Holden, Eivind Brekke

Online Risk Management for MilliAmpere 2

Master's thesis in Ingeniørvitenskap & IKT
Supervisor: Smogeli, Øyvind
Co-supervisor: Utne, Ingrid B
June 2022

Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Engineering
Department of Marine Technology

NTNU
Norwegian University of
Science and Technology

Holden, Eivind Brekke

Online Risk Management for MilliAmpere 2

Master’s thesis in Ingeniørvitenskap & IKT
Supervisor: Smogeli, Øyvind
Co-supervisor: Utne, Ingrid B
June 2022

Norwegian University of Science and Technology
Faculty of Engineering
Department of Marine Technology

NTNU
Norwegian University of
Science and Technology

NTNU

Norwegian University of
Science and Technology

Trondheim
June 11, 2022

Online Risk Management For MilliAmpere 2

Master Thesis

Author:
Eivind Brekke Holden

Supervisors:
Øyvind Smogeli
Ingrid Bouwer Utne

Abstract

This thesis provides a basic framework for Online Risk Management (ORM) for the autonomous passenger ferry, milliAmpere 2. The autonomous passenger ferry will work as a shuttle ferry in Trondheim, between Ravnkloa and Vestre Kanalkai. The idea is a on-demand ferry, push the button and the ferry will come shortly. The ferry will be designed to take maximum 12 passengers, have a crossing time of one minute and to be unmanned. MilliAmpere 2 is currently testing with a captain, an onboard operator, who is responsible for the risk management.

The objective of the ORM, together with a remote operator, is to replace the onboard operator. The ORM will ensure that milliAmpere 2's operation remains safe and that the ferry is at least as safe as a manned ship. The ORM's framework provided in this thesis is built upon the framework proposed by [1]. The proposed framework in [1] was for an online risk model that is supposed to be part of the ORM. The provided framework in this thesis uses a decision-making model to complete the framework of the ORM, so it consists of a online risk model and a decision-making model. The framework also includes a python script that dynamically runs the models to continuously make risk assessments, to ensure a fast response by the decision-making model to make the ORM act when it is needed.

The main focus of this thesis is to design and test the decision-making model. The decision-making model is modeled by an influence diagram. The influence diagram is a type of Bayesian Belief Network, but the model includes decisions and utilities that can be used to compare and predict the best actions in uncertain environments. The actions are compared by multiplying the probability with the corresponding utility. The best action is the one with highest expected utility, given by the probability of the outcome multiplied by the utility associated with the outcome.

To test the designed decision-making model, a finite-state machine simulation is created, with manual input. The python script designed to run the ORM is then used with the simulation data to test the precision of the model's prediction. The thesis also considers a risk model for MilliAmpere 2 presented in [2], which is converted to a decision-making model in this thesis. The results of the thesis also include sensitivity analyses of the models. These results depend on the state of the models, which are not fixed to a single state but change depending on the situation. Therefore, three different sensitivity analyses are made for both models. These analyses are then compared, both the analyses for each model and across models.

Sammendrag

Denne rapporten gir et grunnleggende rammeverk for Dynamisk Risiko Styring (ORM) for den autonome passasjerfergen, milliAmpere 2. Den autonome passasjerfergen vil operere som en ferge i Trondheim, mellom Ravnkloa og Vestre Kanalkai. Ideen er en on-demand ferge, trykk knappen og fergen er på vei. Fergen vil være designet for å ta maksimalt 12 passasjerer, har en overfartstid over kanalen på ett minutt og skal være ubemannet.

MilliAmpere 2 testes for tiden med en kaptein som er ansvarlig for risikostyringen ombord. Målet med ORM, sammen med en ekstern operatør, er å erstatte kapteinen ombord. ORM vil sørge for at milliAmpere 2s aktivitet forblir trygg og at fergen er minst like sikker som på et bemannet skip. Rammeverket for ORM som er gitt i denne oppgaven er bygget på rammeverket foreslått av [1]. Det foreslåtte rammeverket i [1] er for en Dynamisk Risiko Model som er ment til å være en del av ORMen. Det grunnleggende rammeverket for ORMen i denne oppgaven bruker en beslutningsmodell for å fullføre rammeverket, så det består av en Dynamisk Risiko Model og en beslutningsmodell. Rammeverket inkluderer også et Python-script som kan kjøre modellene kontinuerlig og utføre risikovurderinger, med sikte på en raskere respons fra beslutningsmodellen slik at ORMen kan handle når det er nødvendig.

Hovedfokuset i denne oppgaven er å designe og teste beslutningsmodellen. Beslutningsmodellen er modellert som et påvirkningsdiagram som er en type Bayesian Belief Network. Et påvirkningsdiagram inkluderer beslutninger og verdier som kan brukes til å sammenligne og forutsi den beste handlingen i omgivelser med usikkerhet. Handlingene sammenlignes ved å multiplisere sannsynligheten i noden med den tilsvarende nytten, noe som gir forventet nytte. Forventet nytte for ulike handlinger blir sammenlignet, og den beste handlingen er den som gir høyest forventet nytte.

For å teste beslutningsmodellen gjennomføres en manuell simulering i en tilstandsmaskin. Python-skriptet designet for å kjøre ORM brukes deretter med simuleringsdataene for å teste presisjonen til modellens prediksjon. I tillegg ble en risikomodell for MilliAmpere 2 hentet fra [2], og den ble omgjort til en beslutningsmodell i denne oppgaven.

Det gjennomføres også sensitivitetsanalyser av oppgavens resultater. Resultatene av sensitivitetsanalysen avhenger av tilstanden til modellen, som ikke er knyttet til en enkelt tilstand, men endres avhengig av situasjonen. Det er derfor laget tre ulike sensitivitetsanalyser for hver av modellene. Disse analysene sammenlignes, både analysene for hver enkelt modell og sammenligning mellom modellene.

Preface

This paper is a master thesis from the Faculty of Engineering at Norwegian University of Science and Technology (NTNU], the Marine Technology department. The time limit for the paper was 20 weeks, from early January to delivery on June 11th, 2022. This is the final requirement of the MSc. degree at NTNU.

First, I would like to thank my advisers Øyvind Smogeli and Ingrid Bouwer Utne at NTNU for their support the last year. I would also like to thank Tobias Rye Torben who has also been of great help by giving valuable input for this thesis.

Contents

List of figures

List of tables

Abbreviations

Nomenclature

API	Application Programming Interface
BBN	Bayesian belief network
CPT	Conditional probability tables
DP	Dynamic Positioning
GNSS	Global Navigation Satellite System
GUI	Graphical user interface
INS	Inertial Navigation System
IR	Infrared
Lidar	Light Detection and Ranging
MRC	Marginal risk condition
ORM	Online Risk Management
PV	Process variable
RIF	Risk influencing factor
RL	Reinforcement Learning
RTK	Real-Time Kinematic
SA	Situation awareness
SC	Safety constraint
SLH	System Level Hazards
STPA	Systems theoretic process analysis
UCA	Unsafe control action

1 Introduction

This section will outline the background and motivation for the thesis. The included topics are; the motivation behind autonomous vessels, the meaning of autonomy and how the safety is maintained, milliAmpere 2 and its operation and some background theory and information about the methodology in this thesis. The objectives, scope and limitations, and structure of the report are also included in this section.

1.1 Motivation for autonomous vessels

In recent years, the interest in autonomous vehicles has grown, with development and building in different industries and by many research teams. The marine industry is no exception, with numerous research projects to develop autonomous vessels. There are several motives for using autonomous ships. Crewless ships remove the need for accommodation and deckhouse, which saves cost, weight, and space and enables the vessels to carry more cargo[3]. Given that space for accommodation becomes unnecessary, ships can be smaller, creating more flexible transport solutions, which can replace other transport alternatives on short and medium distances[4]. Autonomous ships can also provide better accessibility to potentially dangerous areas and reduce the number of piracy incidents as pirates cannot use the crew as ransom leverage[5]. In addition, the use of autonomous ships can lead to greener shipping, reduce energy consumption, or even make it possible to operate on battery or fuel cells.

An autonomous vessel can plan and act independently of humans. However, a significant part of the human responsibility is shifted to supervising the ship, evaluating the risk level on a continuous basis, and making risk-aware decisions to ensure safe operation. With an autonomous system, an Online Risk Management (ORM) may replace the human navigator's tasks of performing the risk analysis and the decision-making. An ORM can also monitor internal systems and the operative environment, calculate risk levels for a set of hazards, provide early warnings, and undertake tactical decision-making.

1.2 Autonomy

An automation system is often defined as a process or procedure performed with minimal human assistance [6]. The automotive industry has defined a scheme for levels of autonomy, from level 0 (no autonomy) to level 5 (full autonomy) [7]. Levels 1 and 2 denote increasing levels of the system assisting the operator, while levels 3 to 5 denote decreasing levels of monitoring required by the operator [8]. When mentioning an autonomous vessel, it refers to a higher level of autonomy with decreasing level of monitoring. Autonomous control means satisfactory performance under significant environmental uncertainties and the ability to compensate for system failures without external intervention [8]. However, even for an autonomous vessel, it is necessary to have some form of human supervision during the operations since failures in the system may occur regardless of safety protocols[9].

There are two commonly used methods to solve this, both with different strengths and weaknesses.

One method is to keep the human presence on the ship and have a captain on board to supervise. This approach solves many problems, but it removes one of the advantages of an autonomous vessel since the possibility of a loss of life will still be there[10]. The other method is remote supervision, which removes the risk of human life during the operation. One of the weaknesses of remote supervision is the possibility of a signal loss between the vessel and the supervisor, leaving the autonomous vessel without human supervision. There is also the possibility that outsiders may hack the system and take control of the ship, which is unacceptable.

A solution to this dilemma is to create a supervisory control layer in the autonomous system that can replace the human supervisor and take over the supervisory control responsibility. The supervisory control layer provides another layer of safety to the autonomous system and does, among other things, risk assessment and decision making based on the evaluated risk.

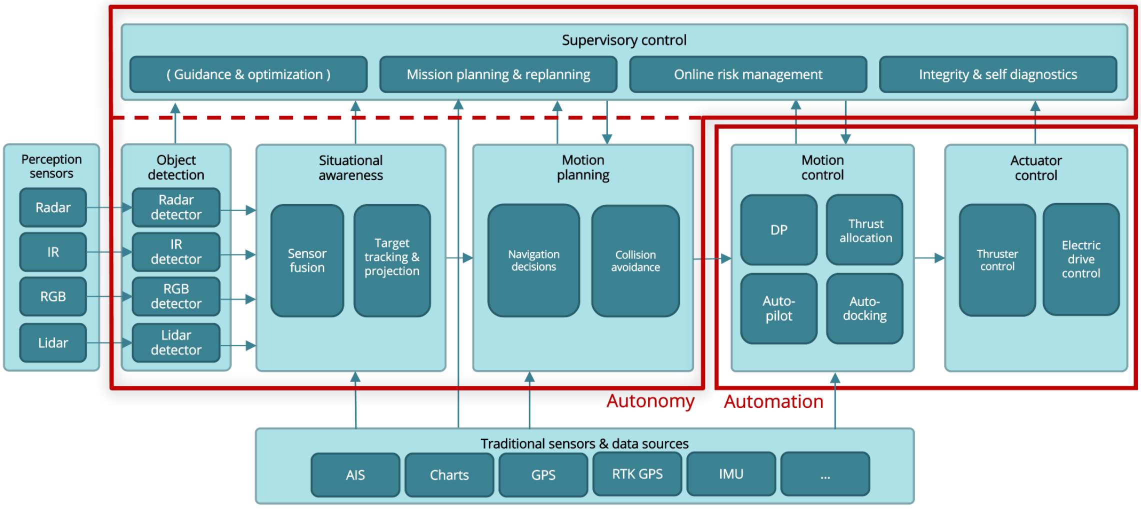


Figure 1.1: The architecture of a fully autonomous system with the supervisory layer. The supervisory layer with the ORM is meant to enable the vessel to operate independently without human supervision[11].

The supervisory control layer consists of multiple subsystems illustrated in Figure 1.1. This thesis focuses on the ORM system for the vessel milliAmpere 2. The ORM communicates with the motion control of the vessel.

The motion control consists of several functions that the vessel needs to be able to follow the directives received from motion planning. The motion control aims to link the motion planning and the actuators and ensure that power consumption is optimized. The ORM and the supervisory control layer, work independently from the rest of the autonomous system to remain a neutral party to minimize the probability of the same failure affecting both motion planning and the ORM. So, the communication between the ORM and the motion control is therefore limited.

The ORM assesses the risk continuously and it will interact with the motion control if it decides that milliAmpere 2 is acting under circumstances where the risk is too high. So, the focus is on risk avoidance; the ORM evaluates the risk and decides if a Marginal risk condition (MRC) should be initiated to reduce risk.

1.3 The autoferry project and milliAmpere 2

The autoferry project is run by NTNU. The main goal of this project is to develop groundbreaking new concepts and methods which will enable the development of autonomous passenger ferries for transport of people in urban water channels. On of the vessels in this project is milliAmpere 2, which has been the object of the analysis.

1.3.1 MilliAmpere 2

From [12], some specs about milliAmpere 2 are gathered.

MilliAmpere 2 design

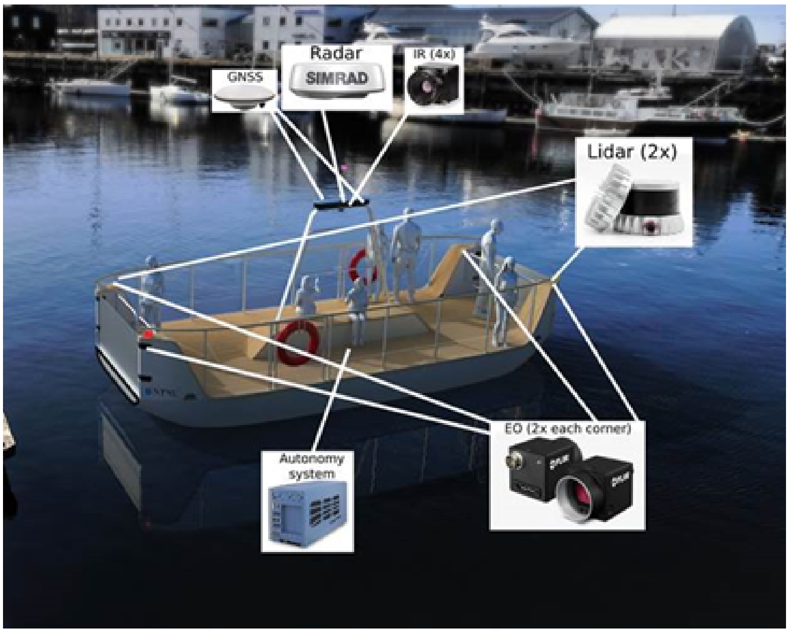


Figure 1.2: Illustration of milliAmpere 2 on the water with the sensors on the vessel.

MilliAmpere 2, shown in Figure 1.2, was designed by Innovation AS located in Trondheim according to "Nordisk Båtstandard 1990" and it was constructed at Ørnli Slipp at Frøya. MilliAmpere 2 is designed for up to twelve passengers, including the captain. The max speed of the vessel is seven knots, but during normal operations, the maximum speed is set to be 5 knots. MilliAmpere 2 is built as an autonomous vessel, so the design includes backups of the equipment and power system in case of failures. The system is also set up with a dynamic positioning (DP) automation system created by Marine Technologies LLC, automatic ramp and passenger gates, and multiple other safety functions described in [12].

The equipment on board includes

- Propulsion: 4 x 10 kW thrusters
- Electrical, battery charging with induction transfer from shore
- Anchor
- Sensors:
  - one radar,
  - two Lidars,
  - four IR cameras,
  - eight RGB cameras, and
  - one RTK GNSS/INS (navigation)

Autonomy and automation system design

The ferry is designed for fully autonomous operation. This capability is based on an autonomy system for motion planning and an automation system to actuate the derived motion planning. The autonomy system comprises the following functions:

- **Perception sensors**
  These include radar, IR cameras, RGB cameras and LIDARs. In addition, the ferry has conventional sensors and data sources for navigation.
- **Object detection**
  Processes sensor data and detects objects of interest for navigational decisions.
- **Situational awareness**
  These include sensor fusion and tracking algorithms that assess the most likely path for detected objects.
- **Motion planning**
  These include modules for navigation based on the surrounding traffic and an analysis of the vessel's own capabilities, and collision avoidance (COLAV) functionality.
- **Automatic docking**
  Additional sensors which will ensure a fully automatic and safe docking of the ferry.

