grown all year round, demanding more digital services.

Our research task was to describe what a smart fairway is, and the second task was to suggest the main elements of a future smart fairway. These are followed by a scholarly rethinking of fairways and services for seafarers.

Method

Empirical data for the study was collected using the Delphi method. It consisted of a series of workshops supported with questionnaires, interviews and feedback rounds. The participants belong to the Fairway consortium, representing authorities, fairway service providers, technology providers, shipping lines, and maritime training and research. In the interviews, we sought to widen the expertise by interviewing additional experts, to include areas not covered by the consortium, such as emergency and military expertise.

The Delphi method is one of the most popular techniques for technological forecasting and prioritizing issues for managerial decision-making (Landela, 2006; Okoli & Pawlowski, 2004). Although it was initially developed for military use cases, it is widely adopted in business and social science as a means of soliciting expert opinions (e.g., on port digitalization, see Rodrigo González et al., 2020 and González-Cancelas et al., 2020). Typically, the goal is to achieve the most reliable consensus on a given topic among a group of experts. This consensus then provides a solid background for making decisions on future actions, but on the other hand, it may limit the exploration of radical ideas (Friis-Holm Egfjord & Sund, 2020). The method has been used in many different ways and is suggested for use in combination with other methods (Melander, 2018).

Our purpose with the Delphi method was to support visioning work in an R&D consortium focusing on future smart fairways. We specifically took inspiration from the recommended Delphi procedures outlined by Melander (2018) and by Okoli and Pawlowski (2004), in which the technique combines several methods and serves the dual purpose of soliciting opinions from experts and having them rank these according to importance.

The study proceeded in several steps:

1. Pre-Delphi survey (n=33): Stakeholders responded to a questionnaire developed by the researchers asking them to provide their judgment on the year by which the smart fairway would be open for vessels, and what the primary target group is, and what improvements should be achieved with the smart fairway.
2. Pre-Delphi interviews (n=23): Stakeholder interviews were conducted by the researchers to get more in-depth understanding of the current fairway system and services, and development work that is related to the maritime transport and fairways.
3. Delphi workshop (n=25): In a Delphi workshop, stakeholders used a Miro board to comment and modify the list of elements. They also provided their views on the importance and challenges of each element. The results from the workshop were plotted by the researchers in a diagram, with the x-axis showing the level of challenge and the y-axis the level of importance.
4. Delphi verification phase: The diagram and the Miro board were sent back to the respondents for review. Several comments and suggestions were received in separate meetings and by email. An improved version of the diagram was constructed based on the comments. More detailed descriptions of the elements were also prepared with the responsible experts.

Survey data The survey was conducted online using webropol. It consisted of questions asking respondents personal views on the reasons for a future smart fairway and its expected benefits, intended user groups and service requirements. A total of 33 experts responded to the questionnaire between October 2020 and March 2021. Nvivo was used to analyze and categorize the responses. The findings were presented to the consortium in May 2021 in a workshop, followed by a discussion on the implications.

Interview data The interviews aimed to collect multiple views on increased utilization of automation and autonomous marine traffic and its impacts, and the need for supporting infrastructure and fairway services. They were conducted online between summer 2020 and summer 2022. The interviews were recorded and transcribed, except when the respondent opted not to be recorded. Conventional qualitative content analysis was the primary analysis method, in which coding categories are derived directly from the text data (Hsieh & Shannon, 2005). Coding was done on interview transcripts using Nvivo software by one of the researchers who, using the coding frame, summarized the interview data (including quotes from the interviews) in a separate document. This document was checked and approved by the other researchers.

Workshop data An initial list of elements of a future fairway was extracted and agreed together with the Finnish Transport and Communications Agency (the authority responsible for setting the Finnish regulations and rules for fairways). A 2-hour workshop was organized as a Teams meeting, at which 22 invited stakeholders were divided into three groups in June 2021. These groups used a Miro board to write down comments and modify the list of elements. They also provided their views on the importance and challenges of each element. One of the authors summarized the results in a diagram, which was then checked and commented on by the participants.

The smart fairway The expert interviews and literature analysis revealed the key trends that underscore the need for smarter fairways:

a) Maritime transport is increasingly digitalized. In future, vessels will differ vastly in their level of digital capabilities, ranging from no autonomous or digital features to fully autonomous vessels.

b) Seafarers on cargo ships are increasingly inexperienced, especially in Nordic weather and fairway conditions.

c) The water area is increasingly used for yachting, motor boating, and rowing, as well as novel outdoors activities such as skating, skiing, canoeing/kayaking, and jet skiing by individuals or groups with typically limited experience in moving in remote water areas.

d) There is increasing concern over environmental demands on marine traffic with reduced carbon, methane, and sulfur emissions; limiting eroding wave formation; and minimizing bilgewater and sewage loading into the sea, as well as underwater noise and artificial light.

The experts describe **a smart fairway as a fairway that uses information, new technology and automation solutions to improve traffic safety and efficiency, as well as to reduce environmental impacts** (e.g. Martikainen, 2022[2]). This would mean that fairway signage or maritime safety devices would be smarter than today. They might have sensors and so on. These, with additional and improved information sharing, could lead to better traffic safety and help in reaching destinations on time and connecting intermodal logistics. Moreover, improved planning and optimization of routing can help in carbon footprint minimization. In addition, vessels can gather information on environmental effects en route.

In future, the smart fairway should also support autonomous shipping (Miettinen et al., 2021). As an example, trials with autonomous road traffic (Manivasakan et al., 2021) show that it is not sufficient to automate the vehicle only in relation to static road objects, but the autonomous vehicle must adapt to dynamically changing traffic situations by, for example, interacting with road users, moving objects, changing weather, and illumination on roads. Automated marine traffic will face similar requirements (Giannopoulos, 2004).

On the other hand, several experts see that a future smart fairway could serve a wide variety of users, ranging from commercial ships to sailing boats to summer cottage residents. A smart fairway could be *"a digital twin showing on a cellphone or tablet what is happening in the fairway when you go there on a small pleasure boat in the middle of all the other traffic."*

When we asked how several vessels can sail on a smart fairway even if some of them are not willing or able to utilize its features, most experts responded that situational awareness and communication should be designed so that vessels with differing capabilities can use the same physical fairway. Some suggested that vessels of different capabilities could have their own routes or 'tubes,' and there should be exact rules and procedures for how ships of different categories meet each other.

[2] https://vayla.fi/documents/25230764/114203946/Vesiväyläpäivä20220322_Esitykset7-8.pdf/229e9c10-aa41-3453-fd6a-8cdc4360bea8/Vesiväyläpäivä20220322_Esitykset7-8.pdf?t=1647939334415

Rather than having only one type of smart fairway, the Finnish authorities share the view that there will be **several classes of fairway based on what levels of automation they support.** An analogy to air traffic and runway classification was sought here. Thus, there would be differing fairway categories providing different levels of services for navigation to/from port (in which the first level, for example, is completely dependent on visual safety devices and so on). Later on, the smart fairway concept can be further refined for other waterways.

In order to introduce the smartness to fairways, it is feasible to start with the safety-critical sections of the fairway, such as pilot entry/exit points, straits and shallows, fairway crossings, and handovers to harbor areas interfacing with international traffic. These are points where infrastructure investments could be shown to augment safety and help in avoiding the escalation of risks. This also enhances the information for SAR, customs, guarding, policing, learning from accidents and near misses, for better safety, efficiency, and environmentally sustainable cargo and passenger traffic, to ensure supplies for the economy.

References

- **Friis-Holm Egfjord, K. & Sund, K. J.** 2020. A modified Delphi method to elicit and compare perceptions of industry trends. MethodsX, 7, 101081.
- **Giannopoulos, G. A.** 2004. The application of information and communication technologies in transport. European journal of operational research, 152(2), 302–320.
- **González-Cancelas, N., Molina Serrano, B., Soler-Flores, F., & Camarero-Orive, A.** 2020. Using the SWOT Methodology to Know the Scope of the Digitalization of the Spanish Ports. Logistics, 4(3), 20.
- **Gucma, S., & Zalewski, P.** 2020. Optimization of fairway design parameters: Systematic approach to manoeuvring safety. International Journal of Naval Architecture and Ocean Engineering, 12, 129–145.
- **Heikkilä M., Saarni, J, Himmanen H., Heikkilä, J.** 2022. Smart Fairways - Co-design of future intelligent fairways in Finland, presentation in International Maritime and Port Technology and Development Conference (MTEC) & 4th International Conference on Maritime Autonomous Surface Ships (ICMASS), 6.4.2022 Singapore.
- **Heikkilä, J., Heikkilä, M. Märtz, G.** 2023. Platforms for Smart Fairways – Enhancing Services for Autonomous Maritime Traffic and Other Emerging Uses of Territorial Sea, Hawaii International Conference on System Sciences HICSS, 2023.

- **Hsieh, H. F., & Shannon, S. E.** 2005. Three approaches to qualitative content analysis. Qualitative health research, 15(9), 1277–1288.
- **Landeta, J.** 2006. Current validity of the Delphi method in social sciences. Technological forecasting and social change, 73(5), 467–482.
- **Manivasakan, H., Kalra, R., O'Hern, S., Fang, Y., Xi, Y., & Zheng, N.** 2021. Infrastructure requirement for autonomous vehicle integration for future urban and suburban roads–Current practice and a case study of Melbourne, Australia. Transportation Research Part A: Policy and Practice, 152, 36–53.
- **Melander, L.** (2018). Scenario development in transport studies: methodological considerations and reflections on Delphi studies. Futures, 96, 68–78.
- **Miettinen, K., Miettinen, A., Hauta, J., Töyrylä, S. and Reinimäki, S.** 2021. Liikenteen automaation lainsäädäntö- ja avaintoimenpidesuunnitelma. Liikenne- ja viestintäministeriön julkaisuja 2021:28.
- **Okoli, C., Pawlowski, S.D.** 2004. The Delphi method as a research tool: an example, design considerations and applications, Inf. Manag. 42 (1), 15–29.
- **Rodrigo González, A.; González-Cancelas, N.; Molina Serrano, B.; Orive, A.C.** 2020. Preparation of a Smart Port Indicator and Calculation of a Ranking for the Spanish Port System. *Logistics, 4, 9.*

Future fairway elements

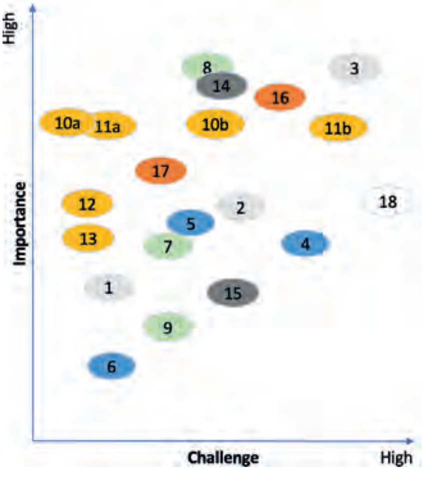
Contributors

- University of Turku, **Marikka Heikkilä & Jukka Heikkilä**
- Traficom, team led by **Heidi Himmanen**
- The Finnish Transport Infrastructure Agency, team led by **Tuomas Martikainen**
- Finnpilot, **Sanna Sonninen**
- Fintraffic Vessel Traffic Services, **Olli Soininen**
- Finnish Meteorological Institute, **Jani Poutiainen**
- **and the other consortium members**

Delphi study

In a Delphi study, we established the elements necessary for enhancing the infrastructure for safer, more efficient and environmentally friendly seafaring toward autonomous maritime traffic in Finnish fairways. In all, 18 different elements were proposed by the experts as being elements of a future fairway.

Content-wise, the elements represent infrastructure, fairway information, weather and sea conditions, navigation and seafaring services, port arrival and departure services, or other services. Figure X depicts how high the experts rated these in relation to the challenge of development (x-axis) and relative importance (y-axis). It should be noted that the elements are not independent, but rather may build on the other elements. For instance, many of the service elements require support from the first three groups (infrastructure, fairway information, and weather and sea conditions).



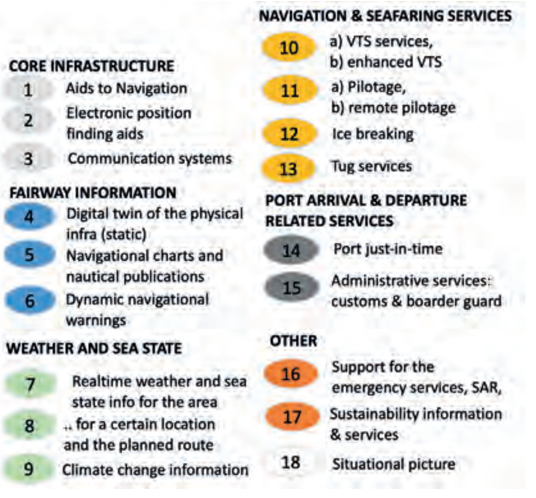


Figure 1. **The fairway elements for safer and more efficient maritime traffic in Finland.**

The elements and the main improvements are:

Core infrastructure:

1) ***Aids to navigation:*** Aids to navigation (AtoNs) are increasingly added with sensors, such as for dynamic weather, traffic and sea conditions, and traffic control. AtoNs connected to the electric grid may share an electricity connection with other devices. Remote control can be used to adjust brightness either manually or automatically, based on traffic (AIS) and/or weather conditions (visibility). In some visions, the AtoNs could also control the traffic. In addition, virtual AIS AtoNs[1] can be used to warn mariners of newly identified hazards (e.g. floating debris).

2. ***Electronic position-finding aids:*** These aids provide vessels with absolute position information that can be displayed on electronic nautical charts. The current GNSS service will in future be accompanied by MF/VDES R-mode and e-Racon, which provide improved interference detection, integrity and accuracy.

3. ***Communication systems:***
a) Dedicated MF, HF and VHF maritime radios are used for speech, such as when communicating with VTS or, in case of distress, with MRCC. In future, VDES (VHF data exchange system) will be used, for example, for eNavigation (AIS, ASM, VDE TER/SAT). Autonomous maritime radio devices also use VHF.

[1] AIS AtoNs are digital aids to navigation broadcast by an authorized service provider using an AIS message that is displayed on navigation equipment (such as ECDIS and radar).

b) Mobile networks and satellites: Today, Inmarsat with VSAT satellite service is the channel for speech and data; 2G-4G commercial mobile networks are used for speech and data; and the authorities utilize the communications network VIRVE (TETRA technology). In future, 4G-5G is being built on a commercial basis; VIRVE2 is being built; and Iridium is approved for the Global Maritime Distress and Safety System. Finally, non-GSO satellites are being launched, but the service level in Finland is uncertain.

c) User and service registries: A platform that enables digital authentication and discoverability of maritime services (such as the Maritime Connectivity Platform, MCP) is to be developed. It is still not clear who would be in charge of this nationally.

Fairway information:

4. ***Digital twin of the physical infra (static):*** In future, there will be high-resolution and up-to-date bathymetric data (seabed) on the major fairways and routes used by merchant shipping (S-102 Bathymetric Surface). The aids to navigation (AtoNs) Information (S-125/S-201) is today physical, and in the future also digital. There is also landscape data (above water). The digital twin could facilitate, for example, remote shipping operations.

5. ***Electronic Navigational Chart:*** The new product specification for Electronic Navigational Chart data (S-57 -> S-101) introduces a fully machine-readable catalog system. ECDIS can then update new elements via a catalog update, which comes together with regular data delivery. This 'plug and play' mechanism will be much simpler to implement by both manufacturers and end users compared to the current process, which requires prolonged software updates.

6. ***Dynamic navigational warnings:*** Navigational, meteorological and safety warning messages are delivered to ships digitally (according to S-124, AIS ASM).

Weather and sea conditions information:

7. ***Weather and sea conditions for the area:*** Improved observations and forecasts of winds, water-level, currents, and so on.

8. ***Weather and sea conditions for a certain location and the planned route:*** Improved weather information with local sensors in port areas and fairways, recording and meshing observations from seafarers and vessels, to foresee surprising and unanticipated local circumstances and traffic patterns. A local design for automated sensor and meshing data is needed.

9. ***Climate change information:*** Climate scenarios for temperature, wind, water level, ice, and so on is provided to the maritime traffic ecosystem, such as shipping companies.

Navigation and seafaring services:

10. ***VTS services and communication:*** These are currently compulsory for vessels over 24 m in length. In addition to current services, VTS could provide active navigation assistance, including confirmed and more accurate position and movement of ships, oncoming and intersecting traffic, time information and anomalies at sea. Extending the requirement to private traffic (e.g., cruisers and yachts) and multichannel broadcasting announcements for all seafarers can increase situational awareness.
11. ***Remote pilotage:*** As an alternative to normal pilotage, vessels are piloted without the pilot boarding the ship. For the vessel, this allows time savings and more flexibility in timetables. Remote pilotage requires reliable ship–shore communication and on-board automation. The master needs to have a qualification to be remote piloted, and the ship's equipment needs to be approved. Remote pilotage is offered to selected fairways.
12. ***Icebreaking:*** This ensures safe waterways for other boats and ships when the fairway is ice-covered. Overall management and prioritization of assistance are the best ways to improve winter navigation.
13. ***Tug services:*** Tugs help vessels in docking, undocking, shifting, escorting, and so on. The improved communication with the vessel, pilot and port makes the service safer and more efficient.

Port arrival and departure related services:

14. ***Port just-in-time:*** Improved information on berthing times and places, and real-time data on estimated time of arrival (ETA) of vessels, would help several parties to coordinate their work and improve efficiency through shorter waiting and faster turn-around times. The ongoing initiatives of the European Maritime Single Window and UNCTAD (2020) accelerate the development.
15. ***Administrative services, customs & boarder guard:*** The upcoming NEMO maritime traffic notification service (European Maritime Single Window) standardizes the process of submitting port visit notifications. This data from NEMO will be utilized in a variety of processes, such as monitoring the border crossings of persons, maritime

search and rescue, overseeing the transport of hazardous substances, collecting fairway dues, port operation, safety and security surveillance, planning port state control, and monitoring infectious diseases.

Other services:

16. *Support for search and rescue (SAR)* requires exchange of information between MRCC, first responders, emergency services, and authorities.
17. *Sustainability services* would utilize sensors on buoys, on-board vessels, and so on, to measure and optimize emissions and erosion caused by maritime traffic. The gathering and analysis of information would require substantial effort, but could, for example, crowdsource the gathering of near-real-time observations for more sustainable routing and timing of traffic.
18. The *situational picture* is an element that would collect and present all relevant information on the conditions, traffic and vessel in an understandable format for the user. At best, it could include predictive measures for avoiding collisions, hazards, and exceptional situations. However, after lengthy discussion in the workshop, and also in group email conversations afterwards, the experts came to the conclusion that situational pictures are user and context dependent; for instance, the sets of information and services that form a situational picture are different for a navy vessel, an oil tanker, or a sailing boat.

References

This research task also produced more detailed descriptions of each element of the smart fairway. These are available from the authors. The results are also presented in following publications:

- Heikkilä M., Saarni, J, Himmanen H., Heikkilä, J. 2022. Smart Fairways – Co-design of future intelligent fairways in Finland, presentation in International Maritime and Port Technology and Development Conference (MTEC) & 4th International Conference on Maritime Autonomous Surface Ships (ICMASS), 6.4.2022 Singapore.
- Heikkilä, J., Heikkilä, M. Märtz, G. 2023. Platforms for Smart Fairways – Enhancing Services for Autonomous Maritime Traffic and Other Emerging Uses of Territorial Sea, Hawaii International Conference on System Sciences HICSS, 2023.

Maritime@TSE community at the University of Turku

The University of Turku (UTU), located in Turku in southwestern Finland, has a strong reputation in maritime research. Maritime@TSE is an active and expanding research community of professionals from different business studies disciplines at the Turku School of Economics. In all, 5 professors and research directors and around 25 post docs and other staff are engaged in maritime-related topics and contexts. Our research activity is systematic, international and expanding. We also work in close collaboration with different maritime sector stakeholders internationally. Our research focus areas include digital and autonomous maritime business, new maritime business models and services, maritime logistics, and maritime sustainability, safety and sustainability, as well as economic development of the maritime sector.

Rethinking smart fairways for all

Contributors

- Jukka Heikkilä, University of Turku
- Marikka Heikkilä, University of Turku

Introduction

At the outset of the S4V fairway project, the participants stated that the central goal of developing fairways should be to improve the safety of all seafarers. Additionally, future fairways should help in achieving more efficient and environmentally sustainable marine traffic.

The situation in Finland is both tricky and promising. Finnish territorial waters are shallow and demanding to navigate. Four seasons, with vastly varying conditions, pose challenges for maintaining safe fairways. The surrounding nature is sensitive to erosion and vulnerable to oil spills. On the other hand, the long-term progress of fairways is promising. We have relatively good coverage of wireless communications, and integrated ECDIS navigational aids are in wide use in territorial waters. The traffic control and rescue services are well developed and efficient, and the authorities are keen to develop novel solutions for future automated and autonomous traffic. In the previous chapter, a large set of elements of improved services are presented and classified in terms of the feasibility of their implementation.

Most modes of traffic by sea have grown. In S4V, we reflected on the need to enhance the smartness of the fairway by introducing new elements from the points of view of various user groups.

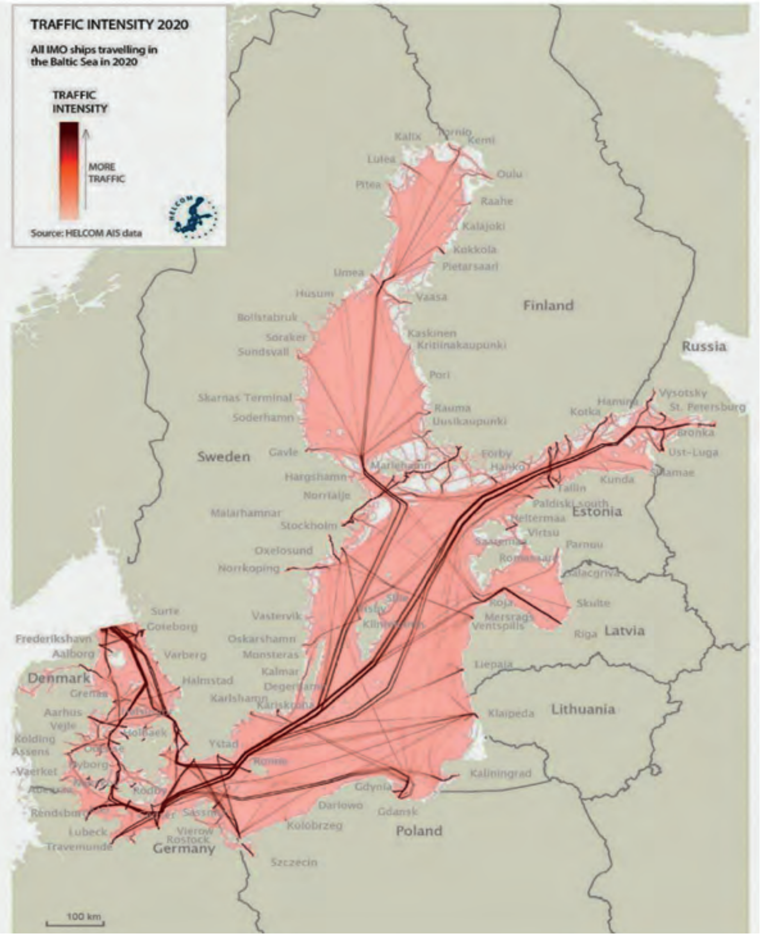


Figure 1. **Traffic intensity map (HELCOM).**

For that purpose, we first analyzed the quantitative and qualitative changes of the traffic by seafarer categories. It is obvious that merchant and commercial traffic has increased substantially; in the last 50 years:

- Inbound international cargo has more than doubled from 20 Mtn/a to 46 Mtn/a.
- Outbound international cargo has almost tripled from 18 Mtn/a to 50 Mtn/a.
- Domestic freight has grown a fifth since 1980.
- The number of passenger voyages has grown sixfold from 3 M/a to 19 M/a.

In total, 30,000-40,000 merchant vessels arrive at the ports of Finland annually.

MRCC = Maritime Rescue Coordination Centers (Turku)

MRSC = Maritime Rescue Sub-Centre (Helsinki)

VTS = Vessel Traffic Service sectors

SRR = Search and Rescue Region

SRS = Search and Rescue Sub-region

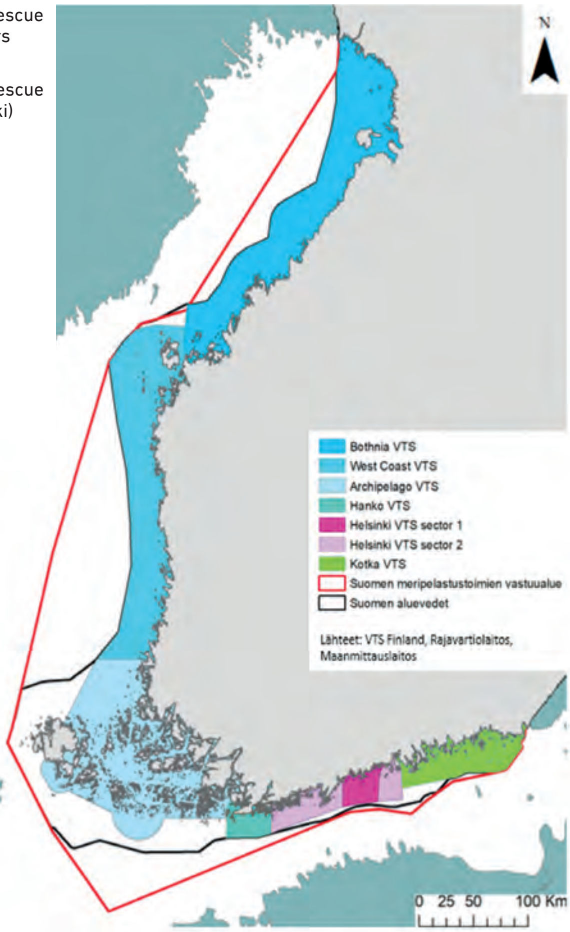


Figure 2. **The responsibilities for organizing coordinated safety and rescue operations along the fairways.**

Most merchant and commercial traffic takes place in the well-maintained merchant fairways class under the control of VTS, class VL1. The traffic in these fairways is indicated in Figure 1, of AIS vessels bigger than 300 gross tons (Helcom, 2022).

The recreational use of the sea area is estimated to have grown even more, but these estimates are based on questionnaires and assessments of face value (e.g., Haaga-Helia, 2021). A lot of this traffic takes place outside the merchant fairways. In other words, recreational seafarers navigate on less secure and less maintained routes (classes VL2 to VL6), and even outside waterways; the latter means on their own and at their own risk. The largest group of unregistered vessels in Table 1 contains a majority of watercraft: small motorboats and rowing boats, the fast-growing categories of water scooters and kayakers, but not including the growing numbers of skaters, skiers, and ice-fishers, all with low to moderate skills in navigating, in looking out for other traffic, and in regulations for preventing collisions.

Despite the above-mentioned growth and changing traffic patterns, safety on the Finnish seas has improved. Fatal accidents diminished by a third from 57/a to 40/a during 2007-2015, and overall the number of accidents has remained nearly constant despite the growth of the watercraft base and increased traffic. However, even though serious accidents happen rarely, there have been reported cases and anecdotal evidence of increasing near misses of various kinds, especially in recreational traffic. We can conclude that the earlier claimed qualitative changes of uses of regional and local water areas seems to hold true: the number of incidents requiring assistance has grown. While VTS and the Finnish Border Guard report about 800 to 900 annual incidents in VL1 and VL2 waterways, the volunteer organizations the SAR Åland Islands Lifeboat Society and the Finnish Lifeboat Institution (FLI) report around 100 and 1600 incidents annually, respectively, mainly in and outside lower-class fairways, and these numbers are growing slightly. Note, too, that the FLI also serves lakes in mainland Finland with regional rescue departments.

What kinds of waterways exist?

A fairway is defined as a channel for waterborne traffic within a channel's edge limit. A channel, in turn, means a water route between two end points. It is marked with a set of markers, both on official maps and along the water route, in a standardized manner. There are tolerances for the markings and physical dimensions of the waterway, which have to be inspected and taken into account while navigating. The responsibilities for organizing coordinated safety and rescue operations along the fairways by Finnish Transport Infrastructure Agency are divided as depicted on the map in Figure 3 (VTS Finland, The Finnish Border Guard & NLS Finland; c.f. Vaimala, 2020). This areal division follows international agreements and is the basis for rescue services and the present sectors for communications.

In more detail, the fairways are classified in six categories and three maintenance classes. The six categories are as follows:

- Merchant fairways for global traffic (VL1) are maintained in all seasons, in all conditions for traffic.
- Local and connecting merchant fairways (VL2) and shallow fairways for commercial (VL3), boating (recreational) traffic routes (VL4) are maintained in open waters season, in all conditions.
- Connecting routes (VL5 and VL6) are checked once a season.

Security devices are maintained during the open waters season as follows:

- Category 1: immediate repair of defects, at the latest in 3 days. On merchant fairways VL1 and VL2, during the first day of defect announcement.
- Category 2: repair in two weeks. On merchant fairways VL1 and VL2, defect announcement in two days.
- Category 3: repair in a month.
- Category 4: on own initiative, or according to a Traficom notice to repair.

The above categories of security device management are thus dependent on the device type and the kind of fairway in which it resides (i.e., the type of traffic it serves). Because of the severe Nordic conditions, many of the markings are moved by drifting ice, storms, and device wear. The official fairways' security devices can be positioned on private property either by consent or with an official decision from the authorities. The private fairways do not have the latter option, so the requirements on fairway markings are more relaxed, but still follow the standards and interoperability requirements.

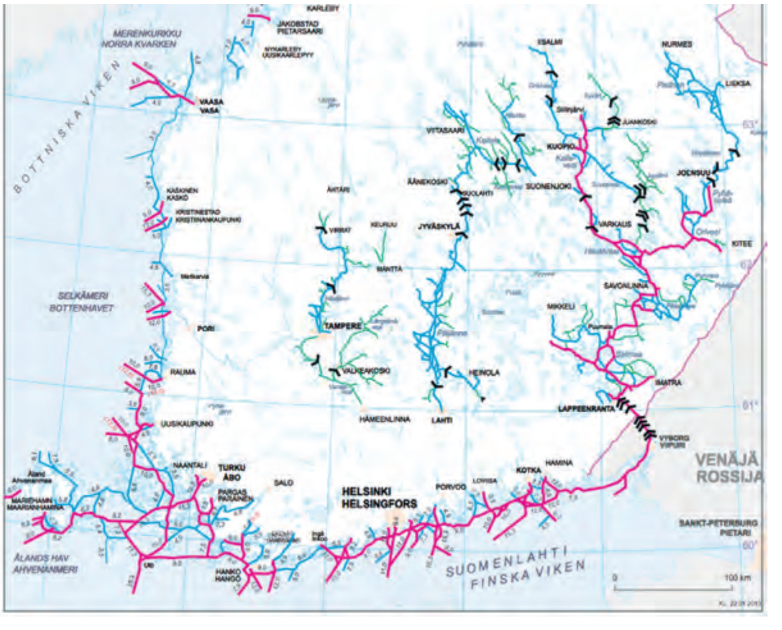


Figure 3. The most important waterways in Finland.

It would be tempting to compare traffic fairways at sea with other methods of transportation by air and on the ground. However, there are some major differences:

First, air traffic is regulated in detail, to avoid collisions and accidents, by using air traffic control (i.e., tower TWR) to manage operations in restricted traffic areas (e.g. control zones, CTZ) in the air and on the ground (ground, GND). The properties of airplanes and airfields are matched to ensure safe and smooth operations. Restrictions on airspace are based on the layered architecture of airways (Flight levels, FL) and, as a consequence, the traffic can be optimized to avoid collisions in the air and on the ground. At sea, there is only one layer for movement, and it is primarily open to everyone: it is a public space. Therefore, the current fairway infrastructure is designed for and open to all kinds of traffic, with the exception of ports and a few restricted safety zones closed to the public. Vessel Traffic Services are more of a recommended informative nature for smaller vessels under 24 m in length, because it is not obligatory to have VTS-compatible equipment even in the VTS area.

Second, road traffic is based on rules and enforced monitoring of traffic. There is a myriad of types of vehicles occupying the traffic infrastructure on highways, roads, and streets: basically, all road users must possess the skills to control their vehicle in all circumstances, and must understand and apply the rules designed for co-operation in traffic. This is shown by a driver's license that can be granted to the operator only with proven education and a test in real traffic. There are lots of dynamic signs and markings to be understood and obeyed without consideration or hesitation, such as a red light at the roadside that stops the traffic flow. Basically, the whole road infrastructure is designed to take into consideration the other users of roads: increasingly cyclists, pedestrians, skateboarders, and newly invented semi-autonomous electric vehicles, both in urban and non-urban areas. The situation at sea is again very different, because basically anyone can jump on a boat (especially in territorial waters). In addition, the education is voluntary, and recently relaxed for smaller watercraft, where as the difference from commercial and merchant traffic is very strict. The skills of mastering vessels versus road vehicles are very different, and the characteristics of fairways and weather and sea conditions restrict the maneuvering: it is not practical, for example, to ask to bring vessels to a complete halt at sea under heavy winds and currents.

Our conclusion is that implementing traffic and safety measures at sea is different from other means of traffic. Of the specific maritime traffic rules, the most important one is the Convention on the International Regulations for Preventing Collisions at Sea (COLREG, 2018), and the safety improvement measures should comply with it.

Where can we start improving waterways?

According to the previous statistics on traffic, vessels and accidents, we suggest starting the safety improvement:

a) in the known high-risk areas for hazards and accidents

b) to improve the safety of the least-favored, less-served seafarers.

An analysis shows high-risk areas for accidents in fairways (Vaimala, 2020). These are located around Helsinki, Turku and Uusikaupunki/-Rauma territorial waters, especially at the crossings of international water routes and intercity traffic between Helsinki and Tallinn (Figure 2[1]). We can conclude that these spots where territorial water channels cross international waterways require special care in terms of VTS, piloting and surveillance services. As a consequence, special attention should be paid to introducing new elements and resources in the above-mentioned areas. The same applies to crossings, straits, and shallow parts of the territorial water channels in the archipelago, and also in proximity to harbors and known short-cut water areas outside fairways.

The fairway infrastructure and services can be improved in the short term by:

- providing more precise information on routing and conditions,
- enhancing on-board indications of an emergency and directions for evasive actions,
- connecting safety devices for automated self-testing and reporting of drifting, malfunctioning, etc.
- providing this information:
    - virtually using ECDIS,
    - using connected fairway physical safety devices, such as traffic signs and lights, and direct on-board communication between vessels and rescue services.

The least-favored user groups belong to the largest and fastest growing categories of recreational watercraft users and people moving at sea by other means during the ice-covered period. This increased recreational traffic would need better guidance and devices to enhance their safety

1 https://vayla.fi/documents/25230764/35414160/Suomen_tarkeimmat_vesivaylat_2022.pdf/dadbc47e-d392-23a0-00cf-cbe6ef3a1cb5/Suomen_tarkeimmat_vesivaylat_2022.pdf?t=1642679606157

at sea. By developing suitable applications on the enhanced infrastructure, the waterways can be enhanced so that they augment seafarers' capacity to:

- plan their precautionary measures in advance
- avoid hazardous situations
- operate in distress and emergency situations

Precautionary measures

Education and training is in need of improvement. There are a number of requirements for qualifications of seafarers that are subject to the ship size and cargo (e.g. a pilot exemption on standard routes on well-maintained merchant waterways), but the biggest gap in education is among recreational seafarers. The education should consist of traditional means of navigating at sea, enhanced by traffic patterns and the means to plan ahead for route and traffic situations, avoid collisions, and act in an emergency using modern means of maneuvering, navigating and communicating. Virtual education by lifeboat associations (such as https://veneilytaito.fi/koulutus/) for recreational users could be utilized.

Predictive routing and scheduling: AIS integrated with web-based services has been expanding both into commercial and merchant vessel planning. AIS is in need of a major overhaul, as the data transfer in heavy traffic areas is limited, causing delays and imprecision, and forging of data is relatively easy. However, it provides a handy means of marking security devices, exceptions, and so on, and there is the potential to introduce priority schemes for authorities' announcements and control. In Finnish waters, the route announcement is compulsory for bigger ships. By using AI, some traffic control can be automated and broadcast for other users. In addition to exceptional situations, according to IHO S124 (Navigational Warnings), VTS requires a standard announcement via GOFREP (see Figure 4) when entering Finnish territorial waters[2]. The Traffic Centers monitor shipping by radar and AIS and provide a 24-hour information service in the Gulf of Finland to all seafarers via VHF radio (official) and AIS (unofficial). There is an additional announcement area for dispatching and redirecting traffic to the Gulf of Bothnia that could be made compulsory for predicting the routes of AIS vessels (Finnish Traffic Infrastructure Authority, 2022). With enhanced AIS tracking and communication networks, the standardized GOFREP information can be enhanced with near-real-time virtual routing information for all seafarers, both for route planning and for safe maneuvering en route.

[2] Mandatory Ship Reporting System, adopted by the IMO (MSC.139(76) and MSC.231(82)), in accordance with SOLAS Regulation V/11. The sea areas in the Gulf of Finland are monitored jointly by Finland, Estonia and the Russian Federation.

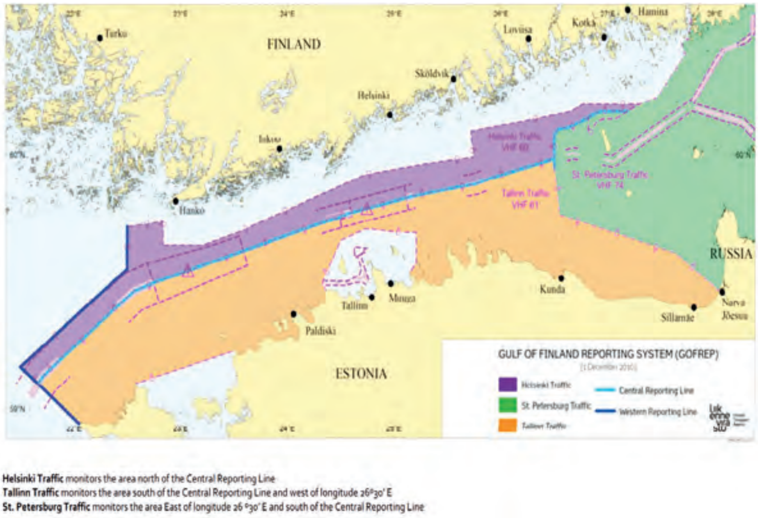
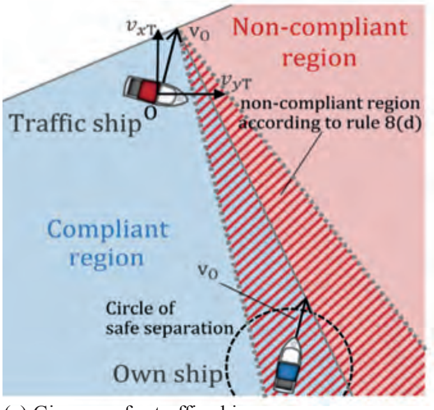


Figure 4. **GOFREP reporting areas in the Gulf of Finland.**

Collision avoidance

Traditional means of looking out and estimating distances are prone to hindrances to observation, fatigue, and loss of attention. Hence, the recent trend is to integrate meshed information on ECDIS (enhanced with maps, sonar, weather and VTS alerts, etc.). Watercraft and travelers by other means at sea seldom carry dedicated ECDIS with them, but mobile terminals and phones could provide assisted, automated location and tracking services via 4G cellular networks. Automated COLREG algorithms could provide information about potential hazards and alerts, and mediate that to vessels in proximity and to VTS traffic controllers (see Figure 5 for an example of COLREG-compliant and non-compliant regions identified by location, speed and directional information that can be implemented with algorithms; Cho et al., 2022). Additional aids and standards are available via the IMO-endorsed IALA Risk Management Toolbox (https://www.iala-aism.org/technical/risk-analysis-and-management/).

Automation could be based on both broadcast VDES-Rmode communication networks and/or enhanced point-to-point 4G cellular networks. 4G networks cover most but not all of the Finnish SRR, comparable to the current VTS VHF radio sectoral division, so the networks should co-exist. If designed correctly, 4G has the potential to serve big crowds with dynamic capacity allocation, at high data transmission rates of up to 100 Mbit/s. This kind of communication network could be implemented with the update of authorities' VIRVE networks by adding to and optimizing its base station network for roaming with priority schemes, directional antennas, and features for broadcasting official announcements, emergency messages, and location tracking, at the edge of the network by HLR/VLR services. There are also proven commercial 2G/4G-based tracking solutions for which use is limited mainly by GDPR (e.g. yepzonsolutions.com).



