Reliability Engineering and System Safety 234 (2023) 109195

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Development and testing of a risk-based control system for autonomous ships

Thomas Johansen [a,b,*], Simon Blindheim [a,c], Tobias Rye Torben [a,b], Ingrid Bouwer Utne [a,b], Tor Arne Johansen [a,c], Asgeir J. Sørensen [a,b]

[a] Centre for Autonomous Marine Operations and Systems (NTNU AMOS), NTNU, Norway
[b] Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, 7491, Norway
[c] Department of Engineering Cybernetics, Norwegian University of Science and Technology (NTNU), Trondheim, 7491, Norway

ARTICLE INFO

Keywords:
Autonomous systems
Risk modeling
Ship control systems
Systems theoretic process analysis (STPA)
Bayesian belief networks
Verification

ABSTRACT

This paper presents a method for designing and verifying a control system with risk-based decision-making capabilities to improve its intelligence and enhance the safe operation of autonomous systems. The decision-making capabilities are improved, compared to existing control systems, using a Bayesian Belief Network (BBN) that is derived from the systems theoretic process analysis (STPA) as a foundation for an online risk model, which represents the operational risk for an autonomous ship. Combined with an electronic navigational chart (ENC) module to get accurate information about the environment, this enables the ship to operate in a safe and efficient manner. In addition, the control system is verified against safety and performance requirements using a formal verification method, based on temporal logic and Gaussian processes. The proposed methodology is tested in a case study where the system's behavior is compared with an existing conventional (manned) ship on experimental data from two routes along the coast. The case study shows that the performance of the Supervisory Risk Controller (SRC) with respect to the autonomous ship speed and maneuvering is similar to how the existing ship is operated. This means that the proposed methodology shows promising results with respect to developing autonomous ships with control systems and leads to intelligent and safe behavior.

1. Introduction

Although conventional ships have control systems for navigation, maneuvering, and power management, they are designed to rely on human input and supervision onboard. For example, Dynamic Positioning (DP) systems are used to maintain a ship's position or to maneuver the ship at low speeds with good accuracy. Nevertheless, a human operator must specify the mission and be ready to take over control if the automatic system fails. Power management systems (PMS) also have a high degree of automation to control electric power generation, power distribution, and prevent blackouts on ships.

There is currently no automation system that monitors or controls the complete ship's operation, replacing the crew onboard. For example, engine control systems may monitor the engine and shut it down if there is a failure, even if this compromises the safety and integrity of the ship. An example is the Viking Sky incident, where the diesel generators were automatically shutdown due to low lubrication oil levels in a severe sea state, which led to a complete blackout and nearly caused the cruise ship with almost 1400 people onboard to ground in storm conditions [1]. In general, for a ship to operate safely and autonomously, its control systems must be able to assess risk (currently the task of the crew onboard conventional ships). Hence, Utne et al. [2] propose a control system framework that can assess and manage risk, replacing some of the cognitive judgements that the crew would normally make while sailing to improve the autonomous ship's decision making. Thieme et al. [3] describe how risk analysis methods can be integrated with control systems and identify four areas for implementing this. Another approach is further demonstrated in Johansen and Utne [4]. A risk model represented by a Bayesian Belief Network (BBN), which is based on a systems theoretic process analysis (STPA), assesses navigational risks for an autonomous cargo ship while sailing as part of a supervisory risk controller (SRC) for high-level control of the ship. This risk model provides information that can be used as a basis for selecting the control mode, machinery mode, and setting control objectives while sailing. Bremnes et al. [5,6] presented a similar control system for autonomous underwater vehicles (AUVs) for under ice operations. In this case, the SRC was used to set the altitude set-point, velocity set-point, and control strategy such that the AUV could avoid collision while performing under-ice mapping with sufficient accuracy.

Relevant risk factors have also been discussed in Fan et al. [7]. A framework to identify navigational risk factors for autonomous ships is presented, but without any further application. Chang et al. [8]

* Corresponding author at: Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, 7491, Norway.
E-mail address: tjoha@ntnu.no (T. Johansen).

https://doi.org/10.1016/j.ress.2023.109195
Received 13 July 2022; Received in revised form 1 February 2023; Accepted 21 February 2023
Available online 24 February 2023

Nomenclature

AIS	Automatic Identification System	LNG	Liquefied Natural Gas
AMMS	Autonomous Machinery Management System	Mech	Mechanical
ANS	Autonomous Navigation System	MPC	Model Predictive Control
AP	Autopilot	MSO	Machinery System Operating
API	Application Programming Interface	PMS	Power Management System
AUV	Autonomous Underwater Vehicle	PTI	Power Take In
BBN	Bayesian Belief Network	PTO	Power Take Out
CONOPS	Concept of Operations	RIF	Risk Influencing Factor
CPT	Conditional Probability Table	ROC	Remote Operation Center
DP	Dynamic Positioning	SLAM	Simultaneous Localization and Mapping
ENC	Electronic Navigational Chart	SO	Ship Operating
FMEA	Failure Mode and Effects Analysis	SRC	Supervisory Risk Controller
GNSS	Global Navigational Satellite System	STL	Signal Temporal Logic
GP	Gaussian Process	STPA	System Theoretic Process Analysis
H-RIF	High-level Risk Influencing Factor	UCA	Unsafe Control Action
HiL	Hardware-in-the-Loop	USD	United States Dollar
HSG	Hybrid Shaft Generator	VHF	Very High Frequency
I-RIF	Input Risk Influencing Factor		

combine Failure Mode and Effects Analysis (FMEA) with evidental reasoning and Bayesian Networks to quantify the risk level of major hazards related to autonomous ships. Johansen and Utne [9] propose to use STPA to identify potential hazards for autonomous ships and discuss some methods for finding additional quantitative data to use in a risk model, but without building and using the model. STPA is also used in Valdez Banda et al. [10] for hazard analysis on autonomous passenger ferries. This paper suggests safety controls to mitigate the identified hazards when designing the ship. Wróbel et al. [11] use STPA to develop a model to analyze safety and make design recommendations for autonomous vessels. Chaal et al. [12] propose a framework to model the ship control structure, based on STPA that can be useful to describe the functionality of the system.

Risk models have also been used to predict the loss of AUVs during missions [13–15] and to manage uncertainty in these missions [16]. However, none of these models are connected or implemented as part of the control system. Other papers have discussed risk as part of collision avoidance but use risk in a very general term and lack a direct link to risk analysis and risk modeling [17–22]. Combining some selected risk aspects with Model Predictive Control (MPC) has also been proposed for collision avoidance systems [23,24] and emergency management but the risk metrics that are used in these studies are not based on risk assessment and are simplified so that they can be used in an MPC application [25].

A quantitative risk model can provide good and useful information got an autonomous control system if it includes reliable information about the ship's position and its surroundings. One option is to use tools such as Simultaneous Localization and Mapping (SLAM) that can be used for AUVs [26–28] operating in areas where localization and mapping are challenging. Mapping the environment is unnecessary for autonomous ships because position data are available from global navigational satellite systems (GNSSs), such as position and speed measurements, and electronic navigational charts (ENC) are available. GNSS measurements are already used in control systems, such as in DP controllers to provide position and speed measurements. ENC data have been used in decision making systems, such as path planners, for ship navigation [29]. The data can then be used directly in the planner, with limitations on extracting and presenting the data. To address these limitations, Blindheim and Johansen [30] developed an open-source application programming interface (API) to process and display the data with high accuracy and in short computation time. Their paper shows how the API can be used for certain tasks, such as path planning based on a dynamic risk optimization. A simple risk metric based on wind speed and direction, and the distance to land is used when planning the route.

Developing better control systems is an important step towards realizing autonomous ships, which in turn is expected to improve safety at sea [31,32]. However, it is important to demonstrate that these ships are safe in operation to achieve approval from the authorities and public acceptance. This means that autonomous ships need to be tested in various scenarios and environmental conditions. Today, verification, validation, and certification in the maritime industry depend on type of ship and operation. On advanced offshore installations and ships, the ship and control system are thoroughly tested through simulations, scale testing, sea-trials, and Hardware-in-the-Loop (HiL) testing. Extensive and thorough tests are necessary to get the systems approved by class societies and coastal states [33]. Suppliers usually test individual components on less advanced ships during commissioning and sea-trials.

The shift towards autonomous ships presents several challenges with respect to verification and testing. Both the complexity and criticality of the software systems increase. In addition, the control system interacts with a highly dynamic and unstructured operative environment, which causes the span of possible scenarios to become enormous. Autonomous systems typically use machine-learning software to some extent, which introduces its own set of challenges (see Torben et al. [34]). Therefore, there is a need for new methodology to formalize and scale the verification and testing efforts to new levels.

Several recent works have aimed to address these challenges. For example, Pedersen et al. [35] propose a test system for autonomous navigation systems (ANSs) and show how it can be used to verify the performance of a collision avoidance system. Torben et al. [36] present an Autonomous Simulation-based testing framework and show how it can be used to verify a collision avoidance system. Xiao et al. [37] propose a quantitative evaluation method to evaluate obstacle avoidance methods for unmanned ships. These studies indicate that although the test systems work, they only work through testing a very limited part of the control system. They also lack a description of how the testing should be integrated into the design process for autonomous ship control systems.

To summarize the gaps identified in the current literature, it is necessary integrate risk with control systems intended for autonomous ships to improve its high level decision making. In addition, these control systems need access to data from ENCs, and they need to be

verified in a formal and systematic manner to ensure the necessary safety and performance. Hence, the overall objective of this paper is to present a novel and interdisciplinary methodology to develop an SRC for high level control of autonomous ships that bridges risk modeling, optimization, ENC, and formalized verification to achieve safer and more intelligent performance of autonomous ships.

The proposed methodology is tested and compared to an existing conventional-manned ship for different coastal routes to assess how the SRC handles failures in the ship's machinery and propulsion system. The main scientific contribution is the demonstration of how the intelligence of an autonomous control system can be improved by combining thorough risk analysis and modeling, detailed data from navigational charts, and novel verification methodology. Compared to existing control systems, this new approach makes it possible to handle a wider range of operations and situations, which reduces the need for human intervention and supervision. Even though the application in this paper is focused on autonomous surface ships, it is expected that the methodology will have relevance for other autonomous applications. A similar methodology might also be used to assist operators by providing additional decision support by assessing how the risk level changes leading to safer ship operations.

The rest of this paper is organized as follows. Section 2 presents the methodology for building and setting up the controller. Section 3 describes the case study. Section 4.1 and Section 4.2 present the results from the case study. Sections 4.3–4.7 discuss how risk can be included in control systems, how to use ENC data, how to test the system, and it also describes some uncertainties in the controller and risk model. Section 5 concludes this paper and outlines further work towards highly autonomous ships.

2. Method

The SRC controller is developed through a five-step process, as shown in Fig. 1. The SRC enables the controller to make risk informed decisions that emphasize both safety and efficiency when operating the ship. These decisions can (for example) determine the ship's operating machinery mode, control mode, or the speed reference for the proposed control system.

The ship and the operation are first described in detail and analyzed using an extended STPA to identify hazardous events that need to be included in the risk model. Thus, the STPA results are used as the basis for building the online risk model in step 2, which is represented here in terms of a BBN. The justification for using STPA combined with BBN is presented in Utne et al. [2]. For situation awareness, the risk model uses data from the ship's sensors and the control system to assess the current conditions. The ENC module is used to extract data from navigational charts with information about the area surrounding the ship. The ENC model is set up in step 3 based on the design requirements to provide the necessary data to the risk model and SRC. The SRC is then developed in step 4 based on the requirements identified in the system analysis and the STPA (step 1), and using data from both the risk model and ENC. Finally, the controller is verified against the performance requirements using the automatic simulation-based testing methodology.

2.1. Step 1: System description and STPA

To setup and build the control system, the ship and operation have to be described and analyzed, such as in terms of a CONOPS (concept of operations). This starts by clearly describing the ship, how it is controlled, its technical condition, and characterization of the operation that it is used for. In terms of control, it is important to know what type of controllers the ship has or will have, how they are connected, and their different responsibilities. Human operators or supervisors (e.g., onshore in a control center) must also be described with information about how they can control or affect the ship. Describing the ship's operation requires a clear statement of why and where the ship is sailing, as well as its operating modes. For example, a coastal cargo ship sailing along the Norwegian coast may be very different to a passenger ferry sailing between islands in the Mediterranean Sea.