The automation system has the following functionality:

- **Motion control**
  The commercial automation systems including dynamic positioning, thruster allocation and actuator control capabilities.

The full system is illustrated in Figure 1.3.

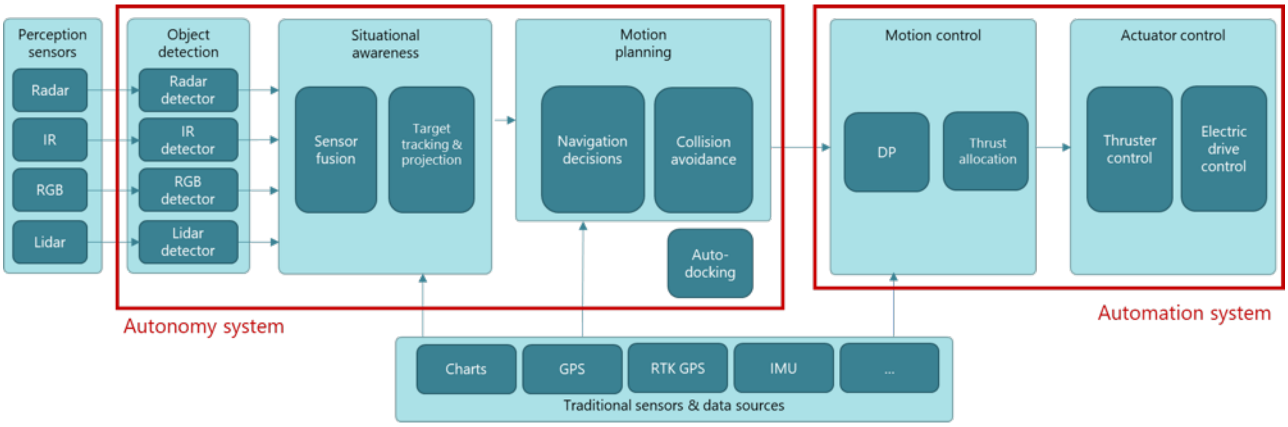


Figure 1.3: Autonomy Architecture of milliAmpere 2 without the supervisory control layer, [12].

1.3.2 Operation

In a ship, the captain has to consider the weather and the vessel's state before deciding on future actions. Given the situation, it may be necessary to include the tide, wind and current speed, wave height, and visibility when considering the weather situation around the vessel. The vessel's condition is also an essential factor, and both the capabilities and the current performance of the ship need to be clarified.

MilliAmpere 2's task is to cross the harbor canal in Trondheim, bringing passengers from Ravnkloa on the downtown side to Vestre Kanalkai on the Brattøra side and back. The crossing follows a fixed path and the approximate duration is 1 minute at normal service speed.

MilliAmpere 2's route in the harbor canal is sheltered from most severe weather conditions, making it unlikely for significant waves to occur. It is also an area with relatively deep water, making the variations due to the tide neglegible. However, the protection Ravnkloa receives from the bay at Vestre Kanalkai has its downside. It concentrates the wind coming from Solsiden like a funnel. The concentrated wind increases the perpendicular force on milliAmpere 2 during transit and this reduces maneuverability. There is also a strong current from Nidelva that can affect milliAmpere 2's mobility. Since milliAmpere 2, so far, is only operating during the day in the summer season, the possibility of weather conditions leading to reduced visibility is less likely.

1.4 Literature review

This thesis builds on previous literature from several fields. Some of this literature is referred to in various parts of the thesis, when relevant for the analysis or discussion in the thesis. This section provides a brief description of a key theoretical framework, (Bayesian Belief Network), as well as key digital tools used in the thesis (GeNIe, SMILE and PySMILE).

1.4.1 Bayesian Belief Network

A BBN is a graphical model for representing knowledge about an uncertain domain based on given observations. The knowledge is represented by modeling the posterior conditional probability distribution of the unknown outcome based on new evidence [11]. The network is a directed acyclic graph where each node corresponds to a random variable. The arcs represent a conditional dependency between the connected nodes (13, 14). Each node can have several incoming and outgoing arcs corresponding to several parent and child nodes. The state in each node is a set of probabilities but this is further expanded to conditional probability tables (CPTs) when the nodes have dependencies shown through connecting incoming arcs. The probabilities are determined according to Bayes' theorem, which gives the posterior probability of event A given evidence B.

$$P(A\,|\,B) = \frac{P(B\,|\,A) \times P(A)}{P(B)}, \quad P(B) \neq 0 \tag{1.1}$$

1.4.2 GeNIe

GeNIe is a graphical user interface (GUI) to SMILE Engine which allows for interactive model building and learning. The SMILE Engine is a reasoning and learning/causal discovery engine for graphical models, such as Bayesian networks, influence diagrams, and structural equation models. Technically, it is a library of C++ classes that can be embedded into existing user software through its Application Programming Interface (API), enhancing user products with decision modeling capabilities. SMILE is fully portable and available for most computing platforms – from data center to embedded. SMILE Engine and GeNIe are provided by bayesfusion.com, which also offers wrappers for SMILE that make it possible to use it from Java, Python, R, .NET, and other development environments[15].

1.4.3 PySMILE

PySMILE is a wrapper for SMILE that makes it possible to use it from python, but it requires a development license from bayesfusion.com. The script can then read, write and run models created in GeNIe. It is a single dynamic loaded library, and it is platform-dependent, meaning the required software version depends on the computer's operating system and python version[16].

1.5 Objectives

The objective for this thesis is to provide the basic framework for implementation of an ORM on the vessel, milliAmpere 2, so that the vessel will do its risk analysis and management, and thus be able to operate almost entirely independently of human interference. The theory behind the design of the ORM is built upon the framework proposed by [1], using an online risk model built as a BBN as part of the ORM. The framework provided in this thesis includes a decision-making model that decides when and how the ORM acts.

1.6 Scope and limitations

The scope of this master thesis is the provided framework of the ORM and to design and test the decision-making model for the autonomous ferry, milliAmpere 2. The thesis focuses on the design of the model, with the aim of being transparent and functional and illustrate the possibilities of the decision-making model. The model is deliberately kept simple to ensure transparency. Input and probability distribution are chosen to obtain plausible actions and outcomes, without any explicit empirical foundation.

The simplicity of the model is also a key limitation. To obtain a more realistic model which can function as an ORM to make milliAmpere 2 operate almost entirely independently of human interference, extensions, expert knowledge and empirical foundation would be necessary. The model should be expanded to include all the relevant risks and all the relevant information variables. Furthermore, the probability distribution for the PVs, and the assumed effect of the PVs on the risks for the vessel, should have an empirical basis and build on expert knowledge. It would also be important to have an empirical basis and expert knowledge for the effect of the possible actions taken by milliAmpere 2, initiated by the ORM in response to increased risk. Finally, it would be necessary with a thorough assessment and evaluation of the utility associated with the possible outcomes. An active ORM which interferes even at very low levels of risk would have the benefit of minimizing the risk of Collision or other important adverse events, but it might also lead to frequent disruptions of the normal operations.

1.7 Contribution

The project thesis provided the initial framework for the ORM and theory for the decision-making model. The contribution in this master thesis is a more complete framework for the ORM and the method to design the decision-making model has been improved. One model is designed and presented in the thesis. In addition, a risk model designed for milliAmpere 2 in [2] has been converted into a decision-making model for comparison. The framework of the ORM includes running the model in a python script which also has been created. To test the models, a finite-state machine simulation was created and implemented manually, including a test with the python script that can run the model.

1.8 Structure of the thesis

This thesis is organized as follows. Section 2 discusses the methodology used to create the decision-making model for a simplified environment for milliAmpere 2. It also demonstrates the framework for the complete ORM and how it works with the decision-making model. Section 3 shows the results from running simulations on two models designed according to the methodology from Section 2 and sensitivity analyses of the models. Section 4 discusses the result and methodology, and the conclusions are found in Section 5.

2 Methodology

This section goes through the methods used to create the ORM. 2.1 introduces the operator's responsibility that the ORM will partially replace and the operational criteria defined for milliAmpere 2. Then 2.2 explains the inner workings of the ORM before going more in-depth on the input in 2.3. 2.4 focuses on the decision-making model, which is the main contribution of this section. It also discusses the information that is needed to make a decision. 2.5 describes the method for setting up the decision-making model as an influence diagram and illustrates two different models. 2.8 completes the presentation of the decision-making model by explaining the software used to make the influence diagram into a dynamic model.

2.1 Operator's Responsibility

MilliAmpere 2 has an autonomous system that controls the vessel, shuttling the passengers back and forth over the canal. However, during the operation of milliAmpere 2, there is an operator on the vessel responsible for the passengers' safety. The reason for keeping the operator even though milliAmpere 2 has an autonomous system is that the autonomous system in itself is not sufficiant to ensure the safety of the passengers. The operator's presence on the ship takes up one of the passenger's slots, even though milliAmpere 2 controls the vessel. A solution to this problem is to include an ORM and a remote operator for milliAmpere 2. The intention is that the ORM and the remote operator together replace the onboard safety operator and take over milliAmpere 2's safety management. This will also save manpower as the remote operator will have a more passive role and can do other tasks at the same time. For the ORM to function, some operational criteria have to be defined to work as guidelines. These Criteria are further explained later in Section 2.8.

2.1.1 Operator's tasks

This section describes the responsibility of the onboard safety operator. As the ORM and the remote operator are intended to replace the safety operator, this will define the task of the ORM. In [12], the operator's tasks are defined. The current crew on milliAmpere 2 is a single safety operator. The safety operator is assumed to have the necessary competence to fulfill the duties and ensure a safe manning level when supported by procedures.

The safety operator has several duties, including

- Responsible operator onboard, responsibility for safe navigation, look-out, ferry operation, and ensuring operational systems,
- To take immediate manual control of the ferry when required for safe operation,
- Responsible for passenger handling, including limiting the number of passengers to

11 pax (12 persons, including the safety operator), and

- External communication, e.g., emergency response.

MilliAmpere 2 does not include automated passenger handling, like automated control of the number of passengers. Therefore, the safety operator is responsible for counting the passenger and ensuring safe embarkment and disembarkment. Without authorized passenger handling, the ORM is unable to take over the responsibility of the passengers. The ferry has a limited operation time, so there is only one shift per day, which prevents any handover issues.

The ORM's responsibility is to ensure the operational systems, manual control in case of internal failure, and communication with external personnel if necessary. The ORM does not focus on planning and motions around the vessel. One reason for this is that the ORM has access to the same sensor components as the motion planning in the autonomous system, implying that the ORM is unlikely to detect failures in the motion planning system. This reflects that the chance that both make the same mistake is too high. Instead, the ORM focuses on quality checking of the sensor data and the equipment's state and evaluating the trust in the autonomous system.

2.2 The Framework of the ORM

The inspiration for this chapter comes from the project thesis, implying that there is considerable overlapping information. The overall framework shown in Figure 2.1 was included in [17]. However, the structure's functionality has been improved, and how the ORM will accomplish its task is now more specific.

The ORM assesses the risk based on input from the process variables (PVs) and the predefined static data in the proposed framework. The PVs is the input data gathered from the vessel's sensors and they represent the controller's belief state and perception. In order to minimize the time lag between observation and action for dangerous situations, the ORM comprises several layers. The design of the first layer focuses specifically on high-risk input values for a fast response time. Figure 2.1 shows the modeled framework with the layers and flow of information.

The first layer aims to filter out the obvious risks that indicate the ORM system should intervene with the control system. This will be if any of the PVs indicate a high risk of accidents. The first layer simplifies this by defining a safety constraint (SC) for the PVs. If the input deviates from the SC, the ORM will consider that the situation involves a high-risk of an accident unless it initiates the correct MRC. An example of such an indicator is the power level of the batteries. If the level of power in the batteries is too low, the probability that the ship will experience technical problems during operations is likely to be high. In the worst case, there might be a power failure during operations, immobilizing the ship in the middle of the canal and consequently stranding the passengers on the vessel. The stranding may imply that the ship endangers the traffic situation because it will be more difficult for other vessels to travel along the canal.

The second task in the first layer is to convert the input from the PVs to probabilistic values used in the risk model and the influence diagram. During the conversion, the ORM will first assess the quality of the input data. From the evaluation of the quality, a probability is given based on the reliability of the information. The final probability represents ORM's trust in the SA to create an accurate digital representation of the surroundings based on the data gathered from this PV. Section 2.3 goes more in-depth on what the ORM considers when assessing the quality of the input data than what is described so far.

The second layer is the online risk model and the decision-making model. However, the online risk model is not part of the contribution of this thesis. The second layer assesses the more complex and stochastic relationships in the environment. [18] arguments for BBN stating that

> BNs can be used for classification and prediction of states or events even when data is partial or uncertain (Newton, 2010), which is a huge advantage over many other traditional statistical models that rely on large amounts of empirical data to be built (Marcot et al., 2006).

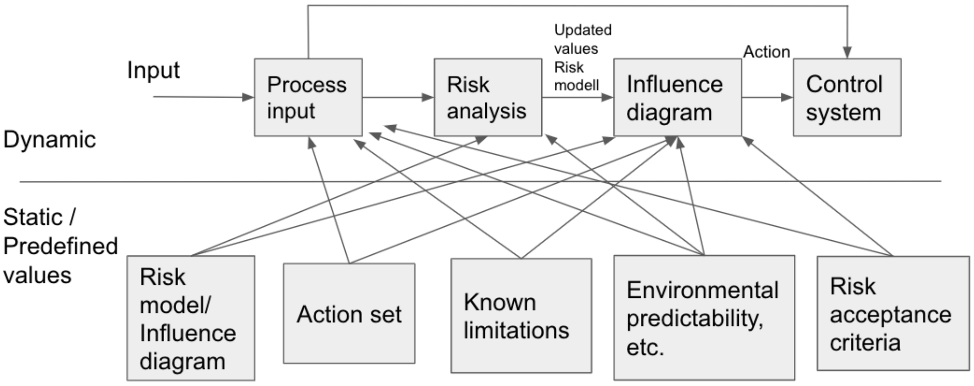


Figure 2.1: This figure illustrates the structure of the ORM. Above the dividing line are the dynamic processes and below are the static data that are used in the dynamic process. The arrows indicate where the information is used. The input is first filtered by checking if any of the PVs has a value outside the SCs. Upon discovery of any such values, it will directly issue an action to the control system. The input is also converted to probabilistic values for the risk model and the influence diagram. Given that there were no values that triggered a response in the filtering process, the risk analysis assesses the risk and finally the influence diagram makes a decision that is sent to the control system.

2.3 Data Sources

This chapter will go more in-depth about the input used in the ORM, how it is handled, and the output sent to motion control.

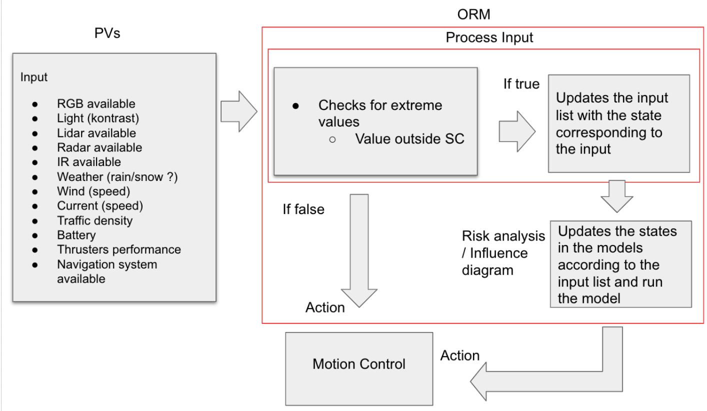


Figure 2.2: This figure illustrates the input that the ORM uses and the subsequent layers. The first box in the ORM represents the filtering that checks if there are any PVs outside the SCs. The arrows indicate the next step based on the outcome of this filter. If all the input passes the filter, it continues to the next box where the input nodes are updated. This step has been adapted to the method used for simulating the models in this thesis. It is only if the input value is outside the defined scope of the initial state that the node will be updated before running the model.