(a) Give-way for traffic ship

Figure 5. COLREG-compliant regions when meeting a merchant ship.

Operation in an emergency

In the case of distress or emergency, actions on the grounded, collided, or to-be capsized vessel depend on the capacity and skills of the crew or seafarers. Educating, preparing, and rehearsing for hazards is of vital importance. Vessels differ in their maneuverability, and maneuvering aids differ and must be mastered with smaller vessels. Inspection of vessels could provide additional services for using the communication devices, maneuvering, and aids to navigation and rescue.

Distress and emergency signals (e.g. according to MIPDANIO; see Fig. 6) could be automated and broadcast to seafarers in proximity and VTS services. Gathering the tracking information and communicating that information over digital channels, with live footage from the site, can potentially speed up SAR and coordinated rescue services with the Border Guard, VTS services, MRCCs, and lifeboat associations, not to mention other seafarers.

Machine-to-machine messaging: e.g. automated **MIPDANIO** distress/emergency message for all seafarers

M AYDAY,MAYDAY, MAYDAY
I dentify – vessel id
P osition – location in georef or heading and distance from a stationary point
D istress – what's going on?
A ssistance – estimated need for help
N umber of crew – and condition
I nformation – additional information
O ver

Figure 6. **MIPDANIO message.**

End note

As of writing, we propose following the directions for the further development of fairways (Figure 7). Here, we have concentrated on improving safety for all seafarers in the near future. Efficient and sustainable traffic has not been treated extensively, but a thorough analysis of the right-hand stream of development could potentially improve the sustainability of the vulnerable nature of the Baltic Sea, avoiding compensation for harm and damage and saving resources by optimizing routing, adjusting speed according to weather conditions, and optimizing harbor capacity and services.

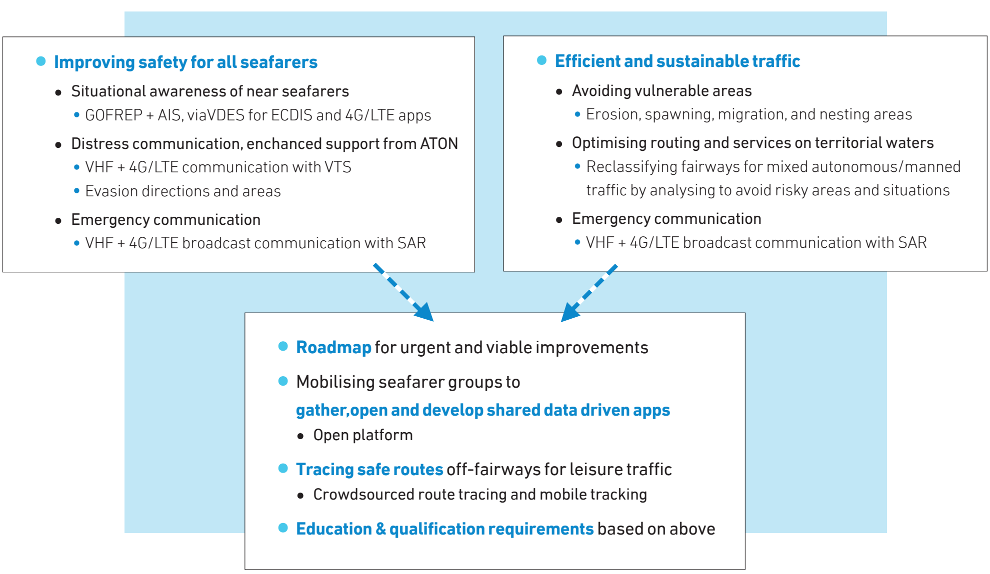


Figure 7. **Suggestion for directions for the further development of fairways.**

References

- **COLREG,** 2018. Convention on the International Regulations for Preventing Collisions at Sea, 1972 Consolidated edition, 2018. 62 pages.
- **Haaga-Helia,** 2021. Veneilyn taloudelliset vaikutukset (The economic impact of boating). Haaga-Helia publications, 8/2021, ISBN 978-952-7474-00-6, ISSN 2342-2939101 pages. Available at https://www.haaga-helia.fi/sites/default/files/file/2021-10/veneilyn-talousvaikutusten-selvitys.pdf (in Finnish).
- **Helcom,** 2022. https://maps.helcom.fi/website/mapservice/index.html
- **IALA,** 2020. G1158 VDES R-MODE. IALA Guideline, Edition 1.1, December 2020, urn:mrn:iala:pub:g1158:ed1.1
- **IMO,** 2018. Revised Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making Process. MSC-MEPC.2/Circ.12/Rev.2 9 April 2018, 2 pages with Annex of 69 pages.
- **Statistics Finland** (2022). Merchant fleet. https://www.stat.fi/en/statistics/klaiv
- **Traficom,** 2021. Vesiliikenneonnettomuudet. Navigation accidents, in Finnish. https://www.traficom.fi/sites/default/files/media/file/VESILONN-2020-vuosi.pdf
- **Vaimala K.,** 2020. "Merionnettomuuksien sekä -poikkeamatilanteiden tarkastelu Suomen meripelastusvastuualueella, sekä riskialueiden estimointi maantieteellisesti painotetulla regressioanalyysillä", Yhteiskuntamaantieteen pro gradu -tutkielma, Itä-Suomen yliopisto.

The fairway of the future: important technical lessons learned

Contributor • **Bilhanan Silverajan,** Tampere University

Background The maritime industry is one of the oldest industries known to mankind, and it is heavily regulated by maritime rules. It remains a vital part of the global economy, responsible for over 90% of trade around the world. There are heavy investments in digital transformation, for the introduction of smart ships and smart ports, which will impact the technology in fairways and waterways. Such investments in digital transformation are significantly based on advanced terrestrial connectivity, industrial IoT developments, data management, image processing, mapping, artificial intelligence, and machine learning.

Finnish fairways and waterways have to become prepared for increasingly intelligent sea-going vessels. While autonomous ocean-going ships are still in the distant future, many ships will become semi-autonomous, with increasingly complex onboard systems and reduced crew operations. Fairway infrastructure, in addition to current types of vessels, will therefore have to cater for more modern fleets that will be equipped with advanced sensing, mapping, navigation and communication subsystems.

Intelligent fairway and services

Figure 1.

As Figure 1 shows, the infrastructure of the intelligent fairway can be perceived as a digital platform offering itself toward supporting several kinds of services atop it. Such a platform can, for example, consist of the following:

- Sensors
  - Bathymetric, acoustic, positioning, movement, environmental
- Processing
  - Visual analytics, sensor fusion, trajectory detection, and forecasting
- Communication and the cloud
  - Base stations, transponders, gateways, access points, VHF
- Auxiliary Systems
  - Vessel-tracking services, AIS

Testbed requirements for intelligent fairways

Testbeds serve as a fundamental technical block to understand what the infrastructure and service needs can be for a future digital fairway. They can form the basis and a stepping stone toward even providing a full-scale digital twin of the fairway. In the Sea4Value Future Fairway Navigation program, the building of testbeds enabled the emulation, development, and deployment of shore-based maritime services, such as clouds and data servers. The construction of a testbed should be flexible, in order to allow and technically delineate how and where the "edge" lies (for example, is it the fairway or is it the intelligent vessel). This would be useful in order to offer the following technical services:

- Provide edge infrastructure for testing digital communication, traffic shaping, and integrating various network topologies
- Deliver connectivity for sensors and equipment
- Understand, model, and visualize security risks and threats

Connectivity and communication considerations

When fairways are close to the shore, current cellular coverage with LTE in Finland is excellent. Nevertheless, different radio technologies are still needed in order to meet connectivity needs. This is because fairway sensors and equipment further away from the coast or in blind spots need connectivity as well, and not all sensors support cellular connectivity. Additionally, incoming vessels may be equipped with other technologies, such as VHF and satellite connectivity for ship-to-shore communication.

The first attempt at the digitalization of maritime transportation was the Automatic Identification System (AIS). The main driver for AIS was safety, and the main goal was broadcast communication. However, new services have arisen, with support for application-specific messages. To prevent overloading the AIS, ITU is standardizing a new radio interface for the VHF Data Exchange System, which can be a hybrid of terrestrial and satellite communications. This is in addition to using only terrestrial and satellite communications. Connections need to be resilient, secure and able to tolerate connectivity disruption or intermittence.

Exchange and transfer of sensor data

Today, a general consensus exists that, in the future, IP-based communication will emerge as the dominant technology in the digital fairway. However, the communication protocols that are used on top of IP can become very confusing, especially for sensor traffic, with current solutions being use-case and business specific. Communication paradigms also differ, based on needs. The available options include Publish/Subscribe, REST (Representational State Transfer), and RPC (Remote Procedure Calls). Communication protocols that implement these paradigms are based on TLS (Transport Layer Security), DTLS (Datagram Transport Layer Security), HTTP (Hypertext Transfer Protocol), CoAP (Constrained Application Protocol), and MQTT.

The exchange and transfer of sensor data can occur over a variety of wired and wireless networks conforming to device and technology-specific requirements (NMEA, CAN bus, etc.) but over IP networks, sensor payloads using JSON (JavaScript Object Notation) are increasingly dominant. JSON is well supported, using HTTP APIs from third-party providers, as well as over REST protocols. Additionally, JSON-based data representations can be converted into other formats such as XML (Extended Markup Language) for compatibility, or compacted into CBOR (Concise Binary Object Representation) to achieve better compression.

Nevertheless, when high-speed broadband communication channels exist and bandwidth is abundant, the choices of security mechanisms, communication protocols, and data payload formats are not significantly different. When radio signaling costs are high compared to the amount of data transferred, again, application layer performance does not matter. However, when the radio channel is congested or lossy, or experiences severe latency, then using security protocols such as TLS and DTLS will become impossible. In such cases, if security is needed for sensor traffic, it is necessary to consider the signing and encryption of data at the application protocol layer instead of the transport layer. However, considerations also should take into account smaller payload formats and sizes to overcome lossiness.

Considerations for data sharing and data models

Any data sharing performed should be scalable and able to allow multiple stakeholders to participate. This means it should be based on open standards, to avoid vendor lock-in, and should have the ability to integrate easily into existing workflows, particularly integration with Web and REST communication. Additionally, it needs to have a standard vocabulary and data models to express data. However, while serialization formats such as JSON are commonplace, interoperability still seems to be highly hampered by a lack of standardized data models to describe maritime-specific sensor data.

Future digital fairways therefore need to have extensible and flexible data models. Such data models should also allow future extensions, such as new sensor and incident data for smart ships and smart ports. The format should allow the expression of multiple measurements occurring within a specific time period, or the association of related data happening in different locations and at different times. The format should also be simple enough for machine-based interaction, so that report generation and processing can be automated.

Conclusions

The Sea4Value Future Fairway Navigation program, as a technical blueprint for a future fairway infrastructure, has been extremely informative. When studying the minimum requirements for enabling remote piloting, it was revealed that it is already technically possible today, with minimal disruptions to ship systems, while increasing the safety and security of piloting services. However, many ports, ships and fleet-based operations systems still depend heavily on legacy systems. Compared with other industrial sectors, cybersecurity awareness is still low in the maritime industry, with cyberattacks ranging from phishing to ransomware attacks being prevalent owing to insecure practices and a lack of proactive action to address cybersecurity. Employing preventive defensive methods, such as securing communication channels, hardening equipment software, firmware and hardware, and endpoint protection, as well as user and device authentication, will be useful. In addition, the development of new defensive strategies is needed for the future fairway, and this depends on information sharing, data correlation, and increasing cybersecurity awareness.

Awake.AI

Awake.AI is a cloud platform startup providing digitalization and AI services globally for maritime logistics actors. Related products include AI-supported tools for planning and situational awareness, ML-based prediction services, computer vision solutions for cargo monitoring, and custom digital solutions for optimizing multimodal logistics operations. Awake.AI is building an ecosystem for smart ports and shipping, and the company's mission is to lead the transition to sustainable and intelligent maritime logistics in which 10 % of the global CO_2 emissions from shipping will be reduced by 2030 with the help of the ecosystem partners.

AI for fairway safety monitoring

Contributors

- Awake.AI: Petri Aarnio, Vaklin Angelov, Mikko Hakila, Sami Jalo, Santeri Kääriäinen, Eero Lehtonen, Jussi Poikonen, Petra Virjonen, Jonatan Wiik
- Brighthouse Intelligence: Karl-Erik Gustafsson, Markku Sahlström, Mika Tolvanen

Background

To support the safety and efficiency of remote pilotage operations, Awake.AI has developed AI systems for automated predictive monitoring of fairway usage and safety of ongoing operations. This includes the development of cloud-based services for predicting the schedules of vessels arriving at a given port or related fairway based on global vessel positioning data, services for estimating dynamic vessel-specific navigational safety margins during pilotage, and implementation of Application Programming Interfaces (APIs) and web application components to provide user interfaces and to enable external system integrations for the services.

The benefit of automated vessel schedule prediction in remote pilotage is that this provides up-to-date estimates of when vessels will be arriving in pilot boarding areas, which is when pilotage is expected to be needed, days or even weeks into the future, depending on port traffic characteristics. Furthermore, this function enables the estimation of congestion periods in the fairway and port areas, which is relevant for both safety and holistic planning of schedules for efficient resource usage.

Estimating navigational safety margins during pilotage provides decision support and independent safety data for remote pilotage, especially in exceptional situations, such as when direct sensor data from the vessel is not available or is degraded, or, for example, when severe environmental conditions cause uncertainty for the remote pilot on the behavior of the piloted vessel in the fairway. The underlying system also enables automated monitoring, logging, and analysis of safe fairway usage, and facilitates the development of automation solutions for remote pilotage and corresponding functions needed in autonomous vessels.

Solution and method

Predictive monitoring of commercial vessel traffic along fairways

Global vessel voyage schedule prediction was implemented in the Awake.AI cloud platform as a pipeline of prediction services, which each contain multiple component algorithms or Machine Learning (ML) models. This type of modular ensemble approach offers benefits such as enabling the explainability and possibility of manual customization of rule-based models, and combining this with the potential for performance improvement offered by ML-based optimization models.

The main components in the developed vessel schedule estimation pipeline are ***destination prediction, trajectory prediction, sea voyage duration prediction,*** and ***pilotage prediction***. Destination prediction monitors Automatic Identification System (AIS) data transmitted by commercial vessels globally and classifies their current destinations based on rules, heuristics, and ML models trained with global historical AIS datasets. Data from vessels classified as headed to destinations of interest are further processed in the trajectory prediction service, which estimates the voyage route from the vessels' current locations to their destinations. This is based on models learned from historical vessel traffic patterns, and it also enables adapting the predictions to vessel characteristics, such as dimensions or draught, which affect the available route options, such as through channels or fairways with traffic restrictions.

Voyage duration prediction uses the trajectory prediction output to obtain the estimated distance to be traveled by the vessel, and it calculates the effective speed of the vessel over the remaining voyage distance. This is based on multiple factors, such as the current speed of the vessel, historical speeds over the predicted voyage route, and machine learning models trained to compensate for systematic location-dependent speed variations. Finally, for selected destinations, dedicated pilotage prediction models are configured, which can take into account, for example, approach restrictions along the fairways to the port or other port-specific characteristics of the pilotage that affect vessel schedules.

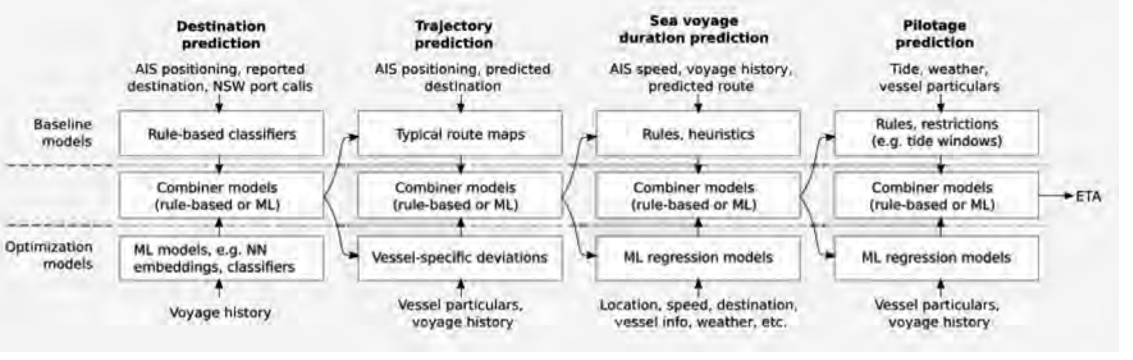


Figure 1. Copyright: Awake.AI

Estimation of dynamic vessel-specific safety margins during pilotage

To analyze navigational safety margins during pilotage, Awake.AI developed a dynamic fairway service that can ingest navigational information (e.g. location, velocity, heading) on the piloted vessel both directly from sensors onboard the vessel (which were available in the project as part of the overall remote pilotage system development) and through standard AIS integrations (as available in Finland, e.g., through Digitraffic). The service was also developed to use environmental data such as wind and current measurements when available, such as from dedicated sensors installed along the fairway. The service was implemented in the Awake.AI Smart Port cloud platform, which provides the necessary computational infrastructure and existing data integrations to many relevant systems, which were expanded with the integrations (e.g. direct vessel navigation data from an API provided by Brighthouse Intelligence - BHI) necessary for the dynamic fairway service as outlined above. API access was also implemented in the dynamic fairway service to enable direct integration with external systems.

The dynamic fairway service uses the above-outlined information to estimate a safe zone for the piloted vessel based on its current navigational status and environmental conditions. The safe zone is here defined as a part of the fairway in which the ship can maneuver at its current speed and still stay safely in the fairway. In other words, the safe zone borders represent the points where the ship needs to begin turning (with the given maximum rate of turn and acceleration) if the current speed is to be maintained, in order to stay in the fairway. User interface components were developed in the Awake.AI Smart Port web application to visualize the safe zones for a selected vessel during fairway passage.

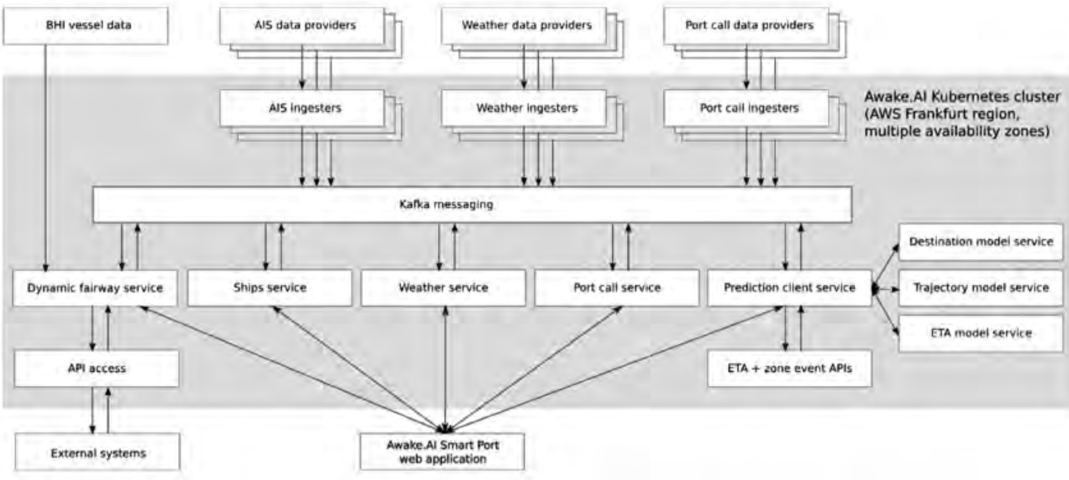


Figure 2. Copyright: Awake.AI

Development of the dynamic fairway service function was implemented in the following main phases:

1. Building a framework for simulation of vessel movement in varying environmental conditions
2. Modeling the vessel type used in the remote pilotage demonstration of the project
3. Building a vessel-specific model for fairway safe zones by simulating the behavior of the target vessels with a relevant range of values for the input variables

For the simulation of vessel dynamics, different vessel types or individual vessels are modeled physically, taking into account various force and torque factors, such as thrust from main and bow thrusters, water friction, wind and air resistance, rudder resistance, residual resistances, and torque effects of the bow thruster, rudder, water, and wind (see references for examples of models and parameters used). The model parameters for each vessel type were fitted by simulation tests to the measured maneuvering characteristics of the vessel, as specified, for example, in the vessel's wheelhouse poster. In the project, this vessel modeling was performed for the ESL Shipping vessels Viikki and Haaga.

For dynamic fairway monitoring, we applied the above outlined simulation model to estimate turning safety margins as a function of environmental variables and the vessel's current velocity. By iterating turning simulations over suitable ranges of initial vessel movement states and environmental parameters (wind and current vectors), dynamic fairway lookup tables (LuT) were constructed to model the respective turning distances of the vessel. The computation of the safe zone is based on the dynamic fairway LuT: the speed and course over ground of the ship are compared to the direction of the fairway boundary, and the turning distance toward the course of the fairway boundary is obtained from the LuT at the considered wind and current conditions. The safe zone boundary is then moved in the direction of the center of the fairway (normal to the fairway direction) by the turn length.

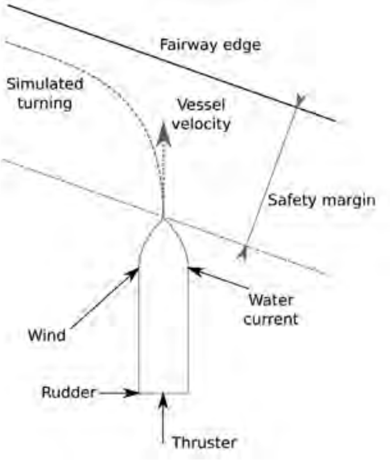


Figure 3. Copyright: Awake.AI

Results, findings, output, and impact

The outputs of the services described above were made available externally through APIs and by developing relevant user interface components in the Awake.AI Smart Port web application. To monitor upcoming vessel schedules, the user can select individual vessels to view their predicted destinations, routes, and schedules, or filter vessels globally based on their predicted destinations, to monitor all incoming vessel traffic for selected ports. For each voyage, estimated arrival times in pilot boarding areas and terminal or berth areas are provided separately. The application also visualizes the pilot boarding areas and official fairway areas, and how the predicted vessel route relates to these.

Figure 4. Copyright: Awake.AI

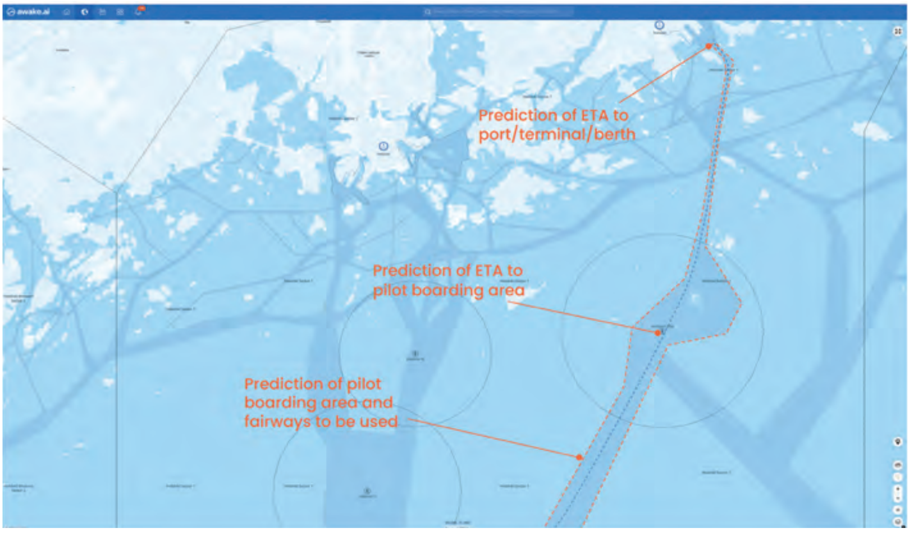


Figure 5. Copyright: Awake.AI

The traffic for a selected port can also be monitored through a timeline view showing an overview of all port calls, with easy access to additional details on vessels and their predicted schedules. Alternatively, the user can view the current and future port occupancy situation using a map view showing the resources of the port (berths, bollards) and the locations and dimensions of vessels in the port over a selected time interval. All of the schedule monitoring functions presented here have been developed to production level and are provided as commercial services to customers globally.

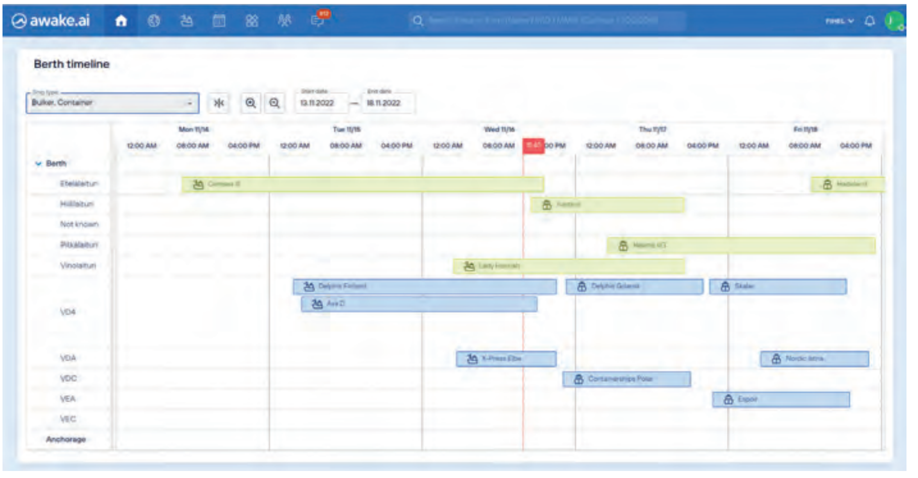


Figure 6. Copyright: Awake.AI

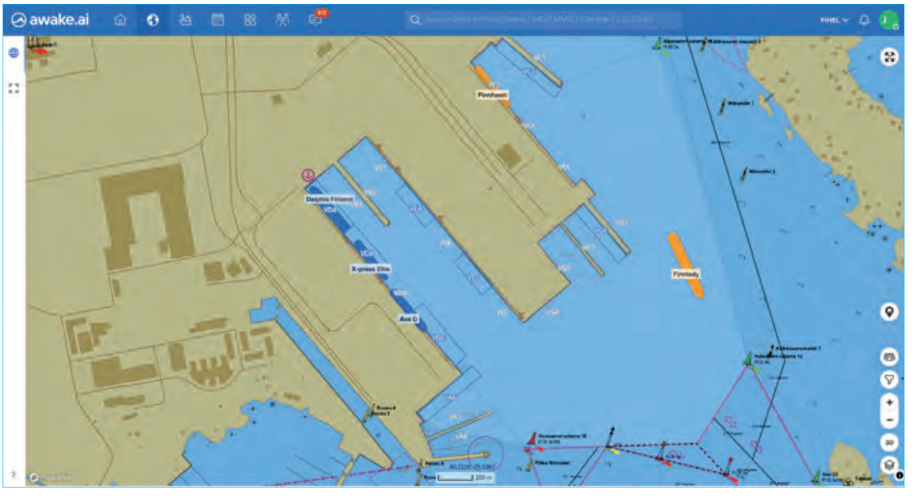


Figure 7. Copyright: Awake.AI

To monitor the dynamic safety margins during fairway passage, the user can enable visualization of the fairway safe zones for selected fairways and vessels that have the relevant models configured. The safety margin computation can currently be rapidly configured for any fairway in Finland, using fairway definitions available from official sources (e.g. väylä.fi). Configuring models for new vessels or vessel types currently requires some development effort and vessel specification data as described in the previous sections; automating the modeling process using, for example, machine learning methods is a potential future development of the system.

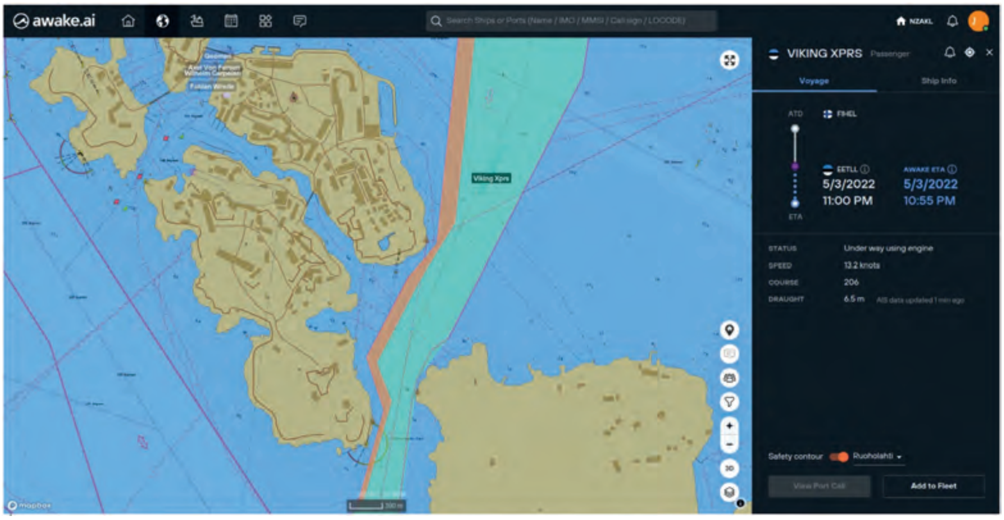


Figure 8. Copyright: Awake.AI

The web application outlined above was provided for use in the landside remote pilotage center in the project demonstration, with especially the dynamic safety margin visualization visible to test users. Additional practical testing is needed to validate this part of the developed functions in varying conditions and more challenging fairway conditions, as the pilotage scenario in the project demonstration was relatively simple and highly controlled. Furthermore, additional development and tests in real pilotage scenarios would be beneficial, to optimize the user experience and usability for the target application. The existing service could also be expanded with additional safety functions such as visualizing predicted vessel passings, congestion, or potential collision risk scenarios along the fairway passage.

References

- Żelazny, K. 2014. *Approximate method of calculation of the wind action on a bulk carrier*. Scientific Journals, Maritime University of Szczecin, 2014.
- Żelazny, K. 2014. *Approximate Method of Calculating Forces on Rudder During Ship Sailing on a Shipping Route*. Transnav – International Journal on Marine Navigation and Safety of Sea Transportation, Volume 8, Number 3, September 2014.
- *Recommended Procedures and Guidelines (7.5-02-02-01), Resistance Test.* 2017, ITTC – International Towing Tank Conference, 2017.
- Guldhammer, H. and Harvald, S. 1965. *Ship Resistance – Effect of form and principal dimensions.*


S.P.T.
FIRE
RADIO
GPS
ME RPM
ME RCF
SPEED
PRINCIPAL DIMENSIONS
INCREASE OF DRAUGHT DUE TO HEEL
ANGLE OF HEEL
INCREASE OF DRAUGHT
0,30 M
0,60 M
0,90 M
1,20 M
1,50 M
30th January 2021

Aalto University

NOVIA UNIVERSITY OF APPLIED SCIENCES

UNIVERSITY OF TURKU

ESL Shipping

ESL Shipping's M/S Viikki was involved in the implementation of the remote piloting experiment. Photo: ESL Shipping Archive

REMOTE PILOTAGE

Aalto University, School of Engineering (Marine and Arctic Technology)

Aalto University, School of Engineering (Marine and Arctic Technology), Research Group of Safe and Efficient Marine and Ship Systems (SEMSS). The research group SEMSS focuses on the development of scientific principles, models and tools for the analysis of marine risks and the management of safety in complex maritime socio-technical systems, with a focus on the development of the concept of smart shipping in diverse operational contexts such as open sea navigation, winter ice navigation, navigation in congested sea fairways, and urban waterways.

Risk management of remote pilotage operation using the basis of a Formal Safety Assessment

Contributors

- M.Sc. **Sunil Basnet,** Aalto University, Espoo, Finland
- Prof. **Osiris Valdez Banda,** Aalto University, Espoo, Finland
- Lect. **Janne Lahtinen,** SAMK UAS, Rauma, Finland
- M.Sc. **Meriam Chaal,** Aalto University, Espoo, Finland
- D.Sc. **Ahmad BahooToroody,** Aalto University, Espoo, Finland
- M.Sc. **Ewelina Ziajka,** Gdynia University, Gdynia, Poland
- Prof. **Jakub Montewka,** Gdynia University, Gdynia, Poland

Background

Technological advancement in remote pilotage is expected to transform the whole pilotage procedure in the near future. With the increased functions and system coupling in remote pilotage, the involved systems can be vulnerable to new emerging risks. Furthermore, the existing safety controls for conventional pilotage can be insufficient or ineffective for controlling risks in remote pilotage. As the cost of managing risks is lower at the initial system development phase, the risks in remote pilotage should be identified and controlled as early as possible.

The International Maritime Organization (IMO) provides a Formal Safety Assessment (FSA) framework for the rule-making process to evaluate new or existing safety regulations. The FSA is described by IMO (2018) as "a rational and systematic process for assessing the risks associated with shipping activity and for evaluating the costs and benefits of IMO's options for reducing these risks." Figure 1 shows the steps in the FSA, which include system description, hazard identification, risk analysis, risk control measures, cost-benefit assessment, and decision-making. Although the IMO provides guidelines and different options for each step, it is still heavily dominated by traditional safety engineering techniques, which were developed for simpler systems with low automation and software implementation. Hence, these methods may not be suitable for identifying the risks due to the increased complexity of systems in ship pilotage (Basnet et al., 2022; Lahtinen et al., 2020).

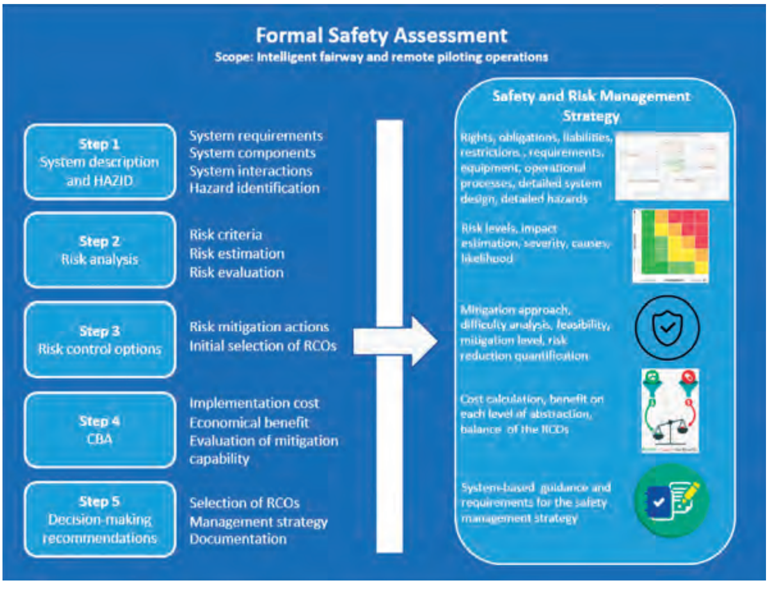


Figure 1. **Steps of Formal Safety Assessment adapted in S4V.**

Solution and results

In S4V, each step of the FSA has been executed by integrating advanced system and safety engineering methods. In this report, the process followed for risk management is briefly explained, and a summary of the results is provided. The detailed methodology and the complete results of each task in risk management will be disseminated in a full report by Aalto University in early 2023. Moreover, some of the results have been already published or are in the process of being published in different scientific journals. Throughout the risk management process, several workshops were conducted to extract knowledge from the end-users of pilotage, such as pilotage management, pilots, and technology providers in the S4V project, and this was used as expert opinion.

The first step in the FSA is to define the system requirements, create a system description, and identify potential hazards associated with it. To identify a suitable method for this step, a decision-making framework was developed and applied to ship pilotage (Basnet et al., 2022). Based on the decision-making framework, the System Modeling Language (SysML) was selected and implemented to create the system description of the remote pilotage. SysML is defined by the Object Management Group as "a general-purpose graphical modeling language for specifying, analyzing, designing, and verifying complex systems that may include hardware, software, information, personnel, procedures, and facilities" (Hause, 2006). Figure 2 shows the list of potential remote pilotage components, such as VTS RADAR, communication devices, 4G/5G connections, cameras, and data sharing devices, which can be installed on the Shore control center, ship, and fairway. Figure 3 shows the description of the process of remote pilotage involving end users such as remote pilots, crew, and VTS. Similarly, the description of the other tasks, such as pilotage planning, request of services, pilotage preparation, and post-pilotage activities, was also developed using SysML. These descriptions were necessary to develop an understanding of remote pilotage before proceeding toward risk management.

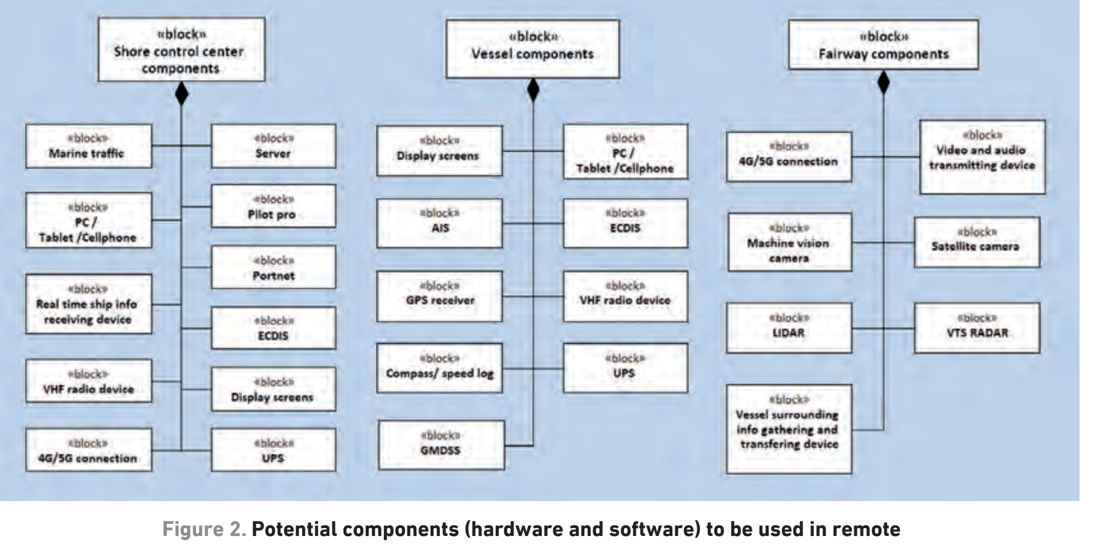


Figure 2. **Potential components (hardware and software) to be used in remote pilotage.**

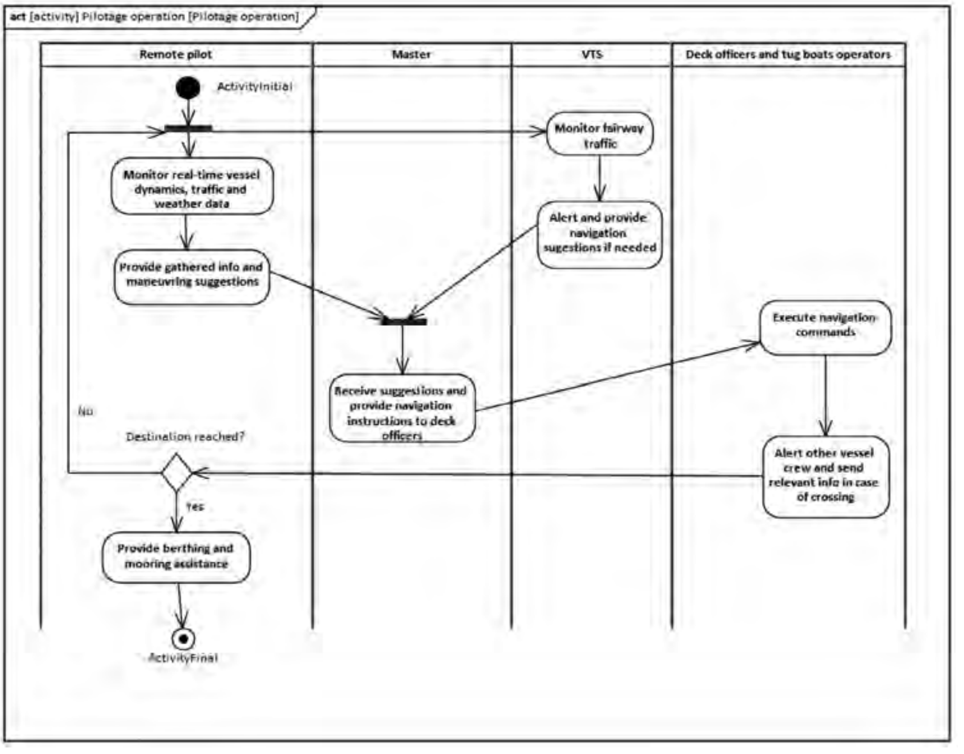


Figure 3. **Activity diagram of pilotage operation presenting the interactions among end users.**

After the system description for hazard identification, the Systems Theoretic Process Analysis (STPA) was selected and applied to the remote pilotage. In addition to direct failure events and component failures, STPA includes unsafe situations due to complex interactions in the system (Leveson & Thomas, 2018). Furthermore, STPA can be used at an early design stage and supports system development by identifying the gaps in interactions between system elements. Hence, the method was considered suitable for identifying hazards in remote pilotage. In STPA, the interactions among remote pilotage components, including end users, are assessed to identify potentially unsafe situations leading to hazards and then ultimately to losses. Figure 4 presents the STPA hierarchical control structure of the remote pilotage operation, in which the interactions are depicted with arrows. As shown in the picture, the remote pilot and VTS are placed at the highest hierarchical level, where they send navigation suggestions or updates to the master at a level below them. Then, based on the received suggestions, the master commands the vessel crew to maneuver the ship. The infrastructure used during the remote pilotage operation is then placed at the lowest hierarchical level.

