Ocean Engineering 251 (2022) 111045

Contents lists available at ScienceDirect

Ocean Engineering

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

Supervisory risk control of autonomous surface ships

Thomas Johansen [*], Ingrid Bouwer Utne

Centre for Autonomous Marine Operations and Systems (NTNU AMOS), NTNU, Norway
Department of Marine Technology, NTNU Norwegian University of Science and Technology, Trondheim, 7491, Norway

ARTICLE INFO

Keywords:
Autonomous systems
Risk modeling
Ship control systems
STPA
Bayesian Belief Networks
Hazard identification

ABSTRACT

The objective of this paper is to develop online risk models that can be updated as conditions change, using risk as one metric to control an autonomous ship in operation. This paper extends and integrates the System Theoretic Process Analysis (STPA) and Bayesian Belief Networks (BBN) with control systems for autonomous ships to enable supervisory risk control. The risk metric is used in a Supervisory Risk Controller (SRC) that considers both risk and operational costs when making decisions. This enables the control system to make better and more informed decisions than existing ship control systems. The novel control system is tested in a case study where the SRC can change: (i) which machinery system is active; (ii) which control mode to run the ship in; and (iii) which speed reference to follow. The SRC is able to choose the optimum machinery, control mode, and speed reference to maintain safe control of the ship over a route in changing conditions.

1. Introduction

This paper will demonstrate how risk models can be utilized by ship control systems (i.e., supervisory risk control) to enable better situational awareness and decision support for autonomous ships (Utne et al., 2020b). The development of Maritime Autonomous Surface Ships (MASS) is an important trend in the maritime industry (Kretschmann et al., 2015; Wróbel et al., 2017), which requires the development of more advanced control systems that can function with less human control. Although many ships in operation today already have systems for autonomous control, none of them are designed for fully unmanned operations. Even the most advanced systems, such as the bastø-ferry crossing the Oslofjord (Kongsberg, 2020) and the Milliampere small passenger ferry that is intended to cross a part of Nidelven in Trondheim (Springwise, 2018), still have human operators who make decisions and supervise the operation.

The control of ships can be divided into three main levels (Ludvigsen and Sørensen, 2016): mission planner level, guidance and optimization level, and control execution level. The mission objective is defined and planned in the mission level. The guidance and optimization level handles way-points for the navigation system and optimization of resources. Control execution controls the actuators (e.g., engines and rudders) and plant, such as Dynamic Positioning (DP) and auto-pilot (Sørensen, 2005). Supervisory risk control focuses on the two highest levels of a control system.

Guidance and optimization have two main challenges: planning an efficient and safe route to follow, and managing resources such that the ship has sufficient power and control but at the same time not use too much energy and lead to higher costs. Many existing ships have systems for planning the route, but this is still a task where human operators are involved by either supervising and controlling, or planning the whole route. The same is the case with optimization, where many ships have power management systems but where humans still supervise and manage these systems. The challenge is similar for mission planning, namely to plan the mission such that safety and efficiency are sufficiently accounted for in the decision process. Risk models can enable the control systems to make better decisions in these cases by showing how decisions affect the risk level.

Control systems for autonomous ships need many of the same functionalities as existing ships but they also require some additional functions to handle higher level decisions. For the ship to maneuver at both high and low speeds, the ship needs two controllers. This can be a DP controller for low speed maneuvering and station-keeping, and a heading and speed controller for higher speeds. Each of these controllers also needs a thrust allocation system to convert the control output to thrust set-points for the different thrusters. An example control system is shown in Fig. 1.

The way-points for the controller to follow are planned by a guidance module. This module must handle both permanent obstacles in the route, and other ships and moving obstacles. For highly autonomous ships, the guidance module also needs a way to prioritize, or handle, multiple obstacles at the same time. For both the controller and guidance module to function, autonomous ships need a system for handling

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

https://doi.org/10.1016/j.oceaneng.2022.111045
Received 10 August 2021; Received in revised form 17 December 2021; Accepted 4 March 2022
Available online 23 March 2022

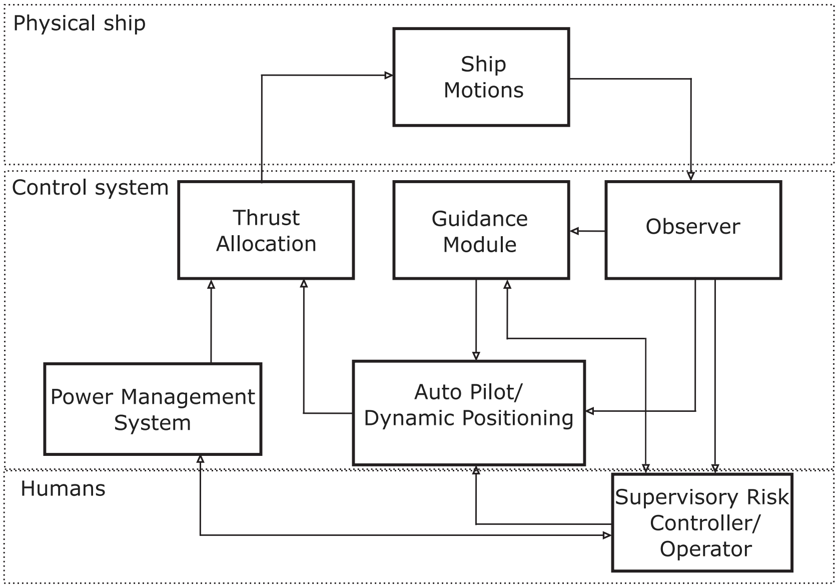


Fig. 1. Ship control system.

sensor-input and sorting this information. Many ships with DP have an observer where position measurements are filtered and processed such that the ship has an accurate position and can handle faulty measurements without losing the position (Sørensen, 2005). Fully autonomous ships need at least this capability, as well as systems for handling cameras and weather sensors. The last main part of the control system is the power management system (PMS). This system must ensure that the ship has enough power available for both propulsion and other loads. Autonomous ships must also have systems for deciding what type of motion controller to use (e.g., DP or auto-pilot). These systems must consider both the type of operation (e.g., cargo or passenger transport) and the specific conditions (e.g., wind, current, and waves) that affect the ship.

Combining and utilizing risk analysis and modeling with existing control systems is one possible way to enable better decisions for autonomous ships and make control systems that can function without human input. In their paper, Utne et al. (2020b) present a framework where the System Theoretic Process Analysis (STPA) is used as a basis for making a Bayesian Belief Network (BBN) risk model. The risk model can then be used to provide information about the current risk level while the ship is sailing by updating the model. The model can then provide information about how different decision options may change the overall risk. This can be especially useful in the two highest control levels: mission planning, and guidance and optimization. The mission, or voyage, can be planned to account for weather information, traffic, maintenance status, and ship conditions such that the voyage can be both safe and efficient. While the ship is sailing, the route can be replanned and optimized to account for changes in weather, traffic, and the condition of the ship such that the risk can be kept at an acceptable level during the whole voyage. The risk model can also be used to optimize the machinery and control of the ship by including risk when optimizing power production and selecting control modes.

Previous work related to risk analysis and control of autonomous ships has focused on these topics separately, and limited emphasis has been put on not how to use risk models as an integrated part of the control system. An exception is the framework proposed in Utne et al. (2020b), which outlines at an overall level how such integration may occur. One of the challenges faced by the current STPA is that consequences are not considered, which is important information for a risk model. The current paper extends the STPA, advances the framework of Utne et al. (2020b), and tests it in a case study.

Johansen and Utne (2020) discuss how STPA can be used for hazard identification for autonomous ships, and focuses on methods for finding additional data for building a risk model. Fan et al. (2020) present a framework for identifying factors that influence navigational risk for autonomous ships. Chaal et al. (2020) present a framework for how the control structure of autonomous ships can be modeled for use in STPA. Valdez Banda et al. (2019b) use STPA for a systemic hazard analysis of two autonomous ferry concepts and suggest safety controllers to manage these hazards. Valdez Banda and Goerlandt (2018) use a similar approach to the design of a safety management system for Vessel Traffic Services in Finland that may be relevant for autonomous ships. Valdez Banda et al. (2019a) present an evaluation framework for a Systems-Theoretic Accident Model and Processes (STAMP) based safety management system. However, even though these studies are useful, none of them use the results further in either risk models or control systems.

Brito and Griffiths (2016) present a Bayesian approach for predicting the risk of losing AUVs during missions. Brito (2016) proposes a method for handling uncertainty in AUV missions. Loh et al. (2020) present a hybrid fuzzy system dynamic risk analysis that can provide recommendations for risk management in AUV operations. These show different tools that can be useful for risk control and management, but they are not combined with a thorough hazard analysis, such as STPA, nor are they implemented in control systems. A few works have used a BBN risk model for control of AUVs (Bremnes et al., 2019, 2020), where the BBN is based on a checklist based Preliminary Hazard Analysis (PHA), and not STPA. These also consider a different type control where the objective is to follow and measure the ice surface above the AUV.

Rødseth and Tjora (2015) discuss how to include risk when designing the control system, but without showing how it can be used in the control system. Risk analysis of autonomous ships have been addressed in Wróbel et al. (2016) and Shuai et al. (2020), and supervisory risk control in Utne et al. (2020a), but not explicitly implemented in the control system as in this paper. Other works have used BBNs for assessing both autonomous ship operations (Chang et al., 2021) and traditional manned ships (Yu et al., 2021; Ung, 2021; Vojkovic et al., 2021) Risk is addressed as a part of collision avoidance for autonomous ships (Hu et al., 2017; Naeem et al., 2016; Campbell et al., 2012; Campbell and Naeem, 2012; Wang et al., 2019; Woo and Kim, 2020; Lyu and Yin, 2019), but without a direct link to risk analysis and modeling.

The rest of this paper is structured as follows: Section 2 presents the method used for supervisory risk control. Section 3 shows how the method can be used in a case study. Section 4 presents and discusses the results. Finally, Section 5 concludes the paper.

2. Method

The proposed method for implementing supervisory risk control is based on three overall stages (Utne et al., 2020b):

(a) Conduct an extended STPA of the ship and its operation, also including consequences;
(b) Build a BBN risk model based on the extended STPA;
(c) Implement the risk model in a Supervisory Risk Controller (SRC).