2.3.1 Input data

The input is gathered from the sensors and the internal systems on the vessel, e.g., the Lidars and the battery monitoring system. By gathering sensor data, the ORM assesses the quality of the input. The ORM bases its trust in the autonomous system's SA performance on evaluating the sensor data quality. Reduced trust may occur if, e.g., lower data quality increases the possibility that the object detection fails to observe an incoming object, potentially leading to a collision. The quality checking of the input gives an additional layer of safety and can reduce the probability of accidents.

Sensors

The value of the input data from a sensor depends on the quality of information that it provides. The sensors used on milliAmpere 2 are Optical/RGB and IR cameras, Lidars, and a radar. For these sensors, this thesis looks at two causes that affect the quality of the input. The first cause is that the sensor fails, so there is no reliable information to gather from the sensor output. The second cause is that the vision is limited by external factors reducing the output quality because of uncertainty in the data [19]. Evaluating the possibly reduced quality because of these causes can help assess the expected real-time accuracy of the decisions taken by the autonomous system.

The estimation of the sensors' accuracy could come from empirical testing. Sensor failure will typically lead to the sensors stopping to send output or the output freezing. The failure can be a temporary situation, which may resolve itself, but this is not until the sensor connects and starts updating again.

The assessment of the quality of the sensor output depends on the type of sensor. For the Optical camera, an essential factor in assessing the quality of the image is the color contrast. An image with a low color contrast can imply a dim light source and, therefore, a low-quality output. Lack of light increases the probability that an object detection, based on the output of the Optical camera, will fail to observe surrounding objects. Unlike Optical cameras, Lidars and IR cameras work both day and night. However, rain, fog, and wet surfaces reduce the accuracy of Lidars and IR cameras [19][20].

The fourth sensor is the radar. Compared to Optical and IR cameras and Lidars, radar sensors are more robust towards adverse environmental conditions like rain or fog [21]. The radar is better at detecting large metal objects, while detecting smaller objects like kayaks is considerably more challenging.

Environmental Data

Environmental forces like the wind and the current affect the mobility of the vessel and power usage during transit. A reduction in mobility reduces the distance milliAmpere 2 can cover in a certain period without going off the path, thus, increasing the probability of an accident like a collision with another vessel. The change in resistance can also lead to significant changes in the amount of power necessary for milliAmpere 2 to cross over. An extra power expenditure increases the probability of a power shortage during transit.

There are at least two options for measuring the effect of these external forces. One option is to use an instrument at the quays and a wind measuring device on milliAmpere 2 to find the wind and current speed. Another option is to use the estimated average of the bias from the observer in the autonomous system to represent the external forces affecting the vessel.

Traffic

The probability of an accident will depend on the amount of other traffic on the canal, with more traffic implying a higher risk. As there typically is considerable regularity in the traffic, historical traffic statistics given the time and date may provide helpful information about the expected amount of traffic. The estimated traffic may be a helpful supplement to information about registered objects for object detection. In the current version of the model, the traffic input is not used in the decisions about actions. It is nevertheless retained in the model, as it would be included in a more realistic model.

Internal integrity - internal monitoring

This input is from the internal monitoring of the system, informing the ORM about the real-time status of the internal components and subsystems of the autonomous system. Essential input is whether the components and internal systems are available and in working order, or if they have failed. More advanced use would be to estimate the performance of the components to give a more accurate assessment of the situation. This could be used to combine input from several PVs. An example of this is that a reduced thruster performance will affect the mobility of the vessel more during intense weather, e.g., strong wind, than during a typical day[22].

2.3.2 Output

In this thesis, the possible actions the ORM can take are limited to 5 different actions. These actions are the four MRCs and Continue, the decision not to deviate from the motion plan. The MRCs may be split into two groups. The first group is the actions when milliAmpere 2 is docked at the quay and consists of Continue and MRC 1. The second group is the actions during transit and consists of Continue, and MRC 2, MRC 3 and MRC 4. The output from the ORM is an action command representing 'Continue' or one of the MRCs.

2.4 Decision-making

The ground work of this chapter was done in the project thesis [17], but changes has been made because of the progress on the ORM and the decision-making model. The fundamental thoughts about the decision-making is unchanged, but the the quality of the input has become a more significant part of the chapter.

The foundation of every good decision is a comprehensive understanding of the situation and the possible outcomes. The answer can often be simple, but it is necessary to know the possible actions and their consequences to make a sound decision. In a complex environment, the available possible actions can be endless, and a comprehensive understanding is crucial for rapid and sound decisions. The humane brain is the most advanced decision-maker we know of [23]. It uses our prior knowledge and senses to learn and adapt to different situations and then act accordingly. AI tries, in some sense, to copy this ability with, for example, RL and neural networks [24]. This paper focuses on creating an influence diagram that can take on the responsibility of quality check of the autonomous system and make decisions limiting milliAmpere 2 to ensure the safety of the passengers.

In order for the decision-making model to take the appropriate risk-mitigating action, the model should know the following elements:

- Understanding of the surrounding and internal situation,
- an online risk model,
- risk acceptance criteria, and
- the set of possible actions.

Firstly, understanding the surrounding and internal situation is needed as input to assess milliAmpere 2's current situation. For milliAmpere 2 to make appropriate decisions, the vessel need to get accurate information from the sensors. If the quality of the information is too low, the possibility of the object detection missing an obstacle increases. With the increasing possibility of mistakes the trust in the autonomous system decreases and the decision-making model will act. However, for this to succeed, the internal situation of the vessel must be working. If milliAmpere 2 is able to observe an obstacle, but is unable to avoid it, the observation made by the autonomous system is worthless.

Secondly, the online risk model provides real-time quantitative risk measures, given the operating conditions. The online risk model represents part of the prior knowledge and gives the system an evaluation of possible risks. An example can be if two ships meet in a narrow passage. Neither an incoming ship nor the narrow passage will by itself indicate a high-risk situation since each can be avoided – the ship by changing the course and the narrow passage by staying in the safe area in the middle. However, when the ship and the narrow passage are combined, the possible actions are reduced and the risk increases rapidly.

Thirdly, defining risk acceptance criteria is required to determine the time of intervention and the appropriate risk-mitigating action. These criteria should be set to ensure that the risk of a collision or other adverse events is sufficiently low. However, the criteria should not be unnecessary stringent, so that they lead to frequent interventions in situations when the risk of an adverse event is low. The tradeoff between these two opposing concerns will depend on the probability of the possible outcomes, and the utilities associated with each outcome. A collision with a risk of serious damage to the vessel, or even worse, to risk of injuries to the passengers or the operator, would be a grave outcome involving a very large negative utility. Thus, the risk of such an outcome should be minimized and ideally set to zero. The defined criteria will be used together with the influence diagram to decide when the system will intervene and predict the most beneficial action. The risk acceptance criteria and the influence diagram, without the dynamic input, complete the knowledge base of the ORM. These are shown together with the predefined action set below the line in 2.1.

Lastly, modeling decision-making with an influence diagram includes defining the available actions. This set of actions is based on the vessel's capabilities, the environment, and the operation. The actions should ensure a good balance between avoiding the risk of adverse outcomes and avoiding excessive disruptions of the normal operation of the vessel. It might be tempting to choose an elaborate design with many possible actions, depending on a precise assessment of the situation. However, an extensive set of actions will inevitably lead to a more complex system and a need for higher precision memory and computation time. The differences between the actions will be reduced with the more extensive set of actions, and the predicted differences in utility may also be reduced. In a setting with considerable uncertainty and where two actions result in similar expected utility, it will often not be possible to state with high confidence that one action is superior. Yet the comparison and evaluation of two actions will require additional memory and computation time. If both actions are acceptable, the similarity in results and additional computational requirements may indicate that one of them can be removed to reduce costs associated with memory and computation time.

2.5 BBN Modeling

This chapter describes the characteristics of BBN's and influence diagrams, before explaining the method used to set up the decision-making model.

2.5.1 BBN

The nodes in the BBN are set after designing the model, thus, making the model fixed. The BBN's nodes, arcs, and conditional probabilities are then optimized for the designed operation. The implication is that the BBN is limited to the environment and the task to a certain degree. A change in either environment or task might make it necessary to redesign the network to adapt to changes.

The BBN can be used to create complex and flexible models, but this will come with a cost of both memory and computation time that might be unnecessary[25]. In [18], it is discussed how to set up a BBN to reduce human bias and unnecessary memory expenditure. One of the main points is to avoid connecting too many incoming arcs to the same node. Instead, it is often better to do it in steps by using multiple nodes to gather the probabilities. This technique is called parent divorcing [26]. The data needed to store the table increases exponentially for every incoming arc. A node with n states and m incoming arcs from nodes with states ≥ 2 will, at a minimum, contain $n \times 2^m$ conditional probabilities. Therefore, to save memory, it is better to aim for a more extensive network with smaller CPTs which will also help minimize the number of conditional probabilities needed in the network.

2.5.2 Sensitivity Analysis

A sensitivity analysis for a BBN determines how different nodes affect a particular node under the given set of assumptions in the network. For this thesis, the set of assumptions in the network refers to the nodes' states. This also imply that if a node changes it's state, the assumptions in the network have changed and this can affect the result of the analysis.

The analysis identifies how different sources of uncertainty from the other nodes in the BBN contribute to the overall uncertainty. In an influence diagram, the sensitivity analysis is used to find nodes that have the possibility to affect the prediction significantly. That is to say, the nodes that significantly affect the predicted expected utility. This can be used to identify the nodes that can potentially have a strong effect on the decision.

However, in a influence diagram where the value node is pointed at by a decision node, the number of predictions depends on the number of decisions in the decision node. Thus, in influence diagrams the sensitivity analyses are completed for every decision the value node is depending on. For the sensitivity analysis in this thesis, since there are four actions, every situation that is analysed will generate four analyses [27]. The reason for the numerous sensitivity analyses is that nodes that are influenced by the decision node will have different probabilities depending on the action.

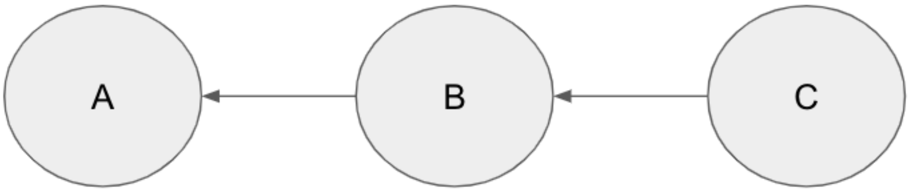


Figure 2.3: A simple BBN, where A is influenced by B, and B is influenced by C.

The sensitivity analysis is executed by changing the posterior probability of a single node given a specific situation. An example of this is if the target of the analysis was node A in the network shown in Figure 2.3. To check the sensitivity of A towards B, the sensitivity analysis would increase and decrease the posterior probability of B and observe the change in A. In this example, this would mean to change the probability of C and observe the changes in A.

The probability is changed within a certain parameter range, both increasing and decreasing the probability. This change of probability is referred to as a parameter change. The analysis observe the effect of the changed probability has on the predicted utility.

2.5.3 Online Risk Model

The online risk model framework written by Utne et al. [1] is built with a system-theoretic process analysis (STPA) and a BBN, and the result is used as input in the influence diagram. An STPA-analysis is a tool to identify the potential causes of critical events that have not yet occurred but may happen in the future. It is one of the inputs in the decision-making model. In an STPA - analysis, the first step includes describing the autonomous system and defining its control system and the necessary PVs. The PVs are the input data gathered from the vessel's sensors. Thus, the PVs will be crucial for the controller's perception of the state of the vessel.

The second step consists of identifying the system-level hazards (SLH). Hazards are triggering events that constitute the basis of any potential unfavorable consequence. The main aim of the ORM is to prevent hazardous events. Identification of system-related hazards and knowledge of combinations of causal factors potentially leading to critical events are necessary to prevent an accident [28]. The actions that lead to SLH are defined as unsafe control actions (UCAs). The UCAs' causal factors that lead to them are identified and defined as risk influencing factors (RIFs).

2.5.4 Influence Diagram

The chosen method for creating the decision-making model is an influence diagram. An influence diagram is an expanded BBN, which also includes decision nodes and value nodes [29]. The fundamental principles of the BBN are unchanged, but the outcome becomes the expected utility of each action instead of the probabilities in the nodes.

Decision nodes represent variables under the decision maker's control and show the available decision alternatives. The available decisions are the possible decision node's states. Value nodes represent a measure of the desirability of the outcomes of the decision process, often referred to as utility. Value nodes are quantified by the utility of each of the possible combinations of outcomes of the parent nodes. This is further explained in section 2.6 when explaining the model's design. The value nodes are always continuous, and their domains are the domains of the utility function [15].

Typically, an arc in an influence diagram denotes an influence between two nodes. The tail of the arc denotes the node that influences the node's state at the tip of the arc. Arcs in influence diagrams can have a causal meaning. An arc from a decision node to a chance node denotes that the decision will impact the chance node by changing the probability distribution of its outcomes [15]. In GeNIe, decision nodes are drawn like rectangles and value nodes are drawn as diamonds.

2.6 Set up the model

The first step is to identify the objective and the vessel's capabilities and the accident situations in which the system should react. The next step is to choose the risk-mitigating actions and build up the model. The risk-mitigating actions affect the probabilities in the node representing the accident situation and the utilities in the value node but do not influence the model's design. Therefore, completing the two tasks independently from each other is possible. After identifying the relevant accident situations and understanding the operational environment, it is possible to design the nodes and arcs in the influence network. The quality of the influence diagram, when created based on 'expert knowledge,´ is therefore interlinked with the designer(s) understanding and capabilities of the environment and the vessel.

The risk-mitigating actions are defined based on the degree of freedom and trust the ORM and the original control system have. The original intent of the control system is to be able to work independently. The ORM is designed to work as a safety net to prevent accidents based on faults in the control system. Therefore, risk-mitigating actions are set to reduce the risk if there is a fault in the control system. Following the principle of least invasive action, the design should choose the action which is appropriate for the situation. As discussed in 2.4, the ORM should also have a limited action set for each model to reduce the memory and computation time. A suggested approach is to define MRCs as the base of the action set to steer the vessel into a safe state.

When designing the arcs and nodes in the model, the goal is to find the utility for the action given the possible accident situations, e.g., a collision. The utility will therefore have incoming arcs from both the decision node and the node representing the accident situation. The rest of the influence diagram branches out from the accident situation based on a top-down approach. The leaf nodes come from the data gathered from the sensors, risk model, statistics of the physical components, and environmental conditions. However, since the risk model development is not completed, the nodes from the risk model are not included in this thesis's model. These nodes are connected up the network through the child nodes and will influence the prediction of the most appropriate action.

This process is not without difficulties. In general, the data used as input in the leaf nodes, except the risk model, are mostly values like distances, degree of visibility, and other types of factual data. In order to use this in the influence diagram, it has to be converted to probabilities. It is also essential to understand the correlation between the nodes when designing the network, i.e., to what extent the outcome at one node affect the outcome of another node. The correlation can help to identifying nodes that directly influence each other, or nodes that affect the same subsystem. The check has at least two benefits. The first is to identify nodes which are strongly correlated so that one can put greater importance on their relation given that the nodes and relation is relevant for the model. Second, identifying and removing nodes and arcs with low correlation can reduce the network's complexity.

The last part is to assign the utilities in the value node. These utilities will have a significant influence on the final decision. There is no fixed method to find the utilities, but one approach is a cost-benefit analysis. The risks and benefits are thus converted into numerical values that can be used for comparison. A cost and benefits analysis focusing on monetary values, may lead to excessive concern for monetary effects, and too little concern for other types of effects. The utilities should represent what the ORM considers when it evaluates the situation. It would, therefore, be irresponsible to only focus on monetary values when, for example, considering a collision for a vessel with people on board. The utility has to reflect the cost of possible fatalities and injuries in such a situation. The cost and benefits analysis then becomes more complicated since it is necessary to define a value to human injuries before it can be included into the calculation. Another factor that can be included in the utility, as it may significantly affect milliAmpere 2's commercial value, is the loss or gain in reputation in case of accidents. As none of these events are certain to happen, they have to be adjusted with their probability of occurring. Implying that it is the excepted utility that determines which decision is taken.