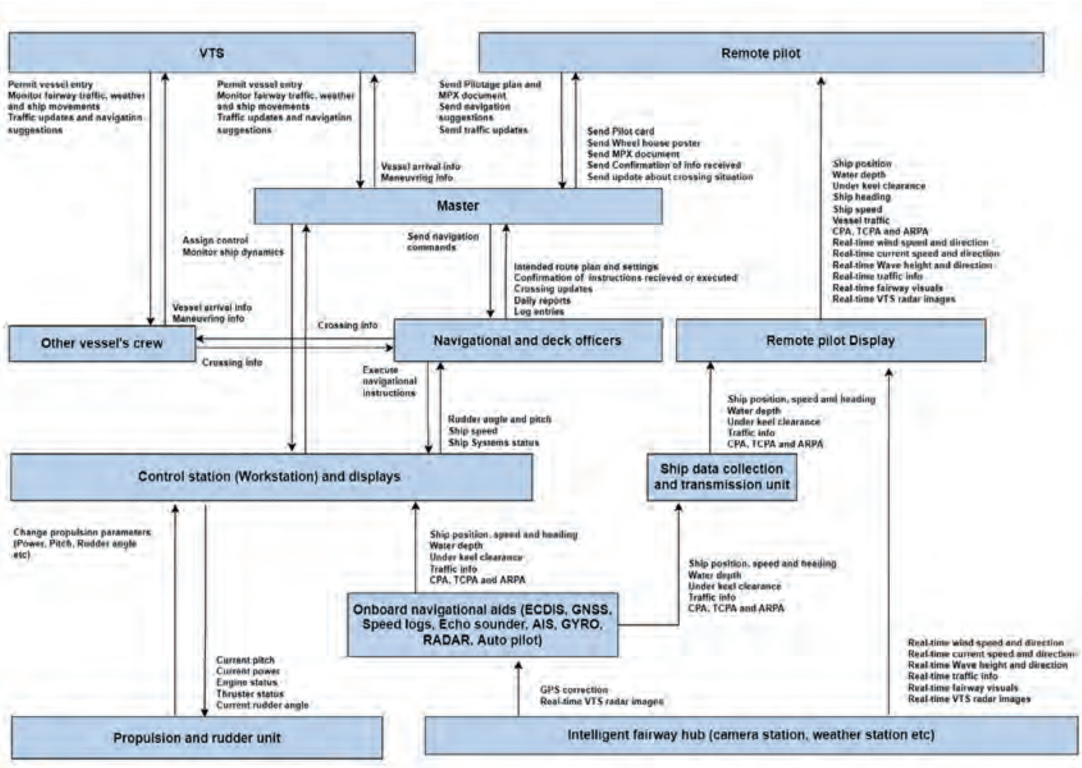


Figure 4. **STPA hierarchical control structure of remote pilotage operation.**

After executing the STPA analysis, more than 800 unsafe scenarios were identified and categorized into 45 different causal factors. Table 1 presents the causal factors that could lead to unsafe situations during remote pilotage operations. Next, in step 2 of FSA, the risk levels, meaning the severity and frequency associated with each causal factor, were estimated. For this purpose, the scales provided by IMO (2018) were adjusted for pilotage and used (see Table 2). In Table 1, the estimated severity and frequency levels associated with each causal factor are also shown. Based on these levels, it can be inferred that the issues that can occur frequently and that can lead to severe consequences are issues such as lack of skills, language issues, real-time ship dynamics information, ship crossing information, autopilot issues, GYRO failure, and RADAR failure. Figure 5 presents the risk matrix, which summarizes the number of categories in each risk level.

Table 1. **The categories of risk causal factors in remote pilotage operation and the associated frequency and severity levels.**

Causal factor Type	Causal factor	Frequency	Severity
1. Human error	1.1 Lack of skills	4	3
	1.2 Fatigue	3	3
	1.3 Stress	3	3
	1.4 Distractions	3	3
	1.5 High level of task complexity	3	3
	1.6 Lack of checklists and guidelines	2	2
	1.7 Lack of standard phrases	2	2
	1.8 Lack of seamanship	3	3
	1.9 Language issues	4	3
	1.10 Wrong assumptions	3	3
	1.11 Poor situational awareness	3	3
	1.12 Lack of trust	3	3
2. Remote pilotage data issues (incomplete, incorrect, unclear, or lack of data)	2.1 Issues with ship information (dimensions, draft, loading, etc.)	2	2
	2.2 Issues with real-time ship dynamics information (speed, heading, course over ground, etc.)	4	3
	2.3 Issues with real-time traffic information	3	3
	2.4 Issues with real-time weather information	2	2
	2.5 Issues with real-time ship systems information (i.e., engine status, rudder angle, power, etc.)	2	3
	2.6 Issues with real-time water depth information	2	3
	2.7 Issues with tug-boat availability information	2	3
	2.8 Issues with berthing, mooring, and quay information	3	3
	2.9 Issues with ship-crossing information	3	4
	2.10 Issues with communication information (channel info, channel status, etc.)	2	2
	2.11 Issues with time format / time zones	1	1
3. Hardware and software errors	3.1 VHF failure (wrong channels, malfunction, wrong settings, antenna failure, power failure, jamming, unwanted channel change, etc.)	2	2
	3.2 Cellphone/tablet failure (loss of connection, bad coverage, malfunction, updates, power failure, harsh temperature issues, connectivity issue with pilot plug via Wi-Fi to tablet, crashes, wrong data, etc.)	2	2
	3.3 Power/battery failure (power cut, high voltage, high discharge, wrong outlet, not sufficient energy for the whole duration, etc.)	1	2
	3.4 Thruster and propulsion unit failure (malfunction, auto shut down, power failure, overload, half power, alarm malfunction, loss of control during control station change, indicator problem, loss of data connection between the control station and engine/thruster, etc.)	2	3

Hardware and software errors	3.5 Rudder and helm failure (indicator problem, freezing, wrong position, jamming, loss of data connection, loss of control when changing station, helm function, not standardized position, bad ergonomics, alarm malfunction, visibility issue to the surrounding indicators and panels, etc.)	2	4
	3.6 Autopilot device failure (malfunction due to lack of adjustments, jamming, alarm malfunction, lack of precise number of steps in knob turning, etc.)	4	2
	3.7 Display failure (lack of brightness adjustments, bad location, lack of information, overload of information, total breakdown, etc.)	2	1
	3.8 ECDIS and E-charts issues (lack of updates, alarm malfunction, unusable due to lack of vessel marking and lagging, freezing, slow function, lagging position of the vessel, ETA prediction error, etc.)	3	1
	3.9 ECHO sounder issues (incorrect values, alarm malfunction, interference from the bottom in shallow water, wrong settings such as scale and range, etc.)	2	1
	3.10 Gyro failure (functionality issues, alarm. malfunction, lack of adjustments, time to recover from turns, changing errors in heading, malfunction, bad visibility, jamming, etc.)	4	4
	3.11 RADAR failure (unclear image, alarm malfunction, heading line error, incorrect input data from GPS, lack of magnetron replacement, not standardized radars, malfunction, etc.)	3	4
	3.12 AIS failure (delay in registering vessels, alarm malfunction, antenna problem, bad coverage, wrong settings, etc.)	2	1
	3.13 GPS failure (lack of connection, alarm malfunction, freezing, wrong settings, wrong installation, bad antenna position, malfunction, delay, etc.)	2	3
	3.14 Engine failure (alarm malfunction, oil leakages, lubrication issue, overheating, etc.)	2	4
	3.15 Data gathering and transmitting device failure (sensor error, transmission error, alarm malfunction)	2	1
	3.16 Fairway infrastructure issues (weather sensors failure, alarm malfunction, camera failure, fairway lights malfunction, etc.)	3	3
	3.17 Onboard lights failure (searchlight malfunction, navigation lights malfunction, inadequate lighting, alarm malfunction, etc.)	3	2
	3.18 Visibility issues (frozen windows, blocked view from the bridge, foggy camera lenses, etc.)	2	3
	3.19 Buoy issues (missing, misplacement, shifting, etc.)	2	3
	3.20 Integrated alarm system failure (alarm malfunction, power failure, etc.)	1	2
	3.21 Sound signaling device failures (Tyfon failure, alarm malfunction, power failure)	1	1
	3.22 Connectivity issues (loss of connection, power failure, harsh weather)	1	4

Table 2. **4-point Likert scale for defining the frequency and severity level of risk causal factors.**

Rating	Frequency level	Severity level
1	Extremely remote (likely to occur once every 500 remotely piloted vessels)	Minor (single/minor injury, local equipment damage, pilotage can continue without any delay)
2	Remote (likely to occur once every 100 remotely piloted vessels)	Significant (multiple minor injuries/severe injury, non-severe ship and external objects damage, pilotage can continue with delay without any external assistance)
3	Reasonably probable (likely to occur once every 50 remotely piloted vessels)	Severe (single fatality / multiple severe injuries, severe damage, pilotage can continue with delay using external assistance)
4	Frequent (likely to occur once every 10 remotely piloted vessels)	Catastrophic (multiple fatalities, total loss of ship, pilotage cannot continue)

Risk matrix		Severity → Minor	Significant	Severe	Catastrophic
Frequency ↓	Extremely remote	2	2	0	1
	Remote	4	10	7	2
	Reasonably probable	1	1	11	2
	Frequent	0	1	3	1

Figure 5. **The risk matrix of the risk causal factors in remote pilotage operation.**

Despite the difference in estimated frequency and severity levels, the risk levels in all the identified causal factors need to be reduced before the deployment of remote pilotage service. Thus, in Step 3 of the FSA, the potential risk control measures were identified for each of the causal factors. These risk control measures include measures that could potentially reduce the frequency of the causal factors, meaning preventive as well as reactive, which involves the severity in case it occurs. In this step, a total of 230 risk control measures were defined for the risk factors related to remote pilotage. Next, in Step 4 of the FSA, the cost of implementing these measures and the effectiveness in risk reduction were roughly estimated. As an example, Table 3 presents the risk control measures related to a lack of skills and its associated cost and effectiveness estimations; and Table 4 presents the 5-point Likert scale used for the rating. Figure 6 shows the number of risk control measures in each cost category and effectiveness category. For the costs, the risk control measures are distributed evenly in categories 1 to 4, with only 2 measures in category 5. However, for effectiveness, most of the risk control measures are in categories 4 and 5, meaning high and very high effectiveness.

Table 3. **Risk control measures related to a lack of skills of the pilot/crew.**

Risk control measures to reduce risks due to lack of skills	Cost	Effectiv-eness
1. Selection of ship and fairway	1	5
2. Certification of remote pilots and its validity	1	4
3. Duplex communication for providing better support to the crew	2	5
4. Remote pilotage tailored training for remote pilots and the ship crew covering all major/minor tasks during remote pilotage	3	4
5. Emergency procedures for remote pilotage (changing to conventional pilotage in case of major issues)	3	5
6. Increased situational awareness (installation of more camera stations in the fairway, assess other technologies)	4	5

Table 4. **The Likert scale used for the estimation of the cost and effectiveness of the risk control measures.**

Rating	Cost	Effectiveness
1	No direct cost (EUR 0)	Very low effectiveness (1%–20% reduction)
2	Low cost (EUR 1–9,999)	Low effectiveness (20%–40% reduction)
3	Average cost (EUR 10,000–99,999)	Medium effectiveness (40%–60% reduction)
4	High cost (EUR 100,000–1 mil)	High effectiveness (60%–80% reduction)
5	Very high cost (above EUR 1 mil)	Very high effectiveness (80%–100% reduction)

In the final step of risk management, an influence diagram was developed to select the most cost-effective risk control measures for remote pilotage. The influence diagram can identify the most cost-effective combination of risk control measures, meaning the risk control option with the highest total expected benefit. For this purpose, the model compares the total cost of implementing all possible combinations of risk control measures against the expected benefit due to the reduction in losses. However, due to time constraints and availability of data, the current model only focuses on causal factors associated with remote pilots and excludes other end users such as crew and management. The influence diagram will be presented in a scientific journal to be published in the first semester of 2023.

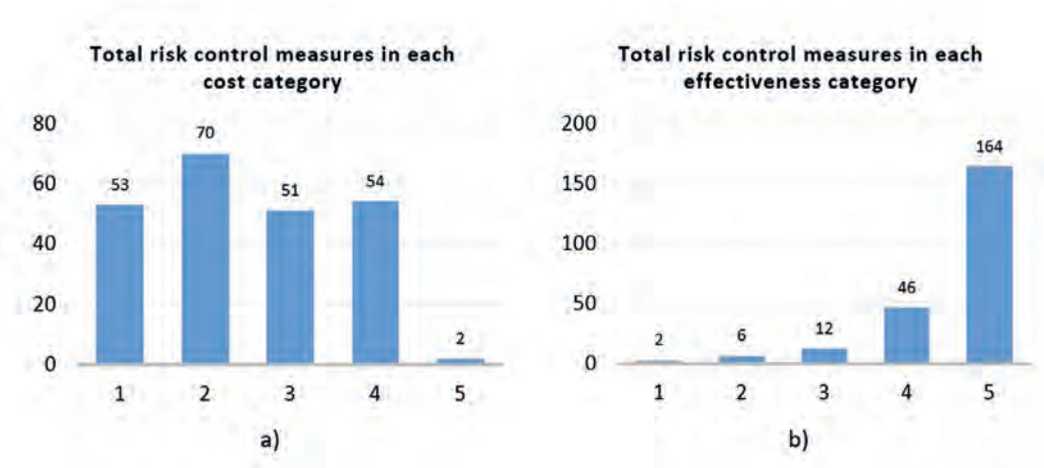


Figure 6. **Distribution of the total number of risk control measures in each cost category (a) and each effectiveness category (b).**

Findings, output, and impact

Risk management is an iterative process that begins in the early design stages and should be iterated throughout the system life cycle, that is, during development, testing, implementation, and maintenance. The results achieved during risk management in the early stages of remote pilotage development in the S4V project contain two major benefits. First, the project has developed a strong foundation, which can be further explored, developed, and strengthened during the next iterations of risk management. All the diagrams, models, and tools used so far in each step of risk management are interlinked, traceable, and support the updates/changes in the next iterations. Furthermore, these are machine-executable models, which means that the results can be easily exported to other tools/software, supporting integration with other system analyses or enabling new ones. Second, the risk management results can be used to generate requirements for remote pilotage operations. While a few high-level requirements have been already specified in the Finnish Pilotage Act, the risk management in S4V already assesses the root-level causal factors and risk control measures for remote pilotage operation, which can support the authorities in defining some early safety requirements for design stages. As mentioned previously, the cost of changes is comparatively low in the earlier stages, which could generate high economic benefit for the system owners.

In the next iteration of risk management, the reliability of the estimations should be improved by replacing the expert opinions with simulation/testing data or operational data once the components are selected and verified for remote pilotage. In addition, risk management should be expanded by including other remote pilotage actors, namely the authorities, VTS, pilotage management, and so on. Furthermore, the verification and validation procedures for each step of risk management should be developed and employed. Moreover, as system reliability changes over time, the current risk models should be developed further and aligned with the incident reporting system from the pilotage provider to enable real-time updating of unsafe observations, as in dynamic risk models. Finally, a safety management system for remote pilotage should be developed for managing and ensuring safety through systematic procedures, practices, and policies.

References

Basnet, S., Bahootoroody, A., Chaal, M., Banda, O. A. V., Lahtinen, J., & Kujala, P., 2022. A decision-making framework for selecting an MBSE language – A case study to ship pilotage. Expert Systems with Applications, 193, 116451.

Hause, M. ,2006. The SysML modelling language. Fifteenth European Systems Engineering Conference.

IMO, 2018. Revised Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process. https://www.imo.org/en/OurWork/Safety/Pages/FormalSafetyAssessment.aspx -> Related links

Lahtinen, J., Banda, O. A. V., Kujala, P., & Hirdaris, S., 2020. Remote piloting in an intelligent fairway – A paradigm for future pilotage. Safety Science, 130, 104889.

Leveson, N. G., & Thomas, J. P., 2018. STPA handbook. Cambridge, MA, USA.

Novia University of Applied Sciences

Novia is a dynamic and international University of Applied Sciences with high-quality education, as well as research, development, and innovation activities that support working life. Novia's automation and maritime simulation research team combines the operational expertise of the maritime field, a deep understanding of safety, and the impact of human factors, with skills that focus on technology, digitalization, and smart solutions. We are experts in maritime operations and safety, and we are constantly developing new, sustainable solutions to improve these areas within the industry.

Critical ship data in remote pilotage

Contributors

- **Jedi Seppänen,** Project Specialist, M.Sc. (Tech.), Master Mariner (B.Sc.)
- **Mirva Salokorpi,** Research Manager, M.Sc. of Maritime Management

Background

Pilots act as navigation and local fairway advisors for vessels' masters. Pilots ensure a ship's safe passage to port, and thus pilotage is a vital element in terms of maritime safety. In Finland, shipping is a critical mode of transport for the economy and security of supply, and the importance of piloting is particularly emphasized in narrow and shallow waters around the coast of Finland. However, while protecting shipping, pilots themselves are put in danger. Boarding and de-boarding the vessels underway poses a substantial risk to pilots' safety, as it means transferring from one moving vessel to another via a ladder even in harsh weather conditions, when their expertise is needed most.

Currently, the pilot is transported to the ship to support the bridge crew in navigation, but the remote pilotage service could also be implemented from shore. This would significantly improve the safety of the pilot and pilot boat drivers. In addition, the reduction in the need for boat transport could be reflected in the partial cost and fuel savings. Furthermore, remote pilotage can help to improve the efficiency of sea transportation, as pilots no longer need to be transported from one ship to another, or from or to the shore. Thus, the waiting times for ships can be reduced.

In Finland, remote pilotage was identified as a potential operating model at the end of the 2010s, and in 2019, an amendment was made to the Pilotage Act (Pilotage Act (940/2003), 2019), which enables piloting to be carried out remotely. However, it is a subject of permit activity, and in the permit application, the operator must demonstrate that the service does not compromise the safety of maritime traffic, harm the environment, or pose a danger to another vessel. In practice, this means that the remote pilotage system needs to be studied, developed, and finally tested and validated systematically and thoroughly. In the Sea4Value / Fairway project, the remote piloting concept was created and studied from many different perspectives.

The project tested remote pilotage practices and technology in numerous ways, and in May 2022, the first remote pilotage experiment in real life was carried out. While the demo set-up presented a valid set of ship-borne streaming data for the remote pilot, the selection of the data was based only on expert assessment. The experts, consisting of maritime, pilotage, safety, and human factors experts, as well as marine and information technology professionals, justified the selection of signals based on their experience. Therefore, there is a need to create a way to justify the necessity of each particular piece of information and to show how it relates to pilotage.

The demonstration pilotage event

In the demonstration, M/S Viikki of ESL Shipping left the port of Kokkola according to its schedule. The remote pilotage took place from the developed remote pilotage center located in Aboa Mare, Turku. For safety reasons, there was a conventional pilot onboard, who took care of the vessel's pilotage, but there was also another pilot on the vessel who communicated with the remote pilot.

M/S Viikki hosts an integrated Furuno navigation system. The onboard interface to the navigation system and connections to the internet streamed the information to the remote pilotage center. The original plan was to install fairway and harbor cameras at the Western harbor, where the pilotage was planned originally. The pilotage was necessary for the ship to relocate to Kokkola, and due to short notice, there was no time to install any external fairway cameras. Instead, a forward-pointing camera was installed on the Viikki bridge.

Ship interface and data connection

The Furuno integrated navigation system runs on an IEC 450 local area network. IEC documentation covers the details of the NMEA (National Marine Electronics Association) and networking[1]. NMEA is a message encoding protocol that contains talker and message identification, data distributed in one or over several messages, and error checking. Devices send messages to everybody in the network, and everybody can also

---

[1] IEC 61162 Maritime navigation and radiocommunication equipment and systems – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection.
IEC 61162 Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 1: Single talker and multiple listeners

send messages. A Smartbox, which is specific to this project, connects to the bridge LAN hub; see Figure 1. The read-only connection for security is implemented using a data diode, marked with 'D.'

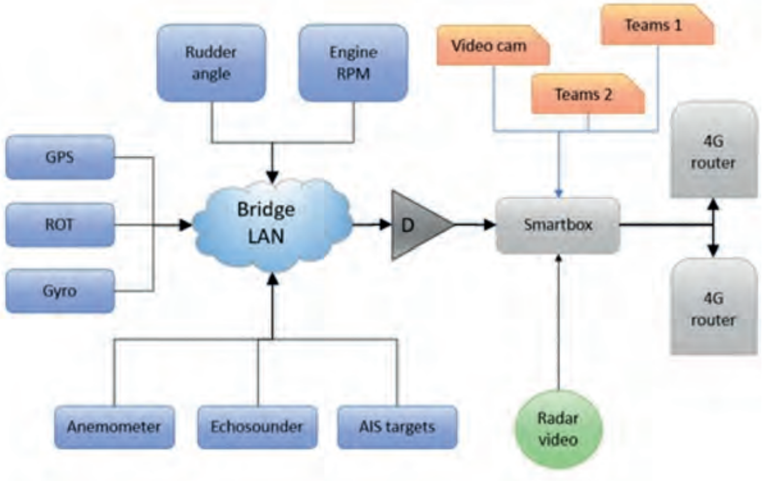


Figure 1. **Smartbox connection on the vessel (adapted from Brighthouse's system description, with permission)**

The devices connect to the bridge LAN output data encapsulated in plain text NMEA sentences. The Smartbox data processing unit translates the messages to JSON files, which are encrypted and sent to the cloud over a 4G network. There are two 4G routers using different operators for redundancy. Bandwidth was shared by the data from navigation equipment, two Microsoft Teams™ audio connections, the radar video, and a bridge video camera stream.

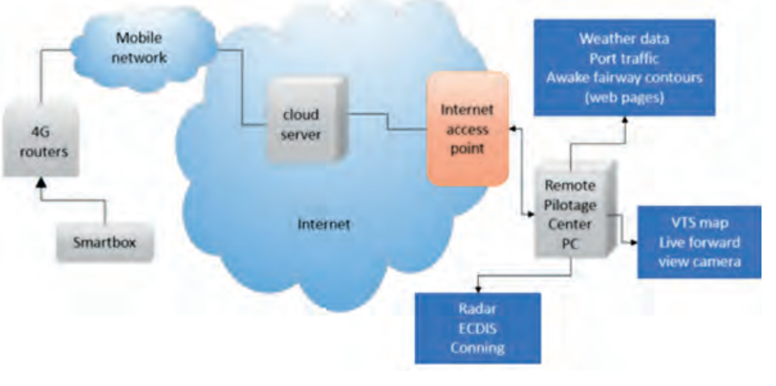


Figure 2. **Connections from the ship to the remote pilotage center over the internet (adapted from Brighthouse's system description, with permission).**

Figure 2 shows the data connections from the vessel to the remote pilotage center. The cloud server stores the data in JSON format[2], from where it can be served to terminal devices. The remote pilotage center connects to the internet via the access point.

Remote pilotage center

The remote pilotage center (PC) has a set of connected displays, accommodating data from the ship and web contents from the internet; see Figure 3. In the top middle, the map view is distributed across three large displays. A list of target vessels is displayed on the right of the map view. The source of the list originated from the Viikki at the Port of Kokkola and the tug Ahti at Sköldvik[3]. The map display shows all AIS (Automatic Identification System) targets on the map.

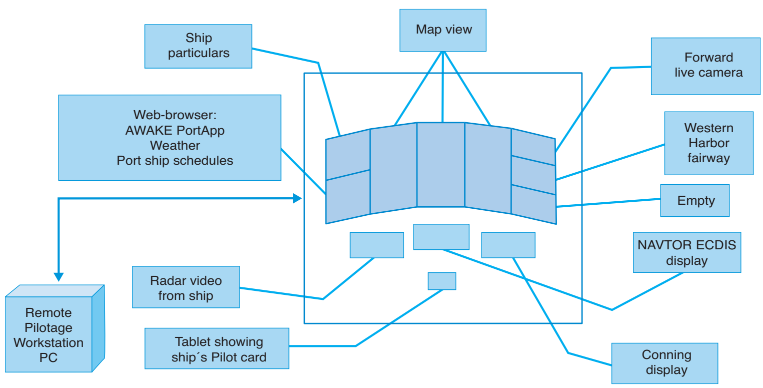


Figure 3. Remote pilotage center displays (adapted from Brighthouse, with permission).

On the left, there are two displays: the upper shows the ship details and the lower shows a web browser with tabs open for the Awake[4] port app, weather, and Port of Kokkola ship schedules. The Awake port app generates dynamic safety contours based on the ship and environmental data.

The three displays on the right, from top to bottom, are reserved for fairway cameras. During the demo, there was a live forward view from Viikki's bridge.

In the middle, below the large displays, there are three office-size displays for radar video from the cloud, shown using the VLC video player, Navtor ECDIS (Electronic Chart Display and Information System) fed by

[2] JSON is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute-value pairs and arrays." Source: Wikipedia.

[3] Tug Ahti was the first test installation of the Smartbox collecting unit.

[4] www.awake.ai

the ship's data. Note that the Navtor ECDIS used as a chart application did not implement the full functionality of ECDIS as defined by SOLAS. However, the charts were up to date, and they used the vessel data, such as position, speed, and heading. At the bottom, there is a tablet that shows the pilot data of the vessel; see Figure 3. The Navtor ECDIS showed other vessels' AIS information received via the vessel's AIS receiver.

The conning display (see Figure 4) showed:

- the rate of turn,
- the rudder angle,
- engine rpm (revolutions),
- transversal bow and aft movement (as speed in knots),
- heading,
- the course over ground,
- the speed over ground,
- position,
- depth, and
- relative and true wind direction and force.

Data for conning was received from the vessel.

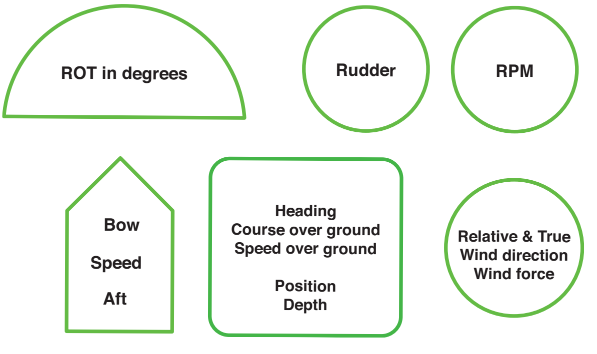


Figure 4. **Conning display (adapted from Brighthouse's system description, with permission).**

The remote pilotage demonstration was recorded at the remote pilotage center using a GoPro camera attached to the roof, a DJI action camera on a table with a stand right of the remote pilot, and a Canon video camera left of the pilot. All these cameras recorded the audio. There was a GoPro camera on the ship's bridge recording a view showing the pilot and the master. In addition, an eye tracker (eye movement tracker) camera was used by the remote pilot sitting at the workstation desk.

Participant tasks

Three pilots participated in the remote pilotage. Two pilots, namely the remote pilot and the observing pilot, were at the remote pilotage center. The former was sitting at the desk in front of the displays wearing eye tracker goggles to record the center of attention during the demo. The observing pilot monitored the remote pilot and pilotage.

The master of the vessel and the conventional pilot were responsible for pilotage and navigation on board. The conventional pilot was sitting at the port side radar, from where the radar video was captured and streamed to the remote center. The third pilot was on board and kept active communication with the remote pilot.

Communication connections

The remote pilot and onboard monitoring pilot communicated through a Microsoft Teams™ audio connection. The onboard monitoring pilot had a headset connected to his tablet, and the remote pilot could hear him through a laptop speaker at the remote center. For the center console of the bridge, a conference microphone was connected to a tablet with a Teams audio connection open to the remote pilotage center. The microphone picked audio from the master, conventional pilot, and VHF[5] radio traffic as planned. Sometimes, too, the observing pilot's sound was audible through the center console microphone. The remote pilot could hear the center console audio through another laptop microphone at the center.

The remote center hosted additional audio from the VTS (Vessel Traffic Service) center over a third Microsoft Teams™ connection. The Bothnia VTS on VHF channel 67 was heard in the call.

Figure 5 shows the essential communication flows listed here:

- The data stream, radar video stream, and forward camera view from the vessel to the remote pilotage center display.
- A remote pilot audio connection from the ship's center console to the remote center.
- The onboard pilot and the master were responsible for communicating with the Bothnia VTS and listening to emergency VHF channel 16.
- The remote pilot listened to the Bothnia VTS.
- The onboard monitoring pilot and the remote pilot had an audio channel open during the pilotage.
- The observing pilot used his PilotPro tablet for monitoring the vessel with Virtual Boarding.

[5] Very High Frequency (radio bandwidth), a short-range radio telephony.

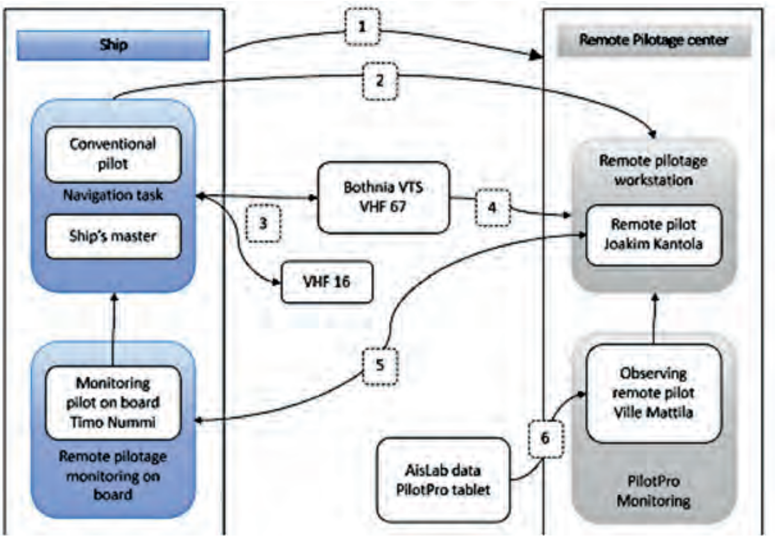


Figure 5. Communication and data flow.

The master and the conventional pilot loosely followed the BRM (Bridge Resource Management) conversation in English. Discussion between the remote and onboard monitoring pilots was also in English and it was more continuous, conversational, and verbose. The remote pilot gave feedback about the remote systems. The discussion was about the system performance, and when he would have executed commands related to navigation. He asked for more information about the vessel's surroundings, such as the location of buoys and the ship's position on the leading line.

The solution to finding the necessary signals

The starting point for searching for the necessary information for remote pilots to perform safe pilotage was found by analyzing the factors that make up the conventional pilot's situational awareness (SA). The legislation guides the role of the pilot and sets the goal for pilotage. The SA model used for analysis is created for goal-based tasks, to support decision-making in a dynamic and complex environment. Five critical elements form the input space for decision-making in the pilotage: the ship's position, the ship's dynamic state, ship controls, external elements, and communication. Each element is essential for gaining and sustaining good situational awareness. On the other hand, the elements are made up of components. The components are the actual sources of information, and they appear in the flavors of data and information, detected from various sources by sensors, devices, or human senses. It is through the choice of crucial components for each critical element that we can satisfy all five critical factors of situational awareness.

The Situational Awareness model

Mica Endsley's (1995) situation awareness (SA)[6] model supports decision-making in a dynamic, complex, and goal-oriented environment. It can receive input data from the environment, upon which decisions are based. A range of factors, such as common human properties, individual capabilities, goals, objectives, and system design, affect the core process; see Figure 6. Information processing, automaticity, and memory are examples of common human properties. The human properties gain from individual capabilities, such as experience and training (Endsley, 1995).

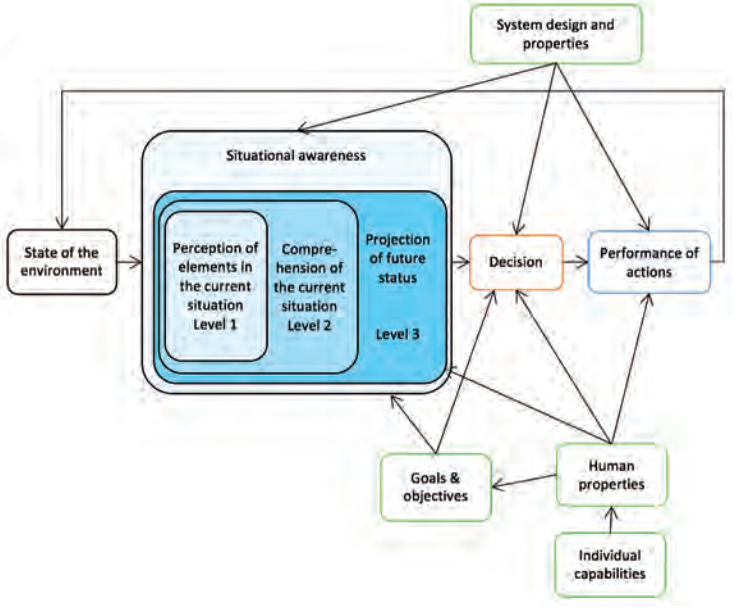


Figure 6. Situation awareness model and the three levels of the SA process (Endsley, 1995, p. 35).

Three levels cover the SA process, as shown in the shaded area in Figure 6. Level one is the perception of the status, attributes, and dynamics of relevant elements in the environment. In level two, the critical factors form the comprehension of the situation based on compounding the individual factors. The factors form patterns that are meaningful (for the pilot) and create an overall picture of the (navigational) environment. A projection of the future status of the elements in the environment happens at level three.

[6] Endsley calls SA "situation awareness." This text uses the term situational awareness.

Endsley (1995) points out that in addition to perceiving the SA process in three levels, there are spatial, functional, and modal subcategories that apply throughout the process, setting the noticed elements in context. For example, noticing the target vessel's position and movement (spatial) affects how collision regulations apply. The pilot can conclude from the target ship's location, course, and speed (spatial) whether the target ship will cause measures in the future. Compensating for the late start of a turn by reducing the autopilot radius in the latter part of the turn is less effective than if it had been done earlier (functional, needs to know how the ship maneuvers). An example of a situational awareness mistake, in which the actor misinterprets the mode, is the radar's automatic rain clutter, which may over-suppress the echoes, making small targets fade away.

How well will the SA model apply to remote pilotage? Let us see the definition of pilotage from the Pilotage Act:

> *"Pilotage means operations related to the navigation of ships in which the pilot acts as an advisor to the master of the ship and as an expert on the local waters and their navigation." (Pilotage Act, section 2, part 1)*

Indeed, decision-making happens in a dynamic and complex environment, where the pilot needs to observe and manage several things at the same time. What can we say about pilotage being goal oriented? Let us look at the Pilotage Decree[7], which defines that:

> *"The pilot must ensure that the vessel stays in the fairway, and inform the master if the pilot considers necessary measures for the safety of the ship." (Pilotage Decree, section 20)*

Pilotage has the important goal of guiding the vessel safely through the passage. Let us agree that the SA model is usable for remote pilotage and figure out which are the inputs "State of the environment" to the model, in Figure 6.

The input elements are specific to each system and context. Endsley (1993) has developed a method for determining the elements: (a) conduct unstructured interviews, (b) complete a goal-directed task analysis, and (c) administer structured questionnaires with expert subjects. This method is suitable for research without prior knowledge of the domain. The remote pilotage project team at Novia has a fair amount of experience in maritime issues and consists of pilotage and human factor professionals, so that the team can evaluate and set up the input elements. The following tasks can be found in the Pilotage Decree[8] . The pilot must:

---

[7] An official translation in English is not available (Pilotage Decree 393/1957, 1957). Translated by author.

[8] Translated by author.

1) ensure that the vessel stays in the fairway;
2) keep unwavering and meticulous attention on the ship's passage and inform the master about the measures they consider necessary for the safety of the ship;
3) inform the master at a suitable time when the ship is approaching a turning point, shallow, or narrow, tight turns or otherwise dangerous places; and
4) point out to the master when, due to darkness, fog, or other reasons, the pilot is not completely sure of the fairway. (Pilotage Decree, section 20)

The above tasks still describe high-level goals instead of the elements of situational awareness. A more descriptive set of critical elements is presented, for instance, in a Finnish accident investigation report (Onnettomuustutkintakeskus, 2001) that studied an accident during a pilotage exemption certificate test voyage. The elements were analyzed by the author, and the Novia team agreed that the list holds the full set of critical elements in pilotage:

- understanding the ship's momentary position;
- perception of the ship's dynamic state;
- understanding the state of the navigation system;
- external elements; and
- communication.

The following figure presents the critical elements in the context of SA. The pilot will observe the domain and make notes of the critical factors. After processing and forecasting the contents, the pilot decides whether to act or not upon the situation. According to the investigation report experts, in general, situational awareness is formed by understanding the position of the ship and the prediction of the future position, accounting for expected risk factors such as traffic and the limits of the fairway (Onnettomuustutkintakeskus, 2001).

When the above report discusses understanding the state of the navigation system, we changed it to 'Ship controls'; see the figure below. The onboard automation system is a complex set of interoperative systems, the functions of which the onboard navigator must understand. The conventional onboard pilot should not need to understand how a particular integrated navigation system works, but they must see the essential ship controls, such as engine telegraph and helm.

Communication is one of the critical factors because, in teamwork, the team's common vision and situational awareness are shared by communicating. The pilot is a guest in the bridge team and must effectively exchange information. Communication also forms the team's common vision, as mentioned in the Onnettomuustutkintakeskus report (2001).

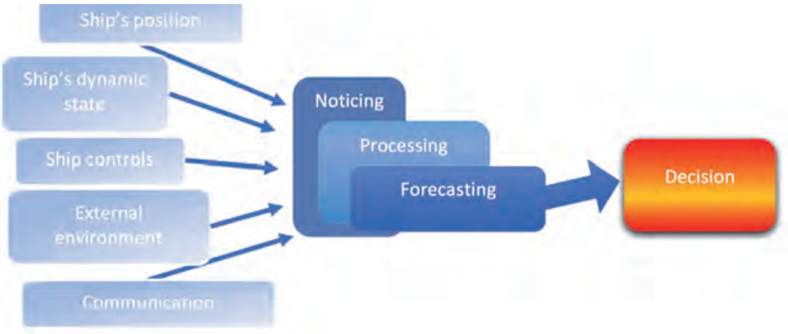


Figure 7. **Five critical factors of pilotage in the context of situational awareness.**

While the list above seems an adequate set of critical factors, let us look at another accident investigation report that mentions situational awareness, to understand that not all factors are inputs to the SA process. That case discusses "underlying factors" that either improve or suppress situational awareness (Onnettomuustutkintakeskus, 2011). These are:

1) the time of day,
2) the weather,
3) the fairway area,
5) the ship's navigation equipment,
6) bridge crew qualifications,
7) navigation methods, and
8) working culture.

Elements 1) – 3) belong clearly to 'external elements'. Number 4) concerns 'the state of the navigation system'. Elements 5) – 7) are system elements. Referring to Figure 6, they appear outside the SA process. A qualification is an individual capability that depends on training. Navigation methods and working culture are a part of system design.

Before concluding this chapter, we will raise a few issues that have appeared, and we will show that they are not relevant inputs for remote pilotage, but belong to the support elements, like system elements 5) – 7) above. These examples help to understand the application of the model.