2.1. An extended system theoretic process analysis

The first stage is to perform a STPA of the MASS in the operational context that it is designed for. The general STPA consists of four main steps (Leveson, 2011):

(a) Define the system
(b) Identify system-level accidents, and system-level hazards
(c) Identify unsafe control actions (UCA)
(d) Develop loss scenarios

An accident can be defined as “a sudden, unwanted, and unplanned event or event sequence that has led to harm to people, the environment, or other tangible assets” (Rausand and Haugen, 2020). Even though the term “accident” is used in the general STPA, the consequences of the system level hazards and accidents are usually not explicitly considered or described with this method. For supervisory risk, control consequences need to be included to support the decision making of the autonomous control system because potential consequences of hazardous events (and hence risk) may change during operation, which may influence the decisions to be made. Therefore, this paper uses the term “system level hazardous event”, instead of accident. This adds the analysis of consequence as a fifth step, meaning that the hazardous event and the potential consequences together may encompass an accident.

The first step of the STPA is to define and describe the system. This includes modeling the control structure and describing control responsibilities, feed-back signals, and process variables for the different controllers. The second step is to define the system-level hazardous events and system-level hazards. Each system-level hazard has a safety constraint. The third step is to identify the UCAs that violate the safety constraints and can lead to hazardous events. The fourth step in the STPA is to develop loss scenarios. These scenarios describe how the hazardous events can occur and what can cause these events. The STPA gives a basis for assessing risk in the supervisory risk controller. Step five is to develop the risk model, it is also necessary to specify the worst-case conditions that, in combination with system-level hazards, lead to the accidents.

2.2. Online risk model

The next phase is to develop the online risk model to be used in the control system. In this paper, this means providing an output that can be used directly in a cost function for finding best set of decisions. The BBN consists of five main type of nodes:

- Consequences
- Hazardous events
- System level hazards
- Unsafe control actions
- Risk influencing factors

The results of the STPA (phase 1) are used to define the nodes and structure of the BBN. The STPA identifies how risk influencing factors (RIF) can lead to unsafe control actions (UCA). These can further lead to system level hazards, hazardous events, and consequences from these events. The same structure is used to build the BBN. The consequences are caused by the hazardous events, and a set of environmental conditions or RIFs. Each hazardous event is caused by system level hazards with certain RIFs, The system level hazards are caused by one or more UCAs. The UCAs are similarly caused by one or more RIFs. For a more detailed explanation of mapping STPA results into a BBN, the reader is referred to Utne et al. (2020b).

The top level nodes and output from the risk model are the consequences. Hazardous events are events that may result in losses (negative consequences). System level hazards are the system states, or conditions, that result from UCAs and which can lead to accidents. The unsafe control actions are control actions that lead to system level hazards. The last type is RIFs, which are either high-level RIFs or input RIFs. High-level RIFs are identified directly from the loss scenarios in the STPA. Input RIFs are causal factors used to characterize high-level RIFs and how hazards can lead to accidents. The risk model is used to assess the risk of accidents at each time step, given the current conditions for the ship in operation.

2.3. Supervisory risk controller

The SRC is the controller that makes the high level decisions based on the risk level and operational costs. The controller has a set of possible decisions that can be made about how the ship is configured, and control objectives and parameters for lower level controllers. The goal is to find the optimum combination of decisions, d, that minimizes a cost function M with both risk, R, and operational costs, C. The risk cost is the cost expected from the accidents and consequences from the BBN risk model. The operational cost is based on the expected fuel consumption for the remaining sailing time. This gives an estimation of the energy cost for the planned sailing route that can be compared to the risk cost from the BBN(1).

$$M(d) = R(d) + C(d) \tag{1}$$

The risk cost is taken directly from the BBN and will vary between zero cost and the cost of the worst consequences considered in the BBN. The operation cost is calculated based on the specific fuel consumption for the ship and the remaining sailing time. A specific example of the cost function is shown in Sections 3.2.1 and 3.3, but these can vary depending on the ship and how it is operated. This make it possible to adjust the cost function based on the specific ship, operation, and available information as long as the cost can be represented as a function of the decisions made by the ship.

The decisions, d, can include which control mode to operate in, the machinery configuration in which the ship should operate, references for lower level controllers, or other decisions that affect the ship. The controller is implemented as a switch that configures the ship based on the optimum set of decisions. The switch checks all possible combinations of decisions to find the best combination. The switching mechanism is implemented with a lower switching frequency to avoid chattering in the controller and to increase the efficiency.

Chattering occurs when the controller switches back and forth between different modes because the system is on the limit between different modes. A switching frequency that is too low means that the controller will not react to changes, such as increased traffic, because the ship passes the traffic before the controller has checked. A switching frequency that is too high will lead the controller to always change, such as constantly switching between DP and auto-pilot, because the conditions are right on the limit between these modes. The frequency can therefore be changed to make sure that the controller reacts fast enough without chattering.

By including consequences and conditions affecting these, the SRC is not only able to prevent hazardous events, but also reduce the severity if such events occur. In a situation, for example, when the weather and area around the ship become so challenging that the ship will most likely collide/allide, the SRC will reduce the speed of the ship to limit the consequences.

3. Case study: Autonomous cargo ship

The case study in this paper uses the presented methodology for an autonomous cargo ship on a voyage between two locations along the Norwegian coast. The purpose of the ship is to deliver fish food to a fish farm. The ship follows a preplanned route, and dock next to a floating fish-farm so that it can unload the cargo. The route consists of both open and congested waters with islands, ship traffic, and other obstacles (e.g., fish farms, oil and gas installations, containers, navigation markers, etc.) that the ship must account for. The case study assumes good weather conditions, i.e., little wind, current, and good visibility, but the SRC is designed to also include different weather conditions. The ship is unmanned with a supervisor on shore that can monitor and, if necessary, take remote control of the ship. The ship is 80 m long and 16 m wide at its widest point.

The ship has a hybrid power system with a gas powered main engine, a set of diesel generators, and a hybrid shaft generator (HSG). The HSG can be used as a generator that is powered by the main engine to produce electricity or as an engine powered by the diesel generators for propulsion. The machinery system can be configured in three different modes:

- Power Take Out (PTO)
- Power Take In (PTI)
- Mechanical (Mech)

In PTO, the main engine is on and the HSG is configured as a generator such that the main engine provides both propulsion and electrical power. In PTI, the diesel generators are used with the HSG configured as an electric engine for propulsion. In Mech, the main engine provides propulsion power and the diesel generators provide electrical power. Of these modes, PTO is the most used mode because the main engine is most economical in normal use. PTI is the least used mode because the diesel generators provide much less power than the main engine and the ship is not able to maintain speeds above 5 m/s. Mech has the most power available because all of the main engine capacity can be used for propulsion, but it is also the most costly because it uses both the main engine and diesel generators.

The ship has two operating modes:

- Heading and Speed Auto Pilot (AP)
- Dynamic Positioning (DP)

Heading and speed auto pilot is used for higher speeds and longer distances. The main propeller provides propulsion and the rudder is used for steering. DP is used at lower speeds when necessary to better control the ship. In DP, the main propeller and tunnel thrusters are used for both propulsion and steering. The SRC is responsible for selecting the best combination of MSO-mode, SO-mode, and reference speed based on both internal and external factors. An example of this is changing MSO-mode when components fail, or lowering the speed and choosing DP when it is necessary with better motion control.

3.1. Phase 1: The extended STPA

The STPA was performed in a workshop with industry participants and risk analysts to facilitate the analysis. The goal was to identify unsafe control actions for an autonomous cargo ship. The main focus was on the machinery system, and how the switching between different modes (see above) can lead to grounding or impacts with ships or obstacles. The workshop had 13 participants and went over three days in the winter of 2019. The participants have thorough knowledge and experience with ship control systems, risk analysis, and system verification. The workshop was conducted as a discussion between the participants where STPA was used to identify unsafe control actions.

3.1.1. Define the system

The system described in Section 3, is first modeled as a hierarchical control structure; as shown in Fig. 2. The system consists of three main control levels; supervisory control, guidance and optimization, and control execution. The case study focuses mainly on the SRC and its responsibilities:

(a) Set ship operating (SO) mode for the Autonomous Navigation System (ANS)
(b) Set reference parameters, such as max speed for the ANS to follow
(c) Set machinery system operating (MSO) mode for the Autonomous Machinery Management System (AMMS)

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

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

3.1.2. Identify hazardous events and system level hazards

The case study focuses on two system-level hazardous events:

- HE1: The ship collides with a ship
- HE2: The ship allides with another object

The corresponding system-level hazard is

- H1: The ship violates the minimum distance of separation to an obstacle

The relationship between the hazard and hazardous event depend on factors such as the type and size of obstacle/ship, what control the obstacle/ship has, and impact speed (DNVGL, 2003).

To structure the analysis more clearly, the hazardous event "collision" is subdivided into two: the first is that the ship collides with another ship, and the second is allision with other objects. This makes it easier to define the consequences. For this case study, the main focus is on the first hazardous event (A1) and first system-level hazard (H1).

3.1.3. Identify unsafe control actions

The STPA workshop identified a total of 60 unsafe control actions (UCA) for the whole control system. Five of these are chosen for further use in the case study as shown in Table 1. The number of UCAs used in the BBN are limited to avoid an unnecessary complex model. The STPA seek to identify all UCAs that can affect the ship, but many of these are caused by the same RIFs, such as sensor failures in the navigation system. A BBN with more nodes will also have a negative effect on the computation time when updating the model as the ship is sailing, and affect the time necessary to define the BBN. When choosing how many and what UCAs to include, the challenge is to have a sufficient number to get a good enough situational awareness, but limit the time necessary for both building and using the BBN in the controller.

The first step to limit the number of UCAs is to only consider UCAs where the SRC is giving a command, since the purpose of the BBN is to enable the SRC to make decisions. Of the 60 UCAs identified in the workshop, 15 are commands where the SRC give a command leading

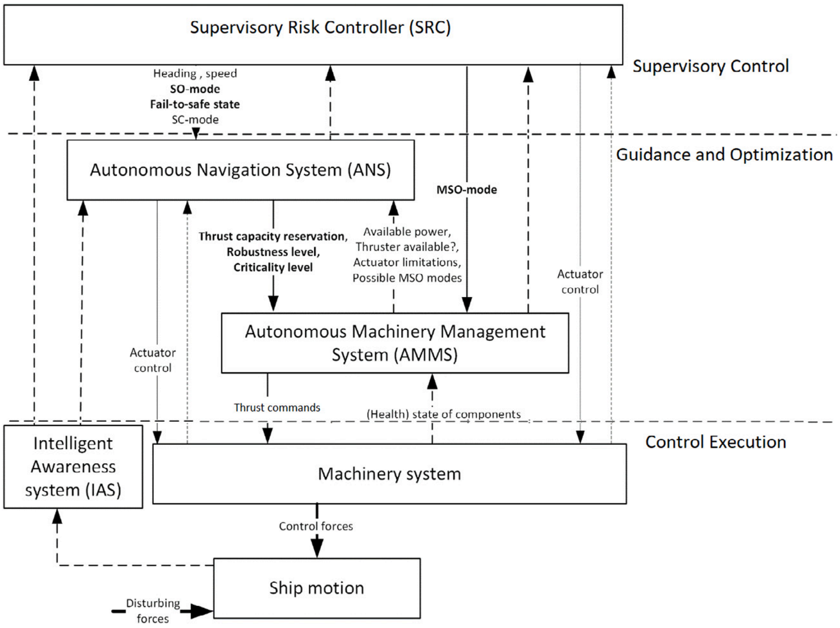


Fig. 2. Hierarchical control structure.