2.6.1 Operation Criteria

The operation criteria are defined limits for the operation given the location, task, and vessel. In case of problematic conditions or failures, the operation criteria reflect the increase in risk by reducing the scope of the operation. The operational criteria for milliAmpere 2 in this thesis define the safety limits for the internal integrity of the vessel. Crossing the boundaries of the safety criteria leads to a reduction of trust in the autonomous system for the ORM. MilliAmpere 2, under optimal conditions, is highly trusted by the ORM. However, a component failure will reduce the ORM's trust in milliAmpere 2's ability to perceive danger and act. The decrease in trust depends on which component fails and the state of the local environmental conditions. This thesis focuses on the risk of collision, with the main potential cause of these collisions are errors in milliAmpere 2's autonomous system. There is also an uncertainty included into the model, so even though milliAmpere 2 or the decision-making makes the correct decision, the possibility of a collision still exists.

The minimum criteria for each MRC are the following:

MRC 1 - Stay at quay;

- Loss of a single sensor type,
- loss of one thruster pack, and
- reasons included in the world of the model where milliAmpere 2 no longer can be trusted to operate with the thrusters without colliding.

MRC 2 - Go to the closest quay;

- Loss of a single sensor type, or
- loss of one thruster pack.

MRC 3 - Dynamic positioning;

- Loss of three sensor types, or
- loss of both Lidars and optical cameras

MRC 4 - Drop the anchor;

- Loss of one thruster pack and strong wind, or
- reasons included in the world of the model where milliAmpere 2 no longer can be trusted to operate with the thrusters without colliding.

One factor that gives reason to worry is the loss of a thruster pack. MilliAmpere 2 is designed to be able to operate with a single thruster pack since one pack is powerful enough to move the vessel. However, this removes the backup in the system, and milliAmpere 2 cannot afford to lose the other because that will lead to milliAmpere 2 being stranded on the water. Environmental forces can also influence milliAmpere 2, especially if one of the thruster packs has failed. If a thruster pack fails, combined with strong environmental forces disturbing the vessel, it is safer to drop the anchor since the additional forces can become too much for the reduced thruster capacity.

2.6.2 Actions

The ORM is designed to overrule the motion planning if it considers that continuing with the motion plan will involve an undesirable or unacceptable risk. If that is the case, the ORM may implement one of the predefined actions defined in operational criteria. Alternatively, if the existing motion plan does not entail high risk, the ORM may choose to let the vessel continue according to the existing plan, Continue.

Below, the predefined actions that may be taken to prevent risk are described. Since the models used in this thesis focus on milliAmpere 2 during transit, the relevant actions during transit are explained first.

Continue

When the ORM concludes that there are no high-risk situations during normal operations, the ORM will not want to intervene with the motion planning and, therefore, pick the Continue action.

MRC 2; Go to the closest quay

If a sensor fails, milliAmpere 2 can still operate, but the risk of milliAmpere 2 ending in unfortunate situations has increased. To minimize this risk, milliAmpere 2 maneuvers to the closest quay. However, other factors need to be considered, for example, the possibility of an object blocking the path. In a real-life setting, there would be multiple situations for initiating MRC 2, but many are in a rocky area at the edge of the boundaries between the other MRCs.

Failures during transit The first scenario is if milliAmpere 2 experiences failures during transit. However, milliAmpere 2, based on the operational criteria, is capable of getting to the quay by itself. Many factors and consequences are considered before making the decision to go to the closest quay, i.e., MRC 2. Firstly, consider the choice between Continue and MRC 2. Should the ship have crossed the halfway point, the actions following from these two decisions will essentially be the same, considering that milliAmpere 2 will continue towards the other side. The consequences, however, are different. Continue will not interfere with the continuation of the operation. On the other hand, MRC 2 will require a more thorough check at arrival. Thus, delays in operations affect the passengers waiting to board and the technician called over.

The situation is different if milliAmpere 2 is still in the first half of the crossing. If the ORM initiates MRC 2, milliAmpere 2 will stop and return. The vessel passengers will then be affected as they have to return to the departure point. Another possible consequence is the increased risk of collision with other vessels moving in the area because of an unnatural change in the vessel's trajectory, which can come as an unexpected development. The increase in risk is because of the surprising maneuver of milliAmpere 2 where other vessels may need to re-plan their course to avoid collisions, or simply that one of the vessels fails to observe this change and are then on a collision course with milliAmpere 2.

It is difficult to evaluate the increase in the risk of collision if milliAmpere 2 stops and returns to the departure quay and, thus, also difficult to asses whether this is worth consideration. Another matter is the increase of displeasure from the passengers. Given the state of milliAmpere 2 when initiating MRC 2 and the short travel distance, an option is to continue despite the failure. Not following the safety procedure increases the risk of milliAmpere 2 being stuck on the water before it can dock because of more failures during the transit. Thus, this will improve passenger satisfaction at the cost of increased risk to their safety. One option is to take advantage of the structural design of the ORM. The requirement for initiating MRC 2 can be raised to only target the situations on the borderline between MRC 2 and MRC 3 where milliAmpere 2 risks stopping midway and can therefore not prioritize the satisfaction of the passengers and need to return. The scenarios that no longer trigger an MRC 2 response from the influence diagram can be handled externally in the python script to ensure that milliAmpere 2 still pauses its operation. So the lower requirements for when the ORM decides to initiate MRC 2 are then increased in the influence diagram so as to only cover the situations where milliAmpere 2 cannot compromise and has to travel towards the closest quay to ensure that it does not stop in a section of the crossing.

Secondly, consider the choice between MRC 2 and MRC 3, i.e., whether to go to the quay or initiate DP. MilliAmpere 2 is close to the limit regarding the backup of sensors. The dividing line is when, given the current visibility and state of the sensors, the risk of collision increases because it can no longer be assumed that milliAmpere 2 is able to observe and react to unforeseen situations. In most scenarios where the ORM initiates MRC 2, the vessel can continue because of the redundancies in the system. However, a sensor failure may still be a concern, as it reduces the capabilities of the vessel. Furthermore, a sensor failure will also reduce the robustness of the vessel, making it more vulnerable to possible additional failures. To explain, consider this hypothetical situation. MilliAmpere 2 is on one of the last trips of the day, and it is getting dark. The RGB cameras cannot see anything, and then the Lidars fail. MilliAmpere 2 is left with the IR cameras and the radar to complete the trip. If milliAmpere 2 were to meet a smaller boat or kayak that both the radar and IR failed to observe, it could lead to a collision and, in extreme circumstances, drowning. Because

Blocked path Another scenario that forces milliAmpere 2 to return is if an object blocks the path for a longer duration. This situation has two different consequences compared to the previously discussed scenarios. Firstly, there are no failures. Therefore, a more extensive check of the system or possibly stopping operations is unnecessary. Secondly, it still has to return regardless of milliAmpere 2's current position, so closest quay does not apply. However, milliAmpere 2 might need assistance to clear the path and notify it when it can continue its operation. This scenario is included to remove the possibility of milliAmpere 2 blocking the path for vessels moving along the canal and hindering traffic. It can be discussed if this should be a separate action or be included as a unique scenario under MRC 2 since the action is similar. However, the consequence regarding the continuation of the operation is different.

The situations where the path is blocked is not included in the models of this thesis. One of the main reasons is that the decision-making model is unable to calculate the time, thus, making it impossible to estimate the duration the path is blocked.

MRC 3; Dynamic positioning

As was briefly mentioned earlier when discussing MRC 2, MRC 3 is designed for more complex situations than MRC 2. MRC 3 changes the vessel's state from moving to stationary. There are two types of scenarios for taking this action, a temporary stop to avoid a passing obstacle or that the collision risk is too high because the quantity and quality from the input sensors are too poor. The first scenario does not interfere with the operation after the path is cleared and is merely an evasive maneuver. This scenario is not included in the models below. The second scenario signals a stop in operation because of multiple sensor failures or bad environmental conditions. The precondition for deciding on MRC 3 instead of MRC 4 is an underlying assumption that the sensor failures are temporary and milliAmpere 2 will after a while be able to continue the operation.

MRC 4; Drop the anchor

For MRC 4, the distinction is more straightforward. Given the capabilities of milliAmpere 2, there is no need to drop the anchor unless the integrity of the vessel is reduced, e.g., thruster or battery failure. Given this conclusion, MRC 2 and MRC 3 cover a different group of scenarios from MRC 4. However, if milliAmpere 2 is in a situation where it wants to stop but cannot stay in DP, e.g., low thruster performance or the sensor failure is not temporary, the decision-making model will choose MRC 4. The consequences of going into MRC 4 is similar to MRC 3, but more severe, since dropping the anchor ties milliAmpere 2 in place, unlike dynamic positioning (MRC 3).

We now considers the possible actions when milliAmpere 2 is docked.

MRC 1; Stay at the quay

MRC 1 is the only action the ORM can take when milliAmpere 2 is docked and this not an available option during transit. The same criteria to pause the operation applies when milliAmpere 2 is docked as during transit. The ORM will therefore initiate 'MRC 1' under similar situations as described for the other actions above.

Summary actions

When milliAmpere2 is in transit. MRC 2, Go to closest quay, is chosen if there is a sensor failure or the maneuverability is significantly affected, but it is still viewed as safe to operate the vessel. If half the distance is covered, the vessel will continue to the destination and the only difference from normal procedure is the additional check at the destination. If MRC 2 is implemented before half way, milliAmpere 2 will return to the departure point. This will be a nuisance for the passengers, but yet worthwhile to prevent risk of more adverse outcomes.

MRC 3, Dynamic positioning, is chosen when there is more severe failures or conditions making it risky or impossible to continue the movement of the vessel. MRC 3 implies that the vessel remains in the position it has, essentially “waits”, on the expectation that it can resume it’s movement when this is possible. The model does not include a method to handle the subsequent situation in case the obstacle does not move. Unless the remote operator overrides the control, milliAmpere 2 may be staying in that position until there are any new developments. Three possible scenarios are; the sensors were only temporarily frozen and the operation may continue, a ship collides with milliAmpere 2, and the power level falls below the critical value so milliAmpere 2 switch to MRC 2 and dock. In case of a temporary stop because the path is blocked there will not be an extra check of the system.

MRC 4, Drop the anchor, is another alternative when there is more severe failures or conditions making it risky or impossible to continue the movement of the vessel. However, in contrast to the waiting with MRC 3, dropping the anchor (MRC 4) will imply that the vessel needs assistance to resume it’s operations. Thus, MRC 4 is chosen if the conditions make it difficult to implement MRC 3, because of e.g. a strong current making it necessary to drop the anchor to avoid drift of the vessel. Alternatively, MRC 4 may be chosen when the problem is considered permanent, so waiting would not help. This scenario is ruled out in the model below.

2.7 The design of the models

In this section, the design of the models is explained. Model 1 was created for this paper to illustrate the method and is described more in-depth. Model 2 was presented in [2]. It was initially a risk model for milliAmpere 2 before it was converted to a decision-making model to be used as a comparison with Model 1 in this thesis. Model 1 and Model 2 use the same method for setting up the CPTs, so Model 2 will not be explained in-depth.

2.7.1 Model 1

Model 1, shown in Figure 2.4, illustrates the system’s performance during transit in a simplified world. In this world the only accident scenario that exists is collisions. The model contains the following nodes giving information to the ORM and listed in Table

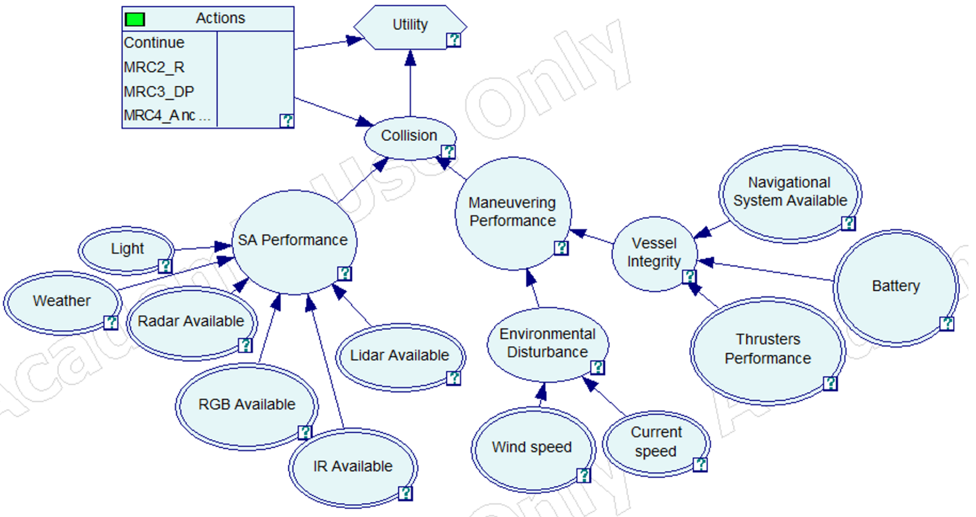


Figure 2.4: This figure shows the design of Model 1. The deterministic nodes, which provides input from the PVs, are drawn with two circles. The children of the input nodes are referred to as as gathering nodes in this thesis and they are drawn with one circle as chance nodes. At the top of the model are the decision node to the left, drawn as a square, and the value node, drawn as a diamond.

2.1.

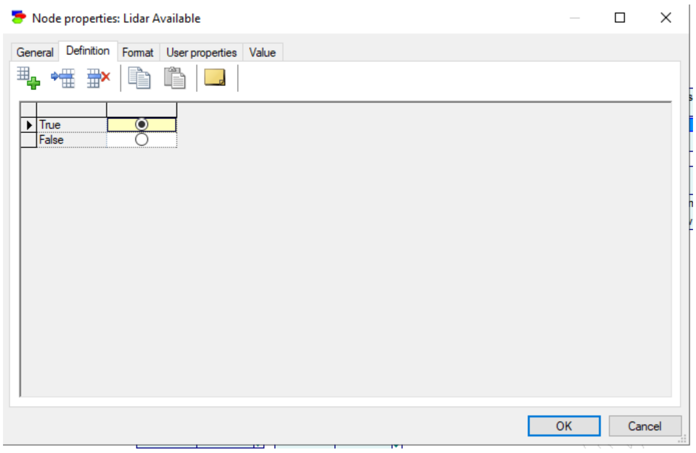
Light	Weather	Radar Available
Lidar Available	IR Available	Wind Speed
Thruster Performance	Battery	Navigational system Available
Current Speed	RGB Available	

Table 2.1: The input nodes in Model 1.

The nodes are PVs included as input nodes in the model and contain two possible states, a normal state and a state that deviates from normal. The exception is Thruster Performance which contains three states. Limiting the possible states is a simplification done in the model to simplify the modeling. The input nodes are deterministic, reflecting that the input value is given by the sensor. Deterministic nodes are drawn with double circles in GeNIe. Figure 2.5 shows how the state of the deterministic input node Lidar Available.

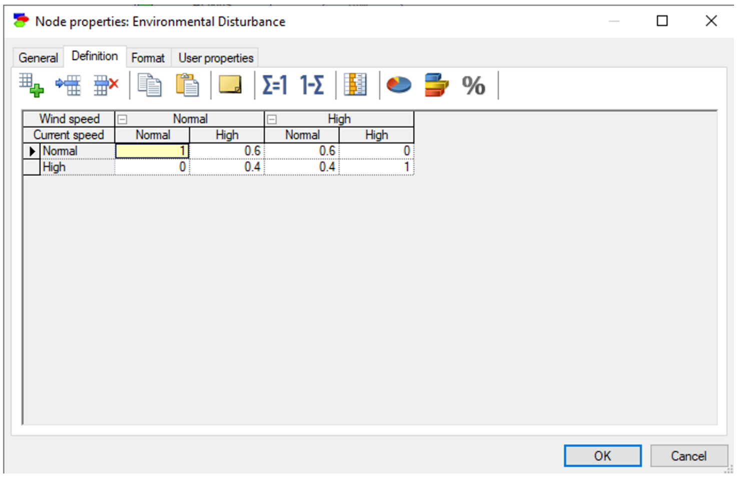
The information from related input nodes is then combined into gathering nodes which show an overall representation of the information. For example, the gathering node SA Performance gathers the information from the input nodes that affect the SA. In model 1, there are 3 gathering nodes which receive information directly from the input nodes (SA performance, Environmental disturbance and Vessel integrity), and one gathering node which receives information from the gathering nodes on Environment disturbance and Vessel integrity. The gathering nodes are Conditional probability tables, CPTs, which are based on information from the input nodes. For every combination of input from the input nodes, a probability is assigned for the state of the gathering node.