One could argue that the conditions change drastically when the pilot is removed from the bridge to the shore center. There are several other things to be considered, such as interfaces, connectivity, and working environment. They certainly matter, but despite the pilot moving away, the input to the SA process stays the same. Technology is an enabler, and its effect either weakens or strengthens the decision-making process. It supports remote pilotage as innovations, such as new sensory information. The interfaces and working environment and ergonomics are a part of the system design, and they support decision-making, but they are not inputs to the SA process.

Another argument is that the pilot does not have control over the vessel anymore. According to a thesis in which Finnish maritime professionals were interviewed about the impact of the roles and responsibilities in piloting, it is usual to have the pilot steer the vessel during the passage (Wederhorn), even if the Pilotage Act assigns the responsibility of navigation to the master:

> *"The master is responsible for the navigation of the ship also when he is following the pilot's navigation instructions."*
> *(Pilotage Act, Section 7, part 1)*

In the thesis, it was concluded that the confusion of roles weakens the performance of both the master and the pilot at the expense of safety. With remote pilotage, the separation of roles becomes more concrete, and it could be assumed that the situation would become clearer for everybody. However, splitting up the team into two locations poses various kinds of communication challenges that must be addressed. Sustaining team situational awareness becomes essential. Endsley's SA can be applied to a group of individuals who work together and make decisions, where each has their area of responsibility so that they share situational awareness (Endsley, 1995). Team awareness is formed by communication, as shown in the next chapter, and thus it is an essential critical factor in the list. Communication should be understood in a broad sense. Technological development creates new ways of communicating and communication can be, for example, the master seeing a real-time note or drawing made by the remote pilot on a ship's display.

Critical communication factor and team SA

Communication is **a key factor** of the pilotage service and a key tool in forming a team's situational awareness. The pilot acts as a local expert on the fairway and area, helping the master by giving advice (Pilotage Act, section 2.1), and the master maneuvers the vessel using their skills. They must be able to trust each other and share situational awareness. In the future, an advanced exchange of SA-enhancing data between the remote pilotage center and ship equipment could be possible, but for now, they must talk to each other.

Communication errors appear rather frequently in maritime operations. Contemporary maritime culture in Finland has also been seen to rely on individual performance (Onnettomuustutkintakeskus, 2004b and 2011). A paradoxical culture prevails in which the other party is excessively trusted so that they are not monitored, and giving advice has been seen as a lack of trust in the individual (Wederhorn and Onnettomuustutkintakeskus, 2009). Communication routines for various activities and observations are a key safety measure (Onnettomuustutkintakeskus, 2001).

Communication without a common language and vocabulary could cause unsafe situations, which could be mitigated by setting up standard phrases and language certification. A procedure to cover prolonged silences can be put into action; for example, during a long leg when there are no events in a communication routine, there could be an agreed message marker that the remote pilot would say to kill the "awkward silence."

Communication creates **trust**. While remote piloting a vessel, the pilot cannot just take over the controls to navigate through a tight spot, but they need to trust the master. Neither can they monitor the actions fully if they do not know what the master thinks and is about to do. Trust works in the opposite direction, as well. The master needs to be assured that the pilot is interested and able to help. A Swedish study of pilotage as a control problem found that **standard communication routines** could create trust and cooperation between the vessel and the pilot (Bruno & Lützhöft). Standard communication is a particularly critical area of remote pilotage, and it should be defined in the pilotage procedures.

The legislation defines communication as compulsory in the Pilotage Act. The master and pilot must exchange the route plan before pilotage (Pilotage Act, section 8) and must keep a continuous exchange of information about all information relevant to pilotage during the voyage (section 9). During pilotage, they need to discuss the forthcoming situations, traffic development, and the ship's position, but also information about the vessel's controls and movement. In effect, they need to speak about the critical factors.

The situation model can be extended to teams (Endsley, 1995). When a group of people works together toward the same goal, making decisions and carrying out actions, they create a comprehensive team SA. They each have specific, responsibility-based elements with which they are concerned. Coordination entails sharing of knowledge either verbally or by common displays. Each member contributes to the team, and the team SA builds at the overlapping responsibility areas; see Figure 8.

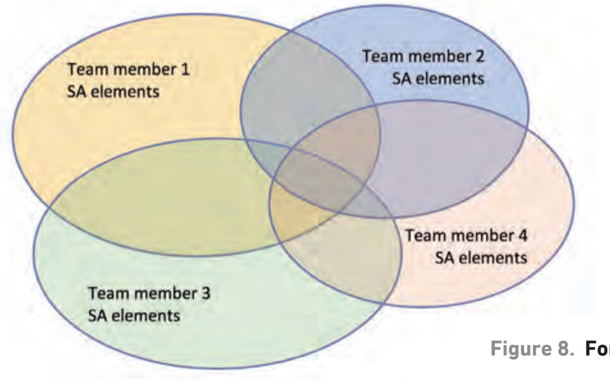


Figure 8. **Forming of team SA.**

In the future, the overlapping part may consist of devices updating the same information on both vessel and remote pilotage screens. In a socio-technological environment, a system can be a team member from the team SA point of view, because it holds and distributes data. Information exchange only over a system does not replace human communication, because the system cannot make sure that the information is disseminated throughout the team (Sharma & Nazir). Thus, human communication remains as a support to the SA despite technology.

Results, findings, output, and impact

Safety-critical information is embedded in the **five critical factors**, which are the inputs for the situational awareness (SA) process; see Figure 7. Safety of navigation is the result of gaining and sustaining good SA. The onboard pilot can use a full spectrum of information within the critical factors. Careful choice of suitable data components from within the critical factors, without degrading the SA, activates the service level and engages the remote pilot in the task. The higher the service level (the level of participation), the more information they will need to create the service and sustain SA. Legislation plays a role in defining the pilotage service level and the remote pilot's role. The future of legislation is still open, so a choice of a closed set of data components cannot be made.

Critical elements component map

The five critical elements that form SA build up from observations and information, called here components. The relationships between the components and critical factors form a chart of components that shows all data and information that the onboard pilot could have at hand to form situational awareness; see Figure 9 and Figure 10. Each factor builds on components that are data sources for the element. The chart can be used to communicate a specific function or data that the remote pilot needs. For example, the ship's dynamic state is determined by rate of turn (ROT), speed over ground (SOG), and true heading. It can be visualized by a predictor in the ECDIS or it can be verified visually. The chart elements are not semantically identical on purpose. The chart is a contemporary presentation of information available on the bridge.

In the future, the data can be acquired from novel devices and data sources. For example, a satellite navigation system objectively measures the ship's position, which is shown as a geographical location on the ECDIS. The position may also be detected as a relative position to fairway objects by sighting fairway surface objects or deducing the position on radar by electronic bearing[9] line and range marker[10]. Now the objectively

[9] EBL, electronic bearing line, is a rotating line with which a bearing can be measured to an object on the radar screen.

[10] VRM, virtual range marker, is a circle centered on one's own ship. The radius of the circle is the distance to the object in the radar screen.

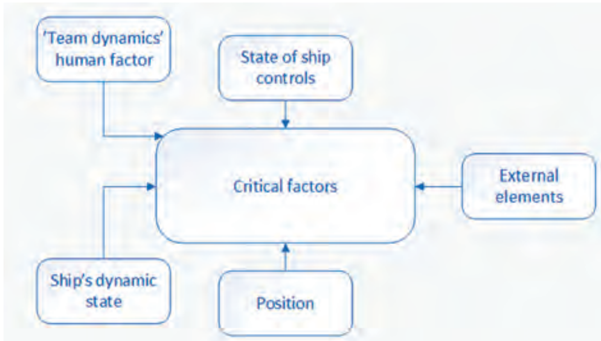


Figure 9. **SA critical elements.**

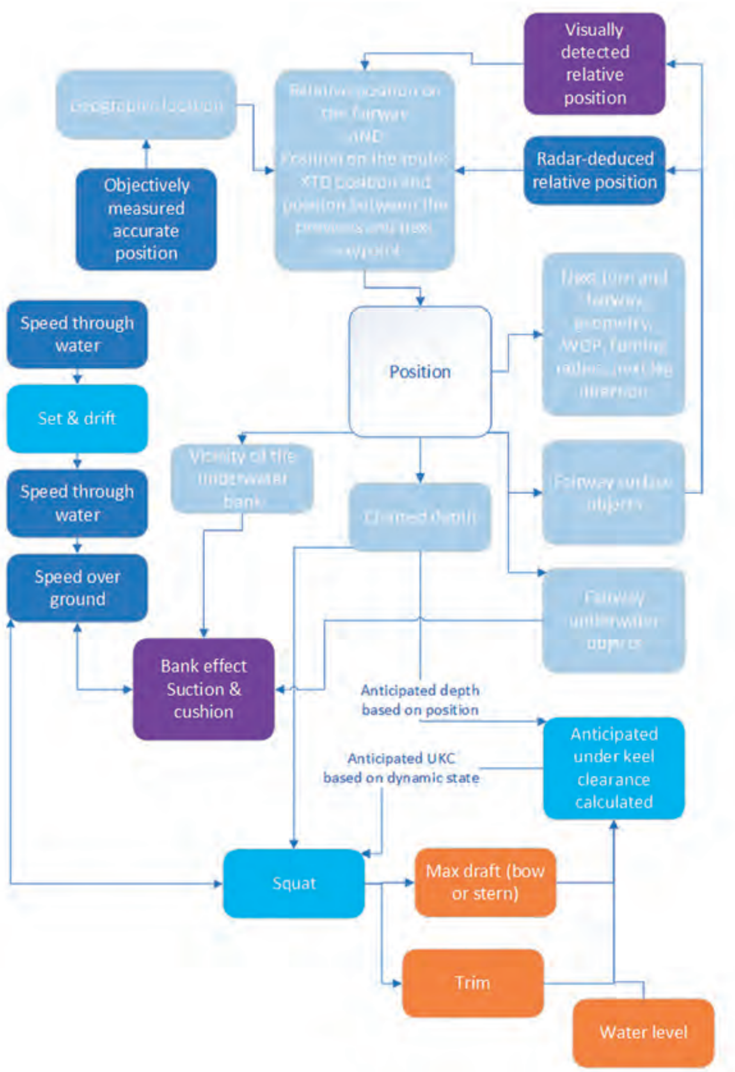


Figure 10. **Example of a critical element 'position' and its components.**

and relatively measured position may be deduced with some innovative technology that is still unseen. Continuing the example, the wheel-over-point (WOP) is a factor of the external environment (or external elements). Deciding the WOP is related to knowing the ship's position.

The chart is also useful for collecting all components in one place for reference. It can be used to pinpoint a necessary function. For example, radar can be used for many tasks, and there has been a lot of discussion about having the most essential radar functions in the remote pilotage center during the S4VF remote pilotage project. What it is necessary to understand is that the radar provides tools for the relative positioning of the vessel, noticing other traffic, and collision detection. While downloading the radar signal stream and implementing ARPA (Automatic Radar Plotting Aid)[11] tools at the remote pilotage center may be an ordeal, these functions are listed, and they can be implemented with any alternative technology.

Data sourcing

The most essential items of information for the remote pilot are the ship's position, dynamic state, and collision detection and avoidance functions. For this information, there should be two independent sources to verify the information. The conventional onboard pilot can compare the vessel's equipment data visually. For example, for the position, either visual or radar observation can verify that the satellite navigation data is correct. GPS (Global Positioning System)[12] is, by design, vulnerable to cyber interference and should not be trusted as a sole source. An alternative should be considered for each sourced device that uses GPS data as a reference, most importantly the position.

In narrow channels, the accuracy of both position and rate of turn (ROT) becomes essential. The ROT source should use two alternative sources for verification. The turning is visualized in the electronic chart with a predictor, which is created from the ship's speed over ground (SOG) and ROT. The reliability of the predictor lies in GPS, which provides SOG and ROT. If either is wrong, the predictor predicts the future path incorrectly. The ROT calculating device is reported to be lagging so that the start can be verified visually but the ROT indicator moves only after a delay. This also causes an onboard predictor delay, which is most pivotal when the ship starts to turn. The onboard pilot will compensate for the delay by always observing the turn visually.

Noticing other traffic becomes an impossible task for the remote pilot if there is only electronic navigation available. The onboard pilot can

[11] ARPA, automatic radar plotting aids, for noticing other traffic and collision detection. Can also be used for calculating the passing distance from fixed objects.

[12] GPS, global positioning service, provided by the U.S. government.

notice the traffic visually or from the radar. The remote pilot will see only the electronic chart AIS symbols of vessels and craft that have an AIS transmitter. AIS data is not considered reliable but only an aid to collision detection. Each vessel's AIS data also has inputs from the GPS.

What are the perspectives for the future, and the next steps?

The critical issue of what data is necessary to provide pilotage remains. The development work continues for a more precise definition of remote pilotage. Finding critical ship data or information to acquire and sustain situational awareness is only a partial answer to what remote pilotage is. Critical data forms the content of the remote pilotage data displays and conveys true and meaningful information about the vessel. The remote pilotage workstation displays, and data presentation should mold the data into an easily digestible and usable format.

Communication remains a critical component even after a virtual connection is established between the vessel and the remote pilot station. Through the virtual connection, the remote pilot can communicate with the master by pointing out objects at the vessel interface. Communicating without words and being together in a shared space is an essential part of human interaction. Communication and interactive tools are essential research and development targets.

Most certainly, part of the data is collected from the vessel. Despite onboard communication standards such as NMEA, in practice, the contents of the onboard data messages vary from ship to ship to such a degree that it is not practical just to forward the data. The data and communication standard development should define what data to collect from which sources, and how to present the data uniformly so that each remote-piloted vessel sends a similar set of similar forms. The onboard collecting unit should standardize the data set for the remote operation center. In particular, automation and alarm-related data acquisition vary from vessel to vessel, so custom work must be done on each vessel. The commissioning process will benefit from creating procedures for collecting data.

Lastly, the means to duplicate the most critical components must be explored. The reference data may exist outside the vessel. The vessel data could be verified against the reference data already at the ship-side edge computing before sending it to the remote pilotage center.

Many interesting development targets still remain. The journey has just begun.

References

- **Bruno, K., & Lützhöft, M.,** 2009. Shore-Based Pilotage: Pilot or Autopilot? Piloting as a Control Problem. The Journal of Navigation, 427–437.
- **Endsley, M. R.,** 1993. A Survey of Situation Awareness Requirements in Air-to-Air Combat Fighters. The International Journal of Aviation Psychology, 3(2), 157–168. Retrieved from https://doi.org/10.1207/s15327108ijap0302_5
- **Endsley, M. R.,** 1995. Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32–64.
- **Onnettomuustutkintakeskus,** 2001. B1/2001M Matkustaja-autolautta ISABELLA, pohjakosketus Staholmin luona Ahvenanmaalla 20.12.2001. Helsinki: Onnettomuustutkintakeskus. Retrieved from https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/fi/vesiliikenneonnettomuuksientutkinta/2001/b12001m_tutkintaselostus/b12001m_tutkintaselostus.pdf
- **Onnettomuustutkintakeskus,** 2004. S1/2004M b Luotsaustyö ja sen kehitys. Helsinki: Onnettomuustutkintakeskus. Retrieved from https://turvallisuustutkinta.fi/fi/index/tutkintaselostukset/vesiliikenneonnettomuuksientutkinta/tutkintaselostuksetvuosittain/vesiliikenne2004/s12004mbluotsaustyojasenkehitys.html
- **Onnettomuustutkintakeskus,** 2009. M/T CRYSTAL PEARL, törmäys Lålättanin reunamerkkiin 26.1.2009. Helsinki: Onnettomuustutkintakeskus. Retrieved from https://www.turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/fi/vesiliikenneonnettomuuksientutkinta/2009/c22009m_tutkintaselostus/c22009m_tutkintaselostus.pdf
- **Onnettomuustutkintakeskus,** 2011. C4/2011M M/S TRADER (FIN), karilleajo Varkaudessa 4.9.2011 ja Sulkavalla 16.9.2011. Helsinki: Onnettomuustutkintakeskus. Retrieved from https://turvallisuustutkinta.fi/fi/index/tutkintaselostukset/vesiliikenneonnettomuuksientutkinta/tutkintaselostuksetvuosittain/vesiliikenne2011/c42011mmstraderfinkarilleajovarkaudessa4.html
- **Pilotage Act (940/2003),** 2019. Pilotage Act (940/2003; amendments up to 1534/2019 included). The Parliament of the State of Finland. Retrieved from https://www.finlex.fi/en/laki/kaannokset/2003/en20030940.pdf
- **Pilotage Decree 393/1957,** 1957. The Parliament of the State of Finland. Retrieved from https://www.finlex.fi/fi/laki/alkup/1957/19570393
- **Sharma, A., & Nazir, S.,** 2017. Distributed Situation Awareness in pilotage operations. TransNav the International Journal on Marine Navigation and Safety of Sea Transportation, 11(2), 289–293. doi:10.12716/1001.11.02.11.
- **Wederhorn, T.,** 2014. Aluksen päällikön, luotsin ja muiden luotsaustapahtuman toimijoiden roolien ja vastuiden vaikutus merenkulun turvallisuuteen. Kotka: Kymenlaakson ammattikorkeakoulu / Onnettomuustutkintakeskus.

Liability aspects of remote pilotage in Finland

Contributor • **Jussi Vaahtikari,** Captain, L.L.M University of Turku / ESL Shipping Oy

Introduction

Traditionally, a ship's voyage is a joint venture in which a group of individuals takes a shared risk to transport something at sea. This venture has for centuries included some type of mechanism to share liability in the case of damage to assets or third parties. Liability sharing systems are ever more important, as we have understood the dramatic consequences of what a mistake can mean to the coastal environment. Thus, it is not surprising that among the first thoughts when implementing any kind of novel navigation technology is how to share liability.

The research paper behind this report is the first legal analysis of liability aspects of remote pilotage. It places on a chart the entities involved in pilotage, analyses the liability relationships between them, and builds an overall picture of how the liability regime is built in remote pilotage. At this stage of the remote pilotage project, research may be used to help in choosing safer technologies and, on the other hand, in recommending changes to legislation to build more trust between the parties and, by that, to further contribute to the safety of piloting in the future. Further, the research preliminarily identifies aspects that require more thorough study.

In the background of all legal jargon is the simple question of who shall pay the bill and clean up the mess in the case that something goes awfully wrong during remote piloting. In this report, the language is intended for the general public, and English is used instead of Finnish, in which the applicable law is written, and thus the accuracy is understandably lower than in the research paper. Therefore, in any case of doubt, it is recommended to consult the author for any needed clarifications.

Background

An amendment of the Pilotage Act in 2018 enabled the testing of remote pilotage in Finland. Legally, remote pilotage was defined as *activity where the pilot conducts piloting from a location other than on board the ship*. Testing permission is only granted to national pilotage company Finnpilot Oy under strict rules and under the guidance of Finnish Transport and Communication Agency. The amendment was not intended to change liabilities or rights between the parties or to affect the current state of the law. However, despite intentions, there is always some level of possibility that new norms cause unexpected consequences, especially when regulating novel technology. Now, as the goal was and is to reorganize one of the traditional concepts of navigation, namely piloting, it was worth visiting this field of law. After all, piloting sits at the core of the rules for channeling liabilities and might have a dramatic outcome on the financial positions of the involved stakeholders.

Traditionally, looking from the legal perspective, the pilot has been physically on board the ship and, as per the Finnish Pilotage Act ("PA" 940/2003), working *as an advisor to the master and as a local water area and navigational expert.* It further defines that *the pilot is responsible for pilotage,* but that only means that they are liable for their mistakes or omissions in giving advice as a professional navigation expert. In every case, as per Maritime Code ("MC" 674/1994), the master remains responsible for the overall situation, including navigation, bridge arrangements and safety. In Finland, as is the case in a majority of other countries, even if the pilot makes a mistake, this does not relieve the captain from their own role and they have a duty to observe the performance of the whole bridge team, including the pilot.

It goes without saying that, traditionally, communication has been face-to-face without anybody intervening in the middle. When conducting remote pilotage, the situation is dramatically different. In between, there is at least some type of communication device, and the pilot needs to have access to ship navigation and fairway data, which is distributed via separate systems. All this requires equipment and software that may fail in different ways. It can, for example, interrupt or distort the communication between the master and the pilot or affect the pilot's decision-making, potentially causing an accident. As the fault in this case lies with someone other than the pilot or the master, we must find new ways to allocate liability.

However, the bridge team, including the remotely participating pilot, must stay vigilant. There are already multiple devices on board, and navigators must be prepared to handle exceptional situations. If they aren't, they are liable at least partly. Consequently, the channeling of liability away from the bridge team must be studied, as well.

Method

The intention of the research was to find answers in respect to what current law, as it was at the end of 2021, says about liability. Therefore, a legal dogmatic method was the most appropriate way to approach the research questions. It was also chosen to limit research to tort situations as, in principle, freedom to contract allows the allocation of liability as the parties choose, hence making analysis uninteresting. This rules out the relationship between the shipowner and its contracting parties, such as cargo owners, but it also takes out of the research the area liability arrangements that underlie the remote pilotage system owner and its different providers. As a second exclusion, it must be noted that the Maritime Code as it stands lays down, in certain cases, strict liability on the shipowner in accidents causing, for example, oil damage. These are clear cases and also have worldwide conventions in the background, so this requires no further investigation.

For the above-mentioned reasons, a relevant question was how tort liability is constructed under the Finnish legal regime in remote pilotage. In order to approach this systematically, first it had to be established how traditional pilotage liability changes when remote pilotage is in use. For this reason, a traditional pilotage liability framework had to be established before remote pilotage liability can be compared. The study began by looking into the main actors: the pilot and the master. When their liabilities were defined, focus turned to the shipowner and the pilotage company and their liability relayed from the master or pilot, channeling through the concept of vicarious liability or by their own fault. As a second step, the research focused on questions that only exist in remote pilotage, namely the communication systems between the master and pilot, and the companies or authorities liable for the said technology.

The research is also limited to the material that was available when it was conducted. Especially the fact that there was no existing remote pilotage trial license – a prerequisite for the use of remote piloting – available, or an existing setup of hardware, affects the results dramatically. In the paper, great care is taken not to presume too much how the system would look or what the terms of the actual license for remote pilotage trials would be.

Finally, it has to be taken account that, since the research was done, the Pilotage Act has gone through a major overhaul. An amendment currently in the pipeline changes the numbering of the sections and some wording of the remote pilotage parts of the law, affecting the future usefulness of research observations. While this report was being written, the government gave its proposal to Parliament. However, the author has been involved in the drafting process for the proposal and does not expect too many changes to the act that could change the results of the research drastically. A similar statement is also written into the government proposal (HE 293/2022 vp) itself. However, before Parliament passes the bill in its final form, some level of uncertainty remains.

In Finland, during recent years, there has not been too much legal research in the field of maritime law. On the other hand, shipping in our territorial waters is rather safe, and so there have not been many accidents creating a generous databank from case law. A major role in the research is given to the government's proposal 225/2018 vp, which describes best the legal background in remote piloting. Unfortunately, it is made in view of the fact that the sections concerning remote pilotage only allow experiments and are not even meant to be in force as they stand when pilots are conducting remote piloting permanently.

Secondly, it must be remembered that the Nordic countries have quite similar maritime laws. We also have a common limitation of liability convention in place, and large parts of the shipping safety side are regulated via EU legislation. It could therefore be interpreted that some case law could be drawn from Scandinavia, as we regularly do in maritime law. This is still not the case when it comes to piloting. Pilotage is still in the hands of national legislators for security and national sovereignty reasons. Due to this, analysis of the liability has to be conducted country by country, and the examples from the Nordic countries are somewhat limited in this research paper.

As a consequence, research material is somewhat vague, creating some level of uncertainty for the analysis. Research is possible, despite these constraints, as piloting itself does have long history, and the basic structure of liability draws its origins from its long history. It is also a benefit for the research that, as the government proposal itself mentions, the liability regime is not intended to be changed too much.

Results, findings, output, and impact

In Finland, the remote pilotage liability framework is mainly constructed from the elements defined in the Pilotage Act (940/2003), Maritime Code (674/1994) and Tort Liability Act (412/1974). Although the liability regime was not intended to be changed substantially, some differences can be detected that actually change the basic setup of liability quite dramatically.

In remote piloting, the master and pilot's roles change somewhat from the traditional setup. However, those roles are still close enough to each other that we can use the same standards of care regardless of whether they are conducting remote pilotage or traditional piloting. In the fairway, this can be seen in reality that the level of vigilance while preparing route, navigating, and making decisions are the same. This derives also partly from the fact that, at this point, while the authorities' permit for remote piloting is absent, the standard of care must be assumed to be at the same level.

However, the situation changes at those points at which these two means of piloting a vessel are different. For example, the monitoring of each other's activities and decisions or advice is noticeably different when you cannot see each other. Clues and hints on the state of the pilot or master's situational awareness are hard to determine without being physically present. The same is true for the status of signals received from the ship or for the lag in the communication signal, which could affect the timing of actions or advice. Both the pilot and the master have the duty to observe and take into account, but the expected standard of care is as yet unknown and must be solved beforehand.

Maybe a bigger difference than changes in monitoring is the limitation of liability as it is described in the Pilotage Act, Section 8 paragraph 4. This states that in the case of a communication or hardware failure, the pilot ceases to be liable for pilotage. Although the pilot is no longer responsible for pilotage in the case of a system breakdown or error, they still have the duty to prevent a maritime accident if there is any means available. Basically, this could mean that if there is a possibility to continue to assist the captain, it should be done and, in any case, the pilot cannot throw the towel into the ring.

It is, of course, natural that one cannot be liable for something one is not able to do, but this has consequences for the master's liability. As the captain of a ship must be prepared, according to the Maritime Code, for troubles such as hardware failures, they have to be ready to navigate the ship in the fairway without the pilot's contribution, or at least to ensure that pilotage may be aborted safely. In short, the master cannot rely on the pilot being available all the time. For the master, this situation is undesirable, as their role in the bridge team may vary significantly depending on whether the pilot is available or not. It goes without saying that the master usually takes into account that situations change, but here, part of their decision-making resources disappear suddenly and, at the same time, the bridge team needs to solve a sudden technical failure and re-establish a remote connection. The on-shore pilot has a similar duty to be ready for breakdowns and to be alert for any symptoms of trouble affecting safe navigation. The level of preparedness and the standard of care that the master and pilot must maintain to react to system failures is yet unknown, and it is something the authorities must describe beforehand, similarly to what was stated above about monitoring.

In shipping, it is understandable that individual persons cannot bear the costs that their liability could cause them. People are also working as servants to others, and therefore the responsibility to pay damages is usually channeled to the companies they are working for. As per maritime law, in a case where the ship's navigation team, including the pilot, is at fault, then incurred costs are channeled to the shipowner. This does not change in remote pilotage, and in fact, as the master takes a bigger role in the case of the pilot's absence due to system failure, it could be said that the shipowner is exposed to bigger risk through its vicarious liability. On the other hand, the shipowner has its own responsibility to take care of the ship's safety, which includes making sure that the captain has all the necessary training and tools available to succeed in navigation if a remote piloting system failure occurs. At least there should be the means to fall back to a safe situation, for example by anchoring the vessel.

Even though the roles and duty of care of the pilot and master are now discussed and, on some level, clear, the elephant in the room is still who bears responsibility if the remote pilotage system itself fails. In tort law, liability attaches to the party who is at fault, and in maritime accidents, the starting principle is the same. In practice, this means that if the pilotage company provides the systems and those fail, the liability falls to Finnpilot Oy. Usually, as states or entities providing services are reluctant to carry such a large economic risk as that of a major shipping accident, different forms of limitation of liability come into play.

When discussing actual damages to be paid, the pilotage company is entitled, according to the Pilotage Act, section 4a and 4b, to limit its liability to a maximum sum of 100,000 euros if the incident happens in pilotage and is caused due to gross negligence or intentionally. In the research, it was established that in pilotage at a decent level of certainty means the actual work, behavior, and acts of the pilot personally. The phrase does not mean the time during which the pilotage is happening, and thus the pilotage company cannot rely on a limitation of liability just because a system failure happened while the pilot was piloting.

As said above, in a majority of coastal states, there is a mechanism in place intended to limit state exposure to costs originating from navigation accidents while a pilot is being used. The traditional view is, as explained, that the pilot is the shipowner's servant, and liability should be channeled to the shipowner. However, in remote pilotage, Finnpilot can no longer rely on this if the reason for an accident can be traced to its fault. This view could also be seen as fair, as its role is now much more pivotal to the safety of navigation than before. The pilotage company no longer serves merely as the transportation and booking entity for pilots, as it was before. Actually, a similar conclusion can be drawn from the pilotage company's positive duty to prepare for and mitigate the likelihood of an accident, which it has, as per the government's proposed amendment to the Pilotage Act.

In a sense, this is a natural trend, as the purpose of pilotage is no longer to be a service to the shipowner, but rather its modern role is as a guarantor of the safety of shipping and coastal waters. In this role, it is more of a tool for the coastal state than for the shipowner. As the pilotage company enters the new area of being a service provider of navigation systems, liability should follow. As a benefit of liability, the shipping community can rely on the fact that the piloting company will do their job carefully. On the other hand, the pilotage company is taking a step closer to providing vessel traffic services, although they still have a significantly different purpose.

The other actors who are involved in remote piloting are system administrators, providers and hardware owners. As it is expected that these parties will settle liabilities between themselves by means of contracts, the relationships were not examined too deeply. Nonetheless, it must be said that, to an innocent third party who has suffered harm, there might be an unacceptable situation if they cannot easily establish which of the above-mentioned entities was at fault. As the basic rule of tort dictates, it is the one who has suffered who has the burden of proof to demonstrate that the other party was at fault. For example, some of the communication and data collecting hardware, such as the data cables, belong to entities such as the defense forces and critical infrastructure companies, who are not allowed to disclose details of their systems. Therefore, it is critical that, in the future, the authorities, in their remote piloting license, clearly state how the responsibilities between the parties are shared. However, in failing to do so, the pilotage company still has a duty to be prepared for system failures, and problems that could be used as an argument by an innocent party to find justice in the case of a clear fault cannot be established as the responsibility of a certain function and the entity controlling it.

At last, it was found that the authorities might expose themselves to a new level of risk, as well, if they don't define the above-mentioned issues clearly enough in the license. Similarly, they could have to pay damages if they accept too loose conditions on a pilotage company or fail to supervise the remote pilotage processes adequately. This analysis follows from the fact that all the other actors are dependent on how the authorities define their duties at the end, which can also be seen from the above discussion.

While the research studied the remote liability framework in its current condition, it also indicated some areas of improvement. In this, the approach was to analyze how to make remote pilotage safer and fairer for parties who have suffered from the mistakes of others. One main point research suggests that the relationship between the captain and the pilot could be strengthened so that the key players trust each other better. It must be ensured that the captain can trust that the people who design and maintain the remote piloting system are really giving their best effort.

Firstly, this is achieved best by clearly stating the standard of care that is expected from the pilotage company and other stakeholders, including the master. At the same time, it should be considered how to deal with issues of burden of proof, and finally, it should be settled that there is no conflict of interest between the pilotage company and the pilot. In today's format, the law could lead to a potential dispute inside the pilotage company, as the pilotage company benefits if it can show that an accident was caused due to pilot error rather than due to a failure of the pilotage system. If it is able to show this, then the accident happened because of the pilot, and in pilotage and liability are channeled to the shipowner. At the same time, liability limitation applies.

One approach could be if the pilotage company, instead of the shipowner, takes vicarious liability for its pilots. Then the pilotage company does not benefit from trying to transfer fault to the pilot in accidents, consequently giving it the ability to limit its own liability, as is currently the case. As a major benefit, the captain can then be more assured that the pilot, who now carries somewhat less responsibility than before, would have someone behind them who benefits from making sure the pilot is doing their best.

Another suggested approach is to require a heightened duty of care from the pilotage company while carrying out remote piloting activities. However, these solutions require modifications to existing laws and further analysis of the consequences to the state's exposure to new economic risks in shipping-related damages. As this solution is somewhat unthinkable among traditional maritime law scholars, it should still be borne in mind that, at the end, as per the Finnish constitution, no one should be without compensation if they suffer damage due to acts or omissions of the state.

Secondly, the authorities must uphold the captain by giving clear guidelines on what the captain is expected to do and what standard of care is considered adequate. This is achieved by publishing instructions about the expected level of competence and the training that is required for successfully conducting remote pilotage.

Reference

- Vaahtikari Jussi. 2021. Etäluotsauksen juridisia karikkoja kartoittamassa: Sopimuksen ulkopuolinen vahingonkorvausvastuu etäluotsauksessa. Master's thesis. University of Turku. https://urn.fi/URN:NBN:fi-fe2022013111390

BRIGHTHOUSE INTELLIGENCE

ERICSSON

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Tampere University

MEYER TURKU SHIPYARD 1737

The archipelago's sensor test station withstood well changing seasons. Photo: Brighthouse Intelligence

ENABLING TECHNOLOGIES

Brighthouse Intelligence offers a one-stop shop for building digital solutions for remote and autonomous applications. We provide intelligent situational awareness, reliable high-performance connectivity and advanced cyber-security solutions. Our services cover the full R&D lifecycle, from innovation and prototyping to development and maintenance. We have been developing remote and autonomous maritime technologies since 2015, but we operate elsewhere as well: indoors, outdoors, offshore. We work in close contact with our customers and build innovative solutions by combining industry knowledge and heavy hands-on experience in complex R&D projects.

Future fairway navigation, technical implementation

Contributors

- Brighthouse Intelligence Oy: Markku Sahlström, Mika Tolvanen, Karl Erik Gustafsson, Riikka Rinne, Miikka Nummelin, Timo Toivoniemi, Timo Saari, Mikko Salokannel, Jyrki Alamaunu, Meri Löfman, Katja Huuskonen, Peter Eriksson, Samuli Hellberg, Timo Kettunen, Kim Sjöholm, Tom Perttala, Timo Räsänen, Matti Sairanen, Sami Kuivala, Matias Tamminen, Iida Lintuaho, Benjamin Biström

Mission

Safer, remotely managed, cost- and emission-optimised usage of fairways: Design, integrate and demonstrate technologies that enable future intelligent fairways and remote pilotage activities.

Background

Our goal in the program was to design, develop and build the technical concept for future intelligent fairways and remote pilotage centres. Three main parts of the concept were defined to be sensor stations along the fairway, data collection units on board vessels, and remote pilotage centres. The concept also included data transfer and cyber-security solutions, and connections to various open data sources, such as FMI. In the program, this technology concept formed a solid backbone and test platform, where collected and generated data was freely accessible by other program partners and used for various development purposes, such as image recognition and tracking algorithm development, for example.

Intelligent fairway architecture

The overall architecture of the intelligent fairway concept is illustrated in Figure 1. The different dependencies and interfaces between the fairway, vessel, remote pilotage centre, open data interfaces and other relevant partners are shown. During this demo, the Google cloud-based solution was selected, but this could be easily transferred to a dedicated secure cloud server running on the authorities' or shipping company's own premises.

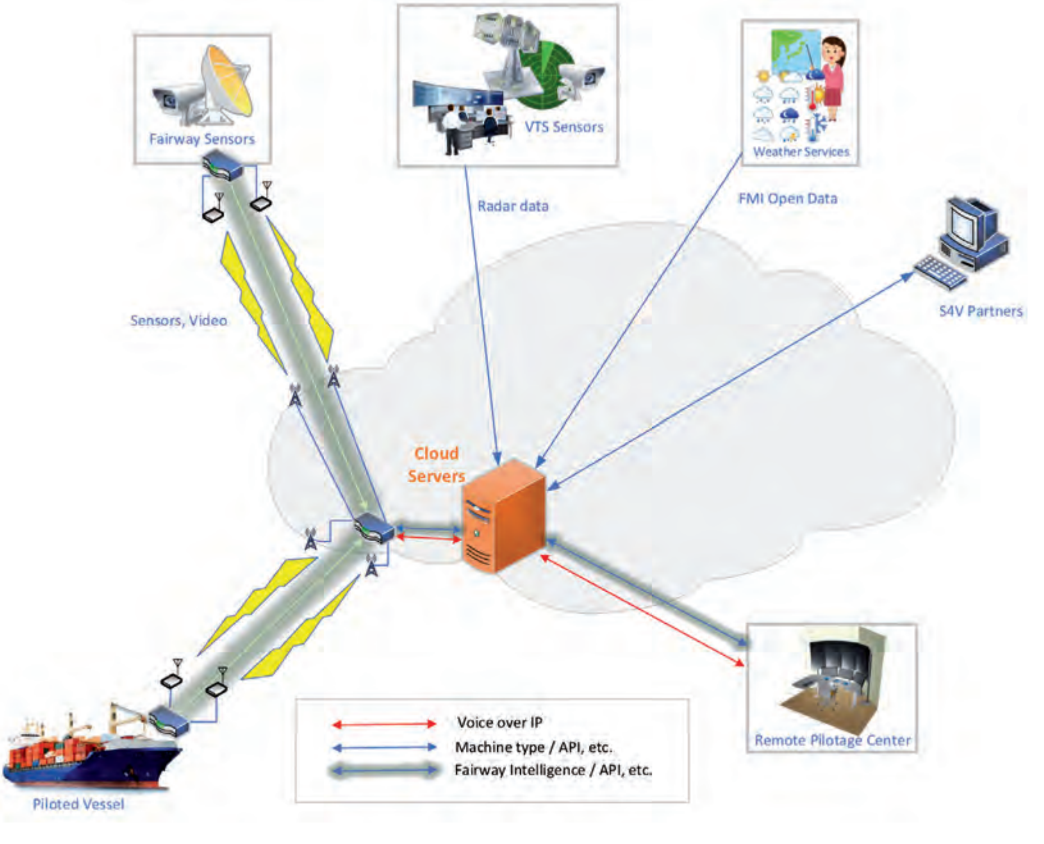


Figure 1. **Intelligent fairway setup, © Brighthouse Intelligence Oy.**

Solutions/ deliverables

Concept for fairway sensor stations

The first sensor station was built already in June 2020 for Airisto, along the fairway to Turku and Naantali. It is still in active operative use. Later, two other sensor stations we built along the western Helsinki fairway, one to Lauttasaari and another one to Ruoholahti. These two stations had been disassembled by the end of the program. The sensor stations consist of a basic unit, the SmartBox, which is a device creating a picture of situational awareness using various sensors, edge computing capabilities and LTE modems (typically two, with Elisa and Telia SIM cards) for fast and reliable data transfer. All this is protected by end-to-end cyber-security solutions. Sensors included day and night vision cameras, LiDARs, and water flow and weather sensors. All data was transferred into the cloud environment, from where it could be accessed by devices in the remote pilotage centre, providing a real-time view and environmental conditions in the fairway for remote pilot operation.

Interface to vessel data

Vessel navigational data were gathered via an IEC 61162-450 interface. Typical data consist of parameters such as speed over ground, rate of turn, rudder angle, and so on. Data are gathered and transferred to the cloud using a similar SmartBox to that used on fairway sensor stations. There were two LTE modems on board the vessel, with one on either side of the bridge. Even though the antennas were placed inside the bridge, surprisingly good performance results were achieved on open sea voyages. The same SmartBox was also used to provide Internet access on the bridge, and that connection was used by the observing pilot on board the vessel. The system was installed on board two ESL vessels: Viikki and Haaga. On Haaga, the installation took place already in June 2021, and the Viikki installation took place just before demo in May 2022. Viikki was a great test and development platform for the whole system, transmitting online data all the time during voyages.

Connections to existing fairway sensors (VTS)

During the program, we got access to the Finnish VTS system in order to get radar-based target vessel location information operating in a certain area. With this information, we also saw vessels that did not have the AIS system at all. The information was added to our situational awareness view in the remote pilotage centre, and it was a great addition to being more aware of what kind of traffic existed and where.

Connections to open data sources

Some open data, such as meteorological data from FMI, were fed into the remote pilotage centre and shown as a part of the bigger situational awareness picture.

Workstation for remote pilot

The remote pilotage centre was a software variant for our remote operation centre, which was originally designed to remotely control vessels or any other moving vehicles. In remote pilotage use, there were five big screens showing the surrounding AIS and VTS radar-based traffic on a chart view, video streams, local pinpoint weather information from sensor stations, and information on the vessel under pilotage. In addition, safety contours of the fairway were shown. The three smaller screens below showed the vessel radar view, ECDIS and conning displays, based on the real-time data coming from the vessel. Communication between the remote pilot and the bridge of the vessel was handled via voice over IP connections.

Connectivity solution

Connectivity was based on multi-radio solutions in order to create reliable communication links between the vessel, fairway sensor stations, and the remote pilotage centre. The core of the system was running in the cloud environment, and wireless connections were made via LTE modems. To ensure optimal data flow in various conditions, at least two modems with both Elisa and Telia SIM cards were used. Data aggregation software was also used to combine the data flows into one bigger connectivity tunnel.