The decisions or control actions relevant for the SRC must also be specified. These are important to consider because they are the only options for the SRC to affect the control of the ship. After describing the ship, STPA can be used to identify potential hazards, causal factors, and safety constraints. The STPA follows the steps defined in Leveson [38] but is expanded to also explicitly consider the consequences of the hazardous events and system-level hazards as follows:

(a) Define the system
(b) Identify hazardous events and system-level hazards
(c) Identify unsafe control actions (UCAs)
(d) Develop loss scenarios
(e) Analyze consequences

The description of the ship can be used as a basis for the first step of STPA, and is a basis for defining the control structure and assigning responsibilities to the different controllers in the system. The next step is to identify hazardous events and to identify UCAs. These are subsequently described in loss scenarios that may lead to UCAs. Scenarios also include how decisions, such as selecting the wrong control mode or using machinery systems with failures, can lead to UCAs. The decisions are included in the same way as risk influencing factors (RIFs). The final part is to describe and classify the potential consequences of the hazardous events (e.g., through cost estimations).

2.2. Step 2: Online risk model

The online risk model is built based on the STPA results and follows the emerging top-down structure, like the results of the analysis, as shown in Fig. 2. The BBN has six main types of nodes:

- Consequences
- Hazardous events
- System-level hazards
- UCAs
- RIFs
- Decisions

The end node in the BBN is the consequences. These are caused by the hazardous events, under given conditions. The hazardous events are caused by one or more system-level hazards identified in the STPA. The next is the UCAs that lead to system-level hazards. UCAs get an input from RIFs that describe the loss scenarios and the conditions where hazardous events have negative consequences. RIFs can be both high-level RIFs (H-RIFs) and input RIFs (I-RIFs), as shown in Fig. 2. For a more detailed description of mapping STPA results to a BBN, the reader is referred to Utne et al. [2] or Johansen and Utne [4]. For a detailed description of BBNs in general, the reader is referred to Fenton and Neil [39].

The BBN is converted to an online risk model by deciding how to update the BBN as the ship sails with online information. This links specific nodes to sensors and systems onboard the ship, and then decides which data are necessary, including the ENC module. Decisions made in the SRC are also included in the BBN to model how they affect the risk picture and consequences. The BBN can also have intermediate nodes to group I-RIFs and decisions to reduce the number of nodes that are connected to each H-RIF. This is more important for larger and more complicated BBNs.

2.3. Step 3: ENC module

The ENC module extracts and manipulate data from electronic navigational charts. These data are necessary in the risk model to

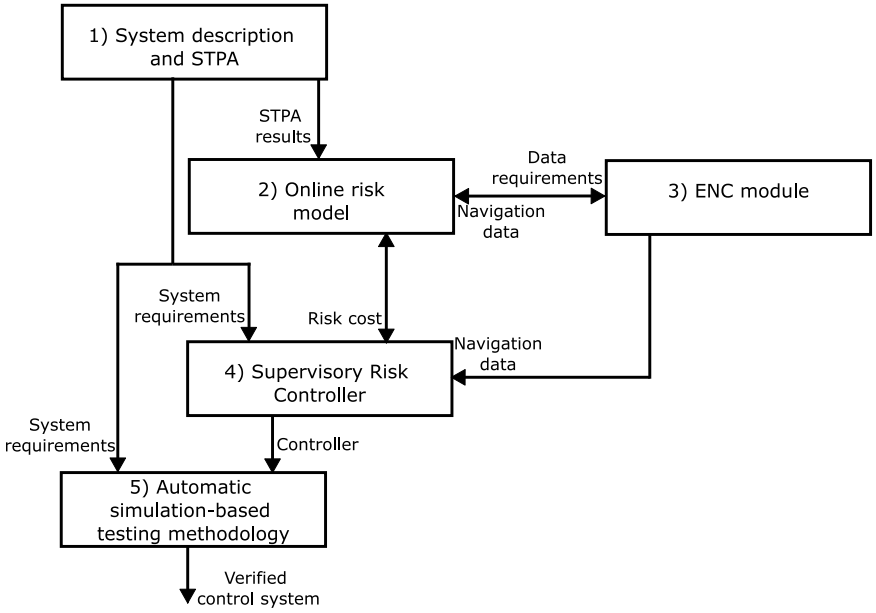


Fig. 1. Methodology flowchart.

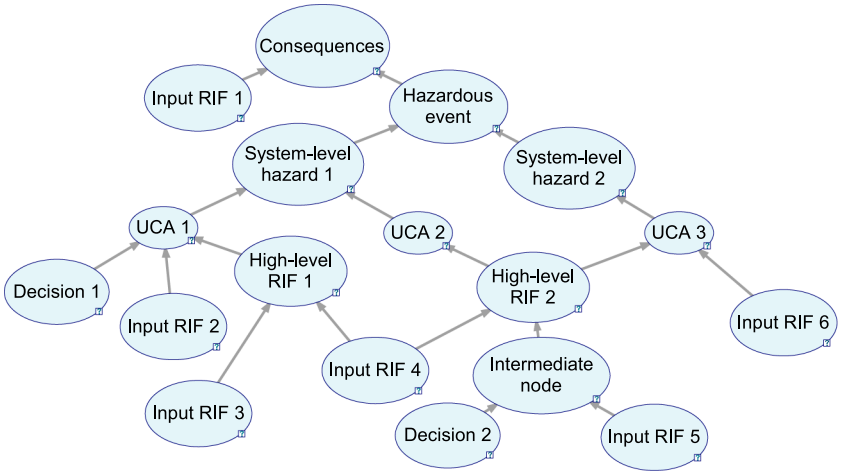


Fig. 2. Example BBN structure, showing how the STPA is linked to the BBN and how different nodes are related .
Source: Adopted from Utne et al. [2].

describe the surroundings and conditions around the ship. The ENC module is based on the open-source Python package SeaCharts [30]. This package use FGDB 10.0 data sets with 2D data of the relevant areas. These are then processed as the application starts, so that they can be stored as shapefiles, where only the relevant depth layers and land areas are stored. This allows for much faster processing because it reduces the time necessary for computation and/or querying. The data is stored as polygons for various water depths and land areas. The stored shapefiles can then be queried to find the distance to points where the ship can collide or ground, and assess how much space the ship needs to maneuver.

The ENC module is set up by first loading the necessary maps for the relevant area. The next step is to define and load relevant layers for the ENC module, depending on the ship and data needed in the control system. This is achieved by defining the minimum water depth that the ship must maintain for safe sailing. To avoid unnecessary quantities of information in the risk model, a planning horizon is set in the ENC to decide how far the ENC should look ahead of the ship. This limits the data size that the ENC must query and reduces the computation time. Connecting the ENC module with the risk model is done by connecting the relevant nodes and updating them with data from the ENC, such as distance to land and shallow areas, combined with position and speed measurements from the GNSS system.

The current ENC module does not account for navigation markers, as this is not currently implemented in the SeaCharts package. This is discussed more in Section 4.5. For a detailed description of the package and all functions, the reader is referred to Blindheim and Johansen [30].

2.4. Step 4: Supervisory risk controller

The controller is set up as an SRC to make high-level decisions or set control objectives. One option is to use costs as a means for implementing the inputs from the risk model into the decision making. For other potential options, see Thieme et al. [3].

For an autonomous ship controller, decisions can be made based on four costs: the risk cost from the online risk model, fuel cost based on the expected fuel consumption, operation costs (other than fuel), and the cost of not starting new missions. The total cost is calculated

using Eq. (1) as a function of the decisions, d, such as setting the speed reference and deciding how the machinery should be operated:

$$C(d) = R(d) + F(d) + O(d) + L(d) \quad (1)$$

The risk cost, $R(d)$, gives the expected cost from the consequences described in the risk model and account for factors such as weather conditions, ship speed, traffic conditions, etc. Fuel cost, $F(d)$, describes the expected cost of fuel of operating the ship under the current conditions. Operation cost, $O(d)$, describes the costs of operating the ship, outside of fuel cost, such as maintenance, insurance, and manning costs. $L(d)$ describes the potential loss of future income caused by the time used. The cost function is set up such that fuel cost, operation cost, and potential loss of future income increase if the ship takes a longer time to reach the final way-point.

The controller checks each possible set of decisions to find the set with the lowest cost. The decisions can vary depending on the ship and can include selecting what machinery mode to use, how the ship should be controlled, and which speed reference to follow. The SRC configures the control of the ship according to the set with the lowest cost.

2.5. Step 5: Automatic simulation-based testing methodology

Step five verifies the controller against a set of design requirements related to safety and efficiency. The verification process is performed using the automatic simulation-based testing methodology from Torben et al. [36]. This methodology automatically runs simulations where the vessel is sailing along its planned route, while varying scenario parameters. The methodology formulates requirements using the Signal Temporal Logic (STL) formal specification language, which enables automatic evaluation of the simulations against the requirements [40]. The result of evaluating a simulation against an STL requirement is an STL robustness score that describes how robustly the requirement is satisfied. If the STL score is greater than zero, then the requirement is satisfied. If it is less than zero, then the requirement is violated.

The methodology selects the simulations to run from a test space that is defined by a set of scenario parameters with corresponding parameter spaces. The test space can, for example, be based on scenarios that are identified in the STPA [41–43] to test the controller in specific situations. A Gaussian Process (GP) model [44] is used to predict the STL robustness score as an unknown function of the test case parameters. The GP model estimates the expected value and the uncertainty of STL robustness over the entire parameter space of a test case. The GP model is iteratively updated by running simulations and observing the resulting STL robustness score. The estimates of the GP model are then used to adaptively guide the test case selection towards cases with low STL robustness or high uncertainty. This results in efficient coverage of the parameter space or alternatively efficient falsification if the controller does not satisfy the requirements.

The testing terminates in a verified state if the lower confidence interval of the GP is greater than zero for the entire parameter space. For example, using 99% confidence intervals, a verification would indicate that there is at least a 99% probability that the system satisfies the requirement for the entire test space of the test case. Alternatively, if a test case that does not satisfy the requirements is identified, then the verification terminates in a falsified state, returning the corresponding counter-example. For a more detailed explanation of the automatic simulation-based testing methodology, the reader is referred to Torben et al. [36].

3. Case study: Supervisory risk control of an autonomous cargo ship

The method for building the SRC is tested in a case study that simulates an autonomous ship operating along the Norwegian coast to assess how the SRC manages and controls the ship in comparison to an existing conventionally-manned ship. The first part of the case study will analyze how the SRC adjusts the speed and configures the ship to maintain control. This is then compared performance-wise to a conventional ship in similar conditions, using position and speed data from the ship navigation system. The second part will study how the SRC handles failures in the machinery and propulsion system.

In the case study, it is assumed that the chart and GNSS measurements are sufficiently accurate to be used in the control system. It is also assumed that the time necessary to start up machinery can be neglected. There are still some delays and thruster dynamics included, such that engines and generators cannot change the load immediately. This is deemed sufficient to show how the SRC functions. Some of the potential ways to include these aspects in the SRC will be discussed in Section 4.3.

The ship simulation uses a simplified kinetic model without wave forces. This makes it easier to simulate and test the system, while it also changes the ship's movement such that the ship drifts more. This makes it more difficult to control the ship, especially in tight turns, without reducing the speed much more than conventional ships. Although the focus in this paper is the design and testing of the SRC, it still provides sufficient results to show that the proposed methodology works.

3.1. Step 1: Describing the ship and operation

The autonomous ship that is considered in the case study is an 80 m long and 16 m wide cargo ship that is sailing along the Norwegian coast. Although the ship is operated unmanned, it has a human supervisor onshore that can monitor and take control remotely if necessary. The ship has an autonomous control system, as shown in Fig. 3, with an SRC as the high-level controller, an ANS to control the navigation, and an autonomous machinery management system (AMMS) to manage the machinery. The ANS has two ship operating (SO) modes: (i) DP and (ii) autopilot (AP), with a corresponding controller for each mode. The DP controller is used during low-speed maneuvering and station keeping, while the AP controller is used for transit at higher speeds. When the ship is operated in DP-mode, it utilizes the main propeller, bow tunnel thruster, and aft tunnel thruster to control the ship's speed, position, and heading. The AP controller uses the main propeller and rudder to control the ship.