Table 1
Unsafe control actions.

UCA	Description
UCA-1	A command is given to change MSO-mode to PTO when a fault inhibits the machinery from producing the necessary thrust
UCA-2	A command is given to change MSO-mode to Mech when the main engine does not function
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 when uncontrolled motion may cause violation of the minimum safe distance to shore or objects
UCA-5	A command is given to change SO-mode to maneuvering when the speed is higher than the maximum maneuvering speed which may result in loss of motion control

the system-level hazard. Of these 15, four changes MSO-mode to PTO, five to Mech, and two to PTI. All these are caused by a failure in the machinery system or inaccurate estimation of the power necessary. Since the same factors affect all the UCAs, it is sufficient for the SRC to have one UCA for each MSO-mode and still have a good situational awareness. Two of the UCAs change SO-mode to transit and two change to DP. Both UCAs that changes to transit are scenarios where the ship need more accurate motion control. Either of these can therefore be used in the BBN as they both have the same causes. For changing to DP, the scenario is either caused by switching with to much speed, or not enough power available. Since power is already included in the BBN, wrong speed is more important to include in the BBN.

3.1.4. Develop scenarios

The next step in the STPA is to develop scenarios that can lead to unsafe control actions. A total of 11 scenarios are developed in this case study, where all UCAs have two scenarios and UCA-2 has three potential scenarios. The scenarios are shown and described in Table 2.

3.1.5. Analyze consequences

For the risk model to be useful, it is necessary to find out more about the consequences related to the accidents. Consequences are identified and categorized based on information in DNVGL (2003) and Kristiansen (2005). These also give information about what conditions affect how serious the different consequences are. The damage to the ship and the object/ship the ship collides with will (for example) depend on factors such as impact speed, type of object, and size of object (DNVGL, 2003).

In this case study, the consequences are:

- Harm to humans
- Damage on other ships/objects
- Damage on own ship

The consequences are analyzed and divided into three categories (IMO, 2018). Severe consequences are fatalities or serious injuries to humans, damage to the ship where it is necessary with assistance to get back to shore and receive extensive repairs, or extensive damage to other ships/objects where extensive repairs are also necessary. Significant consequences are less serious/minor injuries to humans, and damage to the ship or other ships/objects that need extra repairs outside of planned maintenance, but it is not necessary with extra assistance to get back to shore. Minor consequences are insignificant/no injuries to humans, and damage to the ship or other ships/objects that can be fixed during the next planned maintenance. The IMO (2018) manual also include catastrophic consequences, but these are considered unacceptable, and therefore not relevant for the SRC.

3.2. Phase 2: Online risk model

3.2.1. Define end-nodes and UCA nodes

The goal, or top node, in the BBN is the expected risk calculated from Eq. (2).

The BBN includes consequences that are divided into severe, significant, minor, and no consequences. Each of these have a corresponding cost, and the overall cost (i.e., the quantitative risk) is calculated as shown in Eq. (2).

The cost of severe consequences is set to 45 000 000NOK, significant to 4 500 000NOK, minor to 450 000NOK and no consequences give zero cost. These are estimated costs for each category of consequences based on EfficienSea (2012), The Norwegian Agency for Public and Financial Management (2018), and IMO (2018). The highest cost is limited to 45 000 000NOK because costs above this level are unacceptable. In situations with potential consequences in the highest category, the SRC should choose the configuration with the lowest possible expected

Table 2
Scenarios.

Scenario	Description	UCA
SC-1	MSO changed to PTO because PTI delivers insufficient amount of power, but a failure in the ME or propeller shaft results in loss of propulsion.	UCA-1
SC-2	MSO changed to PTO because this is more efficient given the current operational conditions, but a failure in the ME or propeller shaft results in loss of power.	UCA-1
SC-3	MSO changed to Mech because PTI is not producing sufficient power, but a failure with the main engine leads to loss of propulsion.	UCA-2
SC-4	MSO-mode is changed to Mech to have higher margin on power in, a more challenging navigational situation, but a failure in the main engine results in loss of propulsion power	UCA-2
SC-5	MSO changed to Mech because this is more efficient given the current operational conditions, but a failure in the main engine results in loss of propulsion power.	UCA-2
SC-6	MSO-mode is changed to PTI because inaccurate/incorrect measurements leads to underestimated power-need for propulsion.	UCA-3
SC-7	MSO-mode is changed to PTI because the main engine is shut down by another system, resulting in insufficient power for propulsion.	UCA-3
SC-8	SO-mode is changed to transit to early after leaving harbor due to inaccurate/incorrect measurements of the ship states	UCA-4
SC-9	SO-mode is changed to transit when inaccurate/incorrect information about the navigational area leads to underestimation of the navigational complexity.	UCA-4
SC-10	SO-mode is changed to maneuvering when the navigational situation makes it necessary to have better control of the vessel, but the speed is not sufficiently low enough when making the switch.	UCA-5
SC-11	SO-mode is changed to maneuvering as the ship approaches harbor and an inaccurate/incorrect speed measurement results in to early switching	UCA-5

Table 3
Risk influencing factors.

RIF	Description	Scenario(s)
RIF-1	Estimation of necessary thrust	SC-1, SC-3
RIF-2	Power optimization	SC-2, SC-5
RIF-3	Navigational complexity/situation	SC-4
RIF-4	Measurement/estimation of ship's navigational states	SC-6, SC-8, SC-11
RIF-5	Engine control system	SC-7
RIF-6	Route description/information	SC-9
RIF-7	Machinery system status	SC-1, SC-2, SC-3, SC-4, SC-5

risk cost, or minimum risk condition. In this case study, this means a speed of 1 m/s, PTO as MSO-mode, and DP as SO-mode.

$$c = Pr(severe)C_{severe} + Pr(significant)C_{significant} + Pr(minor)C_{minor} + Pr(no)C_{no} \tag{2}$$

The BBN has one node for collision with other ships, and one for allision with other objects. The system-level hazard is hazard H1 in Section 3.1.2 where the ship violates the minimum distance of separation to a ship/obstacle.

3.2.2. *Identify high-level RIFs*

The high-level RIFs are identified based on the scenarios developed in Section 3.1.4. A total of seven high-level RIFs are identified as in Table 3.

3.2.3. *Identify input RIFs*

With the high-level RIFs identified, the next step is to identify the input and intermediate nodes. These are causal factors that describe the high-level RIFs, how the hazard lead to unwanted consequences, or decisions nodes for the different decisions available in the SRC.

The causal factors are identified by going through the high-level RIFs and assessing what may affect these, or how the system-level hazard can lead to different consequences. For example, the machinery system status is dependent on the propulsion system and the power system. The propulsion system in turn depends on the different propulsion components. The consequences will (for example) depend on the impact speed, whether the impact is with another ship or another object, and the amount of humans on the other ship/objects that might be harmed in the impact.

By organizing the BBN in this way, the amount of parent nodes can be limited. This also makes it easier to define states and conditional probability tables (CPT) because these depend on the number of parent nodes and states in the parent nodes.

The system has three decision nodes: MSO-mode switch choosing which MSO-mode to run the machinery in, SO-mode switch to select the active controller, and speed reference to set the reference used in the controller. The input nodes in the BBN can be divided into three categories; Machinery system (M), Environment (E), and Control system/planning (C). The category of each node is shown in Table 4. Weather affects the model in two different ways; ship motions and visual conditions. Ship motions are affected by wind and currents. Wind can be everything from zero wind to hurricane. Current can also vary between zero current and very strong currents where the ship is unable to maintain control. The visual conditions is affected by wind, rain, fog, and snow. High wind combined with snow or rain, or fog give poor visibility that can affect sensors aboard the ship. The area around the ship is described by the node navigational area complexity. This node is affected by ship density, obstacle density, and what type of area the ship is sailing in. Another node that should be explained further is the reliability of own ship's navigational states. This node represents the quality and accuracy of sensor measurements for the ship, which can be affected by faulty sensors, incorrect setup or tuning, or disturbances. A full list of nodes are shown in Table 4. A similar list with the connections for each node are given in Tables 6–8. The full BBN is shown in Fig. 3.

Table 4
BBN Nodes.