Cyber-security solution

All information sharing, computing and data communication were protected by end-to-end cyber security. To minimise the attack surface of the system, devices were hardened, threats identified, and vulnerabilities mitigated. Both HIDS and NIDS solutions were studied to produce a common cyber-security solution to detect possible attacks against the system.

Remote pilotage demo

In the technology demo, the vessel was piloted out from Kokkola harbour (Figure 2) and the remote pilot was operating in the remote piloting centre located on Novia premises in Turku (Figure 3). The vessel had a physical pilot, who was responsible for pilotage, on board. In addition to this, there was a person on board who received and compared the commands from the remote pilot with those of the responsible pilot. Commands from the pilot on board were very consistent compared to the ones given by the remote pilot, who was relying on a technology-produced situational awareness picture.

The demo was originally supposed to run out of Helsinki, but it had to be moved to Kokkola at the last minute due to conflicts in schedules. The ESL vessel Viikki was equipped at the last minute a day before the demo. Initially, the demo was supposed to run on the Haaga. On the other hand, thanks to this change, it was seen that the system can be installed very quickly and flexibly on different vessels. We couldn't move the sensor stations to Kokkola at such short notice, but their lack was compensated by one camera looking forward from the bridge. All the sensor station tests were run through already at Airisto and Helsinki, so the concept was proven to work even though Kokkola did not have the same setup installed.

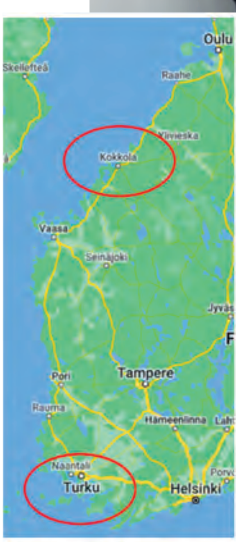


Figure 2. Chart of the demo areas.

Figure 3. Remote 'crew' at Turku Novia Remote Control Centre, © Mika Tolvanen Brighthouse Intelligence Oy.

Ericsson Finland

Ericsson Finland (Oy L M Ericsson Ab) is a 100% owned part of global Ericsson Corporate. We deliver fully fledged solutions—from full scale systems and services to mobile phone applications—both to our Finnish and to international customers. Ericsson Finland employs roughly 800 people and, of those, roughly 70% are working at the R&D Center Finland. The R&D Center Finland is one of the main development centers of Ericsson Corporate. Our focus at Ericsson Finland ranges from research to development, from delivery to support, and from sales to customer service.

NomadicLab (Ericsson Research in Finland) hosts 50 researchers and facilities for them to conduct research in the areas of wireless communication, networking, the cloud, security and IoT. Ericsson Research has built a lab that is used to develop new solutions and networking protocols in our research areas. Ericsson Finland has participated in several EU and nationally funded research projects. Our research organization has key positions in IETF, 3GPP, IPSO standardization forums, and we are also actively participating in GSMA, ETSI and IEEE standardization. We also have long experience of building prototypes that demonstrate the research concepts developed in projects.

5G for maritime

Contributor

- **Patrik Salmela,** Ericsson

Introduction

Smart and connected fairways and ports, and many other aspects of maritime operations, will rely on connectivity to provide the promised optimizations and benefits envisioned for the future. While different access technologies might be used, mobile networks, such as 5G, are sure to play a significant role due to the provided performance, reliability, and global coverage. In addition to pure connectivity, 5G comes with a good set of features that can be used to create an optimized and secure system. In this work, the focus is on various isolation and deployment options that can be used to this end.

Background

The fairway of the future will be heavily reliant on connectivity to implement the various support functions and services needed for remote and autonomous operations. Availability, reliability, and quality of service are important features for the connectivity technology, but when more and more reliance is put on connectivity, the importance of the security and isolation features provided both by the system and by the access technology increases.

While 5G has been developed with 4G as a starting point, there are lots of changes across the board, ranging from the 5G core network (5GC) implementing the so-called Service Based Architecture (SBA), in which each network function is its own web service running in a restful environment, to New Radio (NR), replacing LTE and bringing much-improved radio performance. There are, of course, also lots of other pieces of new solutions and technologies that make up the full 5G system (5GS). Some interesting solutions for industrial and enterprise use cases, such as the maritime sector, include slicing and private 5G networks.

In this work, the 5G system was introduced, including some of the most interesting features that could be used in the maritime context.

Solution, method

The work was done partly as a literary survey, disseminating relevant topics from the 3GPP standards such as [1], but also looking at how the solutions could be applied in a maritime context.

The work started with an introduction to 5G and its architecture. The security of 5G was presented, with a focus on communication between the UE and the network. For completeness, the GSMA eSIM work was also presented, which is a flexible approach for remotely managing the subscription credentials of the UE, thereby significantly improving usability and reducing OPEX for both large deployments and any UE located in hard-to-reach places, such as sensors deployed in a fairway.

After the basics of 5G were introduced, the work looked into various forms of isolation and segmentation that are available to both provide security and improve reliability/availability, including network slicing, which has been introduced with 5G. Further isolation mechanisms were also described in various forms of non-public network (NPN) deployment models. The various tools available for providing isolation for networks used in the fairway and the port were compared, and the benefits and drawbacks were presented. Based on this, selecting a suitable deployment model and tools for maritime operations can, we hope, be made easier.

The work was delivered as a document to the connectivity WP (WP 3.1) in the project.

Results, findings, output, and impact

The isolation mechanisms that were looked at were Data Network Names (DNN), which can be coupled with Secondary Authentication (SA) for added access control, network slicing, and Closed Access Groups (CAG). For private network deployment, both Standalone (SNPN) and Public Network Integrated (PNI-NPN) Non-Public Networks (NPN) were looked at.

DNN can be used to connect the UE to a specific data network via the mobile network, such as an enterprise network. In the maritime context, this could be a port network. With SA, the UE is required to further authenticate itself toward said data network to gain access, thereby having multiple levels of access control; the 5G network operator only interconnects the authenticated and authorized (based on subscriber profile) UE to the data network, and the data network further authenticates the UE using SA. Thus DNN, with or without SA, is a 3GPP/5G tool that can be used to limit access to a private (e.g.) port network to only the authorized UE.

Network slicing is one of the features of 5G that has gained a lot of attention. With network slicing, the UE can be assigned a dedicated and tailormade slice of the network. This can be implemented end-to-end, or the slice might have some dedicated parts, namely "Network Functions" (NF), and might use some parts/NFs common to all UE. For the NFs in the 5G network, this is often implemented by allocating their own instances of the NFs to the slice. This means that the network can provide guaranteed resources for the users of the slice, as well as isolation from any UE that does not belong in or is not using the slice. The slice-specific NFs can run either on shared or their own hardware. Slices can also require access control, similar to SA, to only allow the authorized UE/subscriptions to access the slice.

Slicing can also be implemented on the radio interface. One option for how to implement this is through CAG, which allocates a radio cell to a pre-defined set of UE/subscriptions, which belong to a group identified by a CAG identity. Thus, only the UE that belongs to the CAG group can utilize the cell and thus use those radio resources. This makes it possible to do well-informed radio resource allocation to guarantee a certain level of service in radio access. The radio resources used by the cell could belong to the network operator's radio spectrum. Alternatively, in countries where it is implemented, the pre-allocated radio spectrum reserved for local industrial/enterprise use could be used.

When more control over the data communicated over the 5G network is needed, NPN in its various forms can be utilized. An SNPN is a full 5G network that does not offer public service but that is instead deployed to cater for a private set of subscribers. The whole network, with the possible exception of the radio access network, is only serving the subscribers of the SNPN. A typical use case is a factory, but, for example, a port could also have its own SNPN to provide connectivity for port and fairway services and equipment. The SNPN could be locally operated, but the operation of the network could also be obtained as a service, for example from a public network operator. A PNI-NPN is like a light version of an SNPN; the PNI-NPN is always offered by a public operator, and at least part of the functionality is run by said public operator, including subscription handling. With a PNI-NPN the local entity, such as a port, could operate certain NFs, or the PNI-NPN could be fully provided by the public operator as, for example, a network slice.

The benefit of using an NPN is that locally run NFs could be locally controlled and could run on dedicated and therefore not shared hardware, and the data for the locally deployed parts of the NPN would not exit the local network. Of course, depending on the PNI-NPN deployment model, the data might also traverse the public network operator's infrastructure. However, by selecting the User Plane Function (UPF), which is responsible for handling and routing the application layer data between the 5G network and external networks, to be locally deployed as part of the port network, for example, the user plane data, meaning not 5G control data, can be processed on the premises.

The presented tools and deployment options can be combined and utilized in a manner that provides the needed functions and performance. Choosing the right tools comes from analyzing the needs at hand and evaluating the various tools and options that can be applied to meet those needs.

When selecting a suitable deployment option, there are typically more things to consider than when choosing to use one of the isolation mechanisms. For example, 5G could be deployed/used as an NPN, or a public 5G network could be used. However, if using a public 5G network, there might be availability issues during certain high utilization times such as New Year's Eve. For smart fairway operations that are highly reliant on connectivity, this might not be acceptable. Of course, CAG could be used to reserve radio resources for the maritime operations, for example, even when using a public 5G network, which would mean that the guaranteed radio resources would also be available to the CAG group (e.g. port UE) even when the network would otherwise be overloaded. The NPN alternatives likewise have some of their own limitations that can affect the choice, or at least require some additional planning with regard to subscription management and so on.

Looking at the NPN options, a big difference between the PNI-NPN and SNPN is that the PNI-NPN always uses subscriptions provided by the public operator providing the NPN. This means that global roaming is also possible, as public operators (typically) have good roaming agreements. However, with the SNPN, roaming is not allowed, meaning that to access a public network, or another SNPN, separate credentials would be needed. This is of course not a showstopper for the SNPN, but it is maybe not so convenient in all use cases. For example, a vessel traveling the seas would visit multiple ports and, typically, multiple countries and even continents. This means that to be able to access an SNPN in every port, it would need to have port SNPN-specific credentials, or some additional identity management features would need to be added. The benefit with an SNPN subscription is that the credentials of the subscription can be something other than the traditional 3GPP credentials, so PKI certificates could be used, for example. This could be used to solve the non-roaming constraint mentioned earlier.

Assuming that a global maritime-related or trusted organization, such as the International Maritime Organization (IMO), would act as a root Certificate Authority (CA) for a maritime SNPN, it could issue, for example, country-specific certificates to local maritime organizations, which in turn could further issue certificates to ports and shipping companies, among others. These could, in turn, issue certificates to the port and fairway communication endpoints (UE), as well as to the vessels, respectively. A port could then have its own SNPN and serve the port and fairway UE based on certificates that have been issued by the port. Furthermore, visiting vessels could also be granted access based on their certificates, even if they were not issued by the port SNPN, as the certificate of the vessel could be traced back to the commonly trusted global maritime SNPN CA, such as IMO. The SNPN could further use the information about which local CA has issued a specific certificate to grant different types of access to the UE; it could, for instance, distinguish between port/fairway UE and vessels based on who has issued the certificate. The SNPN could then utilize DNN, with or without SA, and network slicing to isolate and tailor the available access and service for each connecting UE.

The work has presented some tools and deployment options that could be utilized by the maritime industry in various use cases. Their exact setup and use, as well as the form of 5G deployment option that is used, would still need to be selected based on the use case and requirement at hand. While 5G is already here and still evolving within 3GPP, 6G is also starting to evolve, and new use cases and requirements, including from the maritime sector, can still make an impact on the direction of 6G.

Reference

- [1]. 3GPP TS 23.501 – System architecture for the 5G system (5GS).

Many ships are already equipped with servers for on-board computing and data storage, and we expect this trend to increase in popularity. In the near-term future, we envision that ships will include a small datacenter, or an Edge cloud, which can be operated either autonomously or as an extension of a larger datacenter in a federated manner. However, extending a mobile Edge cloud to another cloud introduces some technical challenges. For example, multi-cloud networking is usually based on wired, fiber-based connectivity, whereas ship networking toward external parties is inherently wireless. Another challenge is related to the mobility of the ship: it can have fast 5G connectivity near ports, but it must resort to more expensive and narrow-band communications using satellites when in the open sea. We investigated these challenges by building a wired testbed where we emulated wireless connectivity using a traffic shaper.

Wireless edge cloud connectivity for maritime environments

Contributors

- **Patrik Salmela,** Ericsson
- **Miika Komu,** Ericsson
- **Jimmy Kjällman,** Ericsson
- **Tero Kauppinen,** Ericsson
- **Fayezeh Ghavimi,** Ericsson
- **Sepehr Javid,** (Ericsson
- **Antti Kolehmainen,** Tampere University
- **Billhanan Silverajan,** Tampere University

Background

In this work, which was done as part of the S4VF WP3.3 "Fog and Edge Computing" task, we emulated wireless ship-to-ship or ship-to-shore communications with the assumption that both sides of the communications are equipped with a Kubernetes-based cloud/cluster. We emulated wireless connectivity scenarios (two different 5G and two cellular cases) in a wired network using two different traffic shapers.

Solution, method

We built a wired testbed in which we emulated wireless connectivity using two different traffic shaper types in a Kubernetes-based cloud environment. The first shaper type was external to Kubernetes, and we chose FreeBSD "dummynet" as the tool for experimentation, because it was open source and supported the requirements (i.e., configurable latency, bandwidth, and packet loss rate). The second type of traffic shaper was a Kubernetes internal traffic shaper. For this, we chose Calico and Cilium, because they were the only open-source options available for shaping Kubernetes internal traffic.

We utilized Federated Kubernetes to join the clusters together, although this part was not really measured in our experimentation because our focus was on network throughput measurements. We utilized a Network Service mesh and VxLAN-based connectivity in the measurements with the external traffic shaper. The configuration for the network traffic profiles for 5G and satellite-based connectivity was obtained from the literature. The measurement tool in the TCP-based experiments was iperf3.

Results, findings, output, and impact

The key findings from the experiment are as follows:

- Kubernetes networking overhead is negligible when compared to host networking (i.e., a Linux machine without OS virtualization).
- TCP throughput degrades drastically when latency is increased.
- Kubernetes traffic shapers support only bandwidth shaping, and Calico in particular does not respect bandwidth caps immediately but rather with some delay.

As future work, we should also benchmark CPU usage during the measurements and conduct more experiments with more parallel TCP connections. We would also like to automate network traffic prioritization and shaping, so that high-priority traffic has better quality of service when latency increases (and TCP throughput drops) or when traffic loss is high. For example, in the current testbed, the external traffic shaper could be used to emulate wireless networks with different characteristics, as previously, while one of the Kubernetes internal traffic shapers could be utilized simultaneously to adapt the traffic from the clusters to those characteristics. Moreover, we envision that our findings could be used to realize the connectivity part of a digital twin of a ship.

Reference

- The details of the experiment were published in the following paper:

  Kolehmainen A., Komu M., Javid S., Kjällman J., Kauppinen T., Ghavimi F., Silverajan B., 2022, "Benchmarking of Emulated Wireless Edge Cloud Connectivity for Maritime Environments", IEEE 8th World Forum on Internet of Things, October 26 – November 11, 2022, Yokohama, Japan.

  The measurement graphs can be found in the paper listed in the references (copyright by IEEE).

Secure AIS for maritime operations

Ensuring the data shared across maritime entities is secure, untampered with, and generated by a trusted entity.

Contributors

- **Mukesh Thakur,** Ericsson
- **Patrik Salmela,** Ericsson

Background

A maritime vessel uses the automatic identification system (AIS) for its identification and to increase situational awareness by exchanging different types of data, such as name, call sign, current position, speed, heading, and destination, with other vessels, shore stations, and so on. [1] Here, it is crucial that the data that is shared vessel-to-vessel and vessel-to-shore is secure, untampered with, and generated by a trusted entity. The current AIS contains a potential security risk, as the AIS data is transmitted in plain text, which can be read by anyone with an AIS receiver, tampered with, since the data is unencrypted, and possibly sent by advisory, as the source is not authenticated [4]. In the future, with automated maritime operations, the importance of maritime data such as AIS and/or other vessel digital communication will become more crucial, as there might not be a human on board that could do visual observation of the navigation situation. Thus, the reliance and need for security of a system like AIS, or any other inter-vessel communication, will increase significantly.

To address the need for data security of such data in maritime operations, we have proposed a high-level solution with AIS as one option for communicating AIS-type data, supporting automated maritime operations. In the future, it might be that AIS will remain more or less as it is, and some additional vessel-to-vessel digital communication channel will be introduced for automated maritime solutions. Nonetheless, the proposed solution could be leveraged to ensure the data can be trusted and digital communication between different entities is secure.

The proposed high-level solution is described in the next section.

Solution

We propose two possible solutions: one based on public key certificates and the other based on a verifiable credential (VC).

Certificate-based solution

To secure AIS-type data, we need to have a secure communication channel. This typically means that there is first some form of authentication between the communication parties, so they can be made aware of who they are talking to, which in turn means that the vessels need to have secure identities. After authentication, they agree on the keying material and cryptographic protocols to be used to protect the channel.

The challenge in the maritime sector is that a vessel will often come across other vessels that it might not know from before. In this case, authenticating the peer vessel is not straightforward, especially if there is no connectivity for verifying the credentials of the peer with a trusted back-end service. The credential coupled with an identifier, which together form the identity, can be either symmetric or asymmetric. A symmetric credential is one that is known by both the holder and the peer authenticating the holder. This is clearly not something that can be used when authenticating a previously unknown peer without having connectivity to a backend service that could help. Asymmetric credentials consist of a public part and a private part, where a verifier can verify that the holder possesses the private part corresponding to the public part. Examples of asymmetric credentials are public key certificates and raw public keys.

If two vessels, each with their own asymmetric key pair, want to establish a secure channel between themselves, they can use their key pairs to verify that the other party indeed holds the private key corresponding to the public key it has presented. This will work even if they have never heard of each other. Furthermore, during the asymmetric key-based authentication procedure, they can agree on keying material, meaning a shared secret, to be used to protect the session. The Diffie-Hellman key exchange is a basic example of this in practice.

However, even if we now have two vessels that can authenticate each other and establish a secure channel for exchanging possibly sensitive information, we are not quite there yet. What is missing is the identification of the peer. In just accepting the peer vessel and its public key, there is still no information about who the peer actually is. For example, the peer vessel could, over the secure channel, claim whatever identity, and it would not be possible to verify the claim. To be able to verify the identity of the peer, an entity trusted by the verifier must have claimed it, and the verifier needs to have access to that claim.

With public key certificates, the certificate holds identifying information about the certificate holder. This could be the URI of a service of the holder, the organization the holder belongs to, and so on. The certificate is issued by an issuer, which is called a Certificate Authority (CA), and which acts as a trusted party. Thus, if the verifier trusts the CA that has issued the certificate to the peer, it can trust the identity claimed by the certificate held by the peer, of which the peer can prove possession by using the private key associated with the public key certificate. This means that if two vessels with public key certificates, issued by CA(s) that are trusted by both vessels, want to communicate securely with each other, they can authenticate each other, identify each other, and establish a secure communication channel between themselves. This could be implemented by having one global CA issuing certificates for all vessels. Still, this is not as easy as it sounds.

When issuing a certificate, the issuer, the CA, first needs to verify the claims it is about to certify. For a global CA, this might not be straightforward; how could a CA operating in Japan easily verify all the details of a vessel with a home port in Iceland, for example? It is doable, but would require a lot of work, especially if the CA is keen on maintaining a good reputation and not certifying false data, which means checking and double checking everything it certifies before issuing the certificate. For this reason, public key infrastructures (PKI) often introduce the concept of a certificate chain, which is a hierarchy of CAs: one root CA, which has sub-CAs, which in turn might have their own sub-CAs, and so forth. A holder of a certificate issued by the PKI would have a certificate issued by a sub-CA, the sub-CA would again have a certificate issued by a CA above itself in the hierarchy, and so on, until finally there would be a certificate issued by the root CA. When a verifier wants to verify the certificate of the holder, it would have to verify all these CA/sub-CA issued certificates, the certificate chain, until it reaches a CA that it itself already trusts. This could mean checking all the way to the root CA, but it could also be that the verifier trusts a sub-CA in the chain, and so verifying that the holder certificate is linked to the trusted sub-CA would be enough.

In the maritime context, for example, the IMO could operate the root CA and then have country-specific sub-CAs. With this approach, a vessel would typically trust the country-specific sub-CA of its home country/port, as well as the IMO root CA. A peer vessel would, during authentication, present its own certificate with the CA certificate chain containing the CA of the peer vessel's country and the IMO root CA. The verifier could then verify that the peer vessel has a certificate that has been issued by an entity (country-specific sub-CA) trusted by the root CA, which in turn is trusted by the verifier. Thus, the verifier can trust the identity/certificate of the peer vessel. As long as the verifier has the trusted CA certificates available, it can verify and trust a peer vessel's certificate/identity, even if there is no connectivity to a backend service that could help. In PKI, there is also the concept of certificate revocation. For some reason or another, an already issued certificate can be revoked. In this case, a verifier should no longer trust the revoked certificate. The revoked certificates can be listed in a certificate revocation list (CRL), which the verifier can check against when it is about to verify a peer's certificate. This, of course, requires connectivity to the CRL.

VC-based solution

As discussed in the previous section, certificates are one option to secure AIS. Another option we have been looking at is a verifiable credential (VC), which could be used to secure AIS and provide additional benefits, such as self-verifiable schema-based credentials and selective data disclosure.

A verifiable credential is a standard way of defining credentials on the web that are cryptographically secure, privacy respecting, and machine verifiable [2]. A VC has a set of tamper-evident claims, credential metadata, and proofs that cryptographically prove who issued the VC, as shown in Figure 1. The credential metadata has an identifier and a set of properties, such as the issuer, an expiry date and time, a public key for verification purpose, or the revocation mechanism.

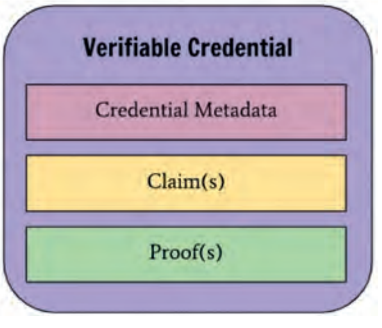


Figure 1. **Verifiable Credential [W3C – 2].**

A VC is much like a public key certificate. It contains a provable identifier (e.g., public key) and some information about the holder, and it is signed by the issuer (e.g., CA). The difference is that a VC is more dynamic with regard to what can be stored in it compared with a public key certificate (claims vs. certificate attributes), and it has the possibility for zero-knowledge proofs (providing information without revealing the actual information) and selective data disclosure (revealing a sub-set of information).

High-level solution description

Compared to the PKI certificate-based approach, this solution provides the added benefits of dynamic schema-based self-verifiable AIS data.

On a high level, the solution works as described below.

First, the solution requires a trust hierarchy, which is similar to a PKI solution, such as [3,5,7], in which the root of trust is the International Maritime Organization (IMO), and a trust hierarchy is established between the IMO and national maritime authorities (NMAs). The major difference in this case is the use of verifiable credentials, instead of PKI certificates, which contain the public key, a hash of the public key, or a URL to access the public key of the issuer.

Second, the NMAs issue VCs to the public entities involved in maritime operations, such as shipping companies, ports, and port authorities. Each VC has a unique identifier and credentials specific to the respective entities, which are published in a global public registry. The associated schemas, based on which the VCs have been issued, are also published in the global public registry.

Third, the shipping companies issue VC-based credentials for their vessels, and optionally crew members, and publish the VC schema(s) of the corresponding credentials in the public registry. The shipping companies also publish the respective schemas for their AIS data in the registry. The vessels and crew members have supporting applications, such as digital wallets, to securely store these VCs.

Fourth, based on an AIS data schema, the shipping company issues the vessel a VC with AIS data, such as the shipping company, vessel name, and so on. This thereby also includes the digital signature of the data via the VC issuer signature. This VC-AIS data is broadcast to other vessels together with the dynamic AIS data generated by the vessel, such as speed, captain, and so on. All the broadcast AIS data is also signed by the vessel using its VC. If required, the VC-AIS broadcasting vessel can utilize the selective data disclosure feature of VC to hide selected pieces of data from the VC, to anonymize the data, or to utilize the cryptographic identifier of the peer VC to encrypt the data if it is targeted at a specific receiving/peer vessel.

The VC-AIS data could be sent over the traditional AIS channel, with digital signatures and other VC-specific data being sent in free-form fields, allowing the receiving party to reconstruct the VC and thus verify its content. Alternatively, some other channel, like the VHF data exchange system (VDES), which is an extension of AIS with limited security measures, could be used for exchanging data utilizing VC features [6].

Lastly, the VC-AIS data receiving vessel parses the VC based on the schema, which it retrieves from the schema URL in the VC, which has been published by the issuer along with its identifier and signature. Next, the receiving vessel verifies the signature of the sender vessel, possibly the signature of the captain if their VC has been used, and the signature of the VC issuer, and decodes the message. If the message has been encrypted for a specific target vessel (based on the target vessel's public key learned from an AIS broadcast), then only that specific vessel is able to read the message by decoding it with its private key. In practice, this would require that the sending vessel somehow indicates the target vessel identifier, so the correct target vessel understands to decode the message. We will not go into protocol-level details of how this could be implemented.

The uniqueness of this solution is that the entities do not need to agree on a pre-defined schema for data exchange; rather, they can encode their data using their own schema, which is accessible via the trusted registry. This freedom to have a dynamic schema enables data interoperability between different ports, authorities and even countries. Still, for interoperability reasons, especially in situations without back-end connectivity, the starts of the schemas should ideally be standardized so that main standard information elements, such as the IMO number, can always be parsed even without the specific schema. For connectionless situations, the peer vessels can agree on a common schema for exchanging any additional information, or each vessel could carry its own schema and share it if needed. When operating in a connectionless situation, there is no way to verify that the issuer of a received VC is indeed registered in the trusted registry (and thereby a trusted issuer). To cover such scenarios, either the verifier must blindly trust the received VC, or there needs to be something similar to a certificate chain linking the VC and its issuer to a well-known entity, such as the IMO, through digital signatures.

The VC-AIS data is self-verifiable, as the data always has the issuer and holder digital signature, which ensures the data has been issued by a legitimate entity, and it has not been tampered with. Apart from this, the sender can utilize the selective data disclosure feature to choose to disclose only limited data and to broadcast messages anonymously, yet it is possible to verify that the message has been broadcast by a legitimate entity.

Results, findings, output, and impact

Using the proposed solution, the data shared in maritime operations across different entities, such as vessel-to-vessel, vessel-to-shore, and so on, can be secure, authentic, and integrity protected. Furthermore, with VC AIS, the (AIS) data can be interoperable between different ports, authorities, and even countries.

Here, it is important to point out that since the current maritime systems use AIS to get secondary situational awareness information and to exchange callsigns to establish preliminary communication, it might not be mandatory to secure the AIS data. However, in the future, with remote pilotage and an autonomous navigation system, security of AIS-type data becomes significantly more important, as navigation will have to rely more and more on cooperation and data-sharing compared to traditional human-based navigation.

References

- 1. **Goudossis, A., & Katsikas, S.K.** Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology 24*, 410–423, 2019. https://doi.org/10.1007/s00773-018-0561-3

- 2. Verifiable Credentials Data Model v1.1. https://www.w3.org/TR/vc-data-model/, Accessed on: 16/11/2022.

- 3. High seas deception: How shady ships use GPS to evade international law | World News, The Indian Express. https://indianexpress.com/article/world/how-shady-ships-use-gps-to-evade-international-law-8129968/

- 4. **Kessler, G. C., Craiger, J. P., & Haass, J. C.** A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 12(3)*, 2018. https://doi.org/10.12716/1001.12.03.01

- 5. **Frøystad, C., Meland, P. H. & Bernsmed, K.** (2017). Protecting Future Maritime Communication. In Proceedings of the 12th International Conference on Availability, Reliability and Security. 2017.

- 6. **Lázaro, F., Raulefs, R., Wang, W. et al.** (2019). VHF Data Exchange System (VDES): an enabling technology for maritime communications. CEAS Space J 11, 55–63, 2019. https://doi.org/10.1007/s12567-018-0214-8

- 7. **Goudosis, A. & Kostis, T.** Automatic Identification System Stated Requirements for Naval Transponder Security Assurance. *2nd International Conference on Applications of Mathematics & Informatics In Military Sciences (AMIMS), Vari, Greece,2012.*

University of Jyväskylä

The University of Jyväskylä is a nationally and internationally significant research university and an expert on education that focuses on human and natural sciences. JYU brings together education and psychology, natural sciences, humanities and social sciences, sport and health sciences, business and economics, and information technology into a multidisciplinary whole, brimming with the latest knowledge and skills. The University focuses on cyber security, one of University's profiling areas.

The Faculty of Information Technology plays a key role in developing one of the University's core fields: human technology. One of the Faculty's primary strengths is its ability to view IT broadly, integrating various perspectives and identifying the joint effects of different phenomena. This is combined with internationally recognized research in the strategic areas, as well as with active societal interaction. Cyber-security research has a national and international focus. Moreover, the development of cyber security at the University of Jyväskylä has created a nationally and internationally important ecosystem in Jyväskylä.

Cyber security architecture in the ePilotage system of systems

Contributors

- **Aarne Hummelholm,** University of Jyväskylä
- **Tiina Kovanen,** University of Jyväskylä
- **Martti Lehto,** University of Jyväskylä
- **Jouni Pöyhönen,** University of Jyväskylä

A modern society is a combination of several critical infrastructures. For example, international and national maritime transportation systems are essential parts of it. Digitalization makes it possible to increase levels of autonomy in maritime systems, which also means cyber environments existing fully in maritime processes. In the cyber environment, it is crucial to have trustable information networks, and usability, reliability, and integrity of systems data in the operating environment.

Introduction

As the smart shipping technologies being developed are highly sophisticated, the cybersecurity risks increase proportionately, too. Awareness of security risks needs to be built in early, in order for threat modeling and risk mitigation techniques to be factored in during system design. The methods of mitigation would be coupled with the smart ship and maritime communication infrastructure design in terms of computational platforms and trusted execution, as well as communication and connectivity constraints with remote operation centers. Cybersecurity information exchange among the fleet, operators and stakeholders, as well as ship-to-ship communication security, is crucial. This has to take into account similarities and differences in cybersecurity threats in the open sea or near coastal areas. Verification of vessel identity and information authenticity must improve from currently used methods. Closely connected to cybersecurity concerns are safety and risk management. Early testing and building of trust in intelligent and smart shipping systems is essential. This also ties in with design concerns in terms of ensuring timeliness of operations and bringing accountability in safety decision-making platforms.

In the cyber world, the most important threat focuses on critical infrastructure (CI). CI encompasses the structures and functions that are vital to society's uninterrupted functioning. It comprises physical facilities and structures, as well as electronic functions and services. Critical infrastructure systems comprise a heterogeneous mixture of dynamic, interactive, and non-linear elements. In recent years, attacks against critical infrastructure, critical information infrastructure and the Internet have become ever more frequent, complex, and targeted, because perpetrators have become more professional. Attackers can inflict damage or disrupt physical infrastructure by infiltrating the digital systems that control physical processes, damaging specialized equipment and disrupting vital services without a physical attack. Those threats continue to evolve in complexity and sophistication. Correctly implemented and appropriately functioning cyber-security architecture is the most important process behind all cyber security. The framework focuses on using organizations to guide cybersecurity activities and considers cyber-security risks as part of the organization's risk management processes. The framework consists of three parts: Introduction, Cyber Threat Intelligence, Risk Management Process.

Background

Cyber security that is driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, and the motives and targets of potential adversaries is required and extends to the entire maritime ecosystem. Securing the cyber aspects of an interconnected system of maritime operations hosted by multiple stakeholders requires a system-of-systems view in cyber security.

The S4FV project's ePilotage environment is an example of a system of systems (SoS) in which an increased number of digital solutions are entering new environments where traditional engineering solutions are still in use. This development introduces an increased risk of a malicious cyber adversary taking deliberate actions against the system, which is why the threat analysis should be done according to the principles of the "system-of-systems threat model."

Solution, method

The research provides a research approach to cyber-security risk investigation at a system level and especially emphasizes the importance of comprehensive risk evaluation in order to increase the resiliency of fairway operations. The findings of the study are related to cyber-security risks in critical information flows between the main system blocks of the automated remote pilotage fairway process.

These risks have been identified, which is necessary to answer the research question: "How can the cyber-security risks of information flows in automated remote piloting fairway operations be evaluated?"

At the strategic level are different types of adversaries based on motivational factors: cyber vandalism, cybercrime, cyber espionage, cyber terrorism, cyber sabotage, and cyber warfare. In the case of cyber vandalism, the arrival of a controversial vessel in a fairway might trigger actions. The controversy might be with the cargo, the vessel's operations, or the vessel's owner. For cybercrime, valuable cargo is more tempting, as financial gain acts as the motivation. Cyber espionage can include business or political espionage. Political factors may arise from national or international issues. From the national side, hacktivism supporting strikes in a harbor could be one scenario. In the worst case, international tensions in the region could escalate to military cyber operations against vessel traffic.

At the operational level, we will discuss the situation with business continuity, including information on the attacker's capabilities to attack ICT (Information and Communication Technology) and ICS (Industrial Control System) systems.

At the tactical level, we have more technical information on the threat actor's tactics, techniques, and procedures. At this level, the follow-up operations may include constant threat evaluations of how changes in an area can affect the strategic and operational levels. Threat analyses in this scope should include both user and technical views of the process. The threat probability tree model has been used for ships' cyber-security evaluation, with maintaining situational awareness as an example of a systems threat analysis and risk assessment method.

The research presents a risk assessment approach at the system level in the remote pilotage process. The findings of the study are related to cyber-security risks in the critical information flows between the main system blocks of the automated remote pilotage fairway process.

Results, findings, output, and impact

In general, an organization's cyber-security management require comprehensive awareness at a system level. The awareness of an organization and decision-makers can be seen as a system-level awareness arrangement. It is possible to integrate an organization's three decision-making levels into a five-layer cyber structure in order to have a comprehensive system view of that organization's cyber-security environment. In the ePilotage process, the system-based approach to the topics and principles are related to the cyber-security dimensions of the stakeholders' comprehensive cyber security.

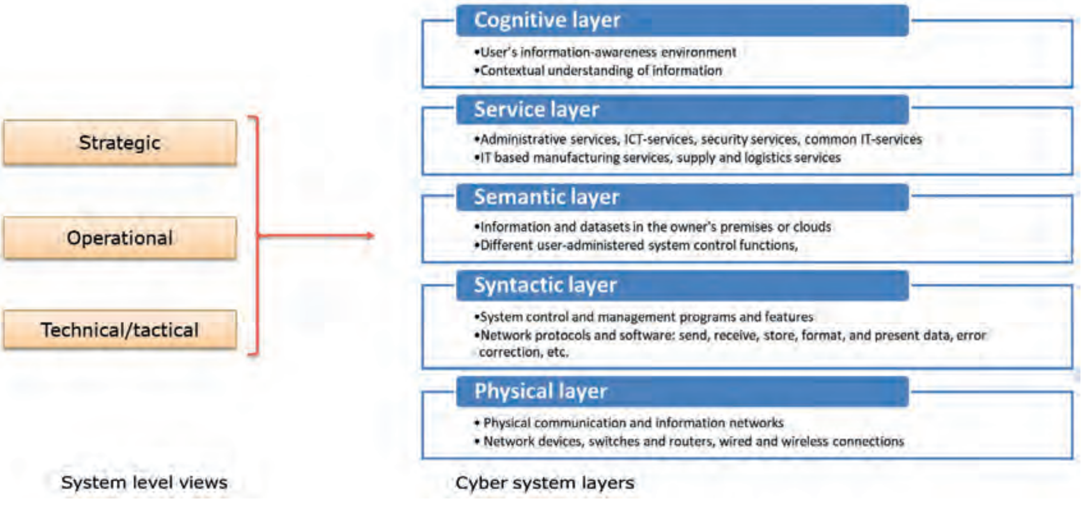


Figure 1. **System level view of organizational cyber security.**

Activities refer to the ePilotage process itself, and security elements are capabilities such as people, processes, and technology, which can be seen as common elements in cyber-security management of the process. The other features of cyber-security management include security dimensions such as those systems that are needed for operations, security awareness, and training. The risk management and continuity enhancement of system operations establish criteria for security management. In that sense, the strategic, operational and technology/tactical viewpoints of the systems of stakeholders support a holistic approach to security. The rest of cyber-security system features include stakeholders and their organizational relationships.

As development of ePilotage fairway systems increasingly uses information systems to exchange information between different integrated systems on the navigation process, and between operating systems via communication lines, the examination of the information flows and used technologies are a very important part of cyber-security risk analysis work. This enables identifying different functions at the system level, carrying out risk assessments, and identifying their residual risks with sufficient accuracy. In the same way, the dependencies of different information systems need to be considered and, based on these dependencies, security and cyber-security risks need to be identified. This chapter presents a probability approach to cyberattacks versus the probability of defending against such attacks, and at the end provides an evaluation of cyber-security risks related to the information flows of ePilotage operations.

ACTION	EXAMPLES	NOTATION
ATTACK IDENTIFICATION	1. Attacks at strategy level (S) 2. Attacks at operational level (O) 3. Attacks at the technical/tactical level (T)	A
PROTECTION CATEGORIES	1. Identity Management and Access Control 2. Awareness and Training 3. Data Security 4. Information Protection Processes and Procedures, 5. Maintenance 6. Protective Technology (Port scan, FIREWALL, IDS, IPS, SIEM...)	P
DETECTION GATEGORIES	1. Anomalies and Events 2. Security Continuous Monitoring and Detection a) SOC	D
COUNTERMEASURE (RESPOND) CATEGORIES	1. Conducting Response Planning 2. Communications and Analysis: a) Real time Situation Awareness b) OODA-procedure 3. Mitigation and Improvements	M
RECOVERY CATEGORIES	1. Recovery Planning 2. Improvements 3. Communications.	R

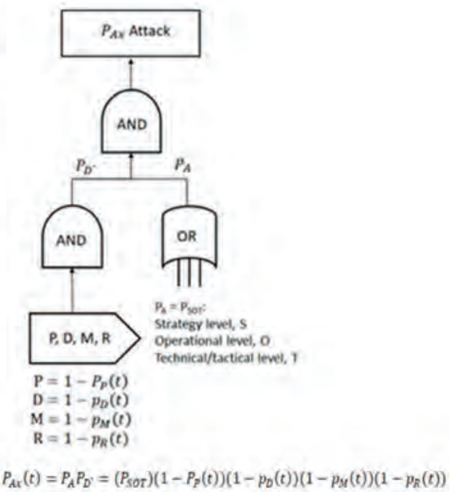


Figure 2. **Probability tree: defense probability PD' versus attack probability PA in the ePilotage process.**

A cyber-threat model captures information about potential cyber threats against a system, an enterprise, a system of systems (SoS), a region, or a critical infrastructure (CI) sector. A cyber-threat model can serve as a basis for a variety of tasks of different scopes. Comprehensive cyber security needs a wide scale of analysis of a system of systems (or sub-system) against a set of threat events. It can be often impractical and, in that sense, analysis of a system of systems could rely on the development and use of threat scenarios. A threat scenario could include the picture of a potential threat materializing and, as a result, the harmful consequences. Potential uses of threat scenarios at three scopes or scales involving a system of systems are: the mission or business function, the enterprise, and the sector (or sub-sector) or region.

The remote pilotage process, ePilotage, is a special environment with a large network of separate systems and stakeholders in the cyber domain. By examining the impacts of cyberthreat actions, and thus risk assessment in this connected environment, it is obvious that the threat impacts affecting one subsystem are propagated to affect other systems. For that reason, people, processes, and technologies should all be considered in risk assessment work, even if we have just one organization's technical level under risk evaluation.

In addition to the likelihood of attack in information flows of the ePilotage process, it is necessary to consider cyber-security procedures of ships, every stakeholder, and the fairway service producer. Threats to information and communication systems, as well as to industrial control systems, can include purposeful attacks, vulnerabilities in the systems, and human or machine errors causing great harm to the services and economy of maritime traffic. Therefore, it is imperative that all stakeholders at all levels of decision processes understand their responsibilities and are held accountable for managing information security risks. The cyber-security architecture of the stakeholder is an integral part of a comprehensive cyber-security architecture in any process case. It represents system resilience and provides cyber-security capabilities to maritime traffic and continuity resilience to its operations.

In order to make the piloting process cyber secure, risks to the main information flows at a system of systems level should be investigated carefully. The proposed risk assessment is an efficient method and key element of making threats and defense capabilities visible. Cyber security is an essential part of the trustful process. The main advantage of the proposed approach is to achieve good results in effective near real-time attack modeling and security evaluation by continually using awareness of threats, vulnerabilities, and defense procedures.