The ship is equipped with a Liquefied Natural Gas (LNG) fueled main engine, a hybrid shaft generator (HSG), and two diesel generators. The HSG can be used as a generator to produce electricity when the main engine is used or an electric engine when diesel generators can be used to produce electricity.

The AMMS is used to control the machinery system depending on the machinery system operating (MSO) mode. The ship has three MSO-modes: power take out (PTO) mode, where the main engine provide propulsion and the HSG is used as a generator to provide electricity; power take in (PTI) mode, where the diesel generators produce electricity, and the HSG is used as an electrical engine to propel the ship; and the mechanical (Mech) mode is where the main engine provides propulsion and the diesel generators produce electricity.

The SRC is responsible for selecting SO-modes and MSO-modes. It also sets the reference speed for the ANS to follow.

The STPA in the case study is based on a workshop with 12 relevant system experts who identified UCAs for the autonomous cargo ship. The participants have 5–30 years of experience from academia and industry working with risk assessment, testing, verification and validation, marine technology and maritime operation, and ship control system design. The workshop where conducted over three sessions. The first two where used to identify UCAs that were discussed and processed by the participants in the third. The result from the workshop was a report sent out to the participants. The main purpose of the workshop was to not only identify how switching between different machinery modes can lead to insufficient power capacity and power losses but also to identify when the wrong SO-mode used by the ANS could lead to accidents.

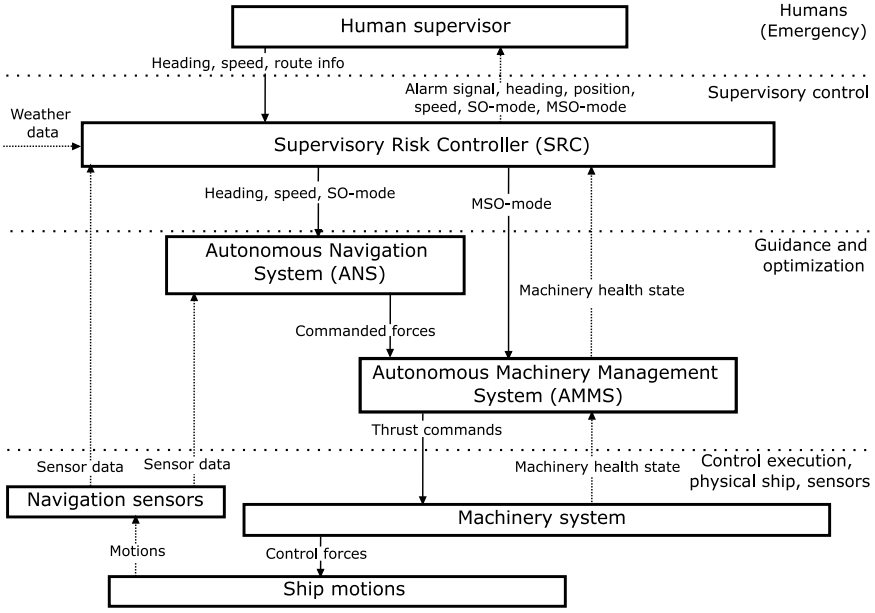


Fig. 3. Hierarchical control structure.
Source: Adopted from Johansen and Utne [4].

The STPA in the workshop considered a slightly different control structure with a remote operation center (ROC) that is responsible for planning, monitoring, and supervising the ship. The ANS and AMMS determine the SO- and MSO-mode, respectively, according to the sailing plan. An SRC in the control system was not included. The results from the workshop have therefore been developed further to account for the different ship control structure considered in this case study.

This case study assumes that the human supervisor plans the mission and the SRC then executes this plan. The human supervisor is also responsible for taking remote control of the ship if notified by the SRC. Selecting SO- and MSO-mode is now done by the SRC, and not the ANS and AMMS. The ANS controls the ship in either AP- or DP-mode depending on the SO-mode. The AMMS manages the machinery system according to the MSO-mode decided by the SRC. The AMMS also contains thrust allocation that computes individual thrust commands, based on the commanded forces from the ANS.

Since the workshop did not include an SRC, the control structure is modified to include this with the associated control actions. However, because setting SO-mode, MSO-mode, and the ship speed were considered when identifying UCAs in the workshop, the results can still be used with some modifications to account for the differences.

The SRC has a set of process variables that are used to make decisions, as follows:

- PV-1: Active MSO-mode
- PV-2: Available power and thrust
- PV-3: Machinery system status
- PV-4: Active SO-mode
- PV-5: Ship's navigational states
- PV-6: Weather conditions
- PV-7: Traffic conditions
- PV-8: Route information

The case study focuses on the following hazardous event (HE) and system-level hazards (H), as follows:

- HE1: The ship grounds or has contact with the seafloor
- H1: The ship violates the minimum separation distance to the shore
- H2: The ship sails in water that is too shallow

Table 1
Unsafe control actions.

UCA	Description
UCA-1	A command is given to change MSO-mode to PTO when the health state of the ME is reduced
UCA-2	A command is given to change MSO-mode to Mech when the diesel generators do not function, or are unable to provide the rated power to the DC bus
UCA-3	A command is given to change MSO-mode to PTI, resulting in insufficient power for the main propulsion
UCA-4	A command is given to change SO-mode to transit/AP when the ship is in harbor/tight areas
UCA-5	A command is given to change SO-mode to maneuvering/DP when the speed is higher than the maximum maneuvering speed

The workshop identified a total of 60 UCAs. However, including all these would make the risk model more complicated to build and evaluate. Therefore, the case study focuses on five different UCAs, as shown in Table 1, to reduce the size and complexity of the risk model. These are chosen to have a good basis for specifying scenarios where the decision making in the SRC, such as setting SO-mode or speed reference, can lead to hazardous events and identify RIFs that affect this.

Nine scenarios are defined to describe the situations that can cause UCAs and hazards, as presented in Table 2.

The extended STPA in this paper also considers the consequences from the hazardous event and the expected resulting costs. The consequences are divided into damage to own ship, damage to others' property, and harm to humans. Consequences are classified as either severe, significant, minor, or no consequences [45]. Fatalities or serious injuries to humans or extensive damage to the ship or other ships/objects where assistance is necessary are considered severe consequences. Less serious/minor injuries to humans and damage that needs repairs outside of planned maintenance are considered significant consequences. Insignificant or no injuries to humans and damage that can be fixed in the next planned maintenance are considered minor consequences. Severe consequences cost 4 550 640 USD, significant 455 064 USD, minor 45 506.4 USD, and no consequences lead to zero

Table 2
Scenarios.

Scenario	Description	UCA
SC-1	MSO changed to PTO because PTI delivers insufficient amount of power but the health state of the ME is reduced, leading to insufficient power production	UCA-1
SC-2	MSO changed to PTO because the extra power in Mech is not necessary but the health state of the ME is reduced, leading to insufficient power production	UCA-1
SC-3	MSO changed to Mech because PTO is not producing sufficient power for propulsion but the diesel generators fail or provide less power than expected, leading to insufficient power on the DC bus	UCA-2
SC-4	MSO-mode is changed to from PTO to PTI due to an underestimate of the power necessary, leading to insufficient power to the ship	UCA-3
SC-5	MSO-mode is changed to from Mech to PTI due to an underestimate of the power necessary, leading to insufficient power to the ship	UCA-3
SC-6	SO-mode is changed to transit while still in harbor due to inaccurate/incorrect measurements of the ship states	UCA-4
SC-7	SO-mode is changed to transit while still in harbor due to wrong understanding of the area around the ship	UCA-4
SC-8	SO-mode is changed to maneuvering with too high speed due to faulty speed estimates/measurements	UCA-5
SC-9	SO-mode is changed to maneuvering with too high speed due to a wrong limit set in the controller	UCA-5

Table 3
Risk influencing factors.

High-level RIF	Description	Scenario(s)
H-RIF-1	Machinery health state	SC-1,SC-2,SC-3
H-RIF-2	Estimation of necessary power	SC-1,SC-2,SC-3,SC-4,SC-5
H-RIF-3	Navigational complexity/situation	SC-1,SC-2,SC-3,SC-4,SC-5
H-RIF-4	Measurement/estimation of the ship's navigational states	SC-6, SC-8, SC-9
H-RIF-5	Situation awareness	SC-7, SC-8
H-RIF-6	Reliability of the ship's control system	SC-9

cost. The costs are estimated based on EfficienSea [46], The Norwegian Agency for Public and Financial Management [47], and IMO [45].

3.2. Step 2: Building the online risk model

The STPA is used as the basis to build the online risk model based on the methodology in Utne et al. [2], as shown in Fig. 4. The output from the risk model is the expected cost from the consequence. The BBN has four nodes describing the consequences: one general consequence node and one for damage to own ship, damage to others property, and harm to humans; one node describes the hazardous event, and one node describes each of the system-level hazards. The two system-level hazards depend on the five UCAs considered in the STPA. Each of these correspond to one node in the BBN.

The nine scenarios described in the STPA are used as the basis to define the six H-RIFs in the BBN. The list of H-RIFs, with the corresponding scenarios are show in Table 3. Each of the high-level RIFs are analyzed further to find I-RIFs, as shown in Table 4.

In addition to the I-RIFs and decisions in Table 4, the type of seabed and shore affect the consequences directly. Intermediate nodes are used between I-RIFs/decisions and H-RIF nodes to reduce the number of inputs to each node. This reduces the size of conditional probability tables (CPTs) and makes it easier to define these. CPTs and states

Table 4
Input to H-RIFs.

High-level RIF	Description	Input RIF/Decision
H-RIF-1	Machinery health state	ME state, HSG state, DG1 state, DG2 state, BT state, AT state, MP state, ST state, MSO-mode (Decision node), SO-mode (Decision node)
H-RIF-2	Estimation of necessary power	PMS, AP performance/accuracy, DP performance/accuracy, SO-mode (Decision node)
H-RIF-3	Navigational complexity/situation	Traffic, Obstacles, Current, Distance to grounding hazard, Wind speed, Wind direction, SO-mode (Decision node) Speed reference (Decision node)
H-RIF-4	Measure-ment/estimation of ship's navigational states	GNSS system, Radar, AIS, SO-mode (Decision node) AP performance/accuracy DP performance/accuracy
H-RIF-5	Situation awareness	GNSS, Radar, AIS, Visual conditions
H-RIF-6	Reliability of the ship's control system	SO-mode (Decision node), AP performance/accuracy DP performance/accuracy, Ship design process

are defined based on the work in Johansen and Utne [4], DNVGL [48], Hassel et al. [49], discussions with crew working on different ships, and control engineers from Kongsberg Maritime. A full list of all nodes, with parent nodes, is shown in Table 5.

The BBN is converted to an online risk model by linking I-RIFs to the control system so they can be updated as the ship sails. Nodes describing the state of machinery parts are updated with information from the AMMS. If the machinery is well functioning and well maintained, then the probability of failure is very low, $9 \cdot 10^{-7}$. In future works, this is intended to be updated as the ship sails since machinery components are more likely to fail as components age, but this is not modeled in the current case study.

Nodes describing the control system and sensors are given a static value based on Johansen and Utne [4], DNVGL [48], Hassel et al. [49]. Weather nodes are linked to sensors where these exist, such as wind and current, or weather forecast and historical data [50]. These nodes are designed to be updated in real-time depending on the available data. Traffic use data is drawn from the automatic identification system (AIS), which is used to transmit the identity, position, course, and speed to nearby vessels using the very high frequency (VHF) band. Obstacle density and distance to grounding hazards are taken from the ENC. The seabed and shore are described with data from Norwegian Mapping Authority [51] over the relevant area. The values used in input nodes describe the probability over the planned mission.

3.3. Step 3: Setting up the ENC module

The ENC module is setup to extract data from electronic navigational charts for use in the online risk model and the rest of the control system. The ENC module here includes charts covering the areas around Brønnøysund and Rørvik in Norway, which are relevant for the type of ship in the case study. The module is set up to consider everything shallower than 5 m as shallow areas or land where the ship cannot navigate safely. The rest of the chart is divided into layers of 10 m, 20 m, 50 m, 200 m, 350 m, and 500 m. This distribution is considered a reasonable combination of chart resolution and efficiency in the control system.