Node description	Type	States
Cost	Output	Cost
Consequences	Top-level consequences	Severe/Significant/Minor/None
Damage to others property	Sub-level consequences	Severe/Significant/Minor/None
Damage to own ship	Sub-level consequences	Severe/Significant/Minor/None
Harm to humans	Sub-level consequences	Severe/Significant/Minor/None
HE1-The ship collides with a ship	System-level hazardous event	Yes/No
HE2-The ship allides with another object	System-level hazardous event	Yes/No
H1-The ship violates the minimum distance of separation to an obstacle	System-level hazard	Yes/No
UCA1-A command is given to change MSO-mode to PTO when a fault inhibits the machinery from producing the necessary thrust	UCA	Yes/No
UCA2-A command is given to change MSO-mode to Mech when the main engine does not function	UCA	Yes/No
UCA3-A command is given to change MSO mode to PTI, resulting in insufficient power for the main propulsion	UCA	Yes/No
UCA4-A command is given to change SO-mode to transit when uncontrolled motion may cause violation of the minimum safe distance to shore or objects	UCA	Yes/No
UCA5-A command is given to change SO-mode to maneuvering when the speed is higher than the maximum maneuvering speed which may result in loss of motion control	UCA	Yes/No
RIF1-Estimation of necessary thrust	RIF	Incorrect/Imprecise/Correct
RIF2-Power optimization	RIF	Poor/Sufficient/Good
RIF3-Navigational complexity/situation	RIF	High/Medium/Low
RIF4-Measurement/estimation of ship's navigational states	RIF	Incorrect/Imprecise/Correct
RIF5-Engine control system	RIF	Poor/Sufficient/Good
RIF6-Route description/information	RIF	Poor/Sufficient/Good
RIF7-Machinery system status	RIF	Failed/Ok
Propulsion system state	Intermediate	Failed/Ok
Power system state	Intermediate	Failed/Ok
Weather conditions	Intermediate	Poor/Sufficient/Good
Visual conditions	Intermediate	Poor/Sufficient/Good
DP propulsion	Intermediate	Failed/Ok
Auto-pilot propulsion	Intermediate	Failed/Ok
PTO	Intermediate	Failed/Ok
Mech	Intermediate	Failed/Ok
PTI	Intermediate	Failed/Ok
Control of ship	Intermediate	Poor/Sufficient/Good
Controller performance	Intermediate	Poor/Sufficient/Good
Ship speed	Intermediate	High/Medium/Low
Navigation area complexity	Intermediate	High/Medium/Low
Controllable speed	Intermediate	No/Yes
Impact speed	Intermediate	High/Medium/Low
Category of obstacle	Intermediate	Ship/Other
MSO-mode switch	Decision	PTO/Mech/PTI
SO-mode switch	Decision	Auto-pilot/DP
Speed reference	Decision	1–8 m/s
Power management system function	Input(C)	Poor/Sufficient/Good
Obstacle density	Input(E)	Low/medium/High
Traffic density	Input(E)	Low/medium/High
Ship safety system function	Input(C)	Poor/Sufficient/Good
Reliability of own ship's navigational states	Input(C)	Poor/Sufficient/Good
Route information	Input(C)	Poor/Sufficient/Good
Bow thruster state	Input(M)	Failed/Ok
Aft thruster state	Input(M)	Failed/Ok
Main propeller state	Input(M)	Failed/Ok
Steering system state	Input(M)	Failed/Ok
ME state	Input(M)	Failed/Ok
Genset 1 state	Input(M)	Failed/Ok
Genset 2 state	Input(M)	Failed/Ok
HSG state	Input(M)	Failed/Ok
Current velocity	Input(E)	High/Medium/Low
Auto-pilot performance	Input(C)	Poor/Sufficient/Good
DP-controller performance	Input(C)	Poor/Sufficient/Good
Wind speed	Input(E)	High/Medium/Low
Fog	Input(E)	High/Medium/Low
Rainfall	Input(E)	High/Medium/Low
Snowfall	Input(E)	High/Medium/Low
Area type	Input(E)	Harbor/Coastal/Open
Speed of ship/obstacle	Input(E)	High/Medium/Low
Control of ship/obstacle	Input(E)	Low/Medium/High
Type of ship/obstacle	Input(E)	Ship/Fish farm/ Oil installation/Wind-farm/ Markers/Containers/Other
Crew and passengers	Input(E)	Many/Normal/Limited/No
Size of ship/obstacle	Input(E)	Big/Medium/Small

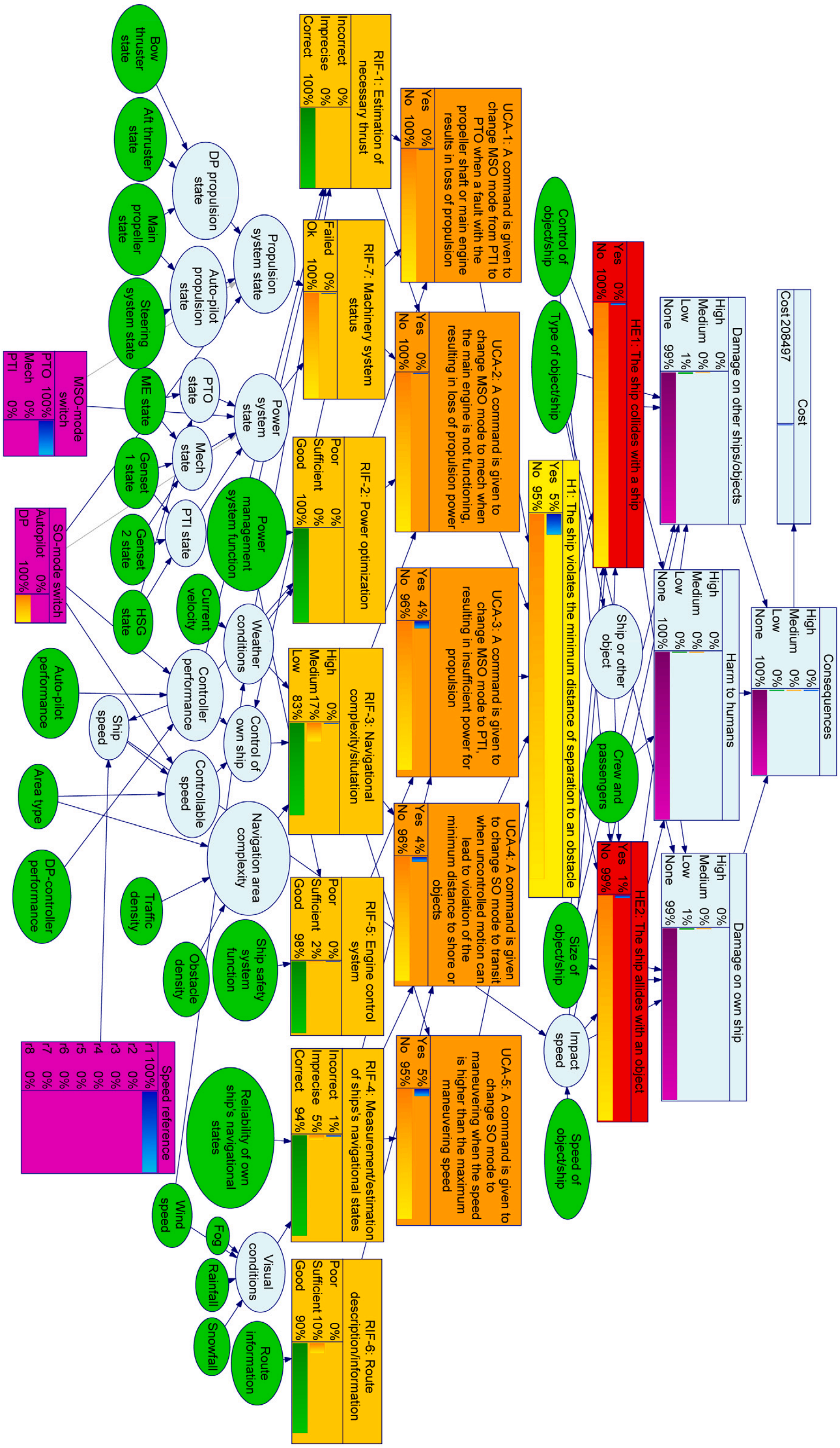

Bow thruster state
Aft thruster state
Main propeller state
Steering system state
DP propulsion state
Auto-pilot propulsion state
Propulsion system state
PTO state
Power system state
ME state
Mech state
Genset 1 state
Genset 2 state
PTI state
HSG state
MSO-mode switch
PTO 100%
Mech 0%
PTI 0%
SO-mode switch
Autopilot 0%
DP 100%
Power management system function
Current velocity
Weather conditions
Auto-pilot performance
Controller performance
Ship speed
Control of own ship
Controllable speed
Area type
Navigation area complexity
DP-controller performance
Traffic density
Obstacle density
Ship safety system function
Speed reference
r1 100%
r2 0%
r3 0%
r4 0%
r5 0%
r6 0%
r7 0%
r8 0%
Reliability of own ship's navigational states
Wind speed
Fog
Rainfall
Snowfall
Visual conditions
Route information
RIF-1: Estimation of necessary thrust
Incorrect 0%
Imprecise 0%
Correct 100%
RIF-7: Machinery system status
Failed 0%
Ok 100%
RIF-2: Power optimization
Poor 0%
Sufficient 0%
Good 100%
RIF-3: Navigational complexity/situation
High 0%
Medium 17%
Low 83%
RIF-5: Engine control system
Poor 0%
Sufficient 2%
Good 98%
RIF-4: Measurent/estimation of ship's navigational states
Incorrect 1%
Imprecise 5%
Correct 94%
RIF-6: Route description/information
Poor 0%
Sufficient 10%
Good 90%
UCA-1: A command is given to change MSO mode from PTI to PTO when a fault with the propeller shaft or main engine results in loss of propulsion
Yes 0%
No 100%
UCA-2: A command is given to change MSO mode to mech when the main engine is not functioning, resulting in loss of propulsion power
Yes 0%
No 100%
UCA-3: A command is given to change MSO mode to PTI, resulting in insufficient power for propulsion
Yes 4%
No 96%
UCA-4: A command is given to change SO mode to transit when uncontrolled motion can lead to violation of the minimum distance to shore or objects
Yes 4%
No 96%
UCA-5: A command is given to change SO mode to maneuvering when the speed is higher than the maximum maneuvering speed
Yes 5%
No 95%
Control of object/ship
Type of object/ship
H1: The ship violates the minimum distance of separation to an obstacle
Yes 5%
No 95%
Size of object/ship
Impact speed
Speed of object/ship
HE1: The ship collides with a ship
Yes 0%
No 100%
HE2: The ship allides with an object
Yes 1%
No 99%
Ship or other object
Crew and passengers
Damage on other ships/objects
High 0%
Medium 0%
Low 1%
None 99%
Harm to humans
High 0%
Medium 0%
Low 0%
None 100%
Damage on own ship
High 0%
Medium 0%
Low 1%
None 99%
Consequences
High 0%
Medium 0%
Low 0%
None 100%
Cost
Cost 208497

Fig. 3. Online risk model.

3.2.4. Identify states and build CPTs

The next part of building the BBN is defining states and building the CPTs for each node. States are defined such that each node provide sufficient information to the BBN, while keeping the number of states reasonably low. Limiting the number of states in each node makes it easier to define the CPTs because they depend on the number of parent nodes and number of states for each of these. CPTs are constructed based on available information about the ship and the environment (DNVGL, 2003; SINTEF, NTNU, 2015; Marine Traffic, 2021; Norwegian Meteorological Institute, 2021; Norwegian Mapping Authority, 2021).

The data from SINTEF, NTNU (2015) is used directly to describe the likelihood of component failures in the machinery system. The information in DNVGL (2003) is used differently based on what node it is used for. To describe the machinery components, it is used to check that the data from SINTEF, NTNU (2015) can also be used for

Table 5
Input probabilities for simulations.