In that sense, all stakeholders should have real-time situational awareness (SA) from the ePilotage process and, in addition, they should use an OODA (Observe – Orient – Decide – Act) loop for SA information sharing with each other. These are the key features when conducting response procedures to risk management across the ePilotage process.

In this research, the research framework for cyber-security risks assessment of maritime automated remote ePilotage fairway systems and processes has been made using probability evaluation in the main ICT information flows between the main fairway systems. The risk assessment methodology that has been used is based on attack probabilities against the probabilities of defending against adversarial actions in the used communication technologies. Risks assessment factors have been identified, and the risk assessment tools have been described. It is a way of thinking of risks and risk prioritization.

Protecting the ePilotage system against cyber threats implies measures taken based on risk assessment, and implies that they ensure confidentiality, integrity, and availability of primarily digital information in the operating processes being examined. The decided measures should be highly significant for the overall availability of the systems that support the stakeholders' processes in the ePilotage environment. Operational availability plays a key role in achieving operational continuity and promoting the reliability of activities. Cyber-security risk management and the central goals of information security are mandatory features from a point of view of operational trust, continuity, reliability, and resiliency.

The Sea4Value program addresses measures undertaken in the digitalization and development of remote fairway navigation. Cyber security is the key area of this development. It is essential to recognize and evaluate cyber risks. The main cyber-security risk assessment elements are:

- cyber threat intelligence
- the risk management process.

The assessment of risks is part of the management process. An automated remote pilotage fairway is a case of system of systems (SoS) construction, and we propose that an assessment can be made by using the main system level information flows.

In this research, we have developed a cyber-security process for critical infrastructure protection. In addition, we have described the risk assessment methodology based on attack probabilities versus the probabilities of defending against adversarial actions in the used communication technologies. Risk assessment factors have been identified, and the risk assessment tools have been proposed. The Delphi method principle is related to the tool.

References

1. **Pöyhönen J., Kovanen T. and Lehto M.,** 2021. *Basic Elements of Cyber Security for an Automated Remote Piloting Fairway System.* Presented in ICCWS 2021– the 16th International Conference on Cyber Warfare and Security 25–26 February 2021, Tennessee, USA.
2. **Kovanen T., Pöyhönen J., Lehto M.,** 2021. *Cyber Threat Analysis in the Remote Pilotage System.* Presented in ECCWS 2021 – 20th European Conference on Cyber Warfare and Security. 24th – 25th June 2021, Chester, UK.
3. **Kovanen T., Pöyhönen J., Lehto M.,** 2021. *ePilotage System of Systems' Cyber Threat Impact Evaluation.* Presented in ICCWS 2021 – 16th International Conference on Cyber Warfare and Security 25 – 26 February 2021, Tennessee, USA.

4. **Hummelholm A., Pöyhönen J., Kovanen T., Lehto M.,** 2021. *Cyber Security Analysis for Ships in Remote Pilotage Environment.* Presented in ECCWS 2021 – 20th European Conference on Cyber Warfare and Security. 24 – 25 June 2021, Chester, UK.

5. **Pöyhönen J. & Lehto M.,** 2022. *Assessment of cyber security risks – Maritime automated piloting process*, Presented in ICCWS 2022 – 17th International Conference on Cyber Warfare and Security 17 - 18 March 2022, Albany, New York, USA.

6. **Pöyhönen J., Hummelholm A. & Lehto M.,** 2022. *Cyber security risks assessment subjects in information flows.* Approved for presentation in ECCWS 2022 – 21st European Conference on Cyber Warfare and Security 16 – 17 June 2022, Chester, UK.

7. **Kovanen Tiina,** 2021. *Cyber-threat aspects in a complex system-of-systems environment: A case study in remote pilotage,* JYU dissertations 409, 3 September 2021. ISBN 978-951-39-8771-8.

Operational maritime cybersecurity visualization

Contributors

- **Hanning Zhao,** Tampere University
- **Bilhanan Silverajan,** Tampere University

Background

Digital transformation has brought the maritime industry efficiency and intelligence. The convergence of information technology (IT) and operational technology (OT) has been leveraged to facilitate maritime operations but also leads to an expanding cyber risk landscape. While many harbors are exploring the concept of creating digital twins, in which IoT sensors deliver situational information about harbor activities in real time to remote locations, the increase in cyber-attacks that target disparate IoT devices has shown that operational cybersecurity management in the harbor and fairway area is an important facet of cyber defense. In addition to smart devices, the cybersecurity of both new and legacy systems associated with critical infrastructure should also be reinforced. Furthermore, another challenge is that the panorama of multiple stakeholders in maritime operations is complex. The variety of backgrounds and knowledge in such a multi-stakeholder environment also becomes a challenge for cybersecurity collaboration. However, cybersecurity has not been fully integrated into different stakeholders' minds. This leads to rather low cyber situational awareness, which refers to an understanding of the current security situation in the operational environment. However, there is still a lack of effective tools for monitoring the cybersecurity status in the harbor and fairway area for different stakeholders, such as terminal operators, managers, and security professionals. That leads to inefficient security incident handling and collaboration among multiple stakeholders.

Cybersecurity collaboration

Cybersecurity collaboration among multiple stakeholders can vary, depending on different scenarios. To gain more understanding of harbor operations, we defined three different stakeholder roles as follows:

- Terminal operators, present in the harbor and responsible for daily operations; very limited knowledge of cybersecurity
- Security analysts, investigate cyber threats and attacks of devices and systems, report incidents to managers and operators; expert users

- Managers, part of a security team, responsible for handling incident reports from analysts and communicating with others

In terms of security incident exchange, each stakeholder role has different tasks and responsibilities. Figure 1 shows the workflow in a multi stakeholder environment for two different use cases.

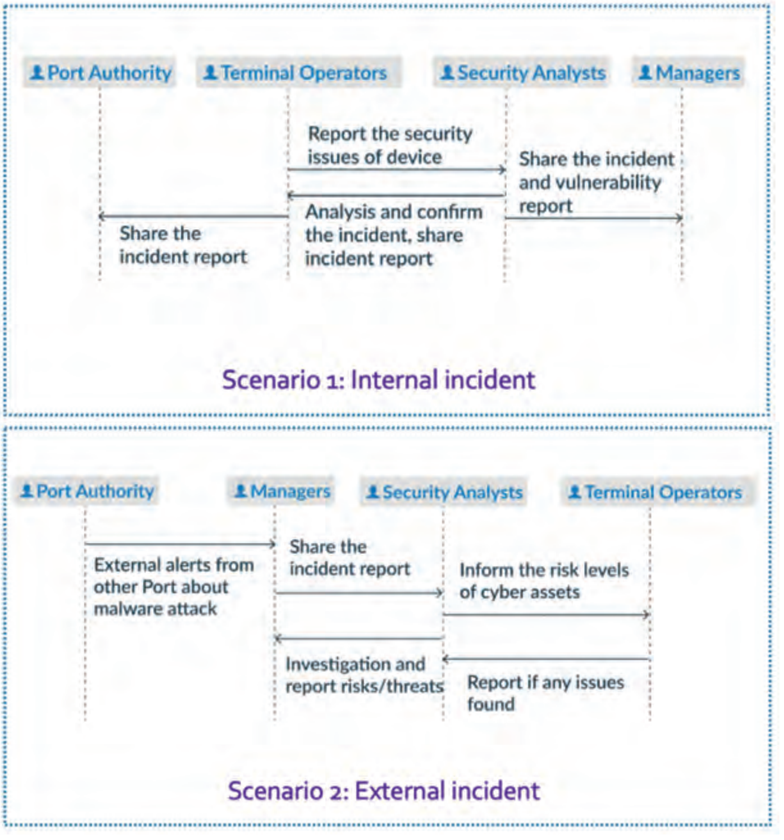


Figure 1. Workflow in multi-stakeholder environment.

In both cases, terminal operators need to monitor all cyber assets in the harbor and fairway areas to ensure cybersecurity health in the operational environment. Such a collaboration would help multiple cybersecurity teams to proactively handle cyber threats in their cyber systems. Furthermore, either security analysts or managers can contact vendors using the incident report, revealing potential vulnerabilities. This incident report can also be shared with manufacturers to increase their cybersecurity awareness in the industrial environment. These two workflows also help to design cybersecurity visualizations tailored to different user roles.

Cybersecurity visualization design

Cybersecurity visualization refers to the graphical representation of cybersecurity-related information, such as network traffic, log data, threats, or attacks. Using visual elements, such as charts and maps, supports human users in dealing with high-velocity security data. In the maritime and future fairway scenario, operational security visualization aims to improve the understanding of the current cybersecurity situation of running devices and systems. Visual representations can support different maritime actors in daily operations, decision-making and mitigation measures.

The proposed design of cybersecurity visualization is a dashboard with multi-coordinated views. Apart from visualizing cybersecurity health, the dashboard also facilitates collaboration by allowing security incident exchange among multiple stakeholders. Figure 2 shows the overall design of cybersecurity visualization on the harbor and fairway side of Turku harbor, Finland.

Figure 2. The overall interface for operational cybersecurity visualization in a maritime scenario.

The security visualization dashboard focuses on delivering the overall security health of devices for terminal operators. As shown in Figure 2, a map-based interface integrated with a scatter chart element encodes the locations of all installed devices, along with their cybersecurity health. More specifically, we designed five colors to represent different cybersecurity health levels of IoT devices as follows:

- Black for under attack; black pulsing nodes indicate devices under an ongoing cyber-attack.
- Green for health; the devices are healthy and working properly.

- Purple for high risk; purple pulsing nodes show devices with a high security risk.
- Yellow for low risk; the devices with a low security risk.
- Grey for offline; the devices are either in maintenance or temporarily disconnected.

In addition to the map interface, three other charts situated next to them depict the operational cybersecurity health of monitored devices and detected incidents, as well as risks. On clicking a device, a pop-up interface will provide more detailed information, including the attributed information of the device, such as the device ID and responsible stakeholders. Through such visual interfaces, operators can effectively monitor the cybersecurity posture and communicate with security professionals in a timely manner by reporting abnormalities and issues with devices near the fairway and waterway.

Data modeling for cybersecurity

Data models have been created to represent the overall security status of the endpoint, which can be an IoT device or other legacy system in the harbor and fairway area. In our proposed system, we developed three data models as below:

- SecurityHealth: a composite object for modeling the overall security state
- SecurityIssue: modeling the potential risks or issues
- SecurityIncident: built on the Incident Object Description Exchange Format (IODEF) standard

The SecurityIncident data model is designed based on the Incident Object Description Exchange Format (IODEF) from the IETF, standardized as RFC 7970. IODEF uses a large set of classes to describe cybersecurity incidents and allows extensions for industry-specific data. It uses three data representations: Extensible Markup Language (XML), JavaScript Object Notation (JSON), and Concise Binary Object Representation (CBOR). All these three data models have been implemented using the lightweight machine-to-machine (LwM2M, https://omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/) specification, which is a widely used protocol for IoT device management.

System architecture and implementation

The proposed system is built on the LwM2M protocol, and three data models have been implemented in the Leshan system (https://github.com/eclipse/leshan), which is a Java implementation of LwM2M.

Figure 3 illustrates the overall architecture. Each organization can build its own LwM2M system for monitoring the cyber assets belonging to the company, while operators can get a holistic view of the cybersecurity status of all devices and systems in the harbor and fairway area.

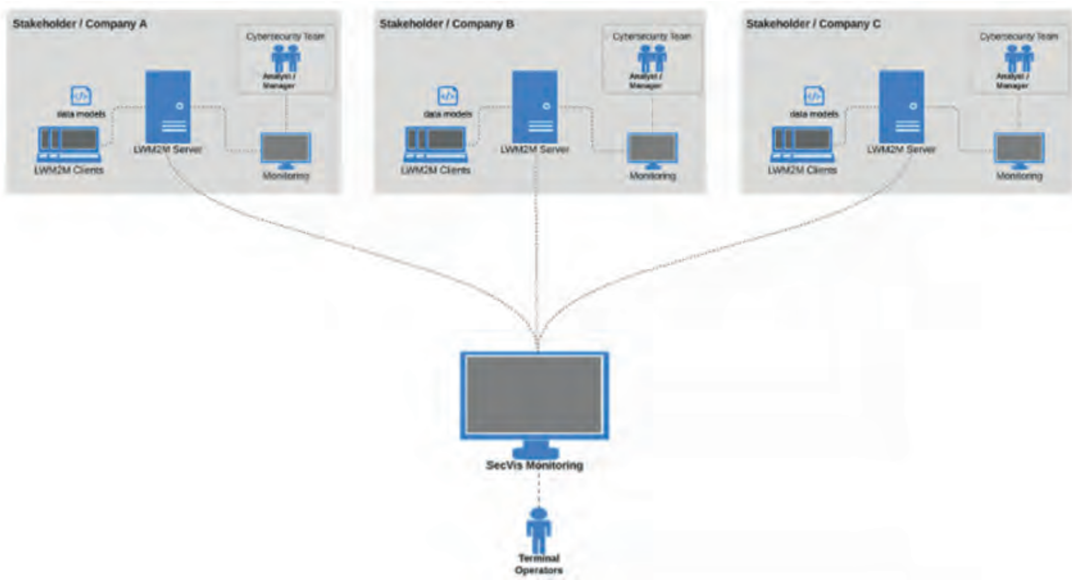


Figure 3. **The overall architecture of the LwM2M system.**

The cybersecurity visualizations are implemented by the open-source libraries based on JavaScript – Apache ECharts (https://echarts.apache.org/en/index.html) and Leaflet (https://leafletjs.com/). The latter is specifically for developing interactive maps.

Evaluation and results

The evaluation of the proposed visualization system consists of two sections. The first is for cybersecurity incident exchange. We evaluated the incident reports based on the IODEF standard, using three data representations: XML, JSON, and CBOR. To demonstrate the common cyber-attack types, we created the incident reports based on six cyber-attacks as follows: malware infection, distributed denial of service (DDoS) attack, GPS spoofing attack, ransomware attack, man-in-the-middle (MITM) attack, and firmware attack. For each incident report, we evaluated report sizes for the different incident types based on the three data formats. The result demonstrated that the IODEF standard can be serialized with different data-interchange formats, such as JSON and CBOR. Overall, security incidents can be exchanged with IODEF effectively in an IoT-constrained environment. Compared to proprietary solutions, the incident exchange solution based on open standards brings a multitude of advantages to facilitate rapid cybersecurity collaboration in industrial multi-stakeholder environments. The standardized solution will aid better processing and collaboration with incident management by allowing incident exchange, processing, and correlation in a more efficient and consistent manner.

Another evaluation was done in the LwM2M system by measuring the data transmitted by the client and server in three payload formats: TLV, JSON, and CBOR. The proposed LwM2M system is tested in three steps:

- Step 1: a security issue is reported by the operator.
- Step 2: the security analyst creates a new SecurityIncident based on the received issue.
- Step 3: the incident is resolved and removed.

The result revealed that using the JSON format payload results in the largest number of bytes transmitted compared to TLV or CBOR. The usage of TLV is most beneficial in IoT environments, but JSON can be applied when integrated with other applications. Moreover, the IODEF-based SecurityIncident object is proved to allow incident exchange in a more efficient and consistent manner and can easily be serialized with different data-interchange formats.

Conclusions

Cybersecurity situational awareness (CSA) is critical in the operational environment of the maritime industry. Security visualization is a powerful tool to reinforce CSA in a multi-stakeholder environment and to facilitate collaboration among different organizations. By using proper and effective visual techniques, operators who are mostly non-expert users can comprehend cybersecurity data better and communicate with others effectively. The designed dashboard also allows more extensions of visualization widgets for other cybersecurity data that needs to be presented in the future. Additionally, the developed visualization can take advantage of different REST-based APIs to obtain and incorporate additional security data, such as potential risks.

Furthermore, the extended LwM2M system can also be utilized for managing cybersecurity status in the harbor and fairway area. In addition, by presenting the feasibility of using an open standard, IODEF, for incident exchange, we evaluated three data representation formats for incident reports: XML, JSON, and CBOR. The evaluation shows that using IODEF is extremely suitable for incident sharing and collaboration.

Water segmentation in maritime navigation

Contributors

- **Moncef Gabbouj,** Tampere University
- **Bilge Can Pullinen,** Tampere University

Background

Water segmentation is a key computer vision task in maritime navigation, and accurate segmentation is even more crucial in fairway channels. This task precedes the object detection and object recognition steps, which are the ultimate target of WP 3.

Semantic segmentation aims to classify each pixel of an image with a corresponding label that describes what is being depicted. The key aspect of semantic segmentation emanates from incorporating the classification of objects and the recognition of their shape, which is paramount for the autonomous transportation industry, including maritime autonomous ships and self-driving vehicles. Various semantic segmentation solutions based on the standard convolutional neural network (CNN) model have been proposed. Nevertheless, recent evidence suggests that self-organized operational neural networks (Self-ONNs) can yield better performance because of their increased heterogeneity and learning capacity. This work presents a novel hybrid network configuration by combining CNNs with Self-ONNs to segment objects in a maritime/urban environment. The main aim of Self-ONNs is to increase the learning capacity of the individual neurons in the network, thus achieving both higher performance and more compact network topology, which means a low computational and memory footprint required in Edge implementation in the S4V Fairway project.

Solution, method

Dataset

Nowadays, there are many general datasets related to segmentation, and so the S4V Fairway project dataset has been chosen according to the labels that would be useful. The ADE20K dataset consists of the following scenery: lake, sea, water, river, boat, ship, and pier (dock), all of which are related to the maritime environment with harbour and city features.

The ADE20K dataset has diverse scene annotations, rich segmentation at the part level, and high annotation complexity [1,2]. Scene parsing means segmenting and parsing an image into regions related to semantic categories, such as sky, car, person, and sea. The MIT Scene Parsing Benchmark (SceneParse150) provides a standardised training and evaluation platform for the algorithms. The data for the benchmark is from the ADE20K dataset, which contains more than 20K images annotated with objects and parts of objects. The benchmark contains 20K images for training, 2K images for validation, and a batch of held-out images for testing. The dataset consists of non-uniform allocations of objects in the images that imitate natural daily scenes.

Self-ONNs

Recent studies [3,4] have demonstrated that conventional CNNs, along with their predecessor MLPs, are homogenous networks based on linear neuron models evolved from the ancient neuron model from the 1950s (McCulloch-Pitts) [5]. To address this drawback, operational neural networks (ONNs) [6] have recently been proposed, which, like their predecessor generalised operational perceptrons (GOPs) [3], are heterogeneous networks with a nonlinear neuron model that can therefore learn highly complex and multi-modal functions or spaces with minimal network complexity and training data. In works [7–9], the latest ONN variants have been published: 1D and 2D Self-ONNs for various image processing, classification, and regression tasks. It was demonstrated that even Self-ONNs with fewer neurons can achieve a superior learning performance, while the performance gap between ONNs and CNNs widens further. Our contribution focuses on the hybrid network of CNNs with Self-ONNs to boost the accuracy of convolutional layers to operational layers.

The baseline and our hybrid model

Instead of dispensing with highly deep and complex CNNs, we propose a variant of the Pyramid Scene Parsing Network (PSPNet) [10] model by converting one or two convolutional layers to operational layers. This will demonstrate that superior semantic segmentation performance can still be achieved without using massively deep and complex CNNs.

In PSPNet, the Pyramid Pooling Module (PPM) is used on the last feature of the extracted map [10]. The PPM observes the entire feature map in subregions with different locations, causing the network to understand the scene and achieve better segmentation results. Reliable predictions come from the fusion of local and global clues.

We label our network as SelfONN. Our networks have either one or two Self-ONN layers with a hyperbolic tangent activation function. Self-ONN-99 means that the 2^{nd} and the 3^{rd} convolutional layers have changed to SelfONNs layers, with the qth order being 9 for both layers. While Q=1, the SelfONN neuron/layer becomes a convolutional neuron/layer. Likewise, we label the 2^{nd} or the 3^{rd} layer as "0" when no change is employed on that layer (original PSPNet).

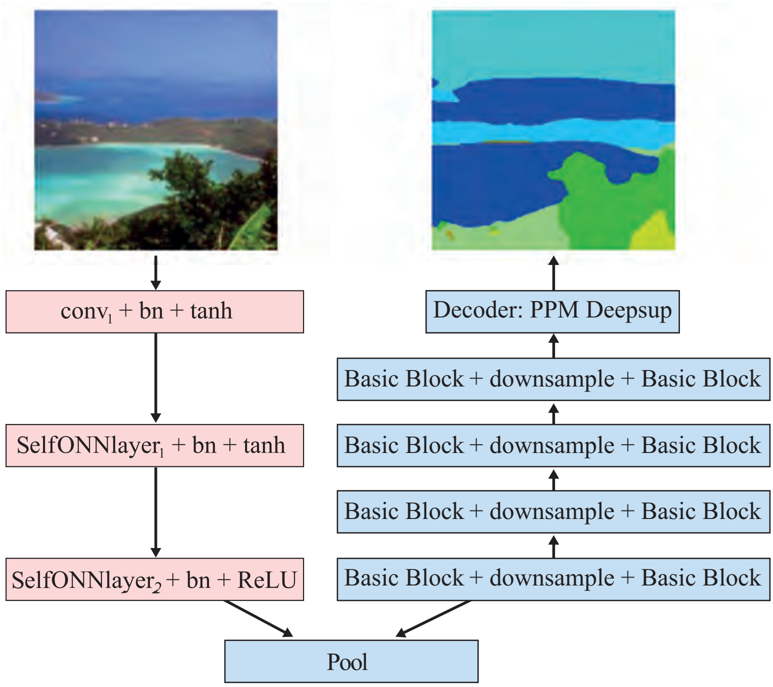


Figure 1. **Overview of the proposed hybrid network, with modified parts displayed in light pink (the first three blocks). The tanh function replaces the ReLU activation function, while the SelfONN layer replaces the convolutional layer.**

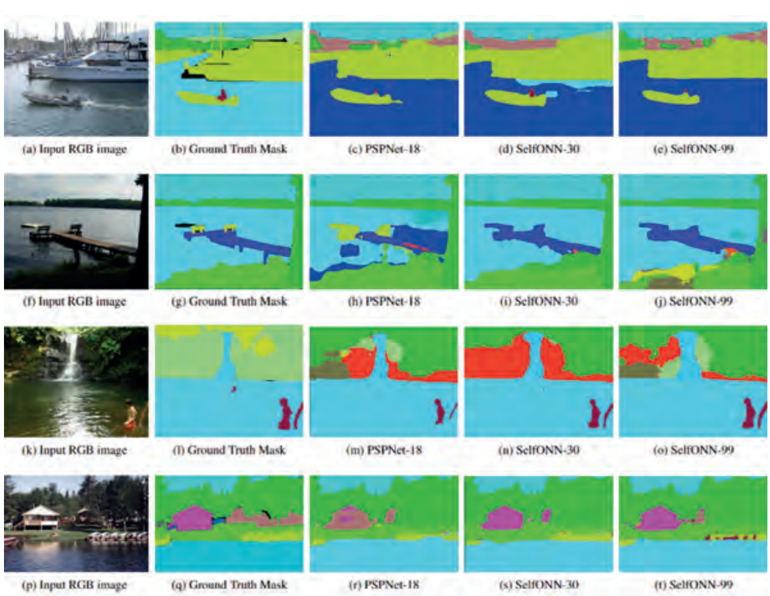


Figure 2. **Example from the ADE20K validation dataset: Column 1 is an RGB image (a,f,k); Column 2 is ground truth (b,g,l); and Columns 3–5 are segmentation results.**

Results

The visualisations of some result images that consist of a body of water from the ADE20K validation dataset are shown in Figure 2. In the first row, boat segmentation differences between models are visible.

Another detail in Figure 2 is human segmentation in the SelfONN-30(d) model. In the third RGB image(k), human segmentation results are clear in the SelfONN-30(n) and SelfONN-99(o) models. In the second RGB image(f), PSPNet-18(h) defines more classes that are wrong, and the difference between the pier segmentations of the models are clear to the eye. Lastly, the RGB image(p) supplements the boat segmentation differences with correct segmentation classes.

Table 1. **Results with Mean-Intersection-Over-Union (Mean IoU) and Pixel Accuracy evaluation units on the ADE20K validation dataset. Baseline model referred to as PSPNet-18*.**

Models	Mean IoU (%)	Pixel Accuracy (%)
PSPNet-18*	34,68	77,48
SelfONN-15	36,09	78,38
SelfONN-30	36,78	78,87
SelfONN-33	36,92	78,45
SelfONN-50	36,74	78,74
SelfONN-99	37,20	78,53

According to Table 1, all the hybrid models outperform the PSPNet-18* model. While the best pixel accuracy is 78.87 % with the SelfONN-30 model, the best mean IoU value is 37.20% with the SelfONN-99 model.

Conclusion

We proposed a novel hybrid network using Self-ONNs for semantic segmentation tasks. Furthermore, we explored the possibilities of operational layers and their compatibility with convolutional layers. The proposed model has achieved the top semantic segmentation accuracy levels with a pixel accuracy of 78.87 % and a mean IoU of 37.20 on the ADE20K validation dataset. Therefore, Self-ONNs are proven to improve the performance of semantic segmentation tasks. Future work for the project will focus on further improving the performance.

References

1. **Zhou B., Zhao H., Puig X., Xiao T., Fidler S., Barriuso A.,** and **Torralba A.,** "Semantic Understanding of Scenes Through the ADE20K Dataset," International Journal of Computer Vision, vol. 127, no. 3, pp. 302–321, 2019.

2. **Zhou B., Zhao H., Puig X., Fidler S., Barriuso A.,** and **Torralba A.,** "Scene parsing through ade20k dataset," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017.

3. **Kiranyaz S., Ince T., Iosifidis A.,** and **Gabbouj M.,** "Progressive Operational Perceptrons," Neurocomputing, vol. 224, pp. 142–154, Feb. 2017.

4. **Kiranyaz S., Ince T., Iosifidis A.,** and **Gabbouj M.,** "Generalized model of biological neural networks: Progressive operational perceptrons," in 2017 International Joint Conference on Neural Networks (IJCNN), pp. 2477–2485, 2017.

5. **Fitch F. B.,** "Warren S. McCulloch and Walter Pitts. A logical calculus of the ideas immanent in nervous activity. Bulletin of Mathematical Biophysics, vol. 5 (1943), pp. 115–133.," Journal of Symbolic Logic, vol. 9, no. 2, pp. 49–50, 1944.

6. **Kiranyaz S., Ince T., Iosifidis A.,** and **Gabbouj M.,** "Operational neural networks," Neural Computing and Applications, vol. 32, no. 11, pp. 6645–6668, 2020.

7. **Kiranyaz S., Malik J., Abdallah H. B., Ince T., Iosifidis A.,** and **Gabbouj M.,** "Self-organized Operational Neural Networks with Generative Neurons," Neural Networks, vol. 140, pp. 294–308, 2021.

8. **Kiranyaz S., Ince T., Abdeljaber O., Avci O.,** and **Gabbouj M.,** "1-d convolutional neural networks for signal processing applications," in 2019 IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP 2019 - Proceedings, pp. 8360–8364, IEEE, May 2019.

9. **Malik J., Kiranyaz S.,** and **Gabbouj M.,** "FastONN – Python based open-source GPU implementation for Operational Neural Neworks," vol. 0, no. 1, 2020.

10. **Zhao H., Shi J., Qi X., Wang X.,** and **Jia J.,** "Pyramid scene parsing network," Proceedings – 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, vol. 2017-Janua, pp. 6230–6239, 2017.

Meyer Turku

The Meyer Turku Oy shipyard is specialized in the construction of very demanding, innovative, and environmentally efficient cruise ships, car ferries, and special vessels. Our share of the global cruise construction market is approximately 15%, and our shipyard's order books extend to 2026. Our largest customers are Royal Caribbean International, Carnival Cruise Lines, TUI Cruises and the Finnish Border Guard.

Meyer Turku employs 2.000 top professionals and operates the Turku shipyard, where vessels have been built since 1373. Meyer Turku's subsidiaries are Piikkiö Works Oy, a cabin factory located in Piikkiö; Shipbuilding Completion Oy, which offers complete deliveries to public spaces; and ENG'nD Oy, a shipbuilding and offshore design company based in Rauma.

Together with the German shipyards Meyer Werft in Papenburg and Neptun Werf in Rostock, Meyer Turku forms the Meyer Group, one of world's leading cruise ship builders.

Meyer Turku tugboat camera and smart fairway experiments

Contributors

- **Marjo Keiramo,** Meyer Turku
- **Henri Suoniemi,** Meyer Turku
- **Kristian Haavaste,** Meyer Turku

Background

The goal for Meyer Turku in this project was to evaluate, develop, and test different modern digital solutions to improve vessel safety, environmental friendliness and system reliability, especially by means of autonomous solutions using modern technologies for safety navigation.

The shipyard's role was to observe and support partners and participate in experiments, including Meyer Turku's own assessment of the "Tugboat Camera project".

Solution, method

In the launch and float out of the vessel, cameras were used on the pier side of the vessel with the shipyard's satellite compass/AIS package. Real-time camera images with real-time AIS info were transferred from the floated vessel to the assisting tugboats and harbor master in dedicated PADs.

In a sea trial of the vessel, cameras were used on the pier side of the vessel, in pilot ports, and in the helicopter area. AIS information was taken from the vessel AIS Plug using the Trenz Pilot Plug.

Real-time camera images with real-time AIS info were transferred from the sea trial vessel to assisting tugboats, and real-time camera images to the sea trial vessel bridge in dedicated PADs/displays.

Results, findings, output, and impact

There was a cybersecurity test of the used system with F-Secure without any findings of vulnerabilities.

There was a need for real-time vessel movement information from the unmanned float-out vessel and the sea trial vessel to the harbor master and assisting tugboats.

The used system/systems were found to be very useful for Meyer Turku in launches and sea trials.

There is an intention and design to create a smart fairway to the shipyard, together with the Port of Turku. Buoys in the shipyard fairway will be replaced with virtual buoys and cameras, including fairway lines, as augmented reality will be added, and all this information will be transferred to tugboats transporting big blocks and whole lower parts of vessels to the shipyard.

All these completed and intended actions will be permanently used in the future, and further development will also be made.

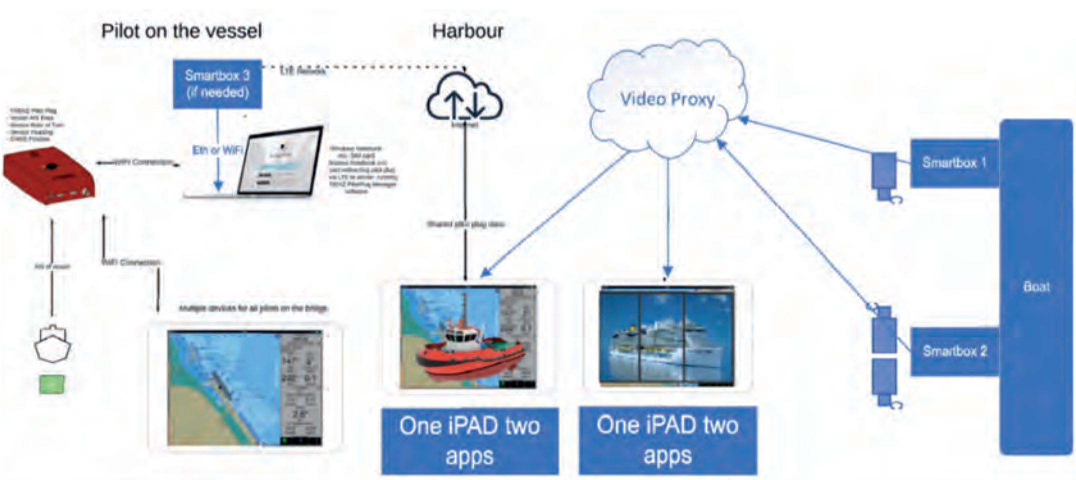


Figure 1.

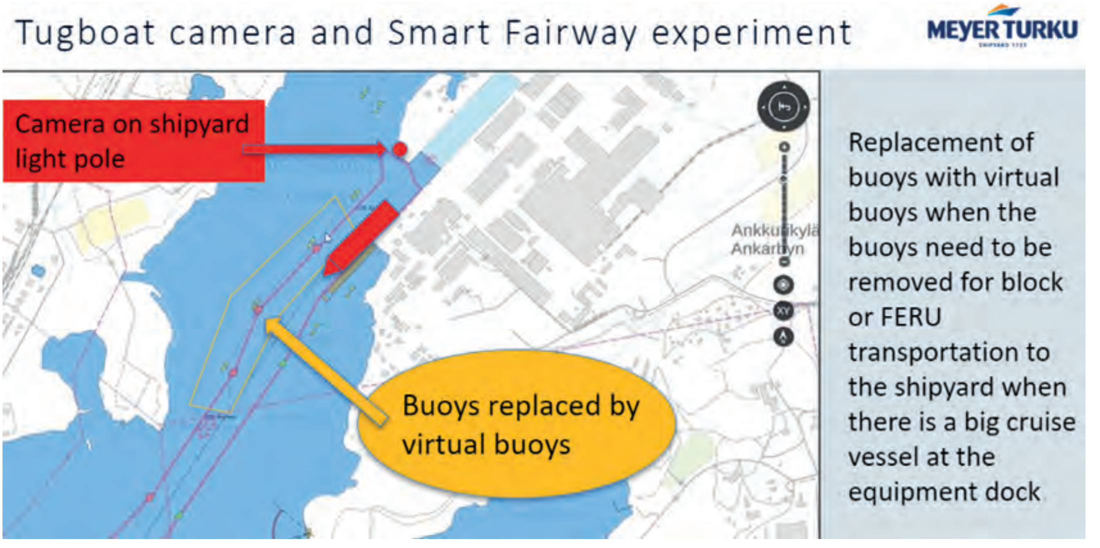


Figure 2.

Figure 3.

Aalto University

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Haltian

Workspace

ETHICS AND HUMAN FACTORS

University of Jyväskylä

The University of Jyväskylä is a nationally and internationally significant research university and an expert on education that focuses on human and natural sciences. JYU brings together education and psychology, natural sciences, humanities and social sciences, sport and health sciences, business and economics, and information technology into a multidisciplinary whole, brimming with the latest knowledge and skills.

The Faculty of Information Technology plays a key role in developing one of the University's core fields: human technology. One of the Faculty's primary strengths is its ability to view IT broadly, integrating various perspectives and identifying the joint effects of different phenomena. This is combined with internationally recognized research in the strategic areas, as well as with active societal interaction. The University of Jyväskylä's empirically oriented AI ethics research has gained international recognition for its empirical orientation and active collaboration with the industry. AI ethics research at the University of Jyväskylä strives to create more human centered and ethically aligned AI systems.

ECCOLA method for designing ethically aware maritime systems

Contributors

- **Ville Vakkuri,** University of Jyväskylä
- **Marianna Jantunen,** University of Jyväskylä
- **Erika Halme,** University of Jyväskylä
- **Mamia Agbese,** University of Jyväskylä
- **Pekka Abrahamsson,** University of Jyväskylä

The future fairway will evidently rely on the digitalization of the maritime industry. Whether it is the higher situational awareness of the fairway provided by the new sensors, or the more extensive communication and network solution for remote pilotage, or the new computational possibilities provided by the AI systems, the application of new technology will change the fairway. In addition, with new technology, new challenges will arise, as technology is never value neutral or error free. The increasing implementation of software for the fairway and for vessels will also introduce new stakeholders, with their own needs and demands, to the fairway and pilotage process. The aim of the ECCOLA method introduced in the following sections is to provide aid in the ethical growing pains of the digitalization of the maritime sector by raising the awareness of ethical challenges related to AI system implementation.

Background

Advances in artificial intelligence (AI) and the deployment of AI-powered systems have made AI a part of our everyday life. These systems are now among us, as AI has grown from the confines of laboratories and is applied in diverse societal and business contexts. Numerous AI applications, from personalized recommendations to autonomous vehicles, have brought AI into the public awareness. Alongside the success stories of AI applications, the need to address ethical considerations related to these systems has become apparent, as numerous AI-related incidents have made news headlines. It is apparent that many of the previously hypothetical threats and ethical issues related to the development, application and use of AI are now a reality. In response, governments, international organizations, and researchers addressed AI ethics through principle-based approaches, and for the past few years, different AI principles and guidelines have been the main way to address ethical issues related to AI applications. This principle-based approach to AI ethics can also be seen in governmental AI strategies, laws, and regulations.

Despite the high popularity of the vastly common AI principles, such as transparency, fairness, non-maleficence, responsibility, accountability, and privacy, the principle-based approach has had its challenges. In particular, AI principles have been criticized for their ambiguity and for lacking in actionability. While principles are at a high abstraction level, tools that can help companies develop their view of ethical AI principles can easily be overlooked in the actual development of the AI systems. For example, software developers have been reported to have struggled with translating abstract ethical guidelines into actions. The lack of actionable methods for implementing AI ethics in practice is a recognized challenge in AI ethics research, although some methods and tools exist. Most of the current methods are specific technical solutions focused on smaller subsets of the AI development process, such as antibias tools. Although these tools can be useful in their specific contexts, they do not consider the AI development process as a whole. Therefore, the question remains about how to influence AI system developers so that they can identify and consider ethical issues in all stages of development, from design to the end of the system lifecycle.

ECCOLA method

To drive the future fairway with higher awareness of AI ethics issues, our research focused on solving the lack of actionable solutions and methods for implementing AI ethics principles in practice. The development of the ECCOLA method was launched to create operational tools similar to ones used in software development to transform philosophical thinking tools and principles into software development practices. ECCOLA was developed using the adaptive and reflective cyclical action research method, which allowed us to meet the agile need of software development and react to the developers' practical needs. Action research allowed us to iteratively test and refine the method to the appropriate maturity needed for industry testing. In developing ECCOLA, three main aspects of feasible and actionable methods were recognized, and these aspects were formulated into goals for the ECCOLA method.

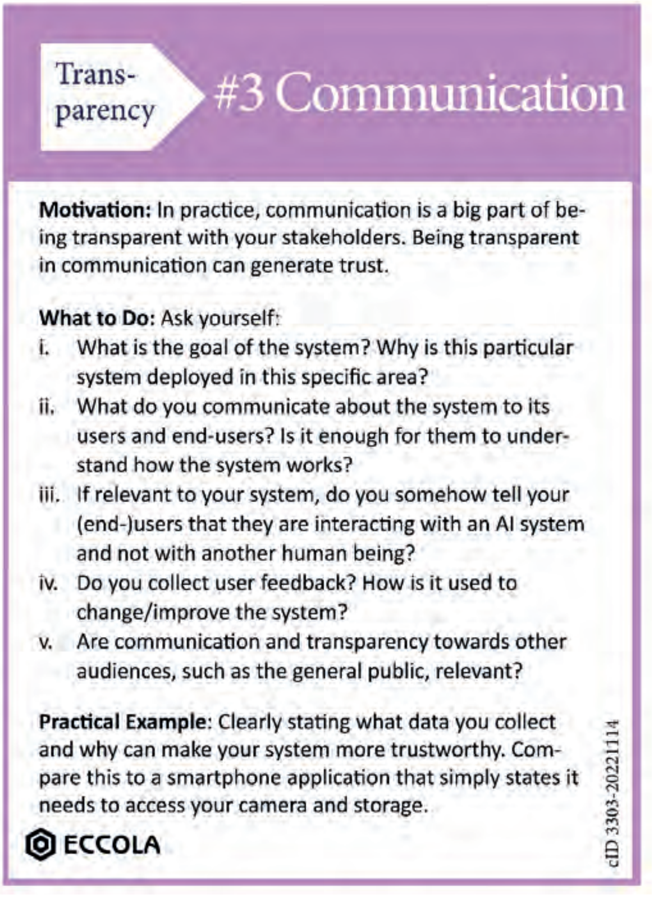
An actionable AI ethics method should:

1. Create awareness of AI ethics and its importance
2. Be a modular method suitable for a wide variety of SE contexts
3. Be suitable for agile development.

Iterative development of ECCOLA gained its mature state in 2021, when it was published for the academic community and public in the distinguished Journal of Systems and Software. This publication described how the ECCOLA method is aimed at software developers to be an actionable tool for implementing [AI] ethics into software development. The method draws from the main topics of AI ethics, aiming to transfer abstract AI ethics principles to be more practical and applicable for development. ECCOLA is presented in the form of 21 cards, to facilitate ethical considerations (*see image 2 ECCOLA card deck*). The cards include eight AI ethics themes, and each theme is divided into one to six subtopics covering a variety of aspects of AI ethics, from auditability to system reliability, and from explainability to wellbeing. The idea is that developers, product managers or even companies acquiring AI systems can utilize the ECCOLA cards to implement the various ethical consideration prompts in software development by using the prompt provided on the cards. Each card is split into three sections: motivation, questions, and practical example (*see image 1 Example card from the ECCOLA method, #3 Communication*).