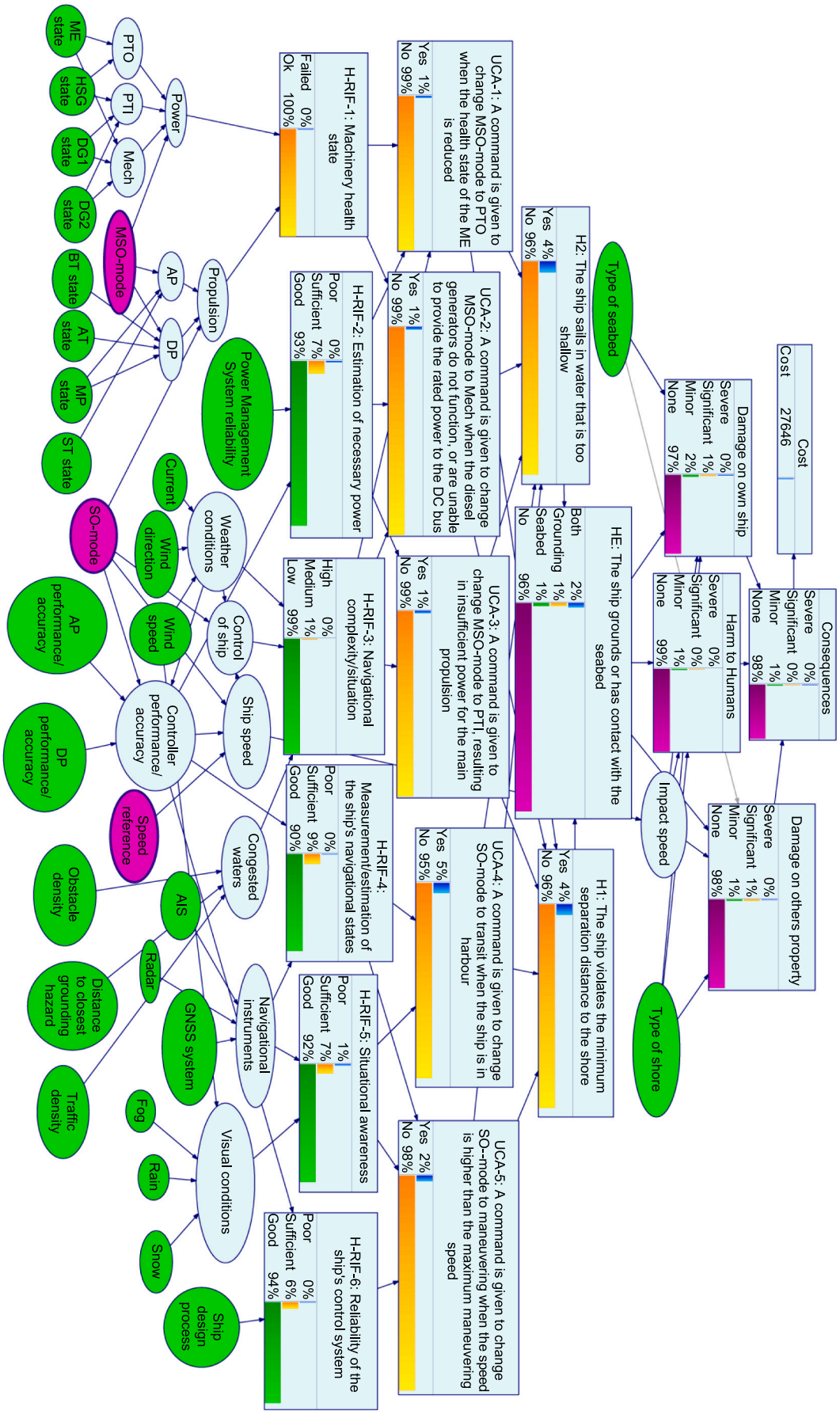


Fig. 4. BBN risk model showing an example of the risk cost. For more detailed information about the BBN, please contact the corresponding author.

The obstacle density is based on the distance to the closest shallow point (i.e., areas with less than 5 m water depth) and the percentage of obstructed water around the ship. The water depth of 5 m is the same as the max draft of the ship. Using this water depth is considered sufficient for assessing the portion of obstructed water in this work. Shallow areas are consequently areas with too little water depth for the ship to sail, which should be avoided with sufficient safety margins. The percentage of obstructed water is calculated by considering a disk with radius 1400 m and finding the portion of the disk with land and shallow water. The radius is set through testing to ensure that the disk gives a good picture of the sea area surrounding the ship, without being unnecessarily large.

The ENC module checks the area around the ship every 15 s and updates the input to the online risk model. Updating every 15 s ensure that the control system has updated data, while limiting the computation time necessary to check the ENC module.

3.4. Step 4: Building the supervisory risk controller

The SRC is the high-level controller that manages and controls the ship. The SRC uses data from the risk model and ENC, combined with operational measurements from the ANS and AMMS, such as position, speed, and machinery status to make decisions. The SRC has four main objectives: selecting the SO-mode, selecting the MSO-mode, setting the reference speed for the ship to follow, and notifying the human supervisor when the situation becomes too severe to continue.

The SRC is implemented as a switch that checks the cost function, as shown in Eq. (1), for each set of decisions. The risk cost is calculated using Eq. (2). This takes the probability of the different consequences, $Pr()$, estimated in the online risk model described, multiplied with the expected cost for each consequence, $C_{()}$, as described in Section 3.1:

$$R(d) = Pr(severe)C_{severe} + Pr(significant)C_{significant} + Pr(minor)C_{minor} + Pr(none)C_{none} \quad (2)$$

The fuel cost is calculated as the specific fuel cost (SFC) multiplied by the expected sailing time. The SFC is taken from a look-up table, depending on wind speed, ship speed, current speed, and MSO-mode. The look-up table is made by simulating the machinery under different conditions to estimate how much fuel is used to sail a set distance. The fuel prices are taken from Ship & Bunker [52] at 1 343.5 USD/ton for LNG and 684.5 USD/ton for diesel. This table provides a cost per distance that is multiplied with the planned sailing distance, as shown in Eq. (3):

$$F(d) = SFC(wind, speed, current, machinery) * distance \quad (3)$$

Operation costs are calculated using Eq. (4). This includes manning in the ROC, maintenance from wear and tear on the machinery, insurance of the ship, lubrication oil, spare-parts, and logistics. These are estimated based on conventional ships of the similar size and type, and using data from Stopford [53] to be 341.3 USD/h for the current ship. This is similar to the fuel cost in normal transit with a speed of 5–7 m/s (9.7–13.6 knots):

$$O(d) = Cost_{operating} * distance/speed \quad (4)$$

The cost of potential future loss is calculated with Eq. (5). This cost is the loss of income if the ship is unable to take on any new missions before finishing the current route, which is set to 910.1 USD/h:

$$L(d) = Cost_{futureloss} * distance/speed \quad (5)$$

The cost function, including the ratio between the different terms, is discussed in Section 4.7. The controller estimates the cost of sailing a distance equal to the initial route distance. This is constant for the whole route which keeps the weight between the different cost terms constant.

The alarm is implemented so that a human supervisor can take over control remotely of the ship if necessary, but unnecessary alarms also need to be avoided. To achieve an acceptable balance, the alarm trips if either the risk cost exceeds 9 267.70 USD, or the probability of the hazardous event exceeds 0.5. The cost limit is set between minor and significant consequences because it is better to have the human supervisor check the ship having an emergency later on. The SRC is implemented to lower the speed to limit the risk cost because impact speed directly affects the consequences. However, this can cause situations where the probability of a hazardous event is too high to continue due to environmental conditions, even though the risk cost is low because the speed is reduced to the minimum. Thus, a probability limit of 0.5 is used to notify the human supervisor in these situations.

If the SRC changes the ship's control configuration, then it is paused for 30 s before checking again. Implementing a time delay in the switching logic ensures that the controller reacts to changes but avoids situations where it gets stuck switching between different modes (e.g., DP and AP) without stabilizing, which is also called chattering [54].

3.5. Step 5: Verifying the control system

After setting up the SRC, verification is done by first determining how to test the system and which requirements to verify against. The autonomous ship should follow the route through Brønnøysund that is shown in Fig. 5. The route follows the same path as a conventional ship and those described in Norwegian Hydrographic Service [55]. This is used to check the ship in situations where the controller is expected to adjust the speed reference, without using much longer time than conventional ships. The ship has to lower the speed reference early enough to slow down when entering narrow and tight areas, and increase it when it opens up again.

To test safety, the ship should maintain a minimum distance of 5 m to shallow areas or provide an alarm to the human supervisor at least 5 min before the minimum distance is violated. Having a minimum distance of 5 m is not realistic for a real ship. However, to account for extra drift caused by simplifications in the simulator this is used to get results reasonable results that can be compared to conventional ships. These assumptions are discussed further in Section 4.8. The following verification focus on wind and how this affect the ship. However, the process is the same for other disturbances, such as current.

To verify that the controller is efficient, the ship should at maximum use 140 min on the whole route segment under consideration in the case study or provide an alarm to the human supervisor. This time limit is set based on the time existing manned ships used on the same route. Both the safety and efficiency requirements are tested in wind speeds ranging from no wind to 20 m/s and from all directions. Other factors (e.g., current, waves, and machinery failures) are not considered in the verification. This simplifies the verification but still gives sufficient results for further testing of the control system. The route is chosen to get a good variation between open water and more narrow straights with tight turns.

The verification is performed using the automatic simulation-based testing methodology that was introduced in Section 2.5. This methodology selects and simulates interesting combinations of wind speed and wind direction to verify or falsify the system. The system is verified to satisfy the safety requirement (minimum distance to shallow) in 161 simulations, and the efficiency requirement (maximum allowed sailing time) in 97 simulations. The STL robustness surfaces for safety and efficiency are shown in Figs. 6(a) and 6(b), respectively. The STL robustness score is normalized to the interval $[-1, 1]$. Fig. 6(a) shows that the robustness score in the case study is always above 0. Similarly, Fig. 6(b) shows that the robustness is always above 0 and is close to 1 when it reaches the final way-point early or trips an alarm because the risk cost or grounding probability becomes too high.

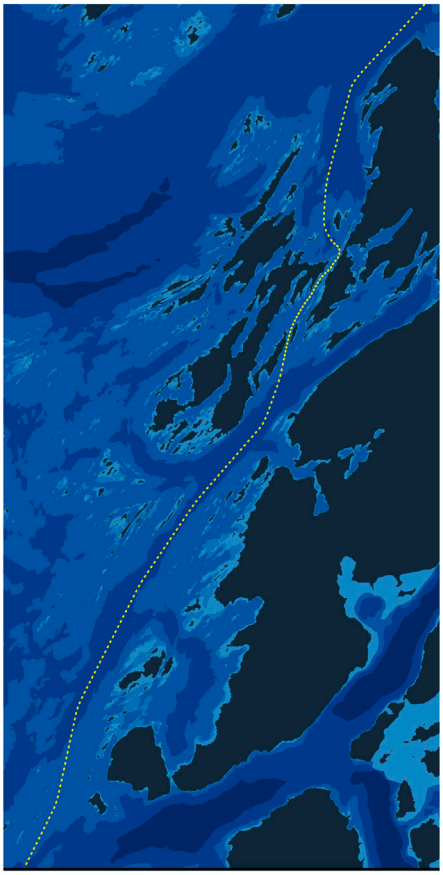


Fig. 5. Route used in the verification process.

The verification shows that the control system makes the autonomous ship follow the route and it also reaches the end of the route in reasonable time in wind speeds of up to 8 m/s. Above this, the planned route forces the ship very close to land in certain spots, which means that it notifies the human supervisor. When the wind speed exceeds 10 m/s, the route leaves too little space for the ship to maneuver. This can cause problems with certain wind conditions. However, the control system provides an alarm to the human supervisor with enough time to pass the safety requirement. Overall, the verification shows that the proposed control system works in the planned route but it is limited by not being able to change the route in accordance with the environmental conditions.