Node	Situation	States	Probabilities	Source
ME state	All systems functioning	Failed/ok	9e−07/ 0.9999991	DNVGL (2003), SINTEF, NTNU (2015)
ME state	Main engine fails after 200 sec	Failed/ok	1.0/0.0	DNVGL (2003), SINTEF, NTNU (2015)
ME state	HSG failed fails after 200 s	Failed/ok	9e−07/ 0.9999991	DNVGL (2003), SINTEF, NTNU (2015)
HSG state	All systems functioning	Failed/ok	9e−07/ 0.9999991	DNVGL (2003), SINTEF, NTNU (2015)
HSG state	Main engine fails after 200 s	Failed/ok	9e−07/ 0.9999991	DNVGL (2003), SINTEF, NTNU (2015)
HSG state	HSG fails after 200 s	Failed/ok	1.0/0.0	DNVGL (2003), SINTEF, NTNU (2015)
Area type	Before way-point four	Harbor/ Coastal/Open	0.0/0.5/0.5	DNVGL (2003) Norwegian Mapping Authority (2021)
Area type	After way-point four	Harbor/ Coastal/Open	1.0/0.0/0.0	DNVGL (2003) Norwegian Mapping Authority (2021)
Obstacle density	Before way-point two and after way-point three	High/Medium/ Low	0.1/0.5/0.4	DNVGL (2003) Norwegian Mapping Authority (2021) Marine Traffic (2021)
Obstacle density	Way-points two - three	High/Medium/ Low	1.0/0.0/0.0	DNVGL (2003) Norwegian Mapping Authority (2021) Marine Traffic (2021)
Traffic density	Before way-point two and after way-point three	High/Medium/ Low	0.1/0.5/0.4	DNVGL (2003) Norwegian Mapping Authority (2021) Marine Traffic (2021)
Traffic density	Way-points two - three	High/Medium/ Low	1.0/0.0/0.0	DNVGL (2003) Norwegian Mapping Authority (2021) Marine Traffic (2021)
Speed of obstacle	Before way-point two and after way-point three	High/Medium/ Low	0.2/0.7/0.1	DNVGL (2003) Norwegian Mapping Authority (2021) Marine Traffic (2021)
Speed of obstacle	Way-points two - three	High/Medium/ Low	1.0/0.0/0.0	DNVGL (2003) Norwegian Mapping Authority (2021) Marine Traffic (2021)
Crew and passengers	Before way-point two and after way-point three	Many/Normal/ Limited/None	0.0/0.1/0.3/0.6	DNVGL (2003) Norwegian Mapping Authority (2021) Marine Traffic (2021)
Crew and passengers	Way-points two - three	Many/Normal/ Limited/None	1.0/0.0/0.0/0.0	DNVGL (2003) Norwegian Mapping Authority (2021) Marine Traffic (2021)

components that are not directly listed. For the node describing the control system and sensors, the data is processed such that they have three states instead of two. Some of the data has also been used as a basis for deciding how CPTs differ between a manned and autonomous ship, such as the control system and sensors. Since the human operator is not present on the ship, the CPTs describing controllers and sensors are changed slightly compared to ships with full crew. Marine Traffic (2021) and Norwegian Mapping Authority (2021) are used to find out how much traffic and obstacles are typical for coastal sailing along the Norwegian coast, both open waters, more coastal areas with islands and more traffic, and highly congested waters with very limited space and much traffic. Marine Traffic (2021) is also used to find how many ships sailing along the coast have passengers and estimate the size of these ships. Norwegian Meteorological Institute (2021) is used to find historical data about weather conditions along the Norwegian coast.

In addition to literature and available data, expert judgment is also used to both build the BBN, assign states, and build CPTs. The experts are deck and technical officers on board ships, and engineers designing ship control systems. The discussions with deck and technical officers have focused on how ships are operated today and how this can change with increased autonomy, such as what SO and MSO-modes should be used in different situations. The control engineers have given input on design and setup of the control system, and how to change this from a manned to more autonomous ship.

3.2.5. Converting the BBN into an online risk model

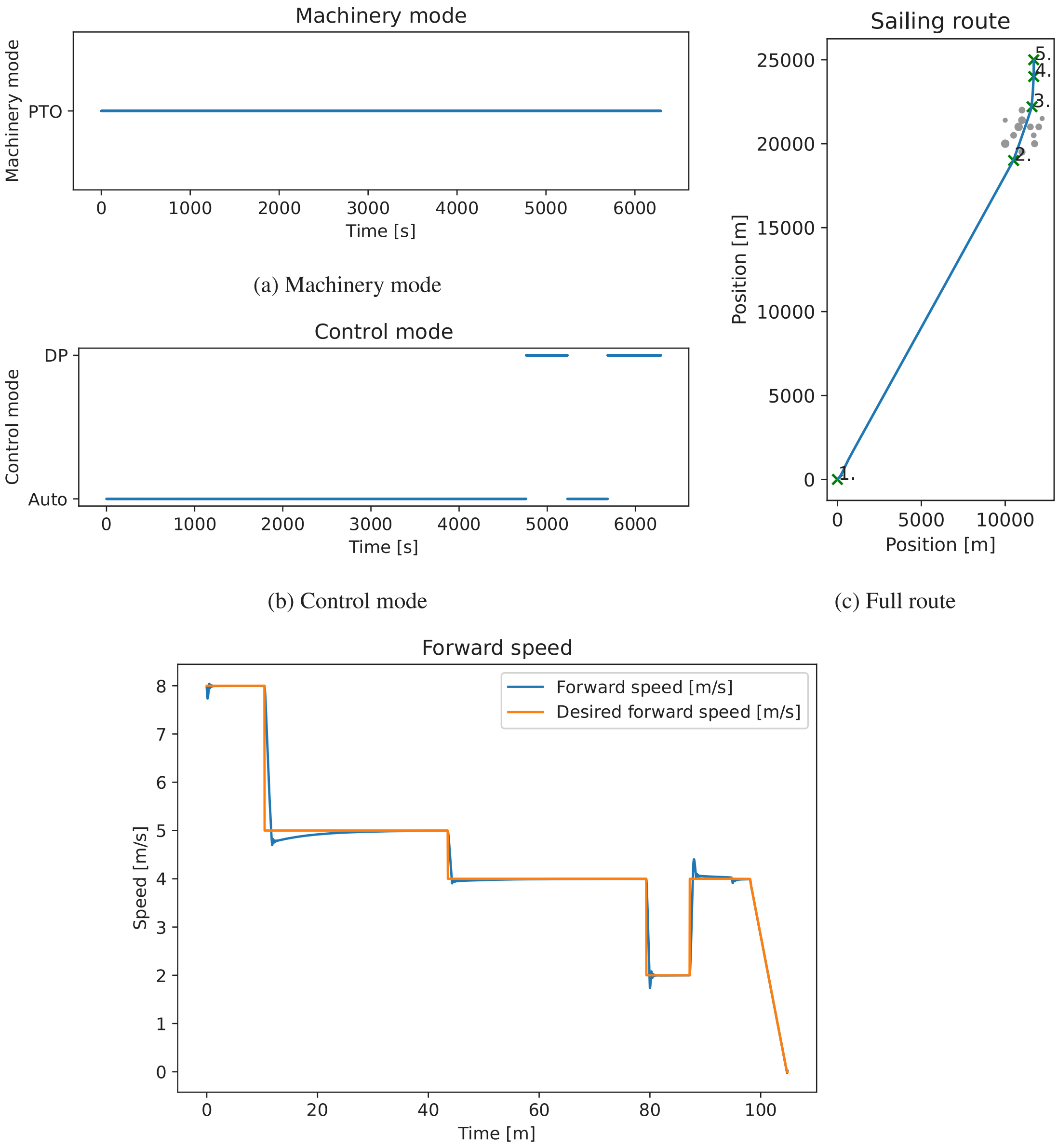
The BBN is converted to an online risk model for use in the SRC, including both probabilities for the nodes' states and the potential consequences. Developing the online risk model includes identifying what nodes that should be updated with data from the ship as it is sailing such that the BBN represent the actual situation.

The risk model in this paper has been tested in simulations to check that the SRC functions and is able to control the ship. The simulated scenario is that the ship is sailing and has five way-points left on a pre-planned route. At first, the conditions around the ship describe a normal situation for ships sailing along the Norwegian coast, based on data from DNVGL (2003), SINTEF, NTNU (2015), Marine Traffic (2021), Norwegian Meteorological Institute (2021) and Norwegian Mapping Authority (2021). Between way-points two and three, the traffic and obstacle density is increased to see if the control can handle situations with more ships and more obstacles around the ship, more similar to high traffic areas such as the English channel. More ships and objects around also increases the amount of people, both crew and passengers, that might be harmed in accidents. After way-point three, the ship is again back in normal conditions, before it reaches the area where it should dock next to the fish farm.

Other input probabilities and CPTs are based on the same sources (DNVGL, 2003; SINTEF, NTNU, 2015; Marine Traffic, 2021; Norwegian Meteorological Institute, 2021; Norwegian Mapping Authority, 2021), combined with expert judgment, such that the BBN represent the actual type of ship and conditions this sail in.

3.3. Phase 3: The supervisory risk controller

The SRC optimizes the decisions, d, based on the risk cost from the risk model, $R(d)$, and the expected cost of running the machinery in the current configuration, $C(d)$, for the remaining distance to the last way-point. The risk cost is taken directly from the risk model based on



(a) Machinery mode

(b) Control mode

(c) Full route

(d) Forward speed

Fig. 4. All systems functioning.

Eq. (2). The machinery cost is calculated based on the expected cost of running the machinery in each configuration for the remaining sailing time (Eq. (3)). This cost will therefore decrease as the ship gets closer to the final way-point because it is a function of the remaining sailing time.

The cost of fuel consumption is calculated using the price per kWh for LNG and marine gas oil (DNV, 2021). The load is taken as the expected mean load percentage times the available power for the remaining sailing time. This gives a good estimation of the fuel cost that can be compared to the risk cost from the BBN with the information available.