An example is the Environmental Disturbance's CPT. Figure 2.6 shows how the probability distribution for the state of gathering node, Normal or High, depend on the input from the influencing nodes. There are two input nodes influencing Environmental Disturbance, Wind Speed and Current speed. Both nodes, Wind Speed and Current speed, have two possible states, Normal and High, implying that there are four possible combinations. Wind Speed and Current Speed are assumed to enter symmetrically in the model, i.e. implying that the probability for High for Environmental disturbance is the same if Wind Speed is High and Current Speed is Normal, as if Wind Speed is Normal and Current Speed is High. In both cases the probability of a High state in Environment disturbance is set to 0.6.



True	●
False	○

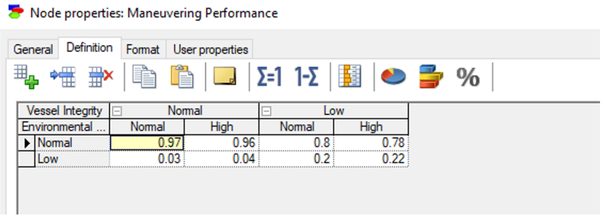
Figure 2.5: This figure shows a screenshot of the deterministic node's state taken from GeNIe.



Wind speed	Normal		High	
Current speed	Normal	High	Normal	High
Normal	1	0.6	0.6	0
High	0	0.4	0.4	1

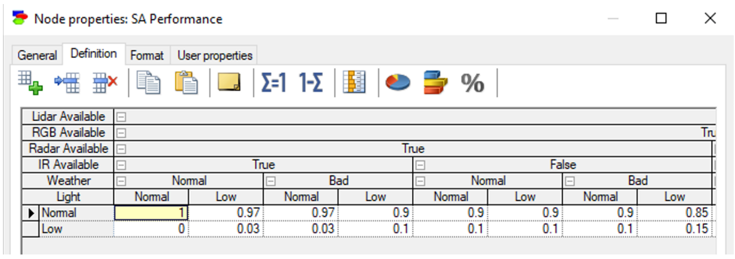
Figure 2.6: This figure shows a screenshot of a state's CPT taken from GeNIe.

The information from Environmental Disturbance and Vessel Integrity are gathered together in the node Maneuvering Performance. The information in Maneuvering Performance and in SA Performance, combined with the decision node Actions, will then determine the probability distribution for a Collision. Actions, the decision node that is drawn as a square in GeNIe, contains the possible actions which the decision-making model may take.



Vessel Integrity	Normal		Low	
Environmental ...	Normal	High	Normal	High
Normal	0.97	0.96	0.8	0.78
Low	0.03	0.04	0.2	0.22

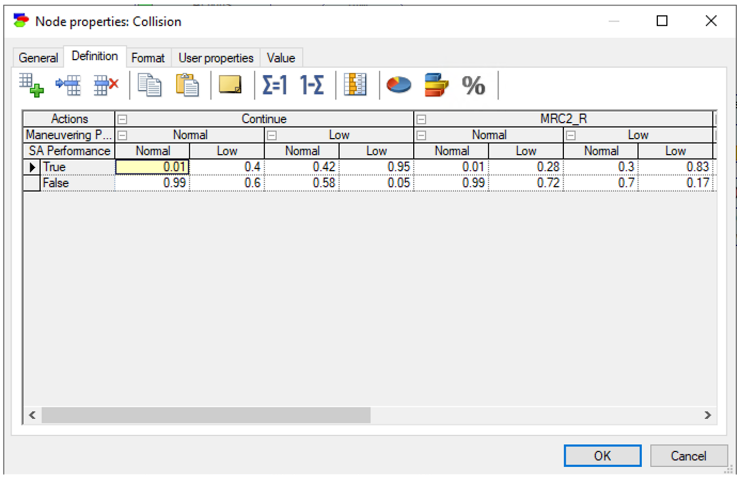
Figure 2.7: This figure shows a screenshot of Maneuvering Performance's CPT.



Lidar Available								
RGB Available								Tru
Radar Available	True							
IR Available	True				False			
Weather	Normal		Bad		Normal		Bad	
Light	Normal	Low	Normal	Low	Normal	Low	Normal	Low
Normal	1	0.97	0.97	0.9	0.9	0.9	0.9	0.85
Low	0	0.03	0.03	0.1	0.1	0.1	0.1	0.15

Figure 2.8: This figure displays a screenshot of a part of the CPT for SA Performance, where both the Lidar and the RGB are available. In this node, we have not included any uncertainty, as can be seen from the figure where the probability that SA Performance is Normal is 1 when all the input nodes are in Normal state.

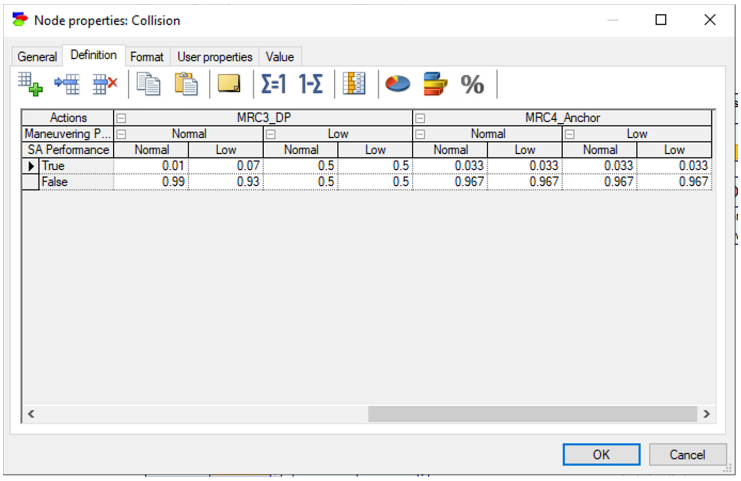
Maneuvering Performance's CPT also contains an element of uncertainty, as can be seen in Figure 2.7. Even though the states of Vessel Integrity and Environmental Disturbance are Normal, the probability that Maneuvering Performance is Low is set to 0.03. the motivation is to make it possible to observe the effect of additional uncertainty in the simulations of the model in Section 3. A similar uncertainty to Maneuvering Performance is not included in SA Performance.



Actions	Continue				MRC2_R			
Maneuvering P...	Normal		Low		Normal		Low	
SA Performance	Normal	Low	Normal	Low	Normal	Low	Normal	Low
True	0.01	0.4	0.42	0.95	0.01	0.28	0.3	0.83
False	0.99	0.6	0.58	0.05	0.99	0.72	0.7	0.17

Figure 2.9: This figure shows a screenshot of Collision's CPT depending on the actions Continue and MRC 2.

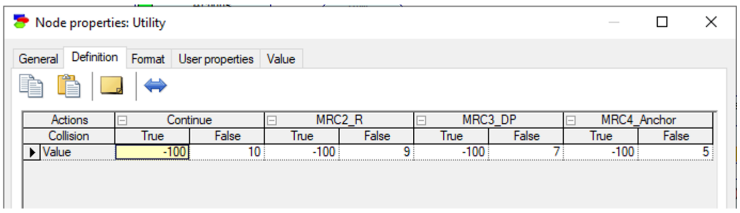
The CPT for Collision is displayed in Figures 2.9 and 2.10. The probability of a Collision depends on both the state of the vessel, as represented by SA Performance



Actions	MRC3_DP				MRC4_Anchor			
Maneuvering P...	Normal		Low		Normal		Low	
SA Performance	Normal	Low	Normal	Low	Normal	Low	Normal	Low
True	0.01	0.07	0.5	0.5	0.033	0.033	0.033	0.033
False	0.99	0.93	0.5	0.5	0.967	0.967	0.967	0.967

Figure 2.10: This figure shows a screenshot of Collision's CPT depending on the actions MRC 3 and MRC 4.

and Maneuvering Performance, and the action taken by the ORM. Figure 2.8 shows the probability distribution for Collision if the action is Continue or MRC 2, while Figure 2.9 shows the distribution for MRC 3 and MRC 4. We observe that if both SA Performance and Maneuvering Performance are Low, the probability of a Collision will close to unity for Continue and very high (0.83) for MRC 2, while it will be 0.5 for MRC 3 and close to zero for MRC 4, i.e. if the anchor is dropped. Thus, if the vessel has both weak situation awareness and maneuverability, Dynamic positioning (MRC 3) will reduce the risk but dropping the anchor is necessary to minimize the risk of a Collision. The probability of a Collision will also be significant if either SA Performance or Maneuvering Performance is Low, and the response is Continue or MRC 2. If the problem is that SA Performance is Low, while Maneuvering Performance is Normal, responding with MRC 3 will reduce the risk considerably (probability of Collision = 0.07), while MRC 4 will minimize the risk (probability of Collision = 0.033). In contrast, if Maneuvering Performance is Low and SA Performance is Normal, the risk will also be fairly high with MRC 3 (probability of Collision = 0.5), reflecting that Dynamic position (MRC 3) is risky with weak maneuverability. Dropping the anchor, MRC 4, will minimize the risk also in this case, as maneuverability and situation awareness are of little direct importance when the anchor is dropped.



Actions	Continue		MRC2_R		MRC3_DP		MRC4_Anchor	
Collision	True	False	True	False	True	False	True	False
Value	-100	10	-100	9	-100	7	-100	5

Figure 2.11: This figure shows a screenshot of the utility depending on the actions and Collision.

The Utility node, which is a value node drawn as a diamond in GeNIe, contains the utilities for the two possible states of Collision, depending on the action that is chosen. If there is a Collision, the action is irrelevant. This is a really bad outcome, and the utility is set to minus 100 as can shown in Figure 2.11. If there is no Collision, the utility depends on the action. The preferred outcome is of course Continue, which is assigned a utility of 10. The other actions yield lower utility, MRC 2 gives utility 9, MRC 3 utility 7 and MRC 4 utility 5. The lower utility associated with more decisive actions, in particular dropping the anchor, reflects that this leads to more assistance and a longer disruption of the normal operations of milliAmpere 2.

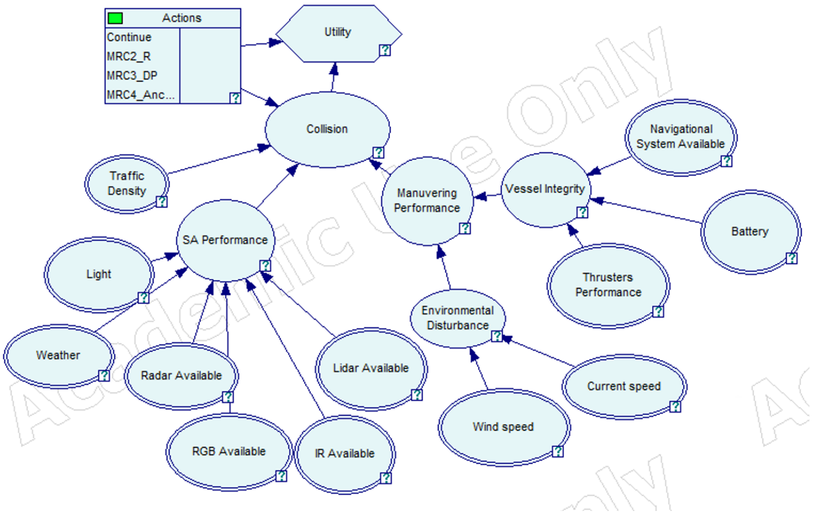


Figure 2.12: This figure illustrates Model 1 where Traffic Density is included into the design.

When testing the model with the simulations, Traffic Density was omitted. It was initially a part of the model, as shown in Figure 2.12. However, due to the simplifications when designing the model, making the input states deterministic, the decision of the influence diagram did not depend on Traffic Density. Therefore, the Traffic Density was unnecessary when testing the model in the simulations.

2.7.2 Model 2

Like Model 1, Model 2, shown in Figure 2.13, illustrates the system's performance during transit in a simplified world. The only accident scenario that exists in this world is a collision. The model contains the following elements found in Table 2.2.

Failure of Lidars	Failure of Optical cameras	Failure of IR cameras
Failure of Radar	Large precipitation	Cyber Attack
Failure of Linear actuator pack A	Strong Wind	Failure of Linear actuator pack B
Failure of Battery pack A	Failure of Battery pack B	Failure of DP computer control
Failure of Backup control computer	Autonomy computer failure	

Table 2.2: The input nodes in Model 2.

The model design is taken from [2] and is converted into an influence diagram from a risk model. The original risk model found the probability of Losing navigational control for

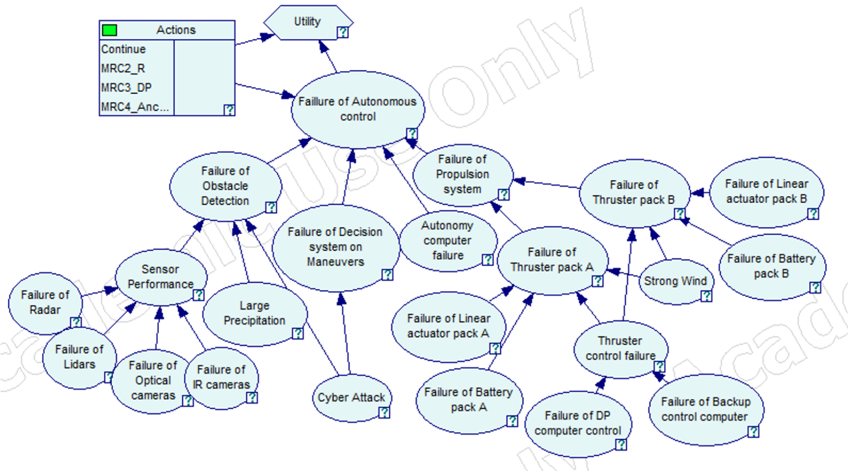

Actions
Continue
MRC2_R
MRC3_DP
MRC4_Anc...
Utility
Failure of Autonomous control
Failure of Obstacle Detection
Failure of Propulsion system
Failure of Thruster pack B
Failure of Linear actuator pack B
Failure of Decision system on Maneuvers
Autonomy computer failure
Failure of Thruster pack A
Failure of Battery pack B
Strong Wind
Sensor Performance
Failure of Radar
Large Precipitation
Failure of Linear actuator pack A
Thruster control failure
Failure of Lidars
Failure of Optical cameras
Failure of IR cameras
Cyber Attack
Failure of Battery pack A
Failure of DP computer control
Failure of Backup control computer

Figure 2.13: This figure illustrates the design of Model 2. The model was taken from [2] and then converted to a decision model. In the illustrated design, the visible changes are the additional nodes, the decision node and the value node, and the connection arcs. The nodes related to remote control was also removed, and Sensor Performance changed its name from Failure of all sensors.

milliAmpere 2. The nodes influencing this probability were Failure of autonomous control and Failure of remote control. The additional information of remote control has not been included in this thesis. Therefore, the nodes and arcs connected to Failure of remote control were removed in addition to Losing navigational control as it became unnecessary.

The model in [2] was initially a risk model, which included the probabilities of the input nodes and the CPTs for most of the nodes. The nodes that needed to change because of the conversion were Sensor Performance, Failure of Obstacle Detection, Failure of Propulsion system, and Failure of Autonomous control. The input nodes were kept as chance nodes to include the probability of the sensors failing, in addition to the nodes are operating or that they are not available.

Sensor Performance was originally Failure of all sensors, which is not an appropriate node for the new purpose of the model since the model should act before all the sensors fail. The distributed probability in the node's state was also changed, using the same grouping of the probabilities as in Model 1. Failure of Obstacle Detection's CPT was also changed due to the change in Sensor Performance. Like Sensor Performance, Failure of Propulsion system and Failure of Autonomous control were also changed to make their CPTs appropriate for a decision-making model.