4. Results and discussion

4.1. Comparing the controller with the maneuvering of a conventional ship

After building and setting up the controller, the autonomous ship is simulated along two different routes to compare it against an existing conventional ship. The first route is through Rørvik and the second is through Brønnøysund. The route through Brønnøysund is similar to the one used in the verification (Fig. 5) but with different start and end points. The start and end points are changed because the GNSS data from the conventional ship is only available for part of the route. The purpose is to see how the SRC sets the speed reference, MSO-mode, and SO-mode, and compare this to how conventional ships operate along the same routes in similar weather conditions. The existing ship is equipped with a similar machinery and control system as the autonomous ship but with a crew who decides MOS-mode, SO-mode, and speed reference.

The conventional ship sailed through Rørvik and Brønnøysund in the fall of 2021 with a wind speed between 5–7 m/s. The routes followed by the conventional ship are plotted with GNSS data taken from the control system aboard the conventional ship. The route through Rørvik is planned by placing way-points along the route that the autonomous ship can follow. The GNSS data for Brønnøysund contain some measurements that place the route over land. The cause of these are not certain but it only affects the data between point 0.5 and 0.7. Therefore, the route was re-planned by placing way-points along the same route into Brønnøysund but following the route recommended in Norwegian Hydrographic Service [55] through and after Brønnøysund. The routes are shown in Fig. 7 for route one and Fig. 10 for route two with the conventional ship in red and the autonomous ship in yellow.

To compare the two ships, the risk model and SRC need position, speed, MSO-mode, and SO-mode from the conventional ship. Position and speed are recorded in the ship's control system. Ship speed is fed directly to the SRC to find the expected fuel cost and is used as input to the risk model. Position data is used in the ENC module to get the distance to the closest grounding hazard and obstacle density. MSO-mode is set to PTO and SO-mode to AP after discussing how the conventional ship is operated with the crew. This provides a cost that can be compared to the autonomous ship. The SRC uses a constant distance when calculating costs, as explained in Section 3.4. The plots therefore show the costs of sailing a distance equal to the distance of the whole route, d_0, estimated at each point.

4.1.1. Comparison on route one through rørvik

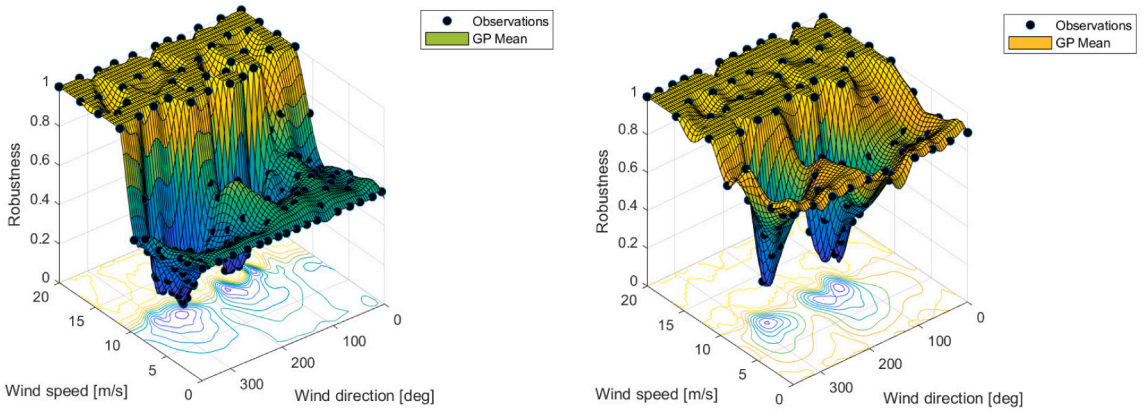
On route one, the conventional ship starts with a speed of 5.25 m/s, before increasing to 6.5 m/s. The speed is then maintained at 6.5–6.75 m/s the rest of the distance. The autonomous ship starts with a speed of 5 m/s. This is later increased to 7 m/s as the ship sails into more open water. Along the rest of the route, the speed varies between 5 m/s and 7 m/s as it passes through more narrow parts of the route and in more open areas. Overall, the autonomous ship varies the speed more as the environmental conditions change, compared to the conventional ship.

The cost is shown in Fig. 8 for the conventional ship and in Fig. 9 for the autonomous ship. The plots show the expected costs of sailing the full route, d_0. The conventional ship has a higher risk cost (blue line) because it maintains a higher minimum speed. Fuel (yellow line), operation (green line), and potential future loss (red line) costs are almost the same but they vary more for the autonomous ship because the expected time varies more corresponding to more changes in the speed. For the conventional ship, both fuel and operation costs are almost constant because the speed is kept more or less constant along the whole route. In contrast, the speed of the autonomous ship is changed more, which leads to more changes in fuel and operation costs. The conventional ship uses 96 min on the whole route and the autonomous ship uses 103 min.

4.1.2. Comparison on route two through brønnøysund

The routes differ slightly more through Brønnøysund, due to the errors in the position data from the conventional ship. This means that the autonomous ship sails around 1 km longer. The conventional ship maintains a speed of around 6.75 m/s before it reaches the narrow parts of the route between 0.5 and 0.6 on the route shown in Fig. 10. In the narrowest part, the speed is reduced to 3 m/s, it is then increased to 6.75–7 m/s as the area opens up. The autonomous ship has a speed of 7 m/s in open water. This is reduced to 5 m/s when it reaches the first narrow straits between points 0.4 and 0.5. It then returns to 7 m/s for a short time in the more open area, before it is reduced to 4 m/s through the narrow harbor area. Overall, the autonomous ship makes more changes to the speed, but maintains a higher minimum speed.

The cost is shown in Fig. 11 for the conventional ship and Fig. 12 for the autonomous ship. Fuel (Yellow line), operation (Green line), and potential future loss (red line) costs are virtually the same along



(a) Safety verification (b) Efficiency verification

Fig. 6. Robustness surfaces resulting from the two verification runs.

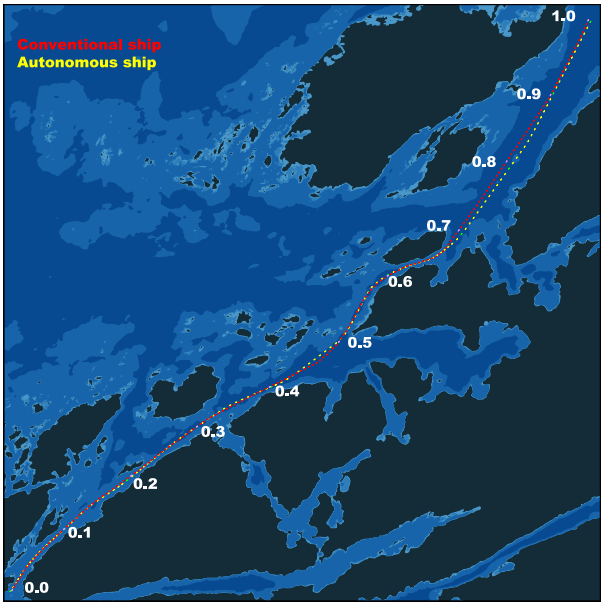


Fig. 7. Map of route one through Rørvik. The conventional ship's route is shown in red and the autonomous ship's route is shown in yellow.

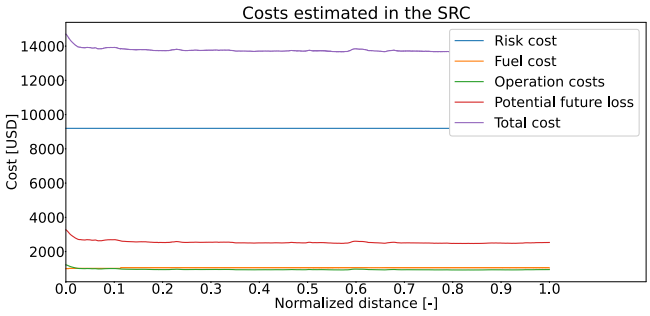


Fig. 8. Conventional ship's costs on route one.

the whole route. The risk cost is similar along the first part where both ships follow the same route, but is much higher for the conventional ship in the middle part of the route. This is caused by the inaccuracies in the GNSS data collected on the conventional ship showing the ship sailing very close and over land, and the conventional ship not reducing the speed between points 0.4 and 0.5. This combination results in a

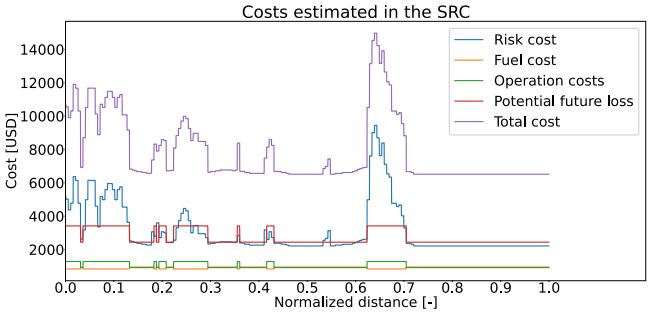


Fig. 9. Autonomous ship's costs on route one.

significantly higher risk cost compared to the autonomous ship. Fuel cost is similar for both ships with a reduced fuel consumption when the speed is reduced in the most challenging part of the route. Operation cost is also similar, but with a higher top for the conventional ship since because reduces the speed more.

4.2. Controlling the ship with machinery and propulsion failures

The second part of the case study tests how the control system manages the autonomous ship when the health of the main engine and steering system is worsened. This is modeled by increasing the probability of failure for these elements in the risk model. The SRC then chooses the best way to operate the ship based on this information. The routes are the same as shown in Fig. 7 for route one and Fig. 10 for route two. The weather is also the same, which ensures that the results can be compared to how the ship is managed when all systems function.

4.2.1. Machinery and propulsion failures on route one through rørvik

In both cases, the failure happens when the ship has sailed approximately 8% of the route, close to point 0.1 on the figures. When the main engine fails, the SRC changes MSO-mode to PTI, which only uses the HSG and diesel generators for power production. The speed reference is also reduced to 4 m/s because the diesel generators produce less power than the main engine. This ensures that the ship still has sufficient power to maneuver. The SO-mode is AP along the whole route in this case.

When the steering machinery fails, the speed is lowered significantly such that the tunnel thrusters can provide steering for the ship and SO-mode is changed to DP. The MSO-mode is Mech for the whole route. The speed reference switches between 2 m/s and 3 m/s, depending on the number of islands and obstacles around the ship.

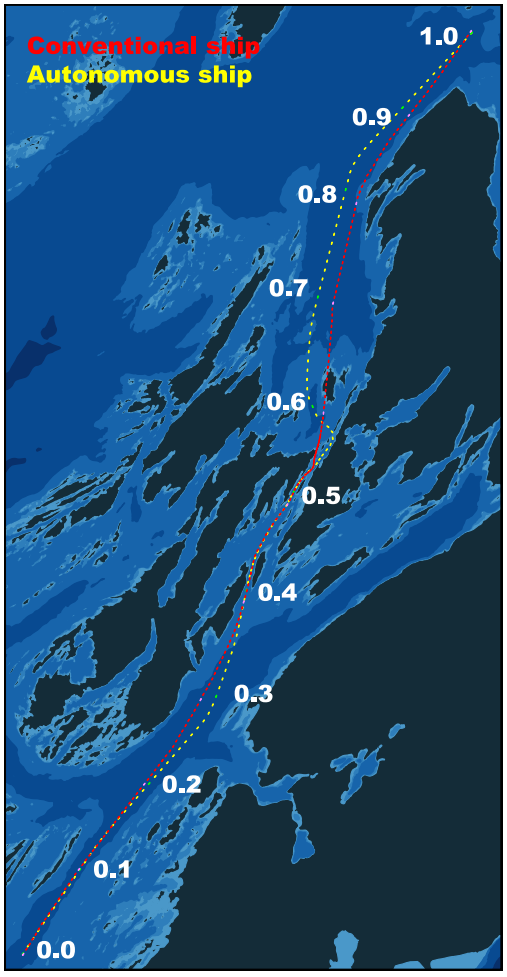


Fig. 10. Map of route two through Brønnøysund. The conventional ship's route is shown in red and the autonomous ship's route is shown in yellow.