$$C(d) = c_{fuel} \times (t_{cruise} \times P \times \eta_{cruise} + t_{dock} \times P \times \eta_{dock}) \tag{3}$$

$$M(d) = R(d) + C(d) \tag{4}$$

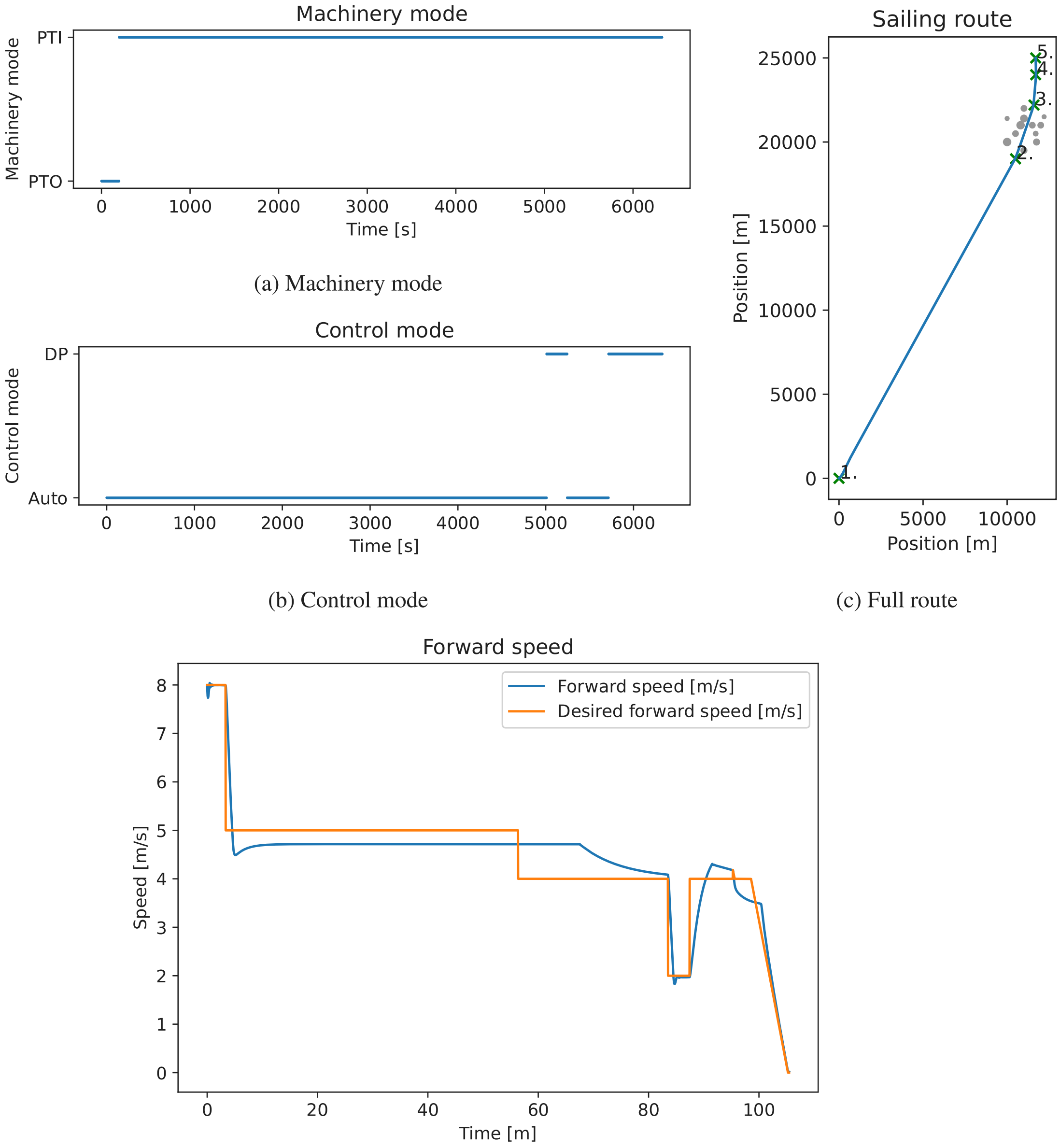
The SRC is implemented such that the optimum set of decisions is checked every 10 s to limit the number of times that the risk model has to be checked. It also avoids chattering, where the SRC is just switching back and forth.

4. Results and discussion

4.1. Results

The SRC is tested in three different simulations to test how the risk model affects the control of an autonomous ship. The case study shows the last part of a route, approximately 27 km over five way-points. Around 2 km, between way-points two and three, there are more traffic and islands. This makes it necessary to lower the speed of the vessel to maintain sufficient control. The input values that change in the simulations are shown in Table 5.

All of the simulations show that the SRC reacts when it becomes more difficult to navigate safely with an increased amount of ships and obstacles around. The speed is then lowered to maintain sufficient control of the ship (Figs. 4(d), 5(d), and 6(d)). The simulations also show that the ship, with the current setup, is more risk averse than similar manned ships because the speed in the normal conditions is lower than a typical cruising speed of 8 m/s. This also mean that the ship uses more time before it reaches the goal.



(a) Machinery mode

(b) Control mode

(c) Full route

(d) Forward speed

Fig. 5. Main engine failed.

Fig. 4 show the simulation with all machinery systems functioning. The ship then operates in PTO because this is the most efficient mode for the ship. The ship uses 105 min from the start point before it has stopped at the final way-point. The ship lowers the speed to 5 m/s after around 10 min, and lowers it further down to 4 m/s after around 40 min. The speed is reduced when the distance to the final way-point is low enough that the reduction in risk cost is lower than the increase in fuel cost. When it reaches the area with more traffic and obstacles, the speed is not immediately reduced because the speed is already at 4 m/s. As the ship gets closer to the final way-point, the speed is reduced further to 2 m/s, and then increased to 4 m/s again when the traffic and obstacle density is reduced. When the speed is reduced to 2 m/s, the SO-mode is changed to DP (Fig. 4(b)) because the speed is then so low that it is difficult to control the ship with only the main propeller and rudder. When it increases back to 4 m/s, it switches back to auto-pilot because the tunnel thrusters have less effect at higher speeds.

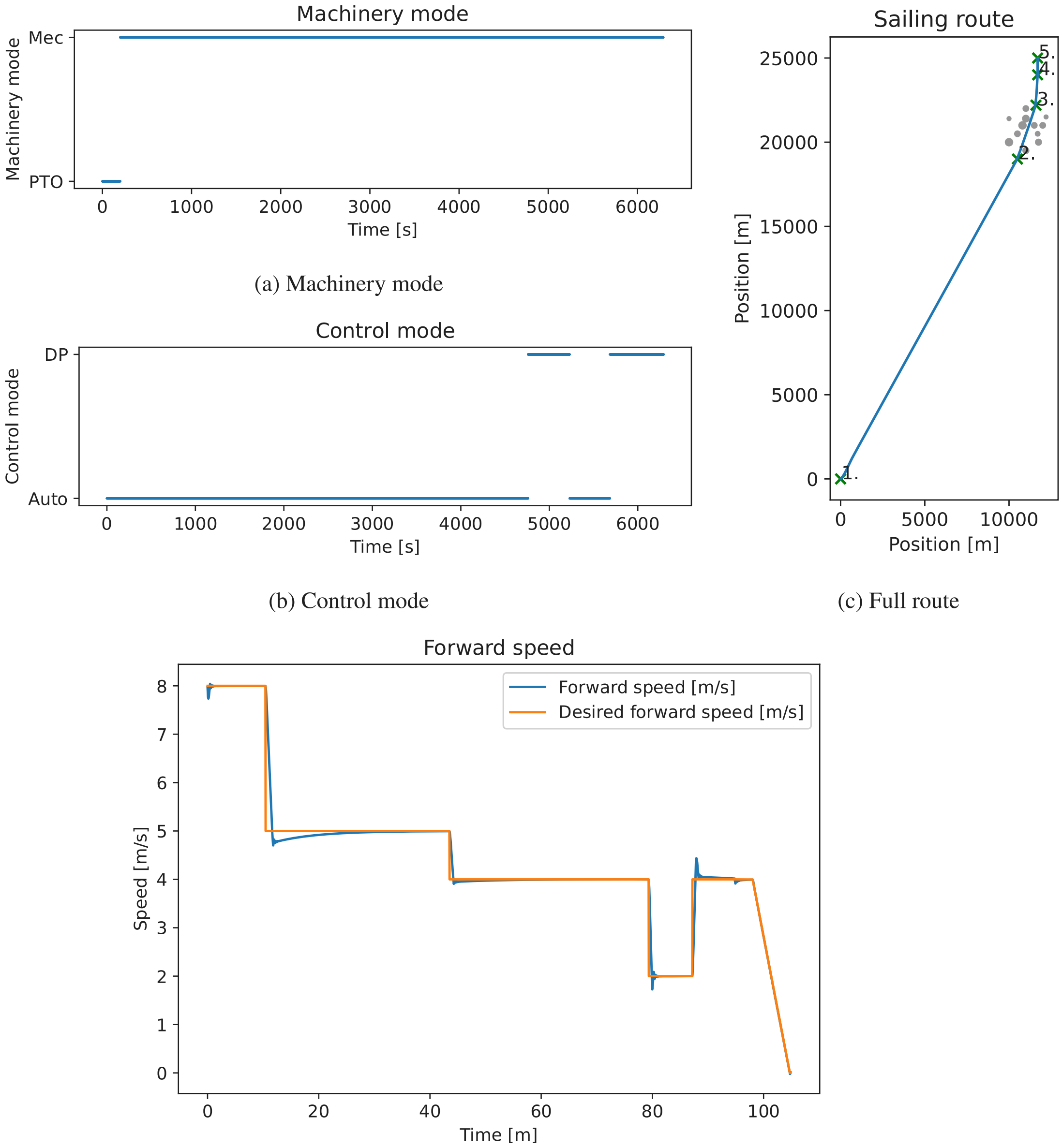
Fig. 5 shows a simulation where the main engine fails after 200 s The ship then goes over in PTI because this is the only available MSO-mode (Fig. 5(a)). This also reduces the maximum speed to 5 m/s because PTI is unable to produce sufficient propulsion power for higher speeds. This increases the total sailing time slightly to 107 min. The rest of the simulation is similar to the simulation with PTO. The speed is lowered when the traffic and obstacle density increases. When the speed is lowered to 2 m/s, it switches to DP.

Fig. 6 show a simulation where the HSG fails after 200 s, which means that the ship must switch MSO-mode to Mech to have power (Fig. 6(a)). The rest of the simulation is the same as when the ship operates in PTO (Fig. 4).

4.2. *Discussion*

4.2.1. *STPA and the online risk model*

One of the most important parts for an SRC is information about how the control decisions affect the risk level for the ship. To find this information, STPA is useful to identify hazards and system losses, with a focus on how control actions can lead to these and what causal factors



(a) Machinery mode

(b) Control mode

(c) Full route

(d) Forward speed

Fig. 6. HSG failed.

affect this. But STPA only gives qualitative information, which is very difficult to use directly in a controller. Furthermore, consequences are not explicitly identified and analyzed in the general STPA. Hence, this was a necessary extension and additional step of the STPA method, and the controller implemented in this paper addresses this problem by including consequences from the losses and an expected cost from these (see Section 3.2.1). Consequences are divided into four categories; high, medium, low, and no consequences. Deciding what cost to give to each category of consequences is one of the biggest challenges and it has a considerable affect on the overall performance. These numbers are therefore based on both literature, previous work, expert judgment, and trial and testing with the BBN to get the desired behavior.

The STPA results are further used as the basis for the development of the BBN risk model. As shown in this paper, this give an online risk model that can be used in the control system where the risk cost can be combined with operation costs. STPA provides qualitative information about causal factors that lead to UCAs and hazards, but no quantitative information. The STPA also provides limited information about the consequences and their cost. In the case study, both CPTs and information about costs are based on a limited amount of reports and the external sources describing them. This makes it difficult to find sufficient information to build the BBN with sufficient detail. A more structured way to find this could make this process easier and give a more accurate risk model.