In the value node, Utility, the cost for Failure of Autonomous control was set as -100, the same as in Model 1. However, for Model 2, the utility for MRC 3 and MRC 4, given that Failure of Autonomous control is False, was reduced to 6 and 4.

Figure 2.14 illustrates an extended version of Model 2 with the remote control included in the model. It shows how Model 2 can further expand to include more variables and be closer to representing reality. The remaining CTP can be found in Section 5.

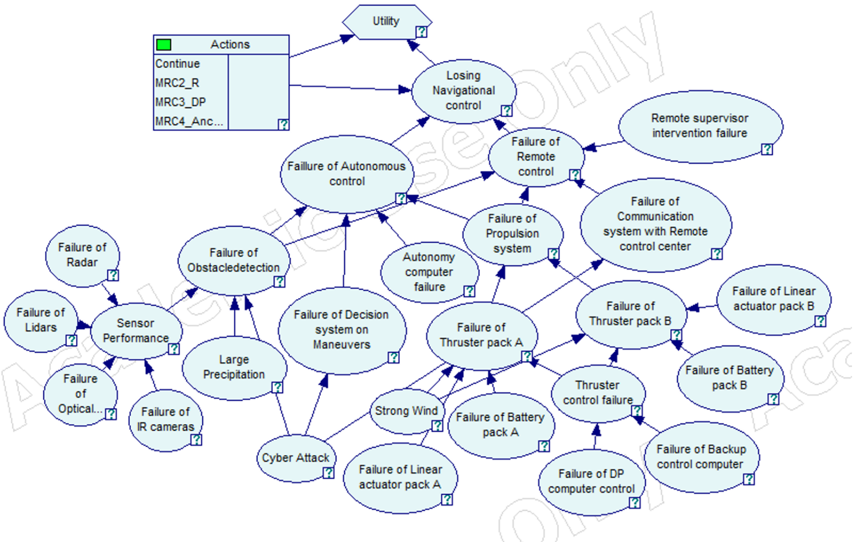

Utility
Actions
🟩
Continue
MRC2_R
MRC3_DP
MRC4_Anc...
Losing Navigational control
Remote supervisor intervention failure
Failure of Remote control
Faillure of Autonomous control
Failure of Communication system with Remote control center
Failure of Propulsion system
Failure of Radar
Failure of Obstacledetection
Autonomy computer failure
Failure of Lidars
Sensor Performance
Failure of Decision system on Maneuvers
Failure of Thruster pack A
Failure of Thruster pack B
Failure of Linear actuator pack B
Large Precipitation
Failure of Optical...
Failure of IR cameras
Strong Wind
Failure of Battery pack A
Thruster control failure
Failure of Battery pack B
Cyber Attack
Failure of Linear actuator pack A
Failure of DP computer control
Failure of Backup control computer

Figure 2.14: This figure illustrates the complete model taken from [2] with the added decision node and value node.

2.8 Simulation Tools

The influence diagram created in GeNIe is not a dynamic model, and the states need to be updated manually. Another problem is that GeNIe does not have an effective method for filtering out the critical PVs in the first layer, as discussed in Section 2.2. Incorporating this filter into the influence diagram can make it very unstable when the PVs are closer to the boundary of the SCs because to ensure that the critical PVs will not be ignored, they will be highly weighted. The weighting will either be directly in the utility or indirectly with the conditional probabilities. The consequence is that these PVs will also strongly affect the system when they are close to the SC and lead to faults in the ORM. Thirdly, as mentioned in Section 2.6, some PVs need to be converted before being used as input in the influence diagram. Converting the input is not something GeNIe can do, so these calculations of the values must be done separately.

To solve the problem of having to run and update the diagram in a GeNIe, PySMILE is used from a python script. The model created in GeNIe is saved as a .xdsl file, and PySMILE can read, manipulate, and even overwrite the file. This solution also helps solve the problem of filtering and converting the PVs. Python can accomplish both of these tasks. Thus, the ORM can continuously take in the input, filter the information, and convert it before updating the probabilities in the influence diagram and running it in the script.

The python script can check the critical PVs in the first layer and directly compare these values to the risk criteria. After that, the script can convert the PVs that are not probabilistic values separately before updating and running the influence diagram. Testing the model through simulations in a software script is also faster than filling the input manually in GeNIe.

The python script used in this thesis focuses on testing the decision-making models. The tests simulate the possible scenarios defined in the model's world. The script first loads the model before redefining the input nodes based on the simulated scenario. Next, the script updates the model and extracts the value node's utilities before identifying the action with the highest utility. The last step compares the predicted best action identified from the extracted utilities to the expected result of the simulation and saves the result of the comparison. Every simulation for a model repeats the same process and calculates the model's precision, the percentage of correct predictions.

3 Results

In order to test the models, a simulation of a finite-state machine has been designed. The simulations are of the same type for both models. However, the data is different because of the different input variables required for the models. The following chapter describes the simulation before presenting the result of the finite-state simulations.

3.1 Finite-state machine simulation

The outline is for a simple simulation to test the influence diagram for milliAmpere 2. The simulation is designed to update the state of the input nodes in the model to simulate a specific scenario, like a finite-state machine. The simulations were created manually, limiting the number of simulation scenarios to test the models with. After running the model with the simulated scenario, the predicted best action from the model is compared with the predefined solution based on the operational criteria. The simulation logs the success or failures and counts the failed simulations. The simulation scenarios do not cover every possible scenario included in the world designed in the models. There are two reasons for this. First, testing all possible scenarios is unnecessary, because many scenarios will by design of the model give the same result as other scenarios, as explained below. Second, the number of possible scenarios is large, and would be much larger in a more realistic model, making it worthwhile to look for simplifications.

The number of scenarios in the models is given by the possible states of states in each input node multiplied together. The number of input nodes in the first model is eleven, and the number of states is two, except for thruster performance with three states. The equation then becomes,

$$3 \times 2^{10} = 3072 \tag{3.1}$$

The same equation applies in the second model, but the number of nodes is now 14, with two possible states each. So the number of scenarios is

$$2^{14} = 16384 \tag{3.2}$$

It is unnecessary to simulate all these scenarios because of the grouping of the probabilities in the CPTs. Testing one situation for a particular scenario group in SA Performance or Vessel Integrity in model 1 is the same as testing every situation for that node. Since the conditional probability is the same, an example of this is if one sensor fails, regardless of which, it leads to MRC 2. Therefore, in theory, it is enough to test the scenario combinations for MRC 2 with a single sensor failure as input to the SA Performance node. The grouping reduces the simulation scenarios for MRC 2 in model 1 by more than 20 times. This is the number of probabilities in SA Performance's CPT with similar probability and fall under MRC 2.

3.1.1 Simulation scenarios

There is only one simulation for each model, but with many simulations scenarios. The simulation scenarios are grouped based on the predefined solution, going systematically through scenarios for each action. The manually created simulation scenarios for both models are included in Section 5.

Normal operation – First scenario group

The first simulation group is for the situations where it is no failure and the decision-making model says Continue. The most essential part of this test group is to test the sensitivity. Making certain that the ORM does not frequently stop the vessel and pause the operation. If the ORM is too sensitive, that will drastically reduce the ORM's value.

MilliAmpere 2 intervenes – Second, Third and Fourth scenario group

The subsequent simulation groups assess the model's responses towards the changing situation as the severity increases. The simulation is designed so that the second scenario group contains scenarios where the response is MRC 2, the third group MRC 3 and the fourth group MRC 4.

As an additional check, and to reduce the possibility of errors in the model that might occur because of mistaken assumptions or wrong probability in the CPT of a few situations, the simulation scenarios include several randomly picked situations within the same probability group given the operational criteria. So, despite theoretical consideration saying that it is enough to test the precision of the model for one probability group in a gathering node with one test, multiple scenarios have been included.

3.1.2 Model 1

Table 3.1 shows the initial input values used in Model 1. The manually created simulation scenarios consist of 70 different states for Model 1. The first simulation scenario group is group 1. The input variables that are included in the first group is Light, Weather, Wind speed, current speed and Thruster Performance. From the second group all the input nodes are included in the simulation scenarios.

Result

In the simulation for Model 1, the number of simulated scenarios used to test the model is 70. The model successfully predicted the correct action for all the states included in the simulated scenarios with 100% precision.

Variables	Possible states	Initial value
RGB Available	True, False	True
LIDAR Available	True, False	True
IR Available	True, False	True
Radar Available	True, False	True
Navigational system Available	True, False	True
Light	Normal, Low	Normal
Weather	Normal, Bad	Normal
Wind Speed	Normal, High	Normal
Current Speed	Normal, High	Normal
Battery	Normal, Low	Normal
Thruster Performance	Normal, Low	Normal

Table 3.1: The initial values of the input nodes and the possible states in Model 1.

3.1.3 Model 2

Table 3.2 shows the initial input values used in Model 2. The manually created simulation scenarios consist of 95 different states for Model 2. The sequence of simulation scenarios are similar as for Model 1, starting with the first group before continuing with the second, third and forth scenario groups.

Variables	Possible states	Initial value
Failure of Optical cameras	False, True	False
Failure of LIDARs	False, True	False
Failure of IR cameras	False, True	False
Failure of Radar	False, True	False
Cyber Attack	False, True	False
Autonomy computer failure	False, True	False
Failure of Linear actuator pack A	False, True	False
Failure of Battery pack A	False, True	False
Failure of Linear actuator pack B	False, True	False
Failure of Battery pack B	False, True	False
Failure of DP computer control	False, True	False
Failure of Backup control computer	False, True	False
Strong Wind	False, True	False
Large Precipitation	False, True	False

Table 3.2: The initial values of the input nodes and the possible states in Model 2.

Result

In the simulation for Model 2, the number of simulated scenarios used to test the model is 95. The model successfully predicted the correct action for all the states included in the simulated scenarios with 100% precision.

In this thesis, the sensitivity analysis is visualized with a tornado diagram. The utility goes along the x-axis with a vertical line indicating the actual utility given the state of the nodes in the model. Along the y-axis the nodes with conditional dependence is ranked form top down with the node that has the highest sensitivity at the top. The tornado diagram uses coloring to identify positive and negative changes in the nodes' probability and a horizontal line indicating if the change has a positive or negative effect on the utility.

3.2 Sensitivity Analysis

The sensitivity analysis aims to identify the factors that strongly affect the predicted utility. A BBN sensitivity analysis depends on the model's network of probabilities, so changing the situation described by the model by modifying the posterior probability of a node's state can lead to significant changes in the analysis. GeNIe can generate two different sensitivity analyses. One of the analyses uses colors to shade the nodes red to indicate the sensitivity. A deeper red indicates a higher sensitivity. The other analysis, a tornado plot, is slightly more advanced. The plot also differentiates the effect from the posterior probability's positive and negative change. The nodes' sensitivity is ranked, so it is easier to differentiate between two nodes where the sensitivity is nearly the same. The last difference is that it analyzes the utilities for the different actions separately, making it possible to identify the node's effect on the utility, given a particular action.

This thesis will use the tornado plot to do the sensitivity analysis. The analysis only tests the sensitivity of the value node when it is performed on an influence diagram. Three different states will be used to compare each model for the analyses.

The three situations will give four analyses for every state because the decision-making model is an influence diagram, as mentioned in section 2.5.2. In the analysis, the utility goes along the x-axis with a vertical line indicating the actual utility given the state of the nodes in the model. Along the y-axis the nodes with conditional dependence is ranked from top down with the node that has the highest sensitivity at the top. The tornado diagram uses coloring to identify positive and negative changes in the nodes' probability and a horizontal line indicating if the change has a positive or negative effect on the utility. The green color indicate an increase in the probability and the red line indicate a decrease in the probability. The parameter change is set to 10% in the analyses. That is to say, the degree of change in the posterior probability of the nodes.

3.2.1 Model 1

In the first sensitivity analysis of Model 1 shown in Figure 3.1, the state is set to the initial values shown in Table 3.1. Considering Continue, Utility is most sensitive to a negative change in the Collision's probability and it has minimal sensitivity to a positive change. However, an increase in Maneuvering Performance posterior probability increases the utility. The three other actions are also significantly more sensitive to a negative change in the probability of Collision. However, there is a clear trend showing increasing sensitivity to a positive change in the probability of Collision. The actions' utilities' sensitivity of

Maneuvering Performance goes opposite to Collision. The exception from this is MRC 3. MRC 4 is comparatively unaffected by Maneuvering Performance.

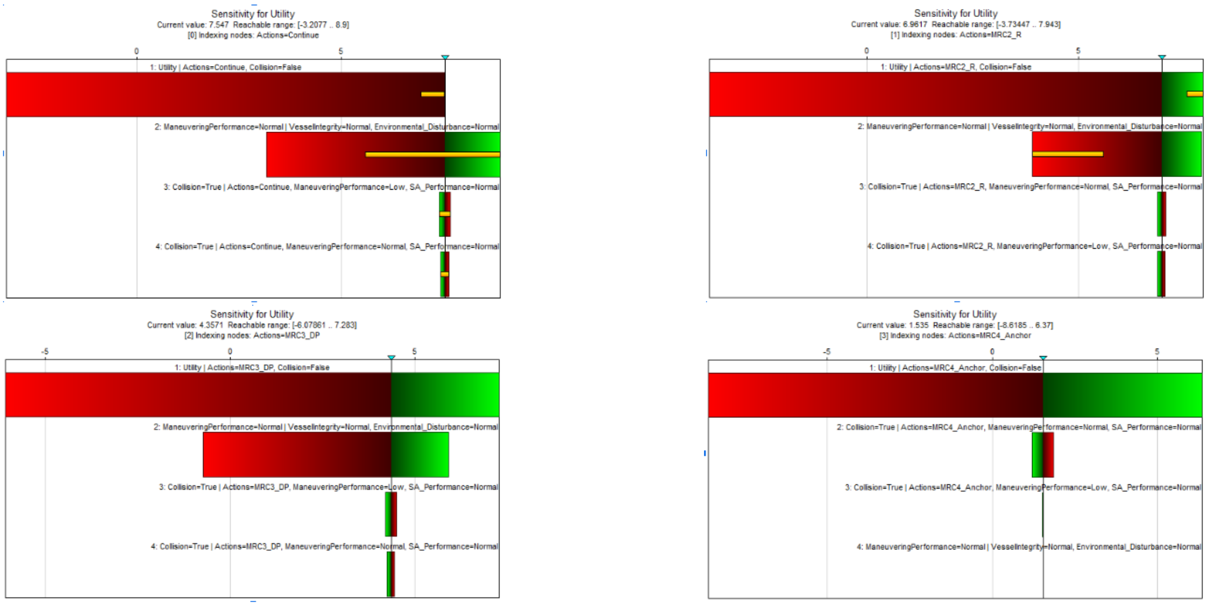


Figure 3.1: First sensitivity Tornado of Model 1 with the input nodes at the initial values. From top left is Continue, top right is MRC 2, bottom left is MRC 3 and bottom right is MRC 4.