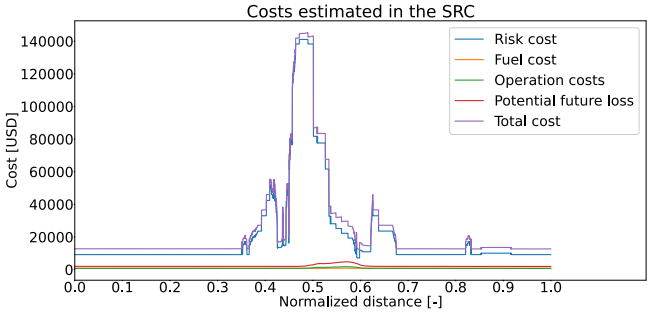


Fig. 11. Conventional ship's costs on route two. The risk cost is here significantly higher since the position data used to estimate the costs include some incorrect measurements placing the ship both very close and on land as shown in Fig. 10, as well as having a .

Figs. 13 and 14 show the costs calculated by the SRC. Overall, the cost is maintained at a similar level as when everything is working by adjusting how the speed is operated. The risk cost is controlled by reducing the speed, compared to how the ship is operated when all systems function as intended, and by switching to MSO-modes and SO-modes with functioning components. Operation and potential future loss is increased because the ship uses a longer time with lower speed.

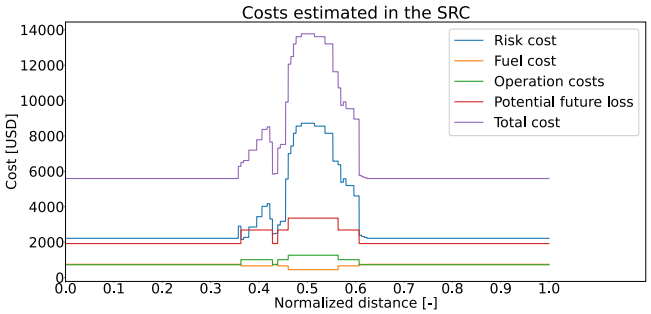


Fig. 12. Autonomous ship's costs on route two.

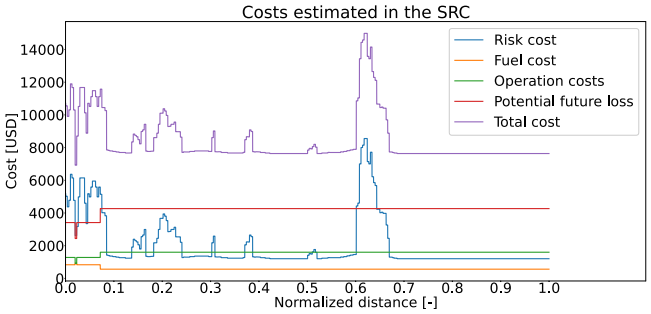


Fig. 13. Costs with failure on main engine on route one.

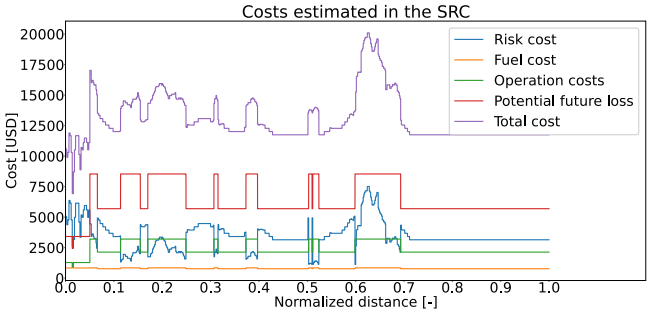


Fig. 14. Costs with failure on steering machinery on route one.

4.2.2. Machinery and propulsion failures on route two through brønnøysund

The main engine fails between point 0.3 and 0.4, and the steering machinery fails between point 0.2 and 0.3. When the main engine fails, the speed is reduced significantly to account for the reduced power production. MSO-mode is also changed to PTI, which do not use the main engine. The SO-mode is AP along the whole route.

When the steering machinery fails, the speed is reduced to 2 m/s and SO-mode is changed to DP, to get more effect from the tunnel thrusters and maintain control of the ship. When the ship has passed the narrowest parts of the route, the speed is increased to 3 m/s.

Similar to route one, the costs that are shown in Fig. 15 for the main engine and Fig. 16 are similar as when everything is functioning by reducing the speed and changing MSO-mode and SO-mode. The biggest difference compared to the cost when all systems function is the time used to finish the route. The time and the time dependent costs, operation costs and potential future loss increase when the ship sails at a lower speed. This is most visible after the ship has finished with the most challenging parts of the route, around 0.4–0.5. However, because the speed was reduced in the narrow and tight parts with all systems functioning as well, the max cost is still at the same level.

Data from conventional ships operating with failures but switching to modes that function without the failed components are limited,

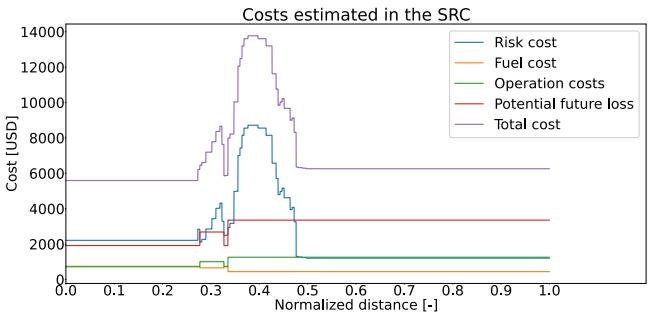


Fig. 15. Costs with failure on main engine on route two.

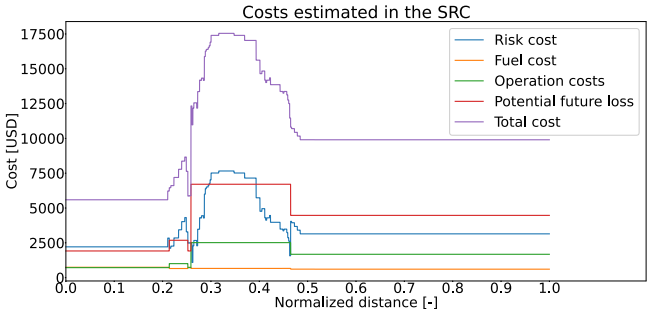


Fig. 16. Costs with failure on steering machinery on route two.

although this is a logical way to mitigate failures. In a conventional ship, the failed components can be fixed by the crew or the ship can be maneuvered to the closest harbor for repairs. On an autonomous ship without a crew, the only option is to maneuver to harbor and get it fixed there or in case of severe failures transport a repair crew to the ship offshore. Because this route change is not included in the SRC and the redundancy of the machinery systems onboard the autonomous ship was not compromised entirely, the ship continues to sail towards the final way-point. With the current control system, this is a reasonable solution. Deviating from the planned route to get to shore and repair damaged equipment, which would be viable solutions in case of critical machinery failures and total loss of propulsion, and notifying the human supervisor are topics for further research that could improve the control system further.

4.3. Risk modeling and implementation in the control system

The proposed control system uses a BBN-based risk model to assess the risk. The model is based on an extended STPA of the ship. STPA provides a systematic way to analyze the ship and identify causal factors that can lead to hazardous events. The results of the STPA also provide a logical way to build and structure the BBN. However, the results depend on the data used and the quality of the analysis.

Another potential challenge using STPA is to decide the refinement level. The refinement level generally depends on the purpose of the STPA. More details mean more data, but it can also make the risk model and the corresponding calculations too time consuming. In this current work, the analysis considers one hazardous event only, two system level hazards, and five UCAs. The scenarios include causal factors, such as wind, obstacles, and the main parts of the machinery system. The scenarios could have been more detailed and could have included information about how machinery parts fail. However, because the purpose of the analysis in this paper is to build an SRC, the level of detail is considered to be sufficient because the controller does not provide detailed control actions to the different parts of the machinery systems. An example of this could be saying that the main engine can only produce limited power because the cooling system is only partially functioning, although in this situation limited power is necessary to maintain control of the ship. Enabling the controller to make such decisions would be an interesting topic for further research to continue to develop the control system.

When building the BBN risk model, the overall structure is determined by the STPA. However, because the STPA is qualitative, it provides very little data for setting up states defining CPTs. Hence, they are generally based on other sources, such as literature, previous works, and expert judgement. The CPTs can also be adjusted later to put more weight on specific risk factors. Given that the CPTs are based on different sources, they contain a certain degree of uncertainty, as discussed in Section 4.7.

To convert the risk model into an online risk model, the risk model is connected to the rest of the control system. This means that all of the nodes in the BBN that can be measured by the control system or sensors should be updated when the ship is sailing. The risk model should be updated often to describe the current sailing conditions. However, updating it too often increases the computation time in the control system. There is also a limit to how quickly the controller can update the decisions. In the case study, the risk model and SRC is paused for 30 s if the SO-mode, MSO-mode, or speed reference is changed. This delay allows the controller to evaluate if the decisions influence the ship and to avoid chattering, where the controller is stuck switching back and forth between different decisions, such as DP and AP.

The control system can be expanded further by including more dynamics in the ship model. The case study assumes that machinery parts can be started immediately, which is not the case. Although the specific time necessarily varies for different engines, it will have to be included when making decisions. This type of dynamics could be included in the control system as limits to how often decisions can be changed. The risk model can also be modified to include starters for the different machinery parts. For example, for the main engine to function, both the starter and engine would be necessary.

Similar dynamics can be included for changing load on the machinery and the speed of the ship. In particular, reducing the speed of the ship takes time, depending on the size of the ship. The ship simulator includes a time delay on load changes and uses some time to change the speed of the ship. However, the SRC does not account for this specifically when it makes decisions. Therefore, including more dynamics in the control system and risk model is an interesting topic for further research.

4.4. Challenges with measuring risk in cost function

The proposed control system uses a cost function to make decisions about MSO-mode, SO-mode, and speed reference. This cost function estimates the cost of operating and sailing the ship, and the potential cost of hazardous events. The cost of sailing and operating the ship is straightforward to calculate and use in a cost function because it is already measured as cost. However, to combine this with risk cost is a bigger challenge. The STPA analysis can identify potential hazardous events but is only a qualitative analysis that does not consider likelihood of these events or the following cost.

This work addresses this problem by extending the analysis to consider consequences and classifying these in terms of cost. The STPA results and consequences are modeled in a BBN to give a likelihood of the consequences. The likelihood is multiplied with the consequence cost to give a risk cost to use in the cost function. Decisions are then made based on the current time, without considering how this can change in the future. Risk could be alternatively assessed by simulating how changing conditions and decisions affect the cost over a longer time. This would make the SRC more like an MPC, which could find the optimum set of decisions to minimize the cost over a longer time period. However, this would mean running a lot of simulations to check all potential combinations. Investigating this further could be subject for further research.

4.5. Risk modeling and integration with the ENC module

In the proposed control system, information about grounding obstacles is important for the risk model because it allows the model to assess the area around the ship. This information, and other data about the relevant area, is available in ENCs. The ENC module is an efficient tool for extracting and filtering this information to enable it to be used to describe the navigation area in the risk model. The control system uses the distance to the closest area where the ship can ground and the density of such areas as inputs to the risk model. Together with weather and traffic data, this determines how challenging it is to maneuver the ship.

The ENC module used in this work do not account for navigational markers, as this is not currently implemented in SeaCharts. For an autonomous ship, knowing where different navigational markers and their meaning is an important part of operating safely. The proposed control system itself can utilize this information in the risk model to get a better understanding of the environment when this become available with the SeaCharts package. However, the current ENC module is still considered sufficient to demonstrate that the proposed control system works.

The ENC module also provides an efficient way to plot the ship during testing, and is used when testing the control system to see how well the ship follows the route and identifies problems in specific areas. Compared to just using the position data, without grounding obstacles and land, this approach makes it much easier to understand and/or verify how the ship maneuvers.

Data from the ENC module can also be used to add more functions to the control system, such as route planning. In addition, a planning algorithm can use the ENC module to check if the route maintains the necessary distance to land and grounding obstacles. When combined with AIS data, this can enable the planner to account for other ships and use this information to avoid collisions. This is an interesting extension of the control system that would reduce the need for human supervision and control even further. This point is left open as a relevant topic for further research.

4.6. The efficiency of testing and verification of control systems in operation

In this work, the proposed control system is verified against the design requirements using the automatic simulation-based testing framework that was introduced in Section 2.5. Using this approach significantly increases the efficiency of building sufficient verification evidence for the control system. [36] show that this reduces the number of simulations necessary to verify the scenario compared to a regular grid search, which is a large time saver when doing several design iterations and verifying the scenario after each iteration.