The BBN risk model is useful to get a good overview over the situation and the risk level for the ship. With good available software tools, BBNs can also be combined with other computer-based control systems. This makes it easy to update the BBN as a new input become available. It also makes it easy to use the output directly in an SRC. The main challenge with using BBNs for this application is constructing the BBN, especially deciding states for each node and building up CPTs. The STPA provides information about how different nodes are connected, but provides very little information for defining states and CPTs. Based on the case study in this paper, both states and CPTs must weigh accuracy against the purpose of the risk model. The amount of states will also directly influence the size of the CPTs, and can also affect the time necessary to evaluate the BBN.

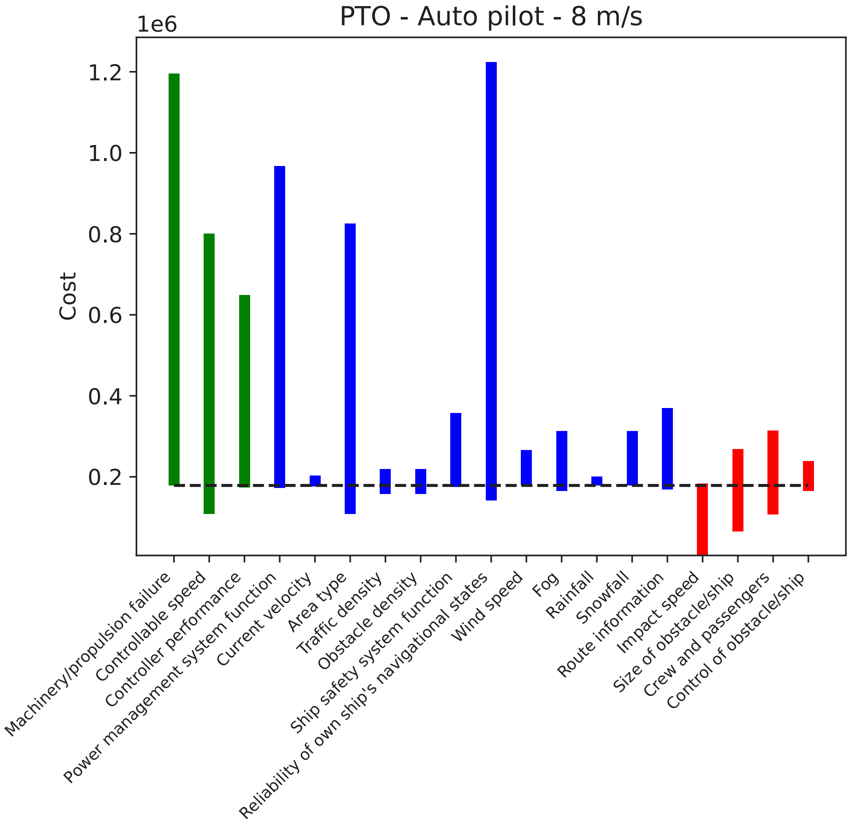


Fig. 7. Sensitivity analysis. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Some states can be found directly from the use an type of node, such as decisions, sensor measurements, or limitations for both the control system and the ship. For other nodes, it might be information available. However, some states will most likely be changed as the system is tested because they influence the risk slightly different than initially expected. It can also be necessary to change states later because they make other nodes too complex to define. CPTs should be defined such that top level node gives an accurate picture of the risk, and changes when conditions or decisions change. To do this, both expert judgment, previous analysis, and specifications for the control system can be used. In the case study, the initial values are set based on a mix of literature and expert judgment, and are then tuned slightly to get the desired output and behavior. Because there is no complete literature on how to make the BBN and define different nodes, it is necessary to make some changes in CPTs based on the testing. By doing this in an iterative process, the ship behaves as expected and as intended but it also increases the overall uncertainty in the model.

4.3. Sensitivity and uncertainty

The BBN is assessed by performing a sensitivity analysis (Fig. 7). Given that the BBN is based on both literature, expert judgment, and testing, this provides useful information about the effect that each node has on the cost. The base cost is operating the ship in PTO with auto pilot and a reference speed of 8 m/s. This gives a base cost of 178 712 NOK with the same initial values for all nodes as in the simulations. The BBN is then checked to find out how much the cost depend on each node. The three first bars (Green bars) in Fig. 7 show how the cost depend on the machinery and propulsion state, whether the speed is controllable, and the controller's performance. These show how the cost changes if the decisions, MSO-mode, SO-mode, and reference speed are wrong. A wrong decision would mean a failed MSO-mode, or a combination of speed and SO-mode where the ship is difficult to control. The machinery status is the most sensitive of these, followed by the speed and the SO-mode. The next bars (Blue bars) show the sensitivity of the input nodes that affect the high-level RIFs. The three most sensitive of these are the reliability of the navigational states, the power management system, and the type of area the ship is sailing in. The four last bars (Red bars) show how the input nodes to the consequences affect the final cost.

The sensitivity analysis show that the sensitivity differs significantly between the different nodes. Some nodes have very little effect on the overall cost, such as rain or current velocity, and others, such as the navigational states and power management system affect the cost much more. The most sensitive nodes are important when assessing the uncertainty in the model as they have higher effect on the end result. Most of the nodes with high sensitivity relate to the reliability of hardware components or the control system. The data used to define these is based on multiple literature sources, which limits the uncertainty from these nodes. But, these should still be addressed further to reduce the overall uncertainty in the model. The base cost is taken in good conditions with good control of the ship. Changing the state of the nodes to the most positive value will therefore have little effect on reducing the cost, except for lower speed and the fewer obstacles around the ship.

4.3.1. The supervisory risk controller in the case study

The purpose of implementing an SRC is to make safer and more efficient control of autonomous systems. By including an online risk model in the control system, the control system should be able to make more informed decisions compared to existing control systems. In the case study, the SRC is tested with three different decisions: selecting SO-mode, MSO-mode, and setting the reference speed for the ship. The case study shows how the SRC enables the control system to select the best combination of these three, considering both operational costs and risk. Other than the SRC, the control system tested is the same type as many ships use today. A DP controller for station-keeping and low speed maneuvering, and a heading and speed auto pilot for use at higher speeds. However, the operators decide MSO-modes, SO-modes, and speed references on existing ships.

This extra functionality comes with both advantages and some challenges compared to existing systems. One of the main advantages is the higher flexibility and functionality in the control system. To get the same type of behavior from existing ships, without human input when sailing, the same decisions must planned ahead of time. Some might be possible to plan ahead, such as switching from auto pilot to DP when the ship is a certain distance from the dock, but this is much less flexible and efficient. If the conditions change before the ship reaches this point, then it might be possible to have a higher speed for longer or it might be necessary to lower the speed and change to DP earlier to ensure sufficient control. Failing to do this would either mean a higher cost in the operation of the ship or increased risk for both the ship owners, environment, the public, and others who might be affected if the ship has an accident. An alternative could be to define rules for how the decisions should be made that also account for changes in the environment. A rule could (for example) say that wind speeds lower than a certain limit make it safe to keep a higher speed longer. But with ships, this would be very complex. In the case study, the BBN contains 27 input nodes that describe either the ship or the environment and situation around the ship. Some rules could be very simple binary rules, such as not leaving dock if the wind is at hurricane force, but most rules would depend on multiple conditions. Even if a rule might not depend on all 27, this would be almost impossible to do based on the number of possible combinations. Uncertainty will also be a problem where it is very difficult to say how rules should depend on different conditions. The SRC still has a certain degree of uncertainty, but the cost is now less dependent on one specific condition but rather a combination of multiple nodes in the BBN. This makes it less likely for the SRC to make critical mistakes compared to specific rules for each condition.

The case study indicates how the SRC behaves when the information is updated as conditions changes. For the SRC to be tested with constantly updated input, it is necessary with more detailed datasets and extend the control system. A potential approach for doing this could be logging data on existing ships on specific routes. By logging detailed weather data, machinery data, position, speed, and what decisions the crew make, the SRC could be tested through simulation and field trials with autonomous platforms in the same conditions. Comparing decisions made by the SRC and crew can then be used to assess how the SRC performs. Another approach is to test if the SRC is able to satisfy a set of constraints for safe and efficient operation in on the same routes and conditions, such as minimum distance to land and max time from start to finish. Assessing the SRC against both human operators and more formal constraints can be used to verify the model and controller. For the BBN model itself, it can also be compared to other models in the literature and be discussed further with experts to verify that it give an good representation of the actual system.

5. Conclusion

The main purpose of this paper is to demonstrate how online risk models and ship control systems can be integrated for improved intelligence and decision support for autonomous ships. This is shown by implementing a supervisory risk controller (SRC), and combining this with existing ship control systems. The SRC is based on an online risk model, combined with operational costs. This enables us to make decisions that consider both risk and operational costs.

The online risk model is based on qualitative information from an extended STPA, including an additional step consisting of identifying and analyzing consequences. This is necessary to enable the SRC to make decisions. The online risk model is represented by a BBN, which is developed based on the results of the extended STPA.

Table 6
BBN nodes.

Node description	Parent node(s)
Cost	Consequences
Consequences	Harm to humans, Damage on other ships/objects, Damage on own ship
Damage on other ships/objects	HE1, HE2, Impact speed, Type of ship/obstacle, Size of ship/obstacle
Damage on own ship	HE1, HE2, Impact speed, Type of ship/obstacle, Size of ship/obstacle
Harm to humans	HE1, HE2, Crew and passengers
HE1	H1
HE2	H1
H1	UCA-1,UCA-2,UCA-3,UCA-4, UCA-5
UCA-1	RIF-1,RIF-2,RIF-7
UCA-2	RIF-1,RIF-2,RIF-3,RIF-7
UCA-3	RIF-4,RIF-5
UCA-4	RIF-3,RIF-4,RIF-6
UCA-5	RIF-3,RIF-4
RIF-1	Power management system, Controller performance, Weather conditions
RIF-2	Power management system, Controller performance, Weather conditions
RIF-3	Navigation area complexity, Weather conditions, Control of ship
RIF-4	Reliability of own ship s navigational states, Visual conditions
RIF-5	Power management system, Ship safety system
RIF-6	Route information
RIF-7	Propulsion system state, Power system state

The SRC is tested in a case study of an autonomous cargo ship, where the purpose is to select the best MSO-mode, SO-mode, and reference speed based on both risk and operational costs. The ship follows a planned route, where the traffic conditions and area around the ship changes along the route. The case study shows that the SRC adjusts the speed with more traffic and obstacles around the ship, even though this reduces the efficiency. When the situation changes again and the risk is reduced, the speed is increased again. As the ship approaches the final way-point where it should dock, the SRC changes SO-mode to DP such that the ship has better control with lower speed.