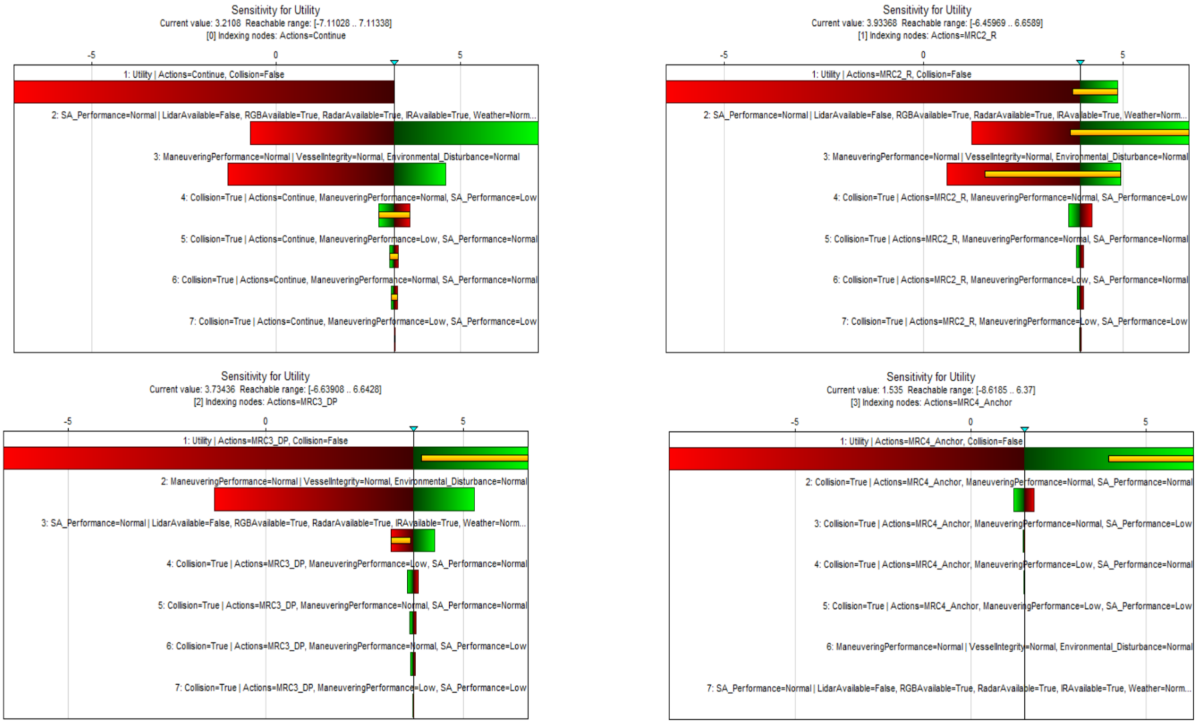


Figure 3.2: Second sensitivity tornado of Model 1 with Lidars failure and low lighting. From top left is Continue, MRC 2, MRC 3 and MRC 4.

Figure 3.2 shows Model 1 after the state of Lidar Available and Light is set to False and Low. Comparing the analysis with the previous, the sensitivity towards the change in

Collision's probability is similar in the two analyses. Utility is significantly more sensitive towards Collision than the other nodes, and the same trend of increasing sensitivity to a positive change of Collision's probability. The similarity between the two models also includes the sensitivity to Maneuvering Performance. However, changing the state of two nodes connected to SA Performance made a significant difference between the two analyses. Continue and MRC 2 are more sensitive towards changes in SA Performance than Maneuvering Performance, contrary to MRC 3, which is still more sensitive to Maneuvering Performance. On the other hand, MRC 4 is not affected by the model's change of state on the two input nodes. Neither the value of the utility nor the reachable range of the utility changed.

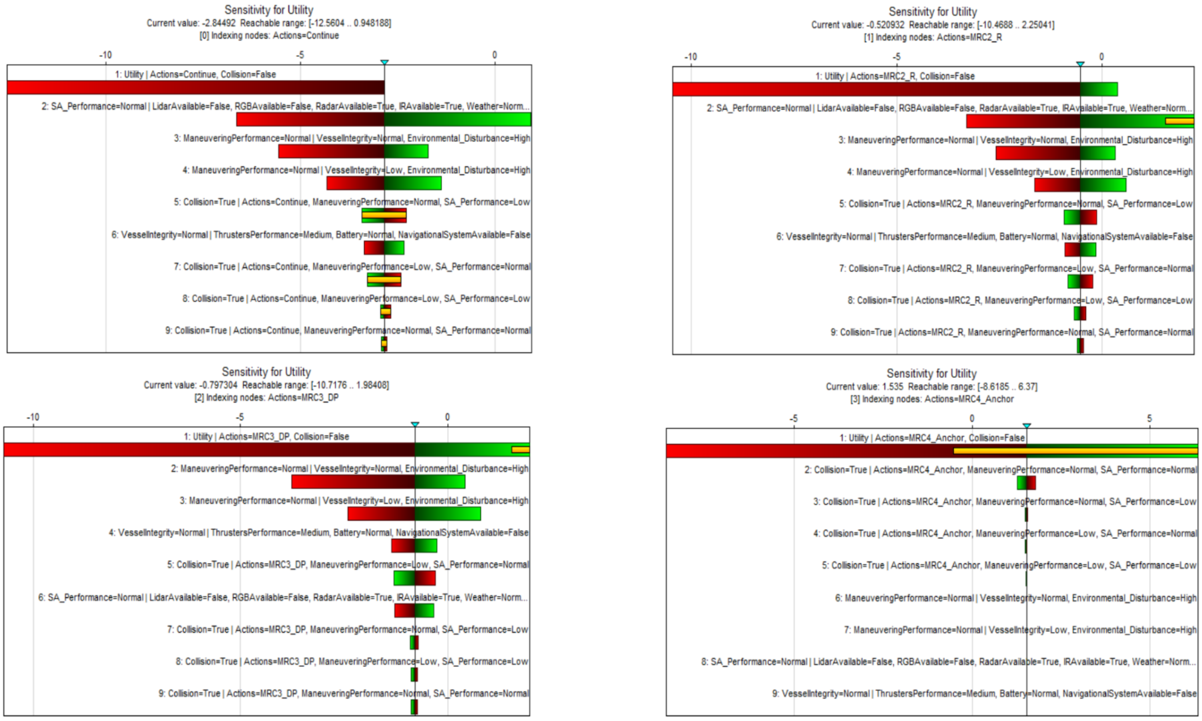


Figure 3.3: Third sensitivity tornado of Model 1 with Lidars failure, RGB failure, low lighting, Navigational system failure, Thruster Performance, high Wind Speed and high Current Speed . From top left is Continue, MRC 2, MRC 3 and MRC 4.

The last analysis of Model 1 shown in Figure 3.3 is of one of the more extreme states. In this analysis of Model 1 the state of seven input nodes was changed from the initial value, and the scenario belongs to simulation scenarios group 4. The Utility node's sensitivity towards Collision remains the most significant with the sensitivity trend of the positive change of Collision's probability. Continue and MRC 2 is more sensitive towards changes in SA Performance than Maneuvering Performance. However, Maneuvering Performance is in both third and fourth place. In the third place, Maneuvering Performance depends on Vessel Integrity's state is normal; in the fourth, it depends on Vessel Integrity's state is low. MRC 3 continues to be more sensitive towards Maneuvering Performance, and SA Performance is now lower on the sensitivity ranking compared to the previous analysis shown in Figure 3.2.

Summary

From the three analyses, the Utility (depending on the action and Collision is false) has significantly higher sensitivity than the other nodes. The sensitivity toward the positive and the negative change is also consistent through the three analyses. For MRC 4, this is the only factor that can significantly affect the Utility. MRC 3 is, through the analyses, significantly more sensitive towards Maneuvering Performance than SA Performance. The sensitivity analysis for Continue and MRC 2 was similar in the three analyses, except for the highest-ranked, Utility (depending on the action and Collision set as false).

3.2.2 Model 2

The first sensitivity analysis of Model 2 is shown in Figure 3.4 and the states are set to the initial values shown in Table 3.2. There are several nodes that that will have a negative impact on the utility with a negative change of the probabilities. However, the trend of an increasing positive effect in the utility from the factor Utility (depending on the action and the Failure of Autonomous controls is False) is still present, like in Model 1. The most significant factor in this analysis is Failure of Autonomous control for Continue and MRC 2 with the Utility (depending on the action and Failure of Autonomous control is False) as the second. For MRC 3 and MRC 4, the opposite is the case, with Utility as the most significant factor and Failure of Autonomous control as the second. The subsequent three on the rankings, Autonomy computer failure, Cyber Attack and Failure of Decision system on Maneuvers, is similar for all four actions. The three nodes can affect the Utility negatively in case they decrease, but have no positive effect with a positive change in the probabilities. The last five nodes in the sensitivity analysis are similar for Continue, MRC 2 and MRC 4, a negative change in the probabilities gives a negative change in the utility. However, MRC 3 is more sensitive towards a negative change in the nodes influencing Thruster Performance.

Figure 3.5 shows the second sensitivity analysis for model 2. In this analysis the state of Failure of Optical cameras and Large Precipitation are set to True. Continue and MRC 2 are most sensitive to changes in Failure of Autonomous control and have the same sensitivity ranking of the first seven nodes. They are more sensitive to negative changes of these nodes while only two for Continue and three for MRC 2 give a positive increase of the utility with a positive change of the probability. MRC 3 and MRC 4 are also more sensitive towards negative changes of the nodes' probability. The utility of MRC 3 and MRC 4 are significantly more sensitive towards Utility (depending on the action and Failure of Autonomous control is False). It differs from the other nodes with the larger sensitivity towards a positive change of the probability.

The third sensitivity analysis is shown in Figure 3.6 and the states of Failure of Optical cameras, Failure of IR cameras, Failure of Backup control computer, Failure of Linear actuator pack B and Strong Wind. Continue is most sensitive to Failure of Thruster pack A and it differs from the other nodes with a significant sensitivity towards a positive

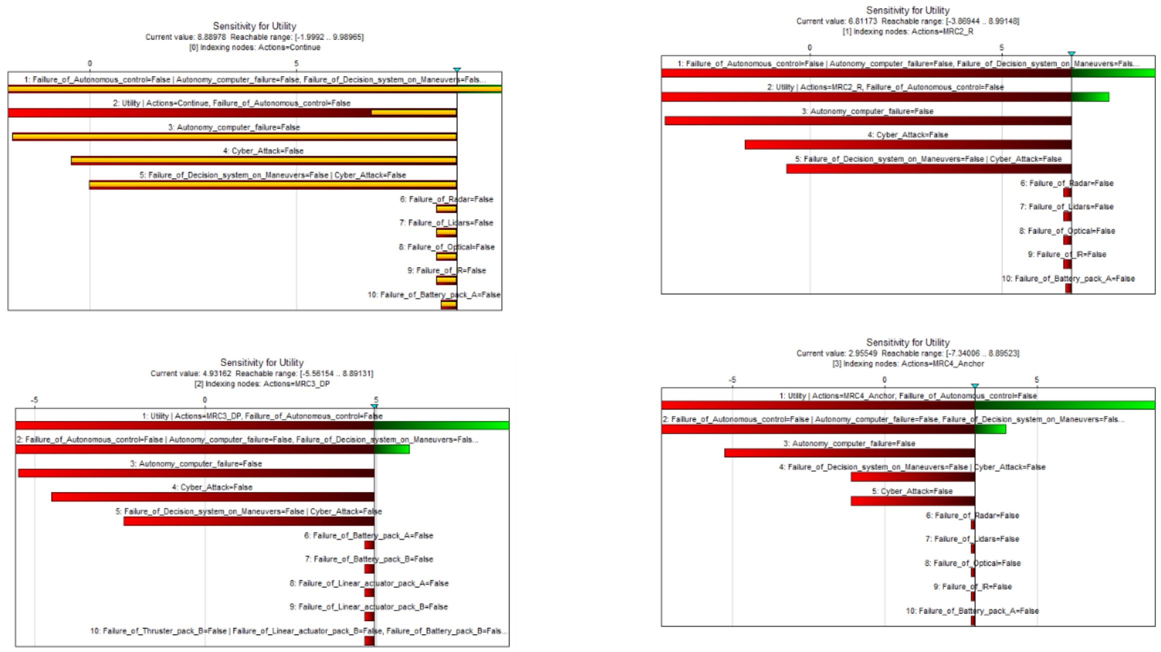


Figure 3.4: First sensitivity Tornado of Model 2 with the input nodes at the initial values. From top left is Continue, MRC 2, MRC 3 and MRC 4.

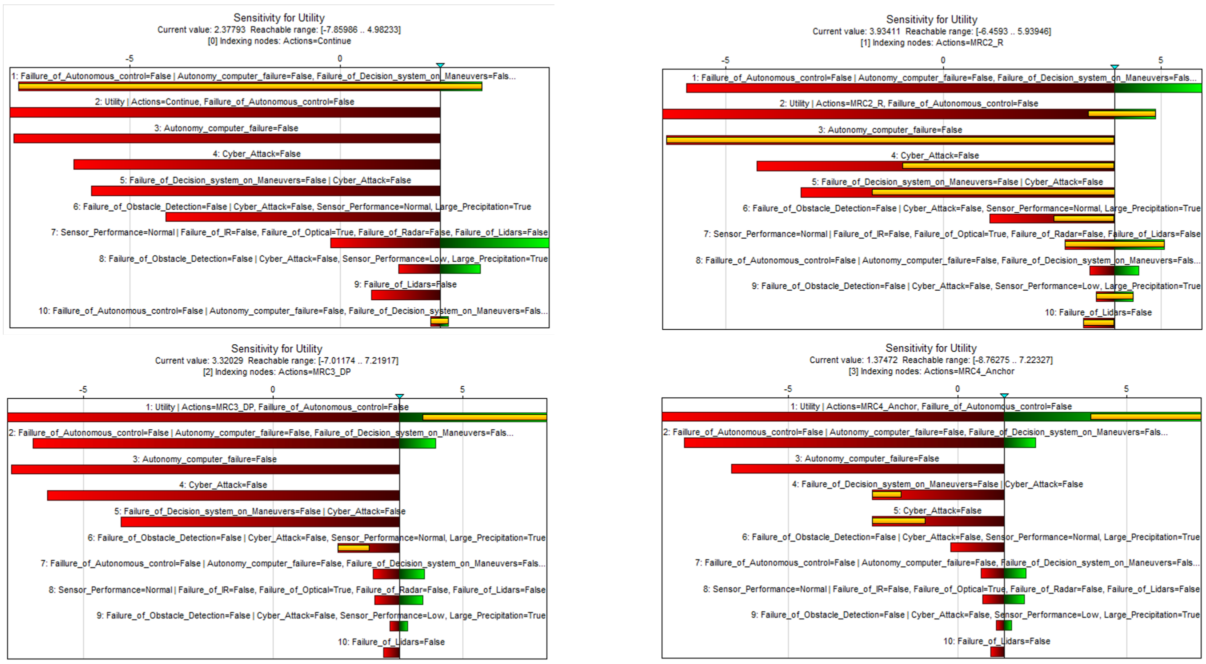


Figure 3.5: Second sensitivity Tornado of Model 2 with the state's of input nodes Failure of Optical cameras and Large Precipitation changed. From top left is Continue, MRC 2, MRC 3 and MRC 4.

change of probability that increases the utility. The sensitivity to the other nodes is large towards negative changes, but Continue is not sensitive to positive changes to most of them. MRC 2 and MRC 3 also have a significant sensitivity towards positive changes of Failure of Thruster pack A's probability, but less than Continue. MRC 2, MRC 3 and

MRC 4 are most sensitive to Utility (depending on Failure of Autonomous control is false). The sensitivity is great towards negative changes in the probability, and to varying degrees towards positive changes. MRC 4 is the most sensitive and MRC 2 is the least sensitive.

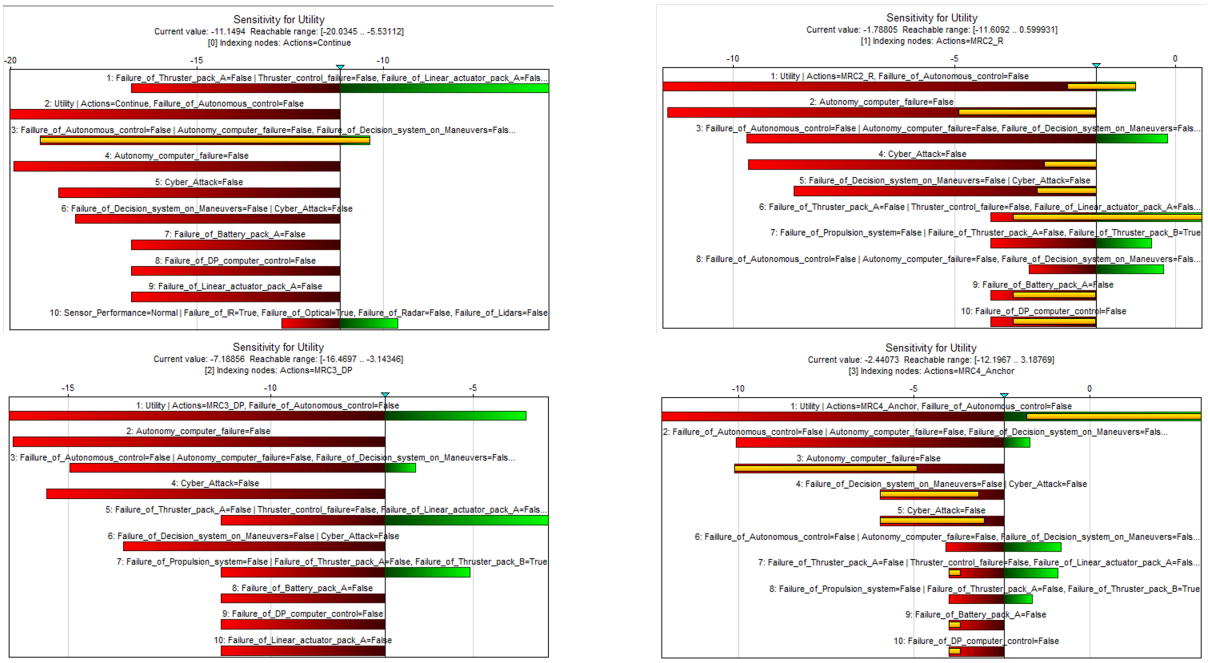


Figure 3.6: Third sensitivity Tornado of Model 2 with the state's of input nodes Failure of Optical cameras, Failure of IR cameras, Failure of Backup control computer, Failure of Linear actuator pack B and Strong Wind changed. From top left is Continue, MRC 2, MRC 3 and MRC 4.

Summary

The utility in Model 2 is most sensitive towards Failure of Autonomous control and Utility (depending Failure of Autonomous control), which is highly ranked by the four action in the analyses. From the first to the second analysis, the sensitivity towards Failure of Obstacle Detection and Sensor Performance increased when Failure of Optical cameras and Large Precipitation was set to True. In the third analysis, the sensitivity towards Failure of Thruster pack A had a sharp increase, when the nodes connected to Failure of Thruster Performance were set to True. Through the analyses, MRC 4 was the least sensitive to the changes in the model's states.

From the analyses done on the two models, the Utility's sensitivity given the actions were similar for the two models. Continue was more sensitive towards nodes related to Thruster performance in Model 2 than in Model 1, but the action was mostly sensitive towards the same factors. MRC 2 acts mostly the same, the largest difference between the two models are the additional nodes, e.g., Cyber Attack, which is not included in Model 1. MRC 3 was most sensitive towards Thruster Performance and Maneuvering Performance in the two models and MRC 4 was less sensitive to the other nodes except those related to Failure of Autonomous control and Collision.

Comparing the two models, the largest difference was that the actions in Model 2 were sensitive to more nodes even with the first analysis. However, the nodes the actions were sensitive towards are not included in Model 1, which makes it difficult to compare the two on this point.

4 Discussion

4.1 The Model

The model is made for illustrative purposes only, as it is far short of a realistic model along essentially all thinkable dimensions. Yet the model may be useful as a starting point for designing a more realistic model. It is simple and transparent, which makes it easy to understand the mechanisms and functions of the model. The model contains the key elements of a more realistic model, by including PVs which provide input data about the vessel and the surroundings, gathering nodes which summarize the input for the PVs, and utilities that ascertain the consequences for success and failure. Thus, the model illustrates how the information/input data from the PVs can be aggregated to a probability of failure or an adverse event. This is also shown from the results of the sensitivity analysis of the model. Moreover, the model illustrates how input data above a chosen threshold or critical value will trigger an action by the ORM, which will reduce the risk of failure or an adverse event.

To make a more realistic model which could be used, there are still challenges that need to be addressed. One challenge is how to design the model without human bias, which is a constant problem with BBNs, but these negative factors can be curbed with statistical analysis of the node's relevance to the decision and how the nodes influence each other. Another challenge is to make the input node more realistic by changing the nodes to chance nodes so not to limit the state, but let it have a wider specter.

Another aspect is the computation time and size of the model. A larger model can bea more realistic representation of reality, but it comes with the extra computation time.This leads to a choice between a precise decision and a faster response time. An essentialpoint is that the computation time can be significantly affected by the size of the CPTs inthe model, so a clever design which reduces computing time may allow for a more detailed and more realistic model

Furthermore, the model illustrates a crucial tradeoff which faces the designer of an ORM system, between the need to prevent accidents and the desire to avoid frequent disruptions of the normal procedure of milliAmpere 2. If critical values for the PVs are selected to minimize the risk of accidents, this may lead to frequent interference by the ORM, involving frequent disruptions of the passage of milliAmpere 2. This may be a nuisance for the passengers, which may lead them to choose alternative ways to cross the canal. On the other hand, if critical values are set loosely, to reduce the frequency of interference of the ORM, this may involve a higher risk of accidents or other adverse events.

Despite the simplicity of the model, it still contains the key elements of a more realistic model. The aim of the model it to illustrate the main elements and mechanisms of an decision-making model, as a starting point for designing a more realistic model. The model is simple and transparent, which makes it easy to understand how the model works.

Thus, the model illustrates the purpose of the various elements of the model, what type of information is needed, and how the information is used in the model.

4.2 Results

4.2.1 Finite-state machine simulation

The finite-state machine testing the models was designed very simply. It completed its purpose of testing the precision of the models and partial error checking, but, like the models, the simulation was more illustrative. A more thorough method would be to auto generate the simulation scenarios instead of making the simulation scenarios list manually. One of the challenges with generating the simulations scenarios is that the program would also have to find the outcome to compare with the prediction from the model. However, with a large number of simulation scenarios, the uncertainty would be small, Another challenge is how to generate the simulation scenarios. One approach is to set up a random generator and run a specified number of simulations scenarios, but this would lead to scenarios being repeated. If one of the repeated scenarios happened to be a failure, it would affect the calculated precision of the model. Another approach is to systematically iterate through every possible combination of inputs for the model. A systematical approach significantly reduces the possibility of repetition of simulations scenarios. However, the code could easily become a mess by trying to create a script that iterates through all the combinations without repeating simulation scenarios.

The main reason for this is grouping of the probabilities, that makes most of the simulation scenarios into error checking. However, even if the model improves past the grouping of probabilities in the gathering nodes, the simulation would still be valid. An example of this is if the model is to be trained with a machine learning method, like Bayesian Reinforcement Learning. The simulation scenarios can still be used for testing the precision of the model after the training.

4.2.2 Sensitivity analysis

In the sensitivity analysis for the utility in Model 1, when the input nodes are at the initial values, Collision dominates the other nodes with Maneuvering Performance as an obvious second, with the exception of MRC 4. The reason for this is the large discrepancy between the utility given the two states of Collision, a slight change in the distributed probability will have significant effect on the predicted utility. Maneuvering Performance has a play in this as an uncertainty has been added to the distributed probability, so even though both Vessel Integrity and Environmental Disturbance states are certain to be normal, a 100 % probability, Maneuvering Performance state has a slight chance of being low. This is also the reason why Maneuvering Performance can have a large effect on the predicted utility. SA Performance does not have this uncertainty included in the model, illustrating the difference the uncertainty has on the sensitivity analysis. Regarding MRC

4 that are unaffected by Maneuvering Performance, the cause of this can be found in the Collision's CPT where the probability is assumed to be unaffected by both the SA Performance and Maneuvering Performance because milliAmpere 2 is securely fasted with the anchor.

In the second and third analyses of Model 1, the other gathering nodes begin to affect the predicted utility, illustrating the effect of deterministic input nodes and not including uncertainty in the gathering nodes. The change in state of Light and Lidar Available in the second analysis have the largest effect on Continue and MRC 2, this also makes sense considering that milliAmpere 2 is moving and needs the SA to avoid obstacles. MRC 3 and MRC 4 stand still and will be less affected by a poor performance of the SA. The influence of the input nodes on the decision is the most obvious in the last analysis. Continue and MRC 2 are affected by both the SA Performance and the Maneuvering Performance, while MRC 3 is strongly affected by the Maneuvering Performance. MRC 4 is the least affected by outside influence, depending on Collision's distributed probability. The explanation for the differences between the actions can be found in Collision's CPT. Continue has low probability of collision when the states is Normal in SA Performance and Maneuvering Performance. However, the probability of collision increases drastically when the probability of the state being Normal decreases. The same situation applies for MRC 2, but the probability of collision is lower, explaining why the sensitivity analysis of the two actions is similar. MRC 3 is less affected by a reduction in the SA Performance, but are sensitive to Maneuvering Performance so milliAmpere 2 does not start drifting on the canal because of, for example, low Thruster Performance and high Environmental Disturbance.

Comparing the two models, Model 2 was more sensitive in the first analysis with the initial values. It was mentioned that the nodes only exist in Model 2 without any equivalent nodes in Model 1, but the sensitivity towards the sensors are also larger and more nodes are included in the sensitivity ranking. A likely reason for the increased sensitivity is that probabilities were included in the initial version of the input nodes in Model 2. The large sensitivity towards the nodes that are only included in Model 2 can be blamed for the large conditional probability of failure for the nodes influenced by them, making even a small change in probability have a large influence on Utility. In the modules the node with one of the largest sensitivity, consistently, were Failure of Autonomous control and Collision, both are the nodes connected to Utility in the model. This confirms the point mentioned earlier, that the sensitivity is because the large negative cost for accident and the small benefit for no accident makes small changes in the probability have large changes in the utility. The sensitivity towards positive changes increasing from Continue, where it is close to zero, to MRC 4, where it is only slightly lower than the negative influence.

5 Conclusions

This thesis aims to provide the basic framework for implementing an ORM on the vessel, milliAmpere 2, so that the vessel will do its risk analysis and management, and thus be able to operate almost entirely independently of human interference. The theory behind the design of the ORM is built upon the framework proposed by [1], using an online risk model built as a BBN as part of the ORM. The framework provided in this thesis includes a decision-making model that decides whenand how the ORM acts.

This thesis builds on a project thesis, which provided the initial framework for the ORM and the theory for the decision-making model. The master thesis provides a complete framework for the ORM, and the method to design the decision-making model has been improved. One model is designed and presented in the thesis. In addition, a risk model designed for milliAmpere 2 in [2] has been converted into a decision-making model for comparison. The framework of the ORM includes running the model in a python script which also has been created. To test the models, a finite-state machine simulation was created andimplemented manually, including a test with the python script that can run the model.

The model presented in the thesis is deliberately kept simple to ensure transparency. Input and probability distributions are chosen to obtain plausible actions and outcomes without basis in expert knowledge or empirical evidence. The simplicity of the model is also a key limitation. To obtain a more realistic model which can function as an ORM to make milliAmpere 2 operate almost entirely independently of human interference, model extensions, expert knowledge, and empirical foundation would be necessary. This is discussed further below, under future work.

When designing the model, it is important to be aware of the tradeoffs that exist. To accept higher risk during the operation will reduce the chance of unwanted interruptions, but this will also involve additional risk for collisions, human injuries, or other adverse events. Another aspect is the computation time and size of the model. A larger model can be a more realistic representation of reality but comes with extra computation time. This leads to a choice between a precise decision and a faster response time. An essential point is that the computation time can be significantly affected by the size of the CPTs in the model, so a clever design that reduces computing time may allow for a more detailed and realistic model.

Looking at the results show that there are clear signs that the designed models work. The finite-state machine simulation shows that the decision-making model can predict the correct outcome accurately. The sensitivity analyses also help to confirm the potential of the decision-making model, and the analyses align with the operational criteria that were used to design the model. The conditional probabilities and the utilities illustrate that the actions are sensitive to the same situations planned in the initial design.

However, many aspects are still lacking to make a realistic model. As mentioned, the model's simplicity is also one of the weaknesses. That is not to say that a good decision-making model cannot be simple, but that some aspects need to be changed. One of these aspects is the number of states in the model. It limits the flexibility and led to Traffic density being removed from the model tested with the finite-state machine. This is also connected to the operational criteria that are too crude to encompass traffic's effect on the risk.

Another aspect is the design of the model. Comparing Model 1 and model 2 shows that there is room for improvements regarding how the nodes are connected. An example ofthis is how the battery points towards the thruster, which is a more realistic representationof the actual design of milliAmpere 2. Model 2 has also included more variables that canlead to high-risk situations such as Cyber Attack. When milliAmpere 2 is connected to aremote operator instead of an onboard operator, the online connection allows hackers to hijack the vessel which is a significant safety concern.

5.1 Future work

The next step from this point is to improve the model, making it more realistic. Multiple aspects need to be improved to realize this. The first point is to improve the input nodes by converting them to chance nodes or increasing the number of states in the deterministic nodes. This development will help the model to be able to reflect the gradual changes that exist in reality and take full advantage of the BBN design. Adapting to gradual changes in the input nodes makes it possible to include, for example, Traffic Density again as the traffic flow greatly affects the probability of collision.

The second point is to improve and expand the structure of the model. The nodes and arcs must represent the causality of reality, at least the more significant aspects, to give accurate predictions. The probability distribution for the PVs, and the assumed effect of the PVs on the risks for the vessel, should be based on expert knowledge and empirical evidence. It is also important that the assumptions concerning the effect of the possible actions taken by milliAmpere 2 are based on expert knowledge and empirical evidence. Finally, assumptions concerning the utility associated with possible outcomes should be based on a thorough assessment and evaluation.

References

[1] Ingrid Bouwer Utne, Børge Roksetha, Asgeir J. Sørensena, and Jan Erik Vinnemb. Towards supervisory risk control of autonomous ships. *Elsevier Ltd.*, 1:15, November 2019.

[2] Chuanqi Guo, Stein Haugen, and Ingrid B Utne. Grisk assessment of collisions of an autonomous passenger ferry. *Autonomous Systems Safety, Reliability, and Security*, 37:134–145, November 2021.

[3] M. Laurinen. Remote and autonomous ships: the next steps. 2016.

[4] Ø.J. Rødseth. Definition of autonomy levels for merchant ships. 2017.

[5] AGCS. Safety and shipping review 2017. 2017.

[6] M. Groover. Fundamentals of modern manufacturing: Materials, processes, and systems. 2012.

[7] SAE. Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems. 2018.

[8] Siegfried Eisinger. The rise of autonomous control systems. https://www.dsta.gov.sg/docs/default-source/dsta-about/performance-challenges-for-high-resolution-imaging-sensors-for-surveillance-in-tropical-environment.pdf?sfvrsn=2. accessed: 2022-05-01.

[9] Luciano Lanz. Is having a risk management can eliminate all risks ?, 01 2019.

[10] Ørnulf Jan Rødseth and Håvard Nordahl. Definitions for autonomous merchant ships. 2017.

[11] Ø. Smogeli. Tmr06 autonomous marine systems module 2: Risk aspects, September 2021.

[12] H.Stray. Conops for autonomous passenger ferry in trondheim. -, 1:19, December 2020.

[13] X. S. Yang. *Introduction to Algorithms for Data Mining and Machine Learning*. Academic Press, 2019.

[14] S. Lieu, J. McGree, Z. Ge, and X. Yang. *Computational and Statistical Methods for Analysing Big Data with Applications*. Academic Press, 2016.

[15] Bayesfusion. Genie models. https://support.bayesfusion.com/docs/GeNIe.pdf, publisher = https://www.support.bayesfusion.com/, note = Accessed: 2022-04-20.

[16] Bayesfusion. Smile wrappers prgrammers manual. https://support.bayesfusion.com/docs/Wrappers.pdf, October 2021. Accessed: 2021-10-12.

[17] Eivind Brekke Holden. Online risk management for milliampere 2. December 2021.

[18] Serena H. Hamilton and Carmel A Pollino. Good practice in bayesian network modelling. *Environmental Modelling Software*, 37:134–145, November 2012.

[19] A. Filgueira, H. González-Jorgea, S. Lagüel, L. Díaz-Vilariño, and P. Ariasa. Quantifying the influence of rain in lidar performance. *IEEE Transactions on Intelligent Transportation Systems*, 95:143–148, January 2017.

[20] LEE Cheow Gim, EE Kok Tiong, and HENG Yinghui Elizabeth. Performance challenges for high resolution imaging sensors for surveillance in