In use, ECCOLA is a modular, sprint-by-sprint process that has been designed to facilitate ethical thinking in the context of AI and software development. Using ECCOLA is an ongoing process in which you choose the cards you feel are relevant for your work currently and then evaluate the situation again after each sprint. One of the main outcomes of using ECCOLA is a paper trail of choices and trade-offs that documents the ethical consideration conducted during development. This documentation provides a way of evaluating how ethics was perceived in the given development. ECCOLA is intended to be used during the entire design and development process, in a three-step process that is repeated in every iteration.

1. Prepare: Choose the relevant cards for the current sprint.
2. Review: Keep the selected cards at hand during work tasks. Write down on the cards the actions you have taken and the (ethical) discussions you have had.
3. Evaluate: Review to ensure that all the planned actions were taken. Revise the card deck as needed and repeat the process.


Transparency

#3 Communication

Motivation: In practice, communication is a big part of being transparent with your stakeholders. Being transparent in communication can generate trust.

What to Do: Ask yourself:

i. What is the goal of the system? Why is this particular system deployed in this specific area?
ii. What do you communicate about the system to its users and end-users? Is it enough for them to understand how the system works?
iii. If relevant to your system, do you somehow tell your (end-)users that they are interacting with an AI system and not with another human being?
iv. Do you collect user feedback? How is it used to change/improve the system?
v. Are communication and transparency towards other audiences, such as the general public, relevant?

Practical Example: Clearly stating what data you collect and why can make your system more trustworthy. Compare this to a smartphone application that simply states it needs to access your camera and storage.

ECCOLA

cID 3303-20221114

Figure 1. Example of Example card from the ECCOLA method, card #3 Communication.

ECCOLA cards are designed to offer a variety of viewpoints to prompt thoughts during the development process, and the idea is to utilize different cards in different stages of development. The cards should be selected based on the project and tasks at hand, while cards irrelevant to the current situation can be discarded.

In our research, we have recognized three main outcomes of the use of ECCOLA:

1. It raises awareness and provides the needed vocabulary to discuss ethical aspects related to development.
2. It provides space to think and talk about the ethical aspects, as introduction of the method makes ethics an accepted and important topic to focus on as a part of development.
3. It enhances the documentation and especially supports the documentation of ethical considerations that otherwise would be overlooked.

Figure 2. **ECCOLA card deck. Photograph by Kim Kauppinen.**

Result and impact

The ECCOLA method and its applications are the main results of this research. The core idea of the ECCOLA method is that it provides practical aid for people developing software systems (companies) to recognize and address ethical consideration related to their AI systems and IT in general. Therefore, it is no surprise that the feedback from companies utilizing ECCOLA has been positive, and companies have reported ECCO-

LA as being impactful on their views on AI ethics. During the Future Fairway Navigation project, ECCOLA has also been showcased in various academic conferences and field tested in companies working in the maritime domain. Additionally, ECCOLA has been used in project presentations to facilitate discussion around the topic, to bring companies, public officials and researchers together to share their views of the future fairway. Based on the practical experiences and company feedback, it can be said that ECCOLA is an actionable tool with an impact that is not just limited to the maritime domain. Following this work, the natural step in a more ethically aligned future fairway would be to go beyond being ethically aware to being ethically aligned. This can be achieved by raising the overall AI maturity of the industry.

References

- Vakkuri, V., Kemell, K. K., Kultanen, J., Siponen, M., & Abrahamsson, P., 2022. Ethically aligned design of autonomous systems: Industry viewpoint and an empirical study. *Journal of Business Ethics and Organization Studies EJB.*
- Vakkuri, V., Kemell, K. K., Kultanen, J., & Abrahamsson, P., 2020. The current state of industrial practice in artificial intelligence ethics. IEEE Software, 37(4), 50–57.
- Vakkuri, V., & Kemell, K. K., 2019. Implementing AI ethics in practice: An empirical evaluation of the RESOLVEDD strategy. In *International Conference on Software Business* (pp. 260–275). Springer.
- Vakkuri, V., Kemell, K. K., Jantunen, M., Halme, E., & Abrahamsson, P., 2021. ECCOLA—A method for implementing ethically aligned AI systems. *Journal of Systems and Software,* 182, 111067.
- Vakkuri, V., Kemell, K. K., Tolvanen, J., Jantunen, M., Halme, E., & Abrahamsson, P., 2022. How Do Software Companies Deal with Artificial Intelligence Ethics? A Gap Analysis. In Proceedings of the International Conference on Evaluation and Assessment in Software Engineering 2022 (pp. 100-109).
- Vakkuri V., 2022. *Implementing AI ethics in software development*, JYU dissertations 526, 27 May 2022. ISBN 978-951-39-9170-8

From vessel to office – Designing work transformation

Contributors

- **Virpi Roto,** Professor of Practice in Experience Design
- **Aarne Leinonen,** Doctoral researcher
- Aalto University, Department of Design

Background

New innovations emerge from a combination of desirability for people, technological feasibility, and business viability (Brown 2008). DIMECC Sea4Value/Fairway investigated all these aspects, and this chapter focuses on the means to design a solution that is desirable for people.

In this project, Aalto ARTS applied the Service Experience Design approach (Roto & Leinonen 2022) to design work transformation. This approach mixes techniques from service design and experience design and sees the new digital tools as services that can provide meaningful experiences for people. It was developed and tested in parallel in the DIMECC InDEx and Sea4Value/Fairway projects. The phases of this design approach are marked in bold.

The co-design process started with a multi-stakeholder workshop in which the needs of maritime pilots and captains were at the center. In this project, the **insights** of pilot work were spread to stakeholders by means of the workshop. Through discussion, we clarified the main service components and the stakeholders needed to enable each component (Fig. 1).

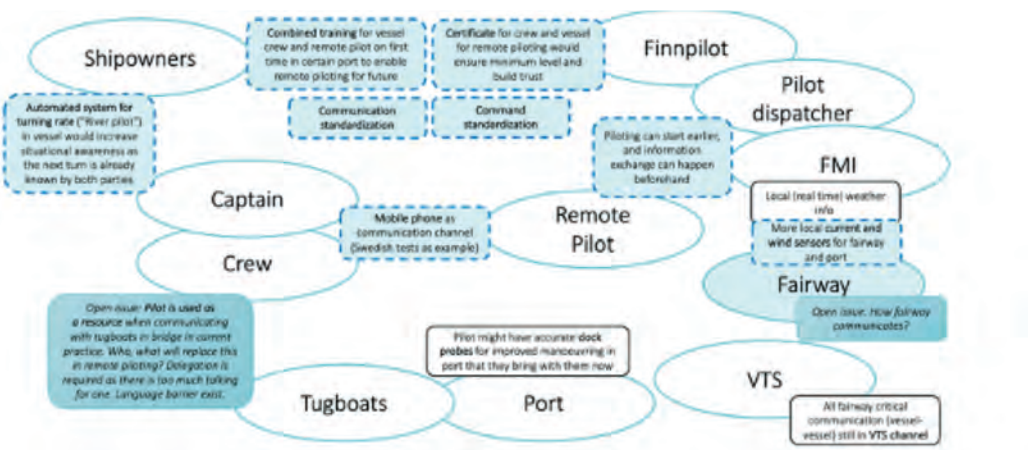


Figure 1. **Early view of the service components required by remote pilots, captains, and crew.**

The workshop opened up several open questions, which, through discussion with project stakeholders, were processed further into a list of assumptions. Each assumption was added to a shared table with a number, a name, status/next steps, and the domain of the project that the assumption concerned. The domains included technology (e.g., real-time traffic information during pilotage); practices related to work transformation (e.g., piloting can start earlier); and mixed (e.g., a feedback loop for messages and commands) for assumptions that require the development of both technology and practices. Some of the assumptions were decided to be outside the scope of this project (e.g., using satellite cameras), but they were kept on the list for the future. Some other assumptions, such as skill certification for vessel crews, remained as topics for the whole project, and were often referred to in discussions on how much trust the remote pilot can have in the crew's skills. The assumptions list thus provided a structure and common language for research and development by many parties in the project, and it acted as a way to reach a common understanding of the scope of the project.

Discussions around the assumptions helped Service Experience Design to define the **customer journey** of the vessel and the **touchpoints** along the remote pilotage service. These were used as the basis for co-designing a service blueprint for remote pilotage. The blueprint provided the first view of the remote pilotage phases and the service contributions needed by the different stakeholders at the backstage of the service journey (Fig. 2).

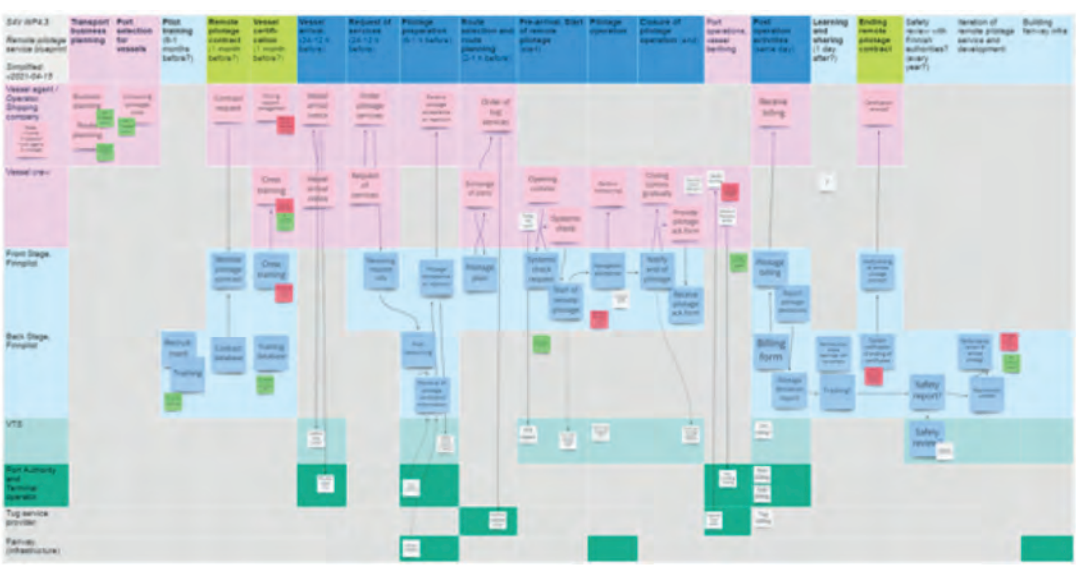


Figure 2. **Overview of the service blueprint for remote pilotage.**

Through a joint roadmapping exercise in the area of operational transformation, we proposed an **experience vision** of humane remote pilotage. This was further developed into a vision statement: "Intelligent systems at people's service, not vice versa." This attitude inspired us to study the in-depth sources of good employee experiences. Several prior studies have shown that meaningful experiences at work are important for improving the employee experience. Rosso et al. (2010) identified a set of sources for meaningful experiences at work, which they call mechanisms of meaningful work. Instead of defining **experience goals**, we used this model in investigating remote pilot experiences. As described in the next section, the results of the investigations showed the needs for **experience actions.** The service blueprint offers building blocks for the **service concept** of remote pilotage, the final step of the Service Experience Design method.

How the pilots experienced remote pilotage

Collecting user experience information for remote pilotage was postponed due to Covid-19, but we managed to interview and survey three pilots on their experiences of remote pilotage simulations in Novia premises, and on the real-life remote pilotage experiment, and to compare these results with their experiences of traditional pilotage. Due to the small sample size of three pilots, the following results are indicative only.

According to qualitative interview data, the three pilots would like to keep some habits from their traditional work in remote pilotage work. For example, they prefer the present rhythm of one week on-duty, one week off-duty. The whole family is used to this rhythm, and moving to shorter daily shifts would mean changing the rhythm of the family. The weekly rhythm preference also means that the location of the remote control center is not that important, if one-way commuting happens just once a week.

In the group interview, the pilots seemed to agree that the best aspects of the work moving to the office include:

- No need for transportation to the piloted vessel and back: comfort and timesaving.
- Increased safety: no dangerous ladder-climbing to the vessel in varying sea conditions.
- No need to be physically fit: office work can be done even with a broken leg.
- New skills: learning future work as a pioneer can be exciting.

On the other hand, the three pilots mentioned some potential downsides of moving to the office:

- Decrease in social contacts: limited contact to the multifaceted vessel crews.
- Safety of the vessels: the remote pilot is safe, but how about the vessel crews?
- New tools introduce new challenges: the best solutions are not here yet.

Although the remote operation station used in the experiment was not a final design and included some challenges with changing delays and usability, the pilots appreciated that the most important functionality was already implemented. They found the camera view from the ship to be very useful as a reference for other data sources, so it would be good to place the camera close to the radar. They also appreciated the good physical ergonomics of the remote operation station.

According to the user experience questionnaire AttrakDiff2, the clearest difference between traditional and remote pilotage was about the social aspect: remote pilotage makes pilots more distant from other people, which is in line with the interview comment on missing the contact with the crews. Naturally, remote pilotage was considered more innovative than traditional pilotage. Both systems were rated as highly technical. Traditional pilotage was seen as more professional, practical, predictable and clear.

We also surveyed the meaningful experiences at work using a short Likert scale for eight statements, asking the three pilots to evaluate traditional pilotage work, the pilotage simulator, and the real-life experiment. The average agreement results (Fig. 3) indicate that pilots feel they are well in control when doing traditional pilotage, while the situational awareness of remote control systems is not yet good enough to create the same level of confidence. The social network at work was not considered very important in any of the conditions. This seems to be in conflict with the other results of the importance of being in social contact with the crews, but apparently the pilots did not consider the crews to be part of the long-term social network at work. While we cannot draw strong conclusions on responses from only three pilots, it seems the remote pilotage work might provide meaningful experiences through improving the life of other people. There is still work to do to make remote pilotage work as meaningful for pilots as traditional pilotage.

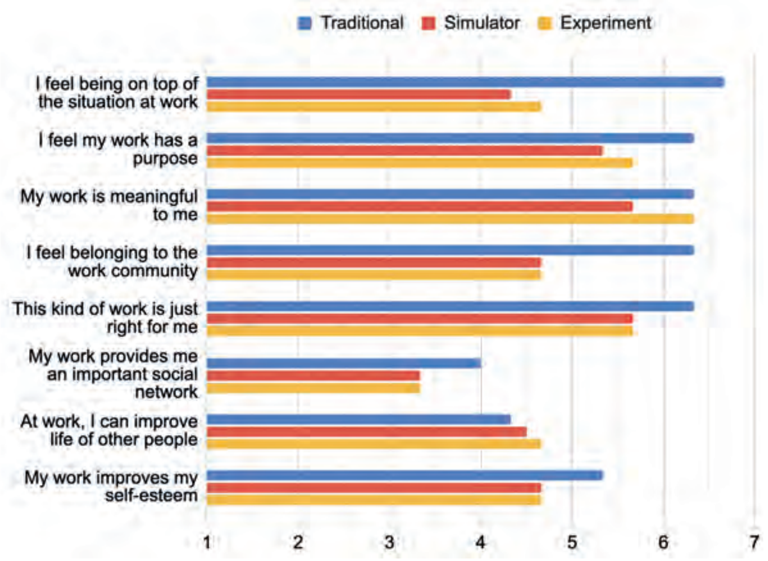


Figure 3. **Meaningful Work questionnaire results for the three pilotage conditions: traditional pilotage on the vessel, remote pilotage with the simulator, and the real-life remote pilotage experiment (1=strongly disagree, 7=strongly agree, average of three pilots' responses).**

Conclusions

By using the Service Experience Design approach, we were able to focus on the remote pilotage service users, and especially on the pilots' perspective of the operational transformation of pilotage work. This design approach can be used in various domains whenever the designers want to bring the best of service design and experience design into one 7-step design approach. As the contexts of design projects change, the technique used in the steps can be adjusted accordingly. For example, in this case, we used Mechanisms of Meaningful Work (Rosso et al. 2010) as the basis for setting experience goals.

According to our small-scale studies, the main experience action would be to pay attention to the social connection between the remote pilot and the ship's crew. This means that the communication protocols between the remote pilot and the ship's crew need to be designed so that they are not only safe, but also allow more free-form social interaction. We are happy to provide more information on the many other results of our interviews and surveys. As the development will continue, we hope the desirability of the systems for people will be considered throughout the development cycles, and the vision of providing intelligent systems as a service for people will be realized.

References

- **Brown, T.** (2008) IDEO Design Thinking. Online resource at https://designthinking.ideo.com
- **Hassenzahl, M., Burmester, M.,** & **Koller, F.** (2003). AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität. In *Mensch & computer 2003* (pp. 187–196). Vieweg + Teubner Verlag.
- **Rosso, B. D., Dekas, K. H.** and **Wrzesniewski, A.** (2010). On the Meaning of Work: A Theoretical Integration and Review. Research in Organizational Behavior 30: 91–127.
- **Roto, V.** & **Leinonen A.** (2022). Service Experience Design. DIMECC InDEx Final Report, pp. 103-108.

The human factor and the sociotechnical system in remote pilotage

Contributors

Haltian:
- Matti Vakkuri

Workspace:
- Mikko Virtaneva
- Nunnu Kotilainen
- Juha Eskelinen
- Pasi Kaitila
- Maria Vihko

Background

Haltian and Workspace have created a visual, dynamic description and design principles of how to improve human performance alongside emerging new technology.

The human factor is an integral part of the work and value creation during remote pilotage service development. Understanding how human factors affect operations, work, and wellbeing provides the means to change, adapt and develop with a changing environment and economy. Haltian and Workspace view remote pilotage as a sociotechnical system, thus providing a broader perspective of the possibilities in developing the social, physical, and technical aspects of pilotage. A human factor is a physical or cognitive property of an individual or a social behavior that may influence the functioning of technological systems. Ideally, organizational goals and human factors can be aligned.

Safe and trustworthy remote pilotage demands much from technology, business, training, and operating culture. Remote pilotage creates a massive change in pilotage service and is a part of the disruptive change of autonomous maritime operations. Remote pilotage is based onshore and, therefore, has a thorough effect on the nature and meaning of work and the personal traits and capabilities needed for remote pilotage. While remote pilotage demands, it also enables different kinds of operational and cultural development, reductions in costs, travel time and emissions, safety in work, flexibility, and predictability.

This work presents dynamic system models and impact assessment logic of the sociotechnical environment and its improvement. It presents a view of what should be focused on when making further remote pilotage service development decisions. This document also provides a visual and verbal description of how to design an excellent operational environment to support human factors and the pilot's performance in remote pilotage stations.

Solution, method

Introduction to the system and the human factor

This work looks at remote pilotage from different system hierarchies, providing means to assess the overall effect on how the system can be developed (Figure 1). In this approach, we aimed to visualize the negative and positive impacts that, for the most part, are created unintentionally and systematically. Systemic modeling tries to model the intricacies of the human factor and demonstrate how there is no simple solution to a complex phenomenon. To provide and argue more concrete solutions, we have used the IOOI model (Figure 2) to support the operationalization of the system and provide tools for more systematic tracking of the development in remote pilotage. This approach uses logic and reasoning to assess the systematic changes that a particular input might provide. To track the changes, we have provided a set of KPIs in this work.

The IOOI-impact mechanism enables the assessment from three perspectives: 1. demonstrating and validating a model from a demonstration, 2. justifying and giving reasons for the impacts and defining the desired outcome(s) and impacts, 3. defining possible shortcomings in the logic or events that might deny the desired positive effects of the system. In this work, we focus mainly on the second and third perspectives, since remote pilotage is not yet an existing service. The focus of this project was to examine the feasibility of remote pilotage and what it requires to be successful.

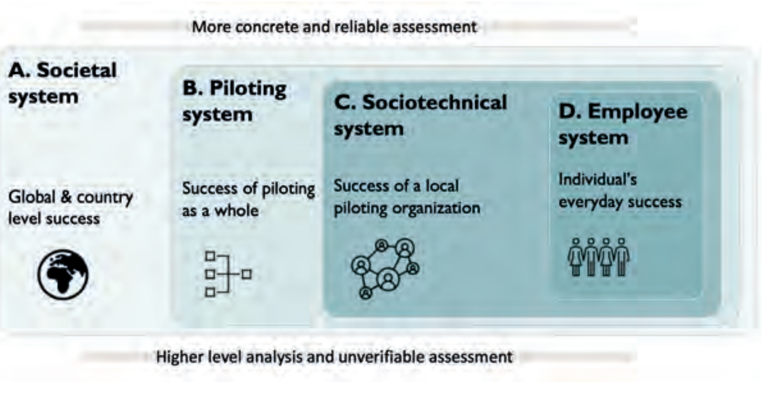


Figure 1. **Systems hierarchy.**

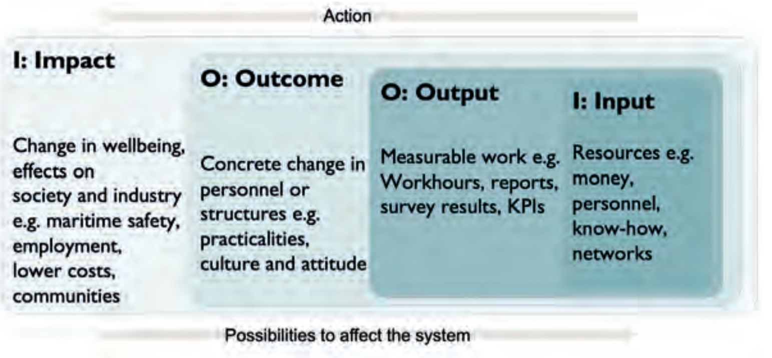


Figure 2. **Adapted IOOI-impact method (Source: The iooi method, Bertelsmann Stiftung).**

Finnpilot's values: trust, learning together, and safety are guiding principles when assessing the human factor aspects in this work.

The values and the human factor are analyzed through three perspectives:

1. Wellbeing
2. Learning together and developing
3. Talent attraction and retention

These perspectives were chosen because they:

- Are critical for the development of remote pilotage (1–3)
- Are critical for everyday performance (1)
- Support everyday performance (1)
- Support strategic development (2&3)
- Are based on Finnpilot's values (2)
- Support human factors in research [1–10]

Remote pilotage is still an ongoing development, and in this work, we will not provide a concrete job design for the remote piloting work, human-machine interfaces, staffing, or training. This work benefits from the work done by other parties in the Sea4Value project in Work Packages 3 & 4, such as Aalto University's work on information flow in piloting, system mapping, and risk assessment; the University of Turku's work on the business; technological and HMI requirements done by Novia and Brighthouse; and Finnpilot's work on providing expertise in piloting.

System analysis

A. Societal system

The phenomenon is the spread of security technologies for fairways

Sea transportation is the cheapest and is an environmentally friendly way to transport cargo (and passengers) compared to other modes of transportation. Due to Finland's remote geographical location, transportation by sea is especially important. It is also challenging since Finnish coastal waters are dangerous to sail in, and piloting and other seafarer safety services are needed.

The success of remote pilotage in Finland connects to the remote pilotage services of other countries. Finland, not to mention a single fairway, is too small an area for ships and technology companies to innovate and develop. How remote pilotage services develop in other countries should also determine what fairway authorities and shipping companies should invest in. When the market and its growth are large enough, technology companies will invest in it.

Consequences

The success of remote pilotage supports the overall development of fairway technologies. The increased safety technology in fairways extends safety to other forms of seafaring. If Finland manages to be at the forefront of fairway technologies, an ecosystem emerges. This ecosystem creates jobs directly in the industry through multiplying effects (indirect jobs) and demand.

Remote piloting enhances trade and industry logistical chains if the new service reduces the time from the fairway to docking and departure. This improvement is possible when: piloting capacity becomes more flexible, less capital is used in shipped cargo, and transportation times are reduced. Other relevant benefits for logistical chains are the safety of pilots and predictability. These benefits increase the more vessels are piloted remotely. One significant benefit of remote pilotage is less usage of fossil fuels.

One of the drawbacks of remote pilotage is the need for fewer personnel and jobs related to traditional pilotage (pilots and pilot boat crew). Possibly pilots are needed less since there is no pilot transportation, thus increasing piloting capacity. However, a new service might provide new work roles and jobs that do not yet exist.

Figure 3. Societal system: safety, environment, economy. (Haltian/Workspace).

B. Piloting system

The effects of growth in remote pilotage

The growth of remote pilotage includes expansion to other countries and vessel types. Growth also comes from the extension of remote pilotage to new fairways and vessels on the Finnish coast (see Figure 4). The benefits and the trust in remote pilotage boost the growth (outcomes on system level B). However, there are limits to growth. The installed base of remotely piloted fairways and vessels decreases the growth potential.

The increase in remote pilotage services drives the growth of the Finnish maritime safety industry. In addition to the traditional hardware and software technology, there are opportunities for engineering and business consulting, training services, and even work environment design. To grow, the Finnish maritime safety industry needs to provide competitive and attractive solutions. The growth of the market attracts competitors. Various forms of government support (such as legal, financial, promotion) for remote pilotage strengthen the growth pf the Finnish maritime safety industry. The willingness to strengthen Finnish maritime safety depends on the potential impact of remote pilotage from economic, societal, and environmental perspectives. This impacts the increase of exports, efficient supply chains for retail and manufacturing, new jobs in the maritime safety industry, and a reduced environmental footprint.

The growth of the Finnish maritime industry generates improved maritime technology solutions. However, the capability to provide new solutions also depends on resources, namely capital and a competent workforce. The competition limits available resources. The development of competitive solutions in the Finnish maritime industry relies on learning from practice and insights from research. Thus, the high level of learning collaboration between the pilotage staff, technology providers, shipping industry, and researchers is essential. This collaboration is a part of the sociotechnical system (system level C). The improved maritime safety technology drives the firms' savings and creates trust in remote pilotage.

The growth of Finnish maritime safety generates exports and jobs. There is also an indirect effect on new jobs through the goods and services purchased from other industries. Jobs maintain and increase the wellbeing of citizens.

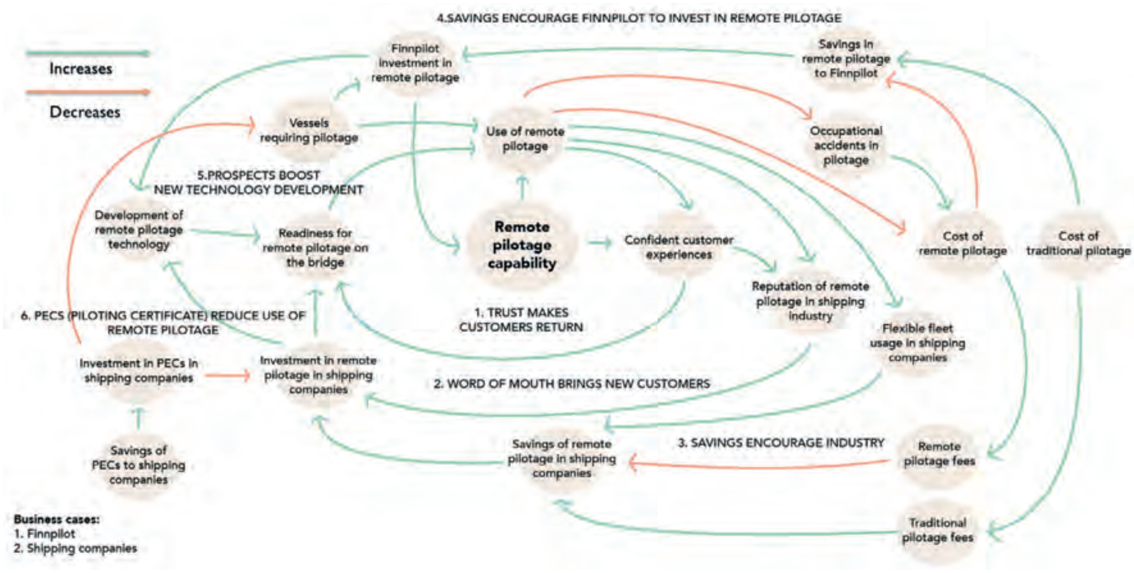


Figure 4. **Finnpilot system map.** (Haltian/Workspace).

The effects of remote pilotage capability

Finnpilot's capability to provide reliable remote pilotage creates positive customer experiences using remote pilotage services, thus improving customer retention. Good experiences improve the reputation of remote pilotage by word of mouth. Companies invest more eagerly in reputable services and measured commercial benefits.

The benefits aggregate mostly from reduced costs (which makes the pricing of remote pilotage a key component), and savings come from other activities regarding remote pilotage. An example of such activity would be more flexible human resourcing and predictable vessel usage (compared to traditional piloting).

Remote piloting needs to have some competitive edge to make it an attractive investment. The possibly reduced operating costs of Finnpilot provide an incentive to invest in remote pilotage. Savings aggregate from fewer personnel, fewer accidents involving people, reduced fuel usage, and possibly a reduced need for transportation vehicles. However, remote pilotage demands investments in training and technology.

C. The sociotechnical system

The sociotechnical system model (Figure 5) describes the dynamic relations between remote pilotage service delivery and the three human factor perspectives: wellbeing, learning and developing, and talent attraction and retention.

Learning and developing

The model describes how learning and developing are essential processes for success. In the model, we can identify four parts of the learning process. Formal learning is done in, for example, simulations or monitored actual operation; learning with customers, in which the pilot learns interacting with the captain and crew; learning with colleagues by sharing information, experiences, views, and other information leading to improvements in performance and community; and learning with stakeholders when developing the service, technology, work environment, and other aspects of remote pilotage.

Intra-role and extra-role are parts of the process of information-sharing and development. Intra-role activities are the core work tasks of the individual, and extra-role activities benefit the bigger picture. The pilots that participate in the Sea4Value project have an important extra-role that helps to develop the whole service.

The starting points for an interaction culture system are the levels of networking, connectivity, a sense of trust, the meaning of collaboration, and power distance. These all affect how much personnel feel psychological safety, an internal motivation to solve problems with others, and share information, and how issues and conflicts are solved. These affect the amount of quality internal interaction, thus how many possibilities there are to learn together in everyday work.

The shared assumptions are the basis of the interaction culture, which is also very strong in the maritime sector and piloting. These assumptions take a long time to change and evolve and are the basis to which someone instinctively refers when feeling ambiguity in a situation.

Talent attraction and retention

The leading theory is that the benefits come from having a good enough resource pool of possible pilots to hire, retaining the existing talent, and having enough pilots to support workload management. Investing in the work environment supports the feeling of appreciation and importance among the personnel and improves motivation. A well-designed work environment also reinforces the brand.

Maintaining wellbeing

The main factors are the workload, strains, and motivation of the pilots. Finding a balance in workload and job resources is essential in managing the strains and recovery, and it has immediate effects on performance and a longer-term impact on motivation. The other socio factors that increase personal resources include responsibility, trust, a good work environment, and a sense of capability. New strains emerge from technostress with new technologies, loneliness, and a sense of loss of control.

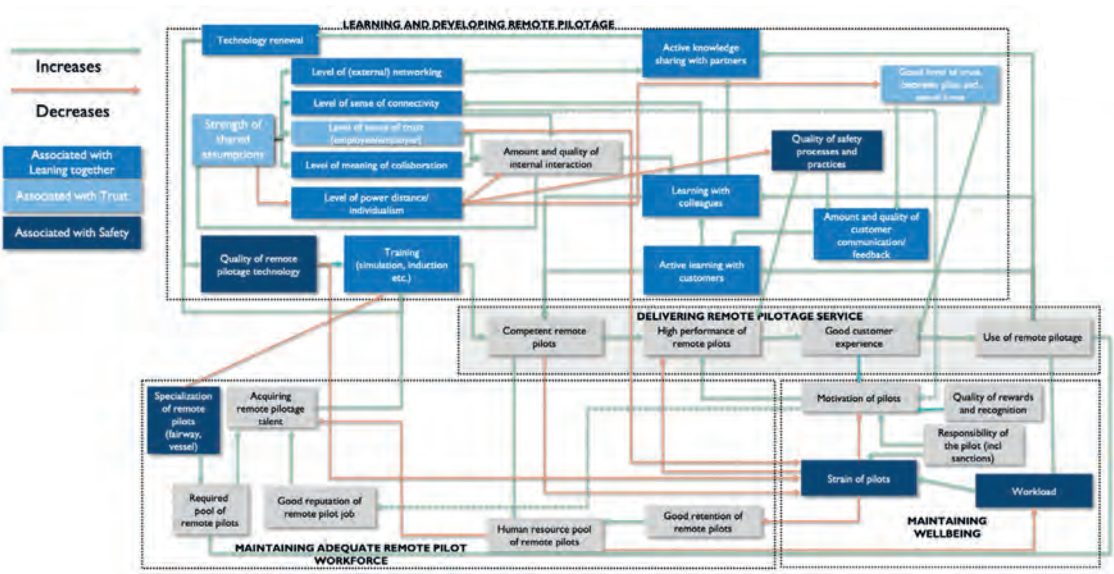


Figure 5. **Pilot and organization system.** (Haltian/Workspace).

The service–profit chain (Figure 6) structures the previous level B (Figure 4) and Finnpilot's remote pilotage service. A good customer experience comes from internal service quality, which provides the means for successful remote piloting.

The factors on the left in the service–profit chain are internal quality factors that can be influenced. These consist of:

- Workplace design (physical, virtual, social), such as remote pilotage workstations and internal communication.
- Job design (how work is conducted, what happens in work). This can be presented as a workday journey.
- Employee selection. What kinds of people are recruited, using what criteria, and where? These affect competence and wellbeing (know-how, motivation).
- Employee development (formal, on-the-job). How is training done, what is learnt on the job, how is the work developed? Providing an efficient learning platform is essential for recruits and promoting continuous learning on-the-job. Development possibilities are a motivational factor, and a lack of capabilities is a strain that can create a negative loop.
- Rewards and recognition. Leadership and feedback loops have a significant effect. However, an individual is very independent in piloting and carries a great responsibility. Are there incentives to develop shared learning from the performance? What kinds of intangible rewards exist (benefits, e.g., services to maintain operational capabilities and recovery)? Remote pilotage causes strain in different ways from traditional pilotage.
- Tools for serving customers with remote pilotage technology. This is probably one of the most important topics. How does technology support remote pilotage, communication connections between the bridge and other parties, situational awareness of location, weather, activities, and other vessels, and other significant factors?
- Internal quality provides know-how and supports wellbeing (motivation, recovery) in a demanding job. Improvements in internal quality result in good work performance in remote piloting and personnel retention. This creates a good customer experience, which enables good experiences from remote pilotage, thus promoting the viability of the whole remote pilotage, which then provides the means to improve internal quality further.

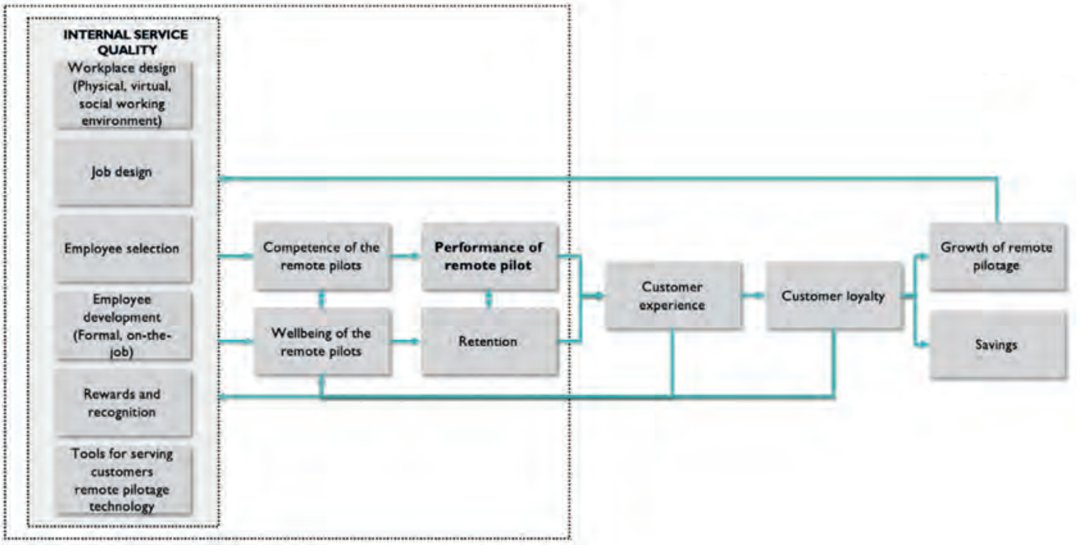


Figure 6. **The service–profit chain and employee system (Heskett et al. 1994).**

Design principles to support functions and the human factor at the station

Remote pilotage is a new service that is still in development, and we have made assumptions regarding the service. We assume that technology and digital work are more relevant in remote pilotage than in traditional piloting. Expertise in seafaring is essential in piloting, and the required skills in remote pilotage will be built on this expertise.

Certain functions change when there is no transportation to the ship, and some functions develop along with the new use of technology. In our workshops, interviews, and discussions with other project partners, we found that remote pilotage requires more intensive focus, provides less direct control of the activities on the ship, and creates more cognitive load. Having a good balance of work–rest times is essential, since fatigue and exhaustion are among the most critical safety human factors. There is no transportation time in remote pilotage, which might lead to higher utilization rates and workload. Remote pilotage also affects the meaning of work for the pilot, since the work is done differently and therefore the demands and strains of the work are also different. The layout design presented is based on present knowledge of maritime pilotage, interviews with pilots working within the Sea4Value project, and shared knowledge among this project's stakeholders.

We then created a grid (Figure 7) to provide a visual tool to understand and prioritize the different work functions at a remote station. The grid also visualizes where it is most beneficial to focus resources to create the most impact. This tool was then discussed and assessed with Finnpilot's pilots. These findings were then transformed to work and space design principles.

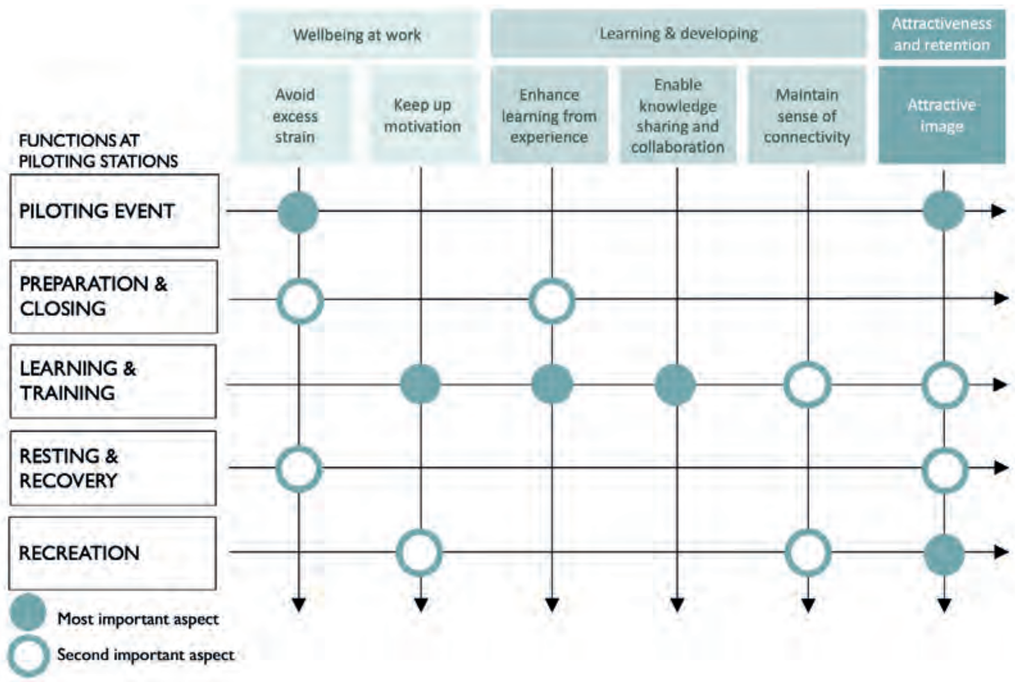


Figure 7. **Functions and objectives in the remote pilotage station.**

Table 1. **Principles of design to develop human factors in space layouts.**

PERSPECTIVES	ORGANIZATIONAL & CULTURAL	WAYS OF WORKING	WORKING ENVIRONMENT
Wellbeing	✓ Trust towards colleagues is created in knowing each other and collaborating ✓ Value oneself, colleagues and organization ✓ Fairness, equality & mutuality ✓ Permission to use all the spaces, feeling of ownership in the premises	✓ Respect the serenity of your colleagues' working hours ✓ The role and content of the work is built according to abilities to avoid stress ✓ Active stress control together with colleagues and organization ✓ Develop social relationships and cooperation ✓ Logical communication inside the organization ✓ Intense collaboration between health care and personnel	✓ Ergonomics, such as lighting, acoustics, temperature, air and furniture are designed to be adjustable by individual ✓ Working desks are situated in a visually and acoustically secure way and only necessary items are in the space ✓ Static working is prevented with necessary guidance of ergonomic furniture such as balance chairs and height adjustable desks ✓ Space is logical and has a clean desk policy ✓ Coffee breaks and preparing meals is enabled in the kitchen
Learning & developing	✓ Shared view of house rules and goals ✓ Participation & feeling of ownership ✓ Collaboration is important but individual accountability is necessary ✓ Motivation to share information	✓ Learn from experience, from methods, from partners ✓ Time is reserved to learn and develop oneself ✓ Easy access to learning methods and space	✓ Possibility to mentor and share information enhances the feeling of trust ✓ Variety of spaces to ad hoc innovate & mentor ✓ Convertible and mobile space to train and learn ✓ Multipurpose space for team and project work ✓ Functional meeting spaces and equipment ✓ Additional accessories such as writing boards and screens to enable easy sharing of information ✓ Stress-free area for rest
Attractiveness	✓ Trust towards organization is supported by honesty, concern for welfare, good quality work environment and design	✓ Possibilities to influence	✓ Variety of workstations to enable different tasks ✓ Guarantee adequate amount of silent space and phone booths ✓ Working cafe provides many varied and unofficial meeting spots to increase collaboration and building of trust to colleagues ✓ Logical and well-organized layout is easy to navigate ✓ Transparent way of working and equity in space usage ✓ Easy to use and reliable booking system and technology ✓ Space is linear to expectations

Work environment designs

Remote pilotage will provide a novel way to pilot. It also frees piloting from a specific location, while expertise in the local area remains essential. Remote pilotage is part of the process of autonomous shipping, which benefits from or even requires being developed in tight collaboration with stakeholders developing smart fairways and technology on ships. The spatially different stations answer to different needs during the development phases of autonomous maritime operations. Furthermore, there will most likely be a different combination of station types, and they are not mutually exclusive.