The robustness surface resulting from a verification run with the automatic testing framework enables us to quickly get an overview of the performance of the SRC system at different regions of the scenario space. This overview is actively used in the design process to iteratively adjust the control system. Compared to the alternative of running simulations manually and evaluating the resulting time series, this offers a significant reduction in the workload. Furthermore, using STL to evaluate the system also gives a robustness score to show not only that it is verified but also how well the system performs.

It is also worth noting that the verification process considers a specific route and area. These can be planned such that the route includes different environments, such as open water, coastal waters with many islands, or tight harbor areas. The results from the verification should then be valid for other routes with similar characteristics, as shown in the case study. However, if the system is only tested in a distinct environment, such as open water without obstacles, then it cannot say anything about how the controller handles other environments.

An interesting extension of the automatic testing framework is to also use it in an online setting and integrate it more closely with the SRC system. This online verification system could repeatably start verification runs at fixed time intervals. A verification run would attempt to verify safe operation for a finite time-horizon ahead and for a set of uncertain scenario parameters, such as environmental conditions, traffic, or internal components failures. It would achieve this by running simulations with the current situation as an initial condition and then intelligently selecting the scenarios to simulate using the Gaussian process model. The simulator should have an exact (software-in-the-loop) replica of the SRC system, thereby also evaluating how future choices of the SRC system will affect the performance in the different scenarios. The result from a verification run would be used as a robustness map for future scenarios. This robustness map, when combined with data on the probability of the different scenarios, could then be used by the SRC system to make risk-based decisions. The concept of an online verification system operating in closed loop with the SRC system appears to be very interesting because it enables the SRC system to consider multiple future scenarios and at the same time evaluate how its decisions would affect future behavior.

Another interesting extension is to use the STPA directly to define safety requirements and simulation scenarios; see, for example, Rokseth and Utne [41],Rokseth et al. [42]. In the current work, the scenarios are set up to test the ship in a wide range of wind conditions and in very different areas. However, testing similar scenarios to those that the STPA identified when controlling the ship is challenging. Therefore, testing in more specific scenarios based on the STPA is left for further research.

4.7. Uncertainties and sensitivity in the data and models in the case study

The proposed control system combines existing control systems, such as DP and autopilots, with an online risk model in an SRC. The DP and autopilot are well described in the literature and are used on conventional ships. However, the use of an online risk model in an autonomous ship system and the concept of a cargo ship sailing without humans onboard is a novel concept. This means that data describing this is very limited, and mostly based on concepts and plans for these types of ships.

To get sufficient data in the case study, a combination of data from traditional manned ships, concepts for autonomous ships, geographic, and weather data is used. The quality of geographical and weather data is good with little uncertainty. However, the case study considers a simplified environment and not all conditions that a real ship would experience. For example, the wind measurements are taken over a long period but only at a general location. The wind is therefore assumed to be the same along the whole route, even though it will likely vary significantly between different locations. Similarly, the charts that are used are the same as ships use for navigation today but are simplified to only consider shallow areas and land, and not other ships or navigational marks. Although these simplifications make it possible to test the system, they also lead to uncertainties in the results (e.g., how the system can handle more obstacles such as other ship traffic and more local variations in wind conditions).

The STPA used in the paper is based on a workshop with academic industry experts. This helps to identify relevant information for the case study, but the quantitative risk models and corresponding calculations could still have limitations affecting the risk costs.

The input uncertainty will have a different effect on the overall uncertainty, depending on the sensitivity of each input node. If a node has high sensitivity, then changing it will change the risk cost more compared to nodes with lower sensitivity. Nodes with high sensitivity have the same effect on the uncertainty in the risk cost. Fig. 17 shows the effect that each node has on the risk cost when setting the node in the best and worst state. This shows that the weather conditions have the biggest potential effect on the risk cost. Other input nodes with a noticeable effect on the risk cost are GNSS accuracy, machinery status, controller performance, and obstacles. However, it is important

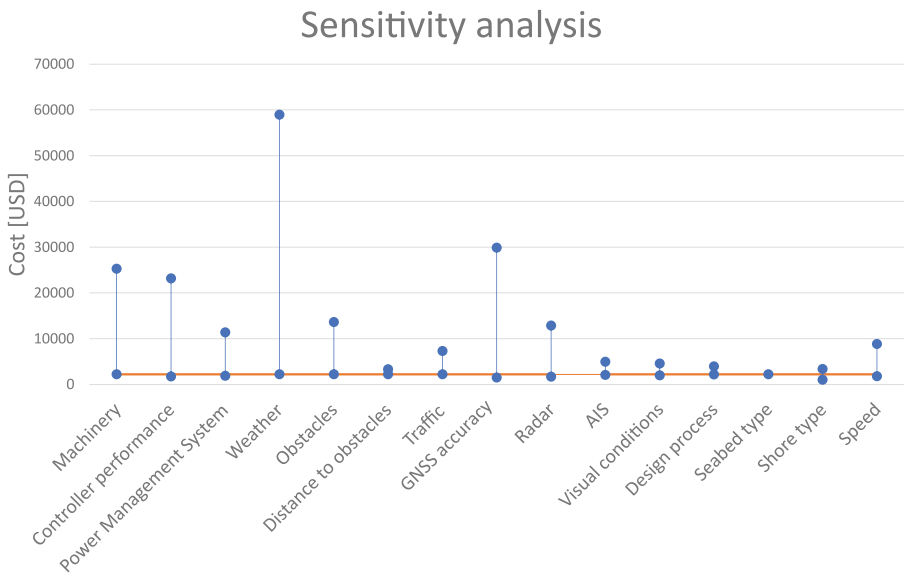


Fig. 17. Sensitivity analysis, showing the effect on the risk cost of setting nodes in the best and worst states.

to note that other factors than weather still give a high risk cost, especially combinations of multiple factors. Fig. 11 shows that the risk cost increases a lot when the GNSS data puts the ship very close to land without reducing the speed. The machinery and control system data are based on multiple sources that describe the system's reliability, and thus have less uncertainty. For weather and obstacles, the main source of uncertainty is the previously mentioned simplifications.

Another source of uncertainty in the risk model is the sensitivity of each input, or how much each input affect the risk cost. It is difficult to say how much weight should be on each input but it is possible to make some general remarks about it based on Fig. 17. For an autonomous ship to function properly, it needs well-functioning machinery, power, and control system. It also makes sense that sensors providing situation awareness influence the ship, and that weather and obstacles affect the decision-making process. The sensitivity analysis and case study show that all these have a significant effect on the risk cost.

The fuel cost, operation cost, and loss of future income also affect the uncertainty in the case study. Because the SRC makes decisions based on the total cost, the balance between different cost elements affect the decisions and the results. The fuel cost is calculated using a lookup table of how much fuel the ship uses in different environmental conditions and speeds. The table is made by simulating the ship to derive the fuel consumption. These simulations use simplified models of the machinery system, but they still give numbers similar to those for existing ships and engines. Both operation costs and loss of future income are estimated based on the type of ship and operation.

Based on the tests, the balance between safety and efficiency is good. The balance between the different costs is also reasonable. Fuel and operation costs are at the same level. The potential loss of future income is slightly higher than the sum of fuel and operation costs because the ship should have a higher income than just covering the expenses. The results can be improved further by advancing the models, and by getting more and better data, but this is left for future work.

4.8. Simplifications in the ship simulator and testing

The proposed methodology and control system is tested using a simplified ship simulator. The simulator is based on the models given in Fossen [56]. This provides a good tool to test the ship's control systems. However, the models include simplifications that affect the ship's behavior and control. Not including wave forces is one such simplification. The most commonly used approach to include waves takes a 3D model of the ship and tests it in a hydrodynamic program. However, the data to make this 3D model is missing for the ship in the case study, and therefore the ship is simulated without waves. Similarly, the simulations consider a simplified propulsion system and use approximations in the kinematic and kinetic equations.

In testing, the simulator works sufficiently to test the proposed methodology and SRC. However, the ship is difficult to control when turning, especially using the autopilot. Therefore, the minimum distance used in the safety verification, Section 3.5, is only 5 m. In real life, the ship should stay further away from land. This would also add more safety margins to the ship draft and more clearance under the keel. Although the system has been tested with a larger minimum distance, it then fails the safety verification at much lower wind speeds. The ship can be operated in DP-mode, which offers much better control at lower speeds using the tunnel thrusters to both control heading and sideways position. However, this would mean sailing at unreasonable low speeds when compared to the conventional ship. To get comparable data, the autonomous ship is allowed to operate with smaller margins in the simulations. Given that the focus of the paper is the method for developing the SRC and how this make high level decisions, this is deemed sufficient. Testing with more accurate ship models is left for further work.

Accuracy in the position data is another challenge when testing the proposed methodology. The case study assumes that the GNSS data is accurate for use in the ship control system. However, GNSS accuracy can be a challenge for autonomous ships, especially when sailing between tall mountains where the signal quality can be affected by bad satellite coverage and signals reflecting off the mountains. How accurate the data is will vary depending on the location, but is something that should be addressed when setting the limits in the system verification and the control system. However, it is still sufficient for testing the SRC and the methodology for building this. Combining GNSS measurements with other sensors, such as radar, LIDAR, sonar, and cameras is an option for improving the accuracy by measuring the distance to land and other objects, instead of just using the GNSS position. However, this is considered to be outside the scope of this paper and is left for further work.

5. Conclusions

This paper presents a control system with risk-based decision-making capabilities to enable the smarter and safer operation of autonomous systems. The proposed control system uses an online risk

model, which is represented by a BBN, to evaluate the operational risk, through an SRC. An ENC module is used to provide accurate data of the environment to both the risk model and the rest of the control system. The online risk model provides decision support in the SRC, which can make high level decisions. The control system has been verified against design requirements for safety (minimum distance) and efficiency (maximum time) using a novel formalized verification method. The combination of the SRC with ENC and formalized verification leads to a risk-based control system that can control autonomous ships in a safe and efficient manner, which currently does not exist.

The proposed control system is first compared to experimental data from an existing conventional ship in a case study along two coastal routes. This shows that the novel controller makes similar decisions to adjust the speed and maintain safe operation as the conventional ship, without using significantly more time to reach the end destination. It also shows that the controller took less risk than the conventional ship, mainly by adjusting the speed earlier when maneuvering in narrow areas, while maintaining a higher minimum speed than the conventional ship. This will make a bigger difference for routes that changes a lot, such as the route through Rørvik. However, it will still have an effect on routes with less variation between open water and narrow straits. The second part of the case study tests how the SRC handles failures in the machinery and propulsion system. This shows that the SRC changes MSO-mode and SO-mode to continue safely to the final way-point.

Further work includes adding more functions to the control system to increase autonomy, such as safe and reliable auto-docking. This will enable the ship to leave harbor, sail to a second location/harbor, deliver goods, and then return and dock in harbor again. This would be a typical cargo ship or passenger operation and would thus be an important step towards achieving highly autonomous ships. Route planning to enable the control system to change route depending on the risk level and environmental conditions, and looking at how a similar system can be used for decision support to human operators are also parts of the future work.

CRediT authorship contribution statement

Thomas Johansen: Writing – original draft, Software, Methodology, Investigation, Data curation, Conceptualization. **Simon Blindheim:** Writing – original draft, Visualization, Software, Conceptualization. **Tobias Rye Torben:** Writing – original draft, Software, Investigation, Conceptualization. **Ingrid Bouwer Utne:** Writing – review & editing, Supervision, Funding acquisition, Conceptualization. **Tor Arne Johansen:** Writing – review & editing, Supervision, Funding acquisition, Conceptualization. **Asgeir J. Sørensen:** Writing – review & editing, Supervision, Funding acquisition, Conceptualization,.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

Acknowledgments

The work by T. Johansen, S. Blindheim, T. Torben, I.B Utne, T.A. Johansen, and A.J. Sørensen is partly sponsored by the Research Council of Norway through the Centre of Excellence funding scheme, project number 223254, AMOS, Norway, and project ORCAS with project number 280655. The authors would also thank Dr. Børge Rokseth at NTNU for his input and help with the simulation setup and in general discussions.

Table 5
BBN Nodes, Input-RIFs are only listed as parent nodes.