The case study also shows that the SRC is able to handle failures in the machinery system and then select the most efficient MSO-mode without using a failed component. The SRC is able to make these decisions while the ship is sailing, without the need for adjusting the controller or human input to the system. This increases the functionality of the control system and reduces the need for human control. For autonomous ships to operate, this capability of assessing risk versus cost and comparing these in a good way is necessary for both safe and efficient operation.

Further work on this type of controller should consider how it can be integrated with different types of controllers. For SRC to be a useful tool for different types of ship, and other autonomous systems, it is important to know that it works with different types of control systems. The risk model itself should also be investigated further, to check how detailed this must be for the system to still function to see if this can make it both more efficient and easier to implement. The risk model may also be expanded with more real-time data such that more nodes change (e.g., machinery components and controller

Table 7
cont.BBN nodes.

Node description	Parent node(s)
Propulsion system state	SO-mode switch, DP propulsion, Auto pilot propulsion, MSO-mode
Power system state	SO-mode switch, MSO-mode, PTO, Mech, PTI
Weather conditions	Current velocity, Wind speed
Visual conditions	Wind speed, Fog, Snowfall, Rainfall
DP propulsion state	Main propeller, Aft thruster, Bow thruster
Auto-pilot propulsion state	Main propeller, Steering system
PTO	ME, HSG
Mech	ME, Genset1, Genset2
PTI	HSG, Genset1, Genset2
Control of own ship	Controllable speed, Controller performance, RIF7
Controller performance	SO-mode switch, Auto pilot performance, DP controller performance
Ship speed	Speed reference, Controller performance
Navigation area complexity	Traffic density, Obstacle density, Area type
Controllable speed	SO-mode switch, Ship speed, Area type
Impact speed	Ship speed, Speed of obstacle
Category of obstacle	Type of obstacle
MSO-mode switch	Decision
SO-mode switch	Decision
Speed reference	Decision
Power management system function	None
Obstacle density	None
Traffic density	None
Ship safety system function	None
Reliability of own ship's navigational states	None
Route information	None
Bow thruster state	None
Aft thruster state	None
Main propeller state	None
Steering system state	None
ME state	None
Genset 1 state	None
Genset 2 state	None
HSG state	None
Current velocity	None
Auto-pilot performance	None
DP-controller performance	None
Wind speed	None
Fog	None
Rainfall	None
Snowfall	None
Area type	None

performance). Further work should also address the uncertainty by testing for a wider variation of input parameters to assess how the behavior changes in a wider range of situations.

CRediT authorship contribution statement

Thomas Johansen: Conceptualization, Methodology, Software, Investigation, Data curation, Writing – original draft, Visualization. **Ingrid Bouwer Utne:** Conceptualization, Writing – review & editing, Supervision, Funding acquisition.

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.

Table 8
cont.BBN nodes.

Node description	Parent node(s)
Speed of ship/obstacle	None
Control of ship/obstacle	None
Type of ship/obstacle	None
Crew and passengers	None
Size of ship/obstacle	None

Acknowledgments

The work by Johansen and Utne is partly sponsored by the Research Council of Norway through the Centre of Excellence funding scheme, project number 223254, AMOS, and project ORCAS with project number 280655.

Appendix. BBN connections

Tables with an overview of child/parent nodes for the BBN. (See Tables 6–8).

References

Bremnes, J.E., Norgren, P., Sørensen, A.J., Thieme, C.A., Utne, I.B., 2019. Intelligent risk-based under-ice altitude control for autonomous underwater vehicles. In: OCEANS 2019 MTS/IEEE Seattle, OCEANS 2019.

Bremnes, J.E., Thieme, C.A., Sørensen, A.J., Utne, I.B., Norgren, P., 2020. A Bayesian approach to supervisory risk control of auvs applied to under-ice operations. Mar. Technol. Soc. J. 54, 16–39.

Brito, M., 2016. Uncertainty management during hybrid autonomous underwater vehicle missions. In: Autonomous Underwater Vehicles 2016, AUV 2016, pp. 278–285.

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

Campbell, S., Naeem, W., 2012. A rule-based heuristic method for COLREGS-compliant collision avoidance for an unmanned surface vehicle. IFAC Proc. Vol. 45, 386–391.

Campbell, S., Naeem, W., Irwin, G.W., 2012. A review on improving the autonomy of unmanned surface vehicles through intelligent collision avoidance manoeuvres. Annu. Rev. Control 36, 267–283.

Chaal, M., Banda, O.A.V., Glomsrud, J.A., Basnet, S., Hirdaris, S., Kujala, P., 2020. A framework to model the STPA hierarchical control structure of an autonomous ship. Saf. Sci. 132.

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

DNV, 2021. Current price development oil and gas. URL: https://www.dnv.com/maritime/insights/topics/lng-as-marine-fuel/current-price-development-oil-and-gas.html.

DNVGL, 2003. DNV Report No 2003-0277 Annex II FSA 2003. Technical Report, DNVGL group technology & research, URL: http://research.dnv.com/skj/FSALPS/ANNEXII.pdf.

EfficienSea, 2012. Methods to Quantify Maritime Accidents for Risk-Based Decision Making. Technical Report, EfficienSea, URL: http://efficiensea.org/files/mainoutputs/wp6/d_wp6_4_1.pdf.

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

Hu, L., Naeem, W., Rajabally, E., Watson, G., Mills, T., Bhuiyan, Z., Salter, I., 2017. COlregs-compliant path planning for autonomous surface vehicles: A multiobjective optimization approach. IFAC-PapersOnLine 50, 13662–13667.

IMO, 2018. Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process. Technical Report, IMO, URL: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/MSC-MEPC%202-Circ%2012-Rev%202.pdf.

Johansen, T., Utne, I.B., 2020. Risk analysis of autonomous ships. In: E-Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference, ESREL2020 PSAM15, pp. 131–138.

Kongsberg, 2020. Automatic ferry enters regular service following world-first crossing with passengers onboard. URL: https://www.kongsberg.com/maritime/about-us/news-and-media/news-archive/2020/first-adaptive-transit-on-bastofosen-vi/.

Kretschmann, L., Rødseth, Ø., Fuller, B.S., Noble, H., Horahan, J., McDowell, H., 2015. MUNIN Deliverable 9.3: Quantitative Assessment. Technical Report, MUNIN project.

Kristiansen, S., 2005. Maritime Transportation: Safety Management and Risk Analysis. Elsevier/Butterworth-Heinemann.

Leveson, N.G., 2011. Engineering a Safer World: Systems Thinking Applied to Safety. In: Engineering Systems, MIT Press.

Loh, T.Y., Brito, M., Bose, N., Xu, J., Tenekedjiev, K., 2020. Fuzzy system dynamics risk analysis (FuSDRA) of autonomous underwater vehicle operations in the Antarctic. Risk Anal. 40, 818–841.

Ludvigsen, M., Sørensen, A.J., 2016. Towards integrated autonomous underwater operations for ocean mapping and monitoring. Annu. Rev. Control 42, 145–157.

Lyu, H., Yin, Y., 2019. COLREGS-constrained real-time path planning for autonomous ships using modified artificial potential fields. J. Navig. 72, 588–608.

Marine Traffic, 2021. Marine traffic. URL: https://www.marinetraffic.com/.

Naeem, W., Henrique, S.C., Hu, L., 2016. A reactive COLREGs-compliant navigation strategy for autonomous maritime navigation. IFAC-PapersOnLine 49, 207–213.

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

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

Rausand, M., Haugen, S., 2020. Risk Assessment: Theory, Methods, and Applications. John Wiley and Sons Ltd.

Rødseth, Ø.J., Tjora, A., 2015. A risk based approach to the design of unmanned ship control systems. In: Maritime-Port Technology and Development - Proceedings of the International Conference on Maritime and Port Technology and Development, MTEC 2014, pp. 153–161.

Shuai, Y., Li, G., Xu, J., Zhang, H., 2020. An effective ship control strategy for collision-free maneuver toward a dock. IEEE Access 8, 110140–110152.

SINTEF, NTNU, 2015. OREDA: Offshore Reliability Data Handbook: Vol. 1: Topside Equipment. SINTEF, NTNU.

Sørensen, A.J., 2005. Structural issues in the design and operation of marine control systems. Annu. Rev. Control 29, 125–149.

Springwise, 2018. Autonomous electric ferry can be called like an elevator. URL: https://www.springwise.com/autonomous-electric-ferry-can-be-called-like-an-elevator/.

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

Ung, S.T., 2021. Navigation risk estimation using a modified Bayesian network modeling-a case study in Taiwan. Reliab. Eng. Syst. Saf. 213.

Utne, I.B., Rokseth, B., Sørensen, A.J., Vinnem, J.E., 2020a. Online risk modelling for supervisory risk control of autonomous marine systems. In: Proceedings of the 29th European Safety and Reliability Conference, ESREL 2019, pp. 3654–3659.

Utne, I.B., Rokseth, B., Sørensen, A.J., Vinnem, J.E., 2020b. Towards supervisory risk control of autonomous ships. Reliab. Eng. Syst. Saf. 196, 106757.

Valdez Banda, O.A., Goerlandt, F., 2018. A STAMP-based approach for designing maritime safety management systems. Saf. Sci. 109, 109–129.

Valdez Banda, O.A., Goerlandt, F., Salokannel, J., van Gelder, P.H.A.J.M., 2019a. An initial evaluation framework for the design and operational use of maritime STAMP-based safety management systems. WMU J. Marit. Aff. 18, 451–476.

Valdez Banda, O.A., Kannos, S., Goerlandt, F., van Gelder, P.H.A.J.M., Bergström, M., Kujala, P., 2019b. A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. Reliab. Eng. Syst. Saf. 191, 106584.

Vojkovic, L., Skelin, A.K., Mohovic, D., Zec, D., 2021. The development of a Bayesian network framework with model validation for maritime accident risk factor assessment. Appl. Sci. 11.

Wang, H., Guo, F., Yao, H., He, S., Xu, X., 2019. Collision avoidance planning method of USV based on improved ant colony optimization algorithm. IEEE Access 7, 52964–52975.

Woo, J., Kim, N., 2020. Collision avoidance for an unmanned surface vehicle using deep reinforcement learning. Ocean Eng. 199.

Wróbel, K., Krata, P., Montewka, J., Hinz, T., 2016. Towards the development of a risk model for unmanned vessels design and operations. Int. J. Mar. Navig. Saf. Sea Transp. 10, 267–274.

Wróbel, K., Montewka, J., Kujala, P., 2017. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliab. Eng. Syst. Saf. 165, 155–169.

Yu, Q., Teixeira, A., Liu, K., Rong, H., Guedes Soares, C., 2021. An integrated dynamic ship risk model based on Bayesian networks and evidential reasoning. Reliab. Eng. Syst. Saf. 216.