In the initial steps, single fairway stations will most likely be viable, since the Finnish coastline is very demanding to pilot, and each pilot has licenses for specific fairways. This argument is further supported by the pragmatic requirements between traditional and remote pilotage. In this station type, the competencies are strongly linked to the fairway the station serves.

When remote pilotage advances alongside smart fairways, it will be possible to present a more centralized model. Pilots will remote pilot the same fairways as they would traditionally, but the actual remote piloting can be done from a more remote station. This makes it possible to have larger, more centralized stations to support the development of piloting communities, sharing and aggregating remote pilotage knowledge and experiences. In this station type, the competence base starts to broaden, and the community strengthens.

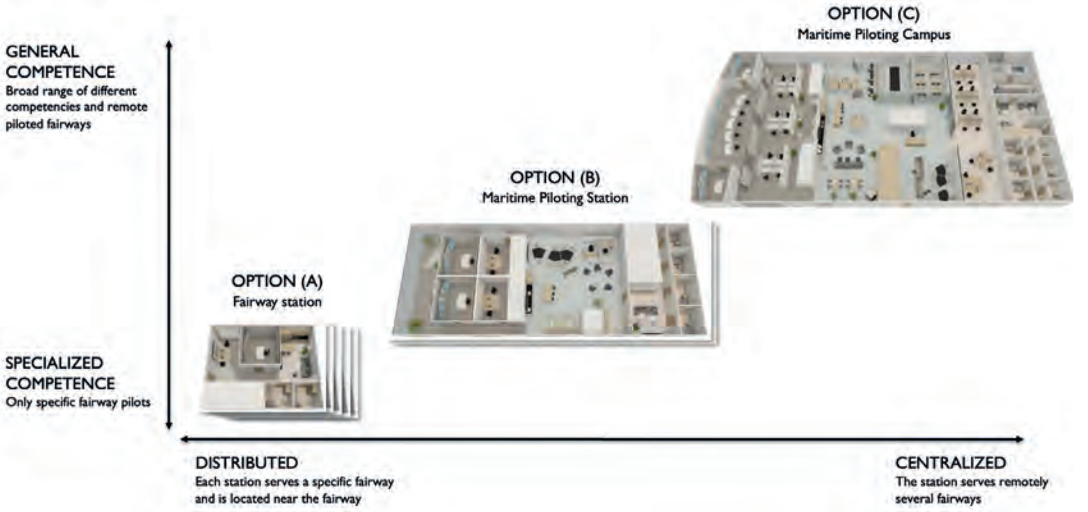


Figure 8. **The three levels of working environments.**

The third model presents a more holistic version of remote piloting stations. The Maritime Campus is a central station where all maritime stakeholders can work in the shared work environment. The main benefits are the networking and innovation possibilities this environment offers, with a broad range of competencies. However, in this model, the piloting requirements are still a priority, and pilots have their own area reserved for them. Remote piloting is done in the proximity of the operating center in an acoustically isolated remote pilotage workstation.

Table 2. **How the spatially different layouts affect human factors.**



PERSPECTIVES	Fairway Station	Maritime Piloting Station	Maritime Campus
Wellbeing	+ Good quality work environment to support traditional and remote pilotage + Has all required spaces to support individual performance and wellbeing - Limited possibilities to support recreational activities	+ Good possibilities to support recreational activities + Good possibilities to network internally and support community development + Possibly good services near-by and good accessibility + Good work environment to support traditional and remote pilotage + Spaces support motivation thru feeling of appreciation and meeting the demands of work - Possible strain coming from extra-role activities	+ Best possibility to support recreational activities + Good possibilities to network and influence + Good services near Campus and accessibility + Good work environment to support traditional and remote pilotage + Good possibilities to support community development + Spaces support motivation thru feeling of appreciation and meeting the demands of work - Possible strain coming from extra-role activities - Finding and maintaining an adequate good work-recovery balance
Learning & developing	+ Separated spaces concentration and collaboration - Focuses on individual performance - Only for few people which will not have a great effect on wider learning and development	+ Spaces to support internal networking, learning and development + Different spaces for different work tasks - Extra-role activities affect how working time must be managed	+ Spaces to support wider piloting and maritime cultural development + Spaces to support internal & external networking, learning and development + Different spaces for different work tasks + Training and simulation facilities - Extra-role activities affect how working time must be managed - Learning and development requires more precise goal-setting in a multi-organizational layout
Attractiveness	+ Good quality work environment to support traditional and remote pilotage	+ Better possibilities to influence, participate, and network bring more meaning to work + Quality and variety of spaces	+ Better possibilities to influence, participate, and network bring more meaning to work + Possibilities to present new meanings of work to remote pilotage + Quality and variety of spaces improve when working in a larger shared work environment + Different skills and competences mix in shared environment - Different than current piloting stations

Examples of the spaces in the stations according to piloting functions

Piloting space

The guiding principle is space design.

Sense of security

- Working desks are situated securely, and only necessary items are in the space.
- The space is easy to adapt, logical, and has a clean desk policy.
- Coffee/kitchen facilities and toilets are situated nearby.

- A technically well-equipped room with a reliable connection and easy-to-use equipment.
- Accessories such as speakers, in addition to screens and wormholes, increase the awareness of the situation at sea.

Learning and developing

- the possibility to mentor and share/obtain information

Attractiveness and retention

- Ergonomics, such as lighting, acoustics, temperature, air, and furniture, are designed to be individually adjustable.
- Furniture such as balance chairs and height-adjustable desks.
- There is a possibility to sit, stand, and take a walk.
- Static working is prevented with necessary guidance in ergonomics.

Figure 9. **Piloting event space.**

Preparation and closing

The guiding principle is space design.

Sense of security

- Working desks are situated securely, and only necessary items are in the space.

- The space is easy to adapt, logical, and has a clean desk policy.
- Coffee/kitchen facilities and toilets are situated nearby.
- A technically well-equipped room with a reliable connection and easy-to-use equipment.
- Accessories such as speakers, screens, and wormholes increase awareness of the situation at sea.

Learning and developing

- The possibility to mentor and share/obtain information.

Attractiveness and retention

- Ergonomics, such as lighting, acoustics, temperature, air, and furniture, are designed to be individually adjustable.
- Furniture such as balance chairs and height-adjustable desks.
- There is a possibility to sit, stand, and take a walk.
- Static working is prevented with necessary guidance in ergonomics.

Figures 10 & 11. **Preparation and closing spaces (above: open version; below: closed version).**

Resting and recovery spaces

The guiding principle is space design.

Sense of security

- A private space for personnel who stay overnight.
- The space is easy to adapt, logical and clean.
- Persons who stay overnight have their own room during on-call duty.

Learning and developing

- The living room provides ventilation and easy talking with colleagues in spare time.
- Possibility to play billiards and PlayStation together or individually.

Attractiveness and retention

- A cozy and private living room.
- The space is inviting, inspiring and cozy.
- Possibility to play sport and go to sauna.
- Standard building structures to ensure silence for resting and peaceful sleep.

Figure 12. **Resting and recovery spaces.**

Learning and training spaces

The guiding principle is space design.

Sense of security

- A technically well-equipped space with reliable connections, wormholes to the sea, and easy-to-use equipment.

- The working cafe provides many varied and unofficial meeting spots to increase collaboration and trust between colleagues.
- Guarantees an adequate number of silent spaces and phone booths.

Learning and developing

- Possibility to mentor and collaborate ad hoc.
- Writing boards and screens to share information.
- Multipurpose space for team and project work.
- Multifunctional meeting spaces and equipment.
- Convertible and mobile space to train and learn.
- Transparent way of working and the space hides no secrets.

Attractiveness and retention

- The working cafe offers a variety of spaces and functions in addition to a good cup of coffee.
- The space is inviting, inspiring and open to everybody.
- House rules to support working roles.

Figure 13. **Learning and training spaces.**

Recreational spaces

The guiding principle is space design.

Sense of security

- Private space for personnel who stay overnight.
- The space is easy to adapt, logical and clean.

Learning and developing

- Possibility to take a break during working hours to lower stress.

Attractiveness and retention

- House rules to maintain attractiveness.
- The space is inviting, inspiring and cozy.
- Possibility to play sport and go to sauna.
- Standard building structures to ensure silence.
- Basic gym and sport.

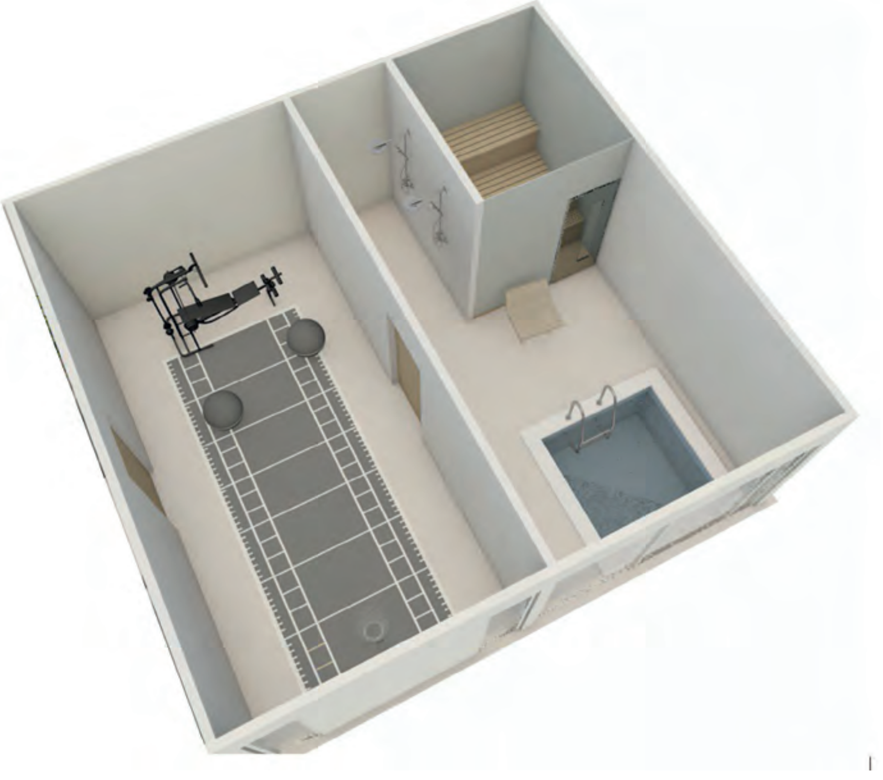


Figure 14. **Recreation spaces.**

KPIs for supporting remote pilotage development

The idea behind the KPIs is to support the development of remote pilotage and human factors. In a fundamental development model, the process is: 1. plan, 2. execute, 3. measure, 4. improve. This means that the planned and measured phenomena are the ones that focus on providing a prolific base for the development of human factors.

During the Sea4Value project, one of the challenges has been the contingency of remote pilotage. Success depends on many different and significant factors, such as advancements in technology in the fairway, legislation, and economic feasibility, at least in the early years of remote pilotage.

These KPIs are either based on general models of human factor measurement, such as Job Demands – Resources Theory [11], or more precise measuring tools such as The Oldenburg Burnout Inventory [12], or Workspace's expertise in workplace development. The KPIs measure three factors: wellbeing, learning, and attractiveness and retention of talent.

The KPIs we chose for the concept were chosen to support the three human factors. We provided each KPI with:

- A socio factor, e.g. Technostress
- Measurement, e.g. Technostress creators survey
- Is the KPI critical to the early development of the service or does it support a long-term objective
- Justification, application suggestions, and remarks regarding the KPI
- A label for the KPI as a Driving, Monitoring, or Outcome KPI [13]

The socio factors in the KPIs were discussed with other parties in the Sea4Value project, and especially Aalto ENG, whose risk analysis reveals that fatigue and stress are among the most influential sources of risk in the human factors. Workspace and Aalto ARTS found in their interviews with pilots that the cognitive load, utilization rate, and different work environments are some of the main concerns when developing remote pilotage and supporting human factors. In addition, during an interview with pilots, the pilots being interviewed regarded the learning together factor as especially important during the early phases of remote pilotage development.

Below are the KPIs with associated measurements and KPI labels.

Table 3. **Wellbeing KPIs. The ones with * are existing KPIs.**

Socio factor	Measurement	KPI label
Workload	Utilization: pilotage - other work – recovery objectively from register data	**Driving KPI**
Technostress	Technostress creators, embedded in employee survey	**Driving KPI**
Health & safety circumstances	Occupational health survey	**Driving KPI ***
Trust between employees and employer	Perceived trust (embedded in employee survey)	**Driving KPI**
Motivation	E.g. Utrecht Work Engagement Scale, embedded in employee survey	**Monitor KPI**
Fatigue/ Exhaustion	Physio metrics Psychometric e.g. Oldenburg Burnout Inventory, embedded in employee survey	**Monitor KPI**
Accidents on fairway	Accidents per year Accident frequency per one million working hours	**Outcome KPI ***
Sick leaves	Sick leaves/employee Number short term sick leaves/employee	**Outcome KPI ***

Table 4. **Learning and developing KPIs. The ones with * are existing KPIs.**

Socio factor	Measurement	KPI label
Working culture	Culture assessment	**Driving KPI**
Training	Training days/employee /year Simulation days/pilot	**Driving KPI ***
Learning opportunities	Perceived opportunity to learn Perceived level of feedback (Embedded in employee survey)	**Monitor KPI**
Trust between pilot and vessel crew	Customer feedback	**Outcome KPI**
Quality of safety processes and practices	Capability Maturity Model (CMM) based assessment or similar	**Outcome KPI**

Table 5. Talent attraction and retention KPIs.

Socio factor	Measurement	KPI label
Employer image	Internally: Employee NPS (net promoter score) Probably not feasible to measure image/reputation externally	**Driving KPI**
Employee attraction	Candidates (=applications) per vacant position	**Outcome KPI**
Employee retention	Intention to leave (employee survey) Voluntary employee turnover % employees/year	**Outcome KPI**

The KPIs are categorized as either critical or strategic. Critical KPIs are linked to socio factors that need to be successful for remote pilotage to be safe and feasible. Strategic KPIs support the development of human factors and provide a competitive advantage, for example, in performance, wellbeing, and talent attraction. The KPIs are labeled as driving, monitor or outcome. Driving KPIs are applied to change, maintain, and reinforce the desired activity. Monitor KPIs provide information on the functioning of the system and activity. Outcome KPIs track the end results of the activity and process.

Context, mechanism, and outcomes of the key performance indicators

In the wellbeing context, the leading theory is that a balance in job resources and strains reduces the risks associated with fatigue and increases motivation in work. The main socio factors for increasing personal resources include responsibility, trust, balanced utilization rate, good work environment, and sense of capability. The main socio factors for increasing strains include stress from too high utilization, technostress with new technologies, loneliness, and a sense of loss of control.

In the learning together factor, the main benefits come from increased know-how, improved trust through quality interaction and shared experiences, the accumulated organizational understanding, and feedback from personnel and customers. The hindrances in learning together are different social phenomena, such as power distance and individualism, that reduce the motivation to share knowledge and information.

The benefits of the talent retention and attraction factor come from having a good enough resource pool of possible pilots to hire, retaining the existing talent, and having enough pilots to support workload management. Investing in the work environment supports the feeling of appreciation and importance among the personnel and improves motivation. A well-designed work environment also reinforces the brand.

The main factor is wellbeing, which, especially during piloting, reduces risks. Many of the other KPIs support performance in the longer run. The outcomes are primarily measured using Finnpilot's existing KPIs. The most influential one is accidents in fairways. From a wellbeing perspective, a reduction in occupational accidents (in both traditional and remote pilotage) and a reduction in sick leave are the primary outcomes. A more intangible result is higher motivation in work.

Conclusion

This work aimed to create a concept of a sociotechnical system in remote pilotage. We used wellbeing, learning and developing, and talent attraction and retention as focused human factors. We provided system models on four different hierarchies and an impact analysis model to promote the operationalization of the more intangible inputs. As remote pilotage is not yet an established business or service, its development is ambiguous. The business environment is constantly changing; therefore, learning and developing is critical in this scenario, so adapting and evolving as experts and as an organization is increasingly important in the early stages of remote pilotage development. Understanding how human factors affect performance in everyday work and on a larger scale provides tools to strategically develop the remote pilotage service and create pragmatic ways of development.

The maritime sector changes slowly, and many ambiguous factors exist when developing remote pilotage. The service will be built on the expertise of the current pilots and will most likely be a complementary service for a long time. The development will rely on the advancement of fairway technology. From a pilot perspective, remote pilotage creates new strains and stressors. Traditional piloting is very rewarding, since the outcome is easily observable, every piloting event is different, and the work generally has a lot of variety. The competence to meet these changing requirements is one of the main points of pride in the work. Remote pilotage could allow pilots to extend their careers when their physical condition is not at an adequate level, or when there is some physical illness preventing traditional pilotage, or it could attract a new generation of pilots who are more interested in remote pilotage than traditional. We provided three different remote pilotage station types to provide possibilities to develop remote pilotage as a single fairway service and as an integral part of all maritime services as the technology on fairways advances. In addition, the work includes design principles for the main functions performed at remote pilotage stations, to improve the human factor. Lastly, we created key performance indicators for the human factors, to drive and monitor change in the service and track the outcomes.

References

1. Arslan, V., Kurt, R.E., Turan, O. and De Wolff, L., 2016. Safety culture assessment and implementation framework to enhance maritime safety. *Transportation research procedia*, 14, pp.3895–3904.
2. Bakker, A. B. & Demerouti, E., 2017. Job Demands-Resources Theory: Taking Stock and Looking Forward. Journal of Occupational Health Psychology. Vol. 22:3. p. 273–285.
3. Barsan E., Surugiu F., Dragomir C.: Factors of Human Resources Competitiveness in Maritime Transport. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 6, No. 1, pp. 89–92, 2012.
4. Borst, R.T., Kruyen, P.M. and Lako, C.J., 2019. Exploring the job demands–resources model of work engagement in government: Bringing in a psychological perspective. *Review of Public Personnel Administration, 39*(3), pp.372–397.
5. Brooks, B., Coltman, T. and Yang, M., 2016. Technological innovation in the maritime industry: The case of remote pilotage and enhanced navigational assistance. *The Journal of Navigation, 69*(4), pp.777–793.
6. Koroma, J. Hyrkkänen, U. & Vartiainen, M., 2014. Looking for people, places and connections: hindrances when working in multiple locations: a review. New Technology, Work and Employment. Vol 29:2.
7. Lahtinen, J., Banda, O.A.V., Kujala, P. and Hirdaris, S., 2020. Remote piloting in an intelligent fairway – A paradigm for future pilotage. *Safety Science,* 130, p.104889.
8. Nielsen, K., Nielsen, M. B., Ogbonnaya, C., Känsälä, M., Saari, E. & Isaksson, K. 2017. Workplace resources to improve both employee well-being and performance: A systematic review and meta-analysis. Work & Stress. Vol: 31:2. pp. 101–120.
9. Sexton, J.B. and Klinect, J.R., 2001, May. The link between safety attitudes and observed performance in flight operations. In *Proceedings of the Eleventh International Symposium on Aviation Psychology* (pp. 7–13). Columbus, OH: The Ohio State University.
10. Torrente, P., Salanova, M., Llorens, S. and Schaufeli, W.B., 2012. Teams make it work: How team work engagement mediates between social resources and performance in teams. *Psicothema*, 24(1), pp.106–112.
11. Demerouti, E., Bakker, A. B., Nachreiner, F., & Schaufeli, W. B., 2001. The job demands resources model of burnout. Journal of Applied Psychology, 86, 499 –512.

- 12. Demerouti, E., Mostert, K., & Bakker, A.B.(2010) Burnout and Work Engagement: A Thorough Investigation of the Independency of Both Constructs Journal of Occupational Health Psychology. 15(3), 209–222.
- 13. Valdez Banda, O. A., Hänninen, M., Lappalainen, J., Kujala, P., & Goerlandt, F., 2016. A method for extracting key performance indicators from maritime safety management norms. WMU Journal of maritime affairs, 15(2), 237–265.
- 14. Heskett, J., L., et al. 1994. Putting the service-profit chain to work. Harvard business review. 72(2), 164–174.

PUBLICATIONS

Aalto University

- **Baldauf M., Fröhlich P., Sadeghian S., Palanque P., Roto V., Ju W., Baillie L.** and **Tscheligi M.**, 2021. *Automation Experience at the Workplace.* In CHI-Conference on Human Factors in Computing Systems Extended Abstracts (CHI'21 Extended Abstracts),May 8–3, 2021, Yokohama, Japan. ACM, NewYork, NY, USA, 6 pages. https://doi.org/10.1145/3411763.3441332

- **Baldauf M., Fröhlich P., Roto V., Palanque P., Lindley S., Rogers J., Ju W.,** and **Tscheligi, M.**, 2022. *Engaging with Automation: Understanding and Designing for Operation, Appropriation, and Behaviour Change.* In CHI-Conference on Human Factors in Computing Systems, Extended Abstracts (CHI'22 Extended Abstracts), April 29–May 5, 2022, New Orleans, LA, USA. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3491101.3503735

- **Basnet,S., Chaal, M., Bahootoroody, A., Valdez Banda, O. A.,** & **Lahtinen, J.**, 2021. ***Selection of Model Based System Engineering Language for Ship pilotage.*** *First International Conference on the Stability and Safety of Ships and Ocean Vehicles (STAB&S 2021).*

- **Basnet, S., Bahootoroody, A., Chaal, M., Valdez Banda, O. A., Lahtinen, J.,** & **Kujala, P.**, 2022. *A decision-making framework for selecting an MBSE language – A case study to ship pilotage.* *Expert Systems with Applications,* 193, 116451.

- **Basnet,S., Bahootoroody, A., Chaal, M., Lahtinen, J., Bolbot, V.,** & **Valdez Banda, O. A.**, 2023. *Risk analysis methodology using STPA-based Bayesian network- Applied to Remote Pilotage Operation.* Ocean Engineering, 270, [113569]. https://doi.org/10.1016/j.oceaneng.2022.113569

- **Bolbot, V., Basnet,S., Zhao, H., Valdez Banda, O., Silverajan, B.**,2022. *Investigating a novel approach for cybersecurity risk analysis with application to remote pilotage operations,* in: Presented at the European Workshop on Maritime Systems Resilience and Security 2022 (MARESEC 2022), Zenodo. https://doi.org/10.5281/zenodo.7143998

- **Chaal, M., Valdez Banda, O. A., Glomsrud, J. A., Basnet, S., Hirdaris, S.,** & **Kujala, P.,** 2020. *A framework to model the STPA hierarchical control structure of an autonomous ship*. *Safety Science,* 132, 104939.
- **Chaal, M., Bahootoroody, A., Basnet, S., Valdez Banda, O. A.,** & **Goerlandt, F.**, 2022. *Towards system-theoretic risk assessment for future ships: A framework for selecting Risk Control Options. Ocean Engineering,* 259, 111797.
- **Cockbill S., Mitchell V., Roto V., Lee J-J., Lai Chong La E.**, 2022. *Introduction to Service Design for UX Designers.* CHI EA '22: Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems, April 2022, Article No.: 143, 3 Pages, https://doi.org/10.1145/3491101.3503762
- **Lee J-J., Ee Ling Yap, C.**, and **Roto V.**, 2022. *How HCI Adopts Service Design: Unpacking current perceptions and scopes of service design in HCI and identifying future opportunities.* In CHI-Conference on Human Factors in Computing Systems (CHI'22), April 29 – May 05, 2022, New Orleans, LA, USA. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3491102.3502128
- **Roto V.**, 2021. *Käyttäjäkokemusten muotoilu älykkäässä ja eettisessä teollisuudessa.* Chapter in the book Muotoilun avaimet 2021. Publisher Teknologiateollisuus ry, Helsinki 2021. ISBN 978-952-238-264-1, ISBN 978-952-238-265-8 (ePub)
- **Roto, V., Lee J-J., Lai-Chong Law, E., Zimmerman J.**, 2021, *The Overlaps and Boundaries Between Service Design and User Experience Design,* DIS '21, June 28–July 02, 2021, Virtual Event, USA. https://doi.org/10.1145/3461778.3462058
- **Roto V.**, 2021. *Automation Experience at the Workplace – Playing the 80's Record.* CEUR Workshop Proceedings, Volume 2905.
- **Roto V., Bragge J., Lu Y., Pacauskas, D.**, 2021. *Mapping experience research across disciplines: who, where, when.* Quality and User Experience (2021) 6:7. https://doi.org/10.1007/s41233-021-00047-4
- **Roto V., Larusdottir M., Lucero A., Stage J.**, and **Smorgun I.**, 2021. *Focus, Structure, Reflection! Integrating User-Centred Design and Design Sprint.* Human-Computer Interaction – INTERACT 2021: 18th IFIP TC 13 International Conference, Proceedings pp. 239–258.

- **Roto, V., Lee, J. J., Lai-Chong Law, E.** & **Zimmerman, J.**, 2021. *The Overlaps and Boundaries between Service Design and User Experience Design.* DIS 2021– Proceedings of the 2021 ACM Designing Interactive Systems Conference: Nowhere and Everywhere. **Ju, W., Oehlberg, L., Follmer, S., Fox, S.** & **Kuznetsov, S.** (eds.). ACM, p. 1915–1926 12 p.

- **Valdez Banda, O. A., Laine, V., Lappalainen, J., Basnet, S., Chaal, M.,** & **Owen, D.**, 2021. *Risk management framework for smart shipping services: a case study in e-piloting.* In *2021 6th International Conference on Transportation Information and Safety* (ICTIS) (pp. 1370–1376). IEEE.

in progress at the time of the final report

- **Basnet,S., Bahootoroody, A., Chaal, M., Bolbot, V., Montewka, J., Valdez Banda, O. A.,** & **Ziajka, E.** (N.D) 2023, Decision-making on the selection of Risk Control Options using Influence Diagrams- Applied to remote pilotage operation.

- **Basnet, S.,** Risk management framework for advanced maritime ecosystems: Applied to Remote pilotage Operation, Doctoral Thesis.

University of Jyväskylä

- **Hummelholm A., Pöyhönen J., Kovanen T., Lehto M.,** 2021. *Cyber Security Analysis for Ships in Remote Environment.* Proceedings of the 20th European Conference on Cyber Warfare and Security, ECCWS2021, p. 169–177.

- **Kovanen T., Pöyhönen J., Lehto M.,** 2021. *Cyber Threat Analysis in the Remote Pilotage System.* Proceedings 20th European Conference on Cyber Warfare and Security, ECCWS2021, p. 221–229.

- **Kovanen T., Pöyhönen J., Lehto M.,** 2021. *ePilotage System of Systems' Cyber Threat Impact Evaluation* Proceedings of the 16th International Conference on Cyber Warfare and Security, ICCWS2021, p. 144–153.

- **Kovanen T.,** 2021. *Cyber-threat aspects in a complex system-of-systems environment: A case study in remote pilotage.* Doctoral theses University of Jyväskylä. https://jyx.jyu.fi/bitstream/handle/123456789/77501/1/978-951-39-8771-8_vaitos03092021.pdf

- Pöyhönen J., Kovanen T. and Lehto M, 2021. *Basic Elements of Cyber Security for an Automated Remote Fairway System.* Proceedings of the 16th International Conference on Cyber Warfare and Security, ICCWS2021, p. 299–308.

- Pöyhönen J. & Lehto M., 2022. *Assessment of cyber security risks – Maritime automated piloting process.* the 17th International Conference on Information Warfare and Security, ICCWS2022, p. 262–271.

- Pöyhönen J., Hummelholm A. & Lehto M., 2022. *Cyber security risks assessment subjects in information* Proceedings of the 21st European Conference on Cyber Warfare and Security ECCWS2022, p. 222–230.

- Vakkuri, V., Kemell, K.-K., Kultanen, J., & Abrahamsson, P. 2020. *The Current State of Industrial Practice in Artificial Intelligence Ethics.* IEEE Software, 37(4), 50–5

- Vakkuri, V., Kemell, K.-K., Jantunen, M., Halme, E., & Abrahamsson, P., 2021. *ECCOLA : a method for implementing ethically aligned AI systems.* *Journal of Systems and Software, 182*, Article 111067. https://doi.org/10.1016/j.jss.2021.111067

- Vakkuri, V., Jantunen, M., Halme, E., Kemell, K.-K., Nguyen-Duc, A., Mikkonen, T., & Abrahamsson, P., 2021. *Time for AI (Ethics) maturity model is now.* In H. Espinoza, J. McDermid, X. Huang, M. Castillo-Effen, X. C. Chen, J. Hernandez-Orallo, S. OhEigeartaigh, & R. Mallah (Eds.), *SafeAI 2021 : Proceedings of the 2021 Workshop on Artificial Intelligence Safety.* RWTH Aachen. CEUR Workshop Proceedings, 2808. http://ceur-ws.org/Vol-2808/Paper_16.pdf

- Vakkuri, V., Kemell, K. K., Tolvanen, J., Jantunen, M., Halme, E., & Abrahamsson, P., 2022. How Do Software Companies Deal with Artificial Intelligence Ethics? A Gap Analysis. In Proceedings of the International Conference on Evaluation and Assessment in Software Engineering 2022 (pp. 100–109).

- Vakkuri, V., Kemell, K. K., Kultanen, J., Siponen, M., & Abrahamsson, P., 2022. Ethically aligned design of autonomous systems: Industry viewpoint and an empirical study. Journal of Business Ethics and Organization Studies EJB.

- Vakkuri V., 2022. Implementing AI ethics in software development, JYU dissertations 526, 27 May 2022. ISBN 978-951-39-9170-8 Doctoral theses University of Jyväskylä.

Tampere University

- **Asif Khan M., Hamila R., Erbad A.,** and **Gabbouj M.**, 2022. *Distributed Inference in Resource-Constrained IoT for Real-Time Video Surveillance*, IEEE Systems Journal, DOI: 10.1109/JSYST.2022.3198711, August 2022.

- **Bolbot V, Basnet S., Zhao H., Valdez Banda O.**, and **Silverajan B.**, 2022. *Investigating a novel approach for cybersecurity risk analysis with application to remote pilotage operations,* European Workshop on Maritime Systems Resilience and Security (MARESEC 2022), June 2022.

- **Furumoto K., Kolehmainen A., Silverajan B., Takahashi T., Inoue D.,** and **Nakao K.**, 2020, *Toward Automated Smart Ships: Designing Effective Cyber Risk Management,* International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), 2020, pp. 100-105. DOI: https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00034

- **Kolehmainen A., Komu M., Javid S., Kjällman J., Kauppinen T., Ghavimi, F.,** and **Silverajan B.**, 2022, *Benchmarking of Emulated Wireless Edge Cloud Connectivity for Maritime Environments.* IEEE 8th World Forum on Internet of Things (WF-IoT). October 2022.

- **Peña Queralta J., Taipalmaa J., Can Pullinen B., Kathan Sarker V., Nguyen Gia T., Tenhunen H., Gabbouj M., Raitoharju J.**, and **Westerlund T.**, 2020. *Collaborative Multi-Robot Search and Rescue: Planning, Coordination, Perception and Active Vision*, *IEEE Access,* pp. 191617 – 191643, October 2020.

- **Viitanen L.**, 2022, *Security Properties of HTTP/3*, Bachelor's Thesis, Tampere University, March 2022.

- **Zhao H., Silverajan B.**, 2020. *A Dynamic Visualization Platform for Operational Maritime Cybersecurity.* In: Luo Y. (eds) Cooperative Design, Visualization, and Engineering. CDVE 2020. Lecture Notes in Computer Science, vol 12341. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-60816-3_23

- Zhao H., and Bilhanan Silverajan B., 2022, *Visual Cybersecurity Collaboration and Incident Exchange in Multi-Stakeholder IoT Environments,* 2022 IEEE International conference on Internet of things (iThings), August 2022.

- Zhao H., and Silverajan B., 2022, *Enhancing LwM2M for Operational Cybersecurity and Situational Awareness in Industrial IoT*, IEEE 8th World Forum on Internet of Things (WF-IoT). October 2022.

- Zhao H., Shafeitel-Tähtinen T., Verkkosaari H., Helenius M., and Silverajan B., 2022, *Security Dashboard Design for Non-Experts in Sigfox-based Smart Spaces*, , IEEE 8th World Forum on Internet of Things (WF-IoT). October 2022.

- Zhang F., Jiang X., Xia Z., Gabbouj M., Jinye Peng, and Xiaoyi Feng, 2022. *Non-Local Color Compensation Network for Intrinsic Image Decomposition*, *IEEE Transactions on Circuits and Systems for Video Technology*, 10.1109/TCSVT.2022.3199428, 17 August 2022.

in progress at the time of the final report

- Can Pullinen B., Kiranyaz S., and Gabbouj M., "*Hybrid Self-Organized Operational Neural Networks for Semantic Segmentation in Maritime and Harbour Scenes*," manuscript under preparation.

- Silverajan B., Laaroussi Z., and Novo O., "*Measuring QUIC and CoAP Performance in Maritime Scenarios*," Conference paper under preparation.

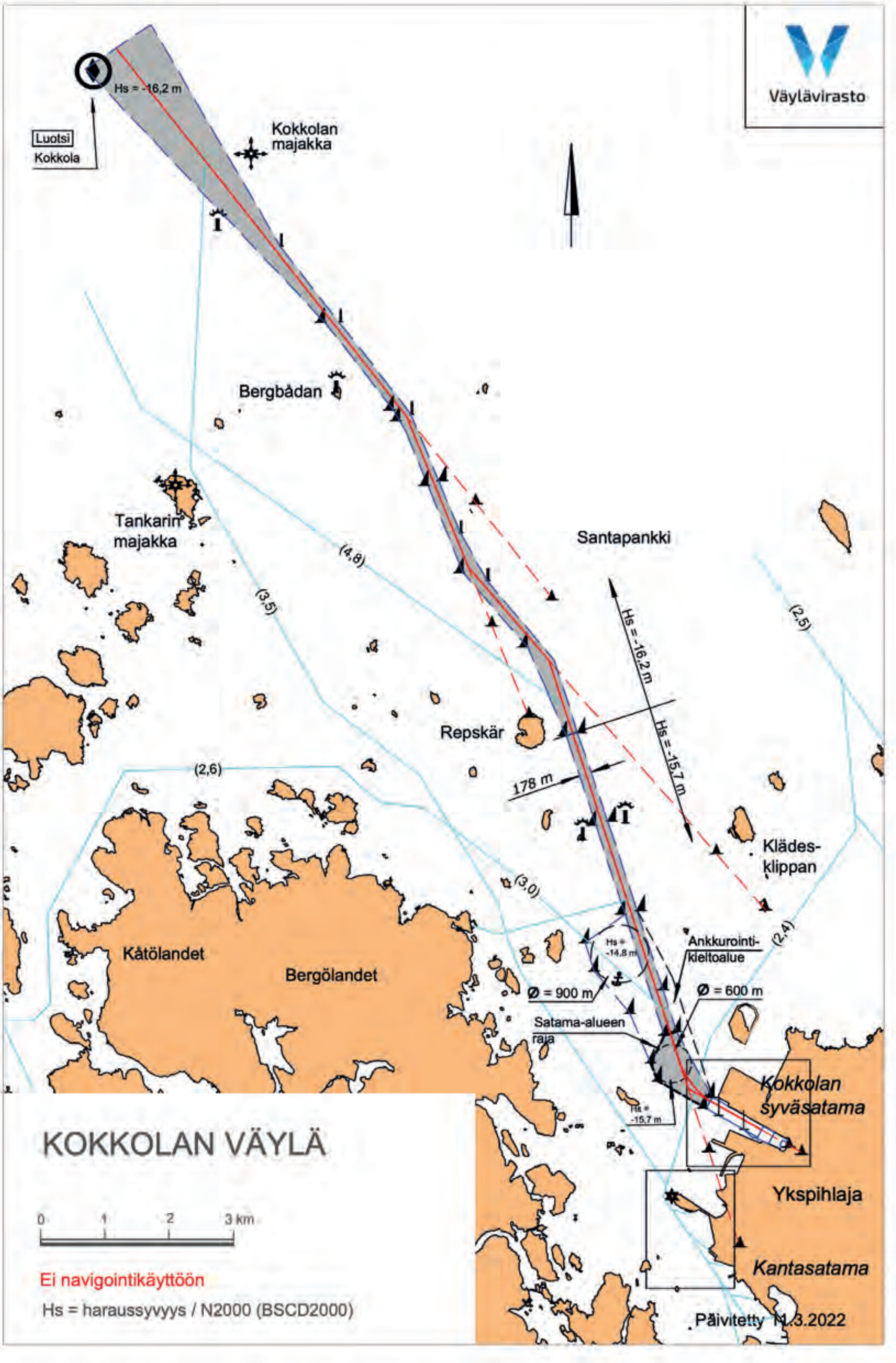
- Can Pullinen B., *Neural Networks Based Semantic Segmentation*, Doctoral Thesis, Tampere University.

- Kolehmainen A., *Edge infrastructure testbeds as tools for understanding security anomalies in IoT and beyond*, Doctoral Thesis, Tampere University.

- Hanning Zhao, *Novel Dynamic Visualization Methods for Cybersecurity Management of IoT Devices and Networks*, Doctoral Thesis, Tampere University.

University of Turku

- Heikkilä M., Saarni, J, Himmanen H., Heikkilä, J., 2022. *Smart Fairways – Co-design of future intelligent fairways in Finland*, presentation in International Maritime and Port Technology and Development Conference (MTEC) & 4th International Conference on Maritime Autonomous Surface Ships (ICMASS), 6.4.2022 Singapore.
- Heikkilä, J., Heikkilä, M., Märtz, G., 2023. *Platforms for Smart Fairways - Enhancing Services for Autonomous Maritime Traffic and Other Emerging Uses of Territorial Sea*, Hawaii International Conference on System Sciences HICSS, 2023
- Vaahtikari, Jussi, 2021. *Etäluotsauksen juridisia karikkoja kartoittamassa: Sopimuksen ulkopuolinen vahingonkorvausvastuu etäluotsauksessa*. Master Thesis, University of Turku. https://urn.fi/URN:NBN:fi-fe2022013111390



The first ship equipped with the technology of future fairway services was directed from the Port of Kokkola to the fairway. Image: Finnish Transport Infrastructure Agency

DIMECC Oy

Åkerlundinkatu 8, 33100 Tampere, Finland

Eteläranta 10, 00130 Helsinki, Finland

Citykulma, Yliopistonkatu 31, 20100 Turku, Finland

www.dimecc.com

DIMECC Program
Sea4Value – Future Fairway Navigation

ISBN 978-952-238-298-6
ISBN 978-952-238-299-3 (pdf)

DIMECC Publications series