Node description	Parent node(s)
Cost	Consequences
Consequences	Harm to humans, Damage on own ship, Damage on other ships/objects
Damage on other ships/objects	HE, Impact speed, Type of seabed, Type of shore
Damage on own ship	HE, Impact speed, Type of seabed, Type of shore
Harm to humans	HE, Impact speed, Type of shore
HE	H1, H2
H1	UCA-1, UCA-2, UCA-3, UCA-4, UCA-5
H2	UCA-1, UCA-2, UCA-3, UCA-4, UCA-5
UCA-1	H-RIF-1, H-RIF-2, H-RIF-3
UCA-2	H-RIF-1, H-RIF-2, H-RIF-3
UCA-3	H-RIF-2, H-RIF-3
UCA-4	H-RIF-4, H-RIF-5
UCA-5	H-RIF-4, H-RIF-5, H-RIF-6
H-RIF-1	Power, Propulsion
H-RIF-2	Power management system reliability, Controller performance/accuracy
H-RIF-3	Weather conditions, Control of ship, Congested waters
H-RIF-4	Controller performance/accuracy, Navigational instruments
H-RIF-5	Navigational instruments, Visual conditions
H-RIF-6	Controller performance/accuracy Ship design process
Power	PTO, PTI, Mech, MSO-mode
Propulsion	AP, DP
Weather conditions	Current, Wind direction, Wind speed
Control of ship	Weather conditions, SO-mode, Ship speed, Propulsion
Congested waters	Obstacle density, Distance to closest grounding hazard, Traffic density
Controller performance/accuracy	AP performance/accuracy, DP performance/accuracy, SO-mode, Weather conditions
Ship speed	Controller performance/accuracy, Speed reference
Navigational instruments	AIS, Radar, GNSS system
Visual conditions	Wind speed, Fog, Rain, Snow
PTO	ME state, HSG state
PTI	HSG state, DG1 state, DG2 state
Mech	ME state, DG1 state, DG2 state
AP	MSO-mode, MP state, ST state
DP	MSO-mode, MP state, BT state, AT state
Impact speed	Ship speed

Appendix. BBN connections

Tables with an overview of child/parent nodes in the BBN shown in Fig. 4.

References

[1] NSIA. Interim report 12 november 2019 on the investigation into the loss of propulsion and near grounding of viking sky, 23 march 2019. Technical report, Norwegian Safety Investigation Authority; 2019, URL https://havarikommisjonen.no/Marine/Investigations/19-262.

[2] Utne IB, Rokseth B, Sørensen AJ, Vinnem JE. Towards supervisory risk control of autonomous ships. Reliabil Eng Syst Saf 2020;196:106757.

[3] Thieme CA, Rokseth B, Utne IB. Risk-informed control systems for improved operational performance and decision-making. Proc Instit Mech Eng Part O: J Risk Reliabil 2021. 1748006X211043657.

[4] Johansen T, Utne IB. Supervisory risk control of autonomous surface ships. Ocean Eng 2022;251:111045.

[5] Bremnes JE, Thieme CA, Sørensen AJ, Utne IB, Norgren P. A bayesian approach to supervisory risk control of AUVs applied to under-ice operations. Mar Technol Soc J 2020;54(4):16–39.

[6] Bremnes JE, Norgren P, Sørensen AJ, Thieme CA, Utne IB. Intelligent risk-based under-ice altitude control for autonomous underwater vehicles. In: OCEANS 2019 MTS/IEEE seattle. 2019, p. 1–8.

[7] Fan C, Wróbel K, Montewka J, Gil M, Wan C, Zhang D. A framework to identify factors influencing navigational risk for maritime autonomous surface ships. Ocean Eng 2020;202:107188.

[8] Chang CH, Kontovas C, Yu Q, Yang Z. Risk assessment of the operations of maritime autonomous surface ships. Reliab Eng Syst Saf 2021;207.

[9] Johansen T, Utne IB. Risk analysis of autonomous ships. In: E-proceedings of the 30th european safety and reliability conference and 15th probabilistic safety assessment and management conference. 2020, p. 131–8.

[10] Valdez Banda OA, Kannos S, Goerlandt F, van Gelder PHAJM, Bergström M, Kujala P. A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. Reliab Eng Syst Saf 2019;191:106584.

[11] Wróbel K, Montewka J, Kujala P. Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. Reliabil Eng Syst Saf 2018;178:209–24.

[12] Chaal M, Valdez Banda OA, Glomsrud JA, Basnet S, Hirdaris S, Kujala P. A framework to model the STPA hierarchical control structure of an autonomous ship. Saf Sci 2020;132.

[13] Brito M, Griffiths G. A Bayesian approach for predicting risk of autonomous underwater vehicle loss during their missions. Reliab Eng Syst Saf 2016;146:55–67.

[14] Loh TY, Brito MP, Bose N, Xu J, Nikolova N, Tenekedjiev K. A hybrid fuzzy system dynamics approach for risk analysis of AUV operations. J Adv Comput Intell Intell Inform 2020;24(1):26–39.

[15] Loh TY, Brito MP, Bose N, Xu J, Tenekedjiev K. Fuzzy system dynamics risk analysis (FuSDRA) of autonomous underwater vehicle operations in the antarctic. Risk Anal 2020;40(4):818–41.

[16] Brito M. Uncertainty management during hybrid autonomous underwater vehicle missions. In: Autonomous underwater vehicles 2016, AUV 2016. 2016, p. 278–85.

[17] Hu L, Naeem W, Rajabally E, Watson G, Mills T, Bhuiyan Z, et al. COLREGs-compliant path planning for autonomous surface vehicles: A multiobjective optimization approach. IFAC-PapersOnLine 2017;50(1):13662–7.

[18] Wang H, Guo F, Yao H, He S, Xu X. Collision avoidance planning method of USv based on improved ant colony optimization algorithm. IEEE Access 2019;7:52964–75.

[19] Woo J, Kim N. Collision avoidance for an unmanned surface vehicle using deep reinforcement learning. Ocean Eng 2020;199:107001.

[20] Lyu H, Yin Y. COLREGS-constrained real-time path planning for autonomous ships using modified artificial potential fields. J Navig 2019;72(3):588–608.

[21] Li M, Mou J, Chen L, He Y, Huang Y. A rule-aware time-varying conflict risk measure for MASS considering maritime practice. Reliab Eng Syst Saf 2021;215.

[22] Gil M. A concept of critical safety area applicable for an obstacle-avoidance process for manned and autonomous ships. Reliab Eng Syst Saf 2021;214.

[23] Tengesdal T, Brekke EF, Johansen TA. On collision risk assessment for autonomous ships using scenario-based MPC. IFAC-PapersOnLine 2020;53(2):14509–16.

[24] Tengesdal T, Johansen TA, Brekke E. Risk-based autonomous maritime collision avoidance considering obstacle intentions. In: Proceedings of 2020 23rd international conference on information fusion, FUSION 2020. 2020.

[25] Blindheim S, Gros S, Johansen TA. Risk-based model predictive control for autonomous ship emergency management. IFAC-PapersOnLine 2020;53(2):14524–31.

[26] Yin J, Wang Y, Lv J, Ma J. Study on underwater simultaneous localization and mapping based on different sensors. In: Proceedings of 2021 IEEE 10th data driven control and learning systems conference. 2021, p. 728–33.

[27] Willners JS, Carreno Y, Xu S, Luczynski T, Katagiri S, Roe J, et al. Robust underwater SLAM using autonomous relocalisation. IFAC-PapersOnLine 2021;54(16):273–80.

[28] Sandøy SS, Hegde J, Schjølberg I, Utne IB. Polar map: A digital representation of closed structures for underwater robotic inspection. Aquacult Eng 2020;89:102039.

[29] Mąka J, Magaj J. Data extraction from an electronic S-57 standard chart for navigational decision systems. In: Proc. zeszyty naukowe/akademia morska szczecinie. 2012, p. 83–7.

[30] Blindheim S, Johansen TA. Electronic navigational charts for visualization, simulation, and autonomous ship control. IEEE Access 2022;10:3716–37.

[31] Wróbel K, Montewka J, Kujala P. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliab Eng Syst Saf 2017;165:155–69.

[32] de Vos J, Hekkenberg RG, Valdez Banda OA. The impact of autonomous ships on safety at sea – a statistical analysis. Reliab Eng Syst Saf 2021;210.

[33] IMO. MSC.1/Circ.1580: annex: guidelines for vessels with dynamic positioning systems. IMO; 2017.

[34] Torben T, Smogeli Ø, Utne IB, Sørensen AJ. On formal methods for design and verification of maritime autonomous surface ships. In: Proceedings of the world maritime technology conference. 2022.

[35] Pedersen TA, Glomsrud JA, Ruud EL, Simonsen A, Sandrib J, Eriksen BOH. Towards simulation-based verification of autonomous navigation systems. Saf Sci 2020;129:104799.

[36] Torben T, Glomsrud JA, Pedersen TA, Utne IB, Sørensen AJ. Automatic simulation-based testing of autonomous ships using Gaussian processes and temporal logic. Proc Inst Mech Eng Part O: J Risk Reliabil 2022. 1748006X211069277.

[37] Xiao G, Ren B, Tong C, Hong X. A quantitative evaluation method for obstacle avoidance performance of unmanned ship. J Mar Sci Eng 2021;9(10):1127.

[38] Leveson N. Engineering a safer world: systems thinking applied to safety. Engineering systems, MIT Press; 2011.

[39] Fenton N, Neil M. Risk assessment and decision analysis with bayesian networks. CRC Presss; 2019.

[40] Maler O, Nickovic D. Monitoring temporal properties of continuous signals. In: Lecture notes in computer science, no. 2004. 2004, p. 152–66.

[41] Rokseth B, Utne IB. Deriving safety requirement hierarchies for families of maritime systems. Trans R Inst Naval Archit Part A: Int J Marit Eng 2019;161:A229 – A243.

[42] Rokseth B, Utne IB, Vinnem JE. Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis. Reliab Eng Syst Saf 2018;169:18–31.

[43] Pedersen TA, Neverlien Å, Glomsrud JA, Ibrahim I, Mo SM, Rindarøy M, et al. Evolution of safety in marine systems: From system-theoretic process analysis to automated test scenario generation. In: International conference on maritime autonomous surface ships. 2022.

[44] Rasmussen CE, Williams CKI. Gaussian processes for machine learning. MIT Press; 2006.

[45] IMO. Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process. Technical report, IMO; 2018, URL https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/MSC-MEPC%202-Circ%2012-Rev%202.pdf.

[46] EfficienSea. Methods to quantify maritime accidents for risk-based decision making. Technical report, EfficienSea; 2012, URL http://efficiensea.org/files/mainoutputs/wp6/d_wp6_4_1.pdf.

[47] The Norwegian Agency for Public and Financial Management. Guide in socio-economic analysis. 2018, URL https://dfo.no/fagomrader/utredning/samfunnsokonomiske-analyser/verdien-av-et-statistisk-liv-vsl.

[48] DNVGL. DNV report no 2003-0277 annex II FSA 2003. Technical report, DNVGL group technology & research; 2003, URL http://research.dnv.com/skj/FSALPS/ANNEXII.pdf.

[49] Hassel M, Utne IB, Vinnem JE. An allision risk model for passing vessels and offshore oil and gas installations on the norwegian continental shelf. Proc Inst Mech Eng Part O: J Risk Reliabil 2021;235(1):17–32.

[50] Norwegian Meteorological Institute. Met. 2021, URL https://www.met.no/en/weather-and-climate.

[51] Norwegian Mapping Authority. Norgeskart. 2021, URL https://norgeskart.no.

[52] Ship & Bunker. Rotterdam bunker prices. 2022, URL https://shipandbunker.com/prices/emea/nwe/nl-rtm-rotterdam#LSMGO.

[53] Stopford M. Maritime economics. 3r ed.. Routledge; 2009.

[54] Utkin V, Lee H. Chattering problem in sliding mode control systems. IFAC Proc Vol 2006;39(5):1, 2nd IFAC Conference on Analysis and Design of Hybrid Systems.

[55] Norwegian Hydrographic Service. The norwegian pilot guide. 2018, URL https://kartverket.no/en/at-sea/nautical-publications/the-norwegian-pilot-guide-sailing-directions.

[56] Fossen TI. Handbook of marine craft hydrodynamics and motion control. John Wiley and Sons Ltd; 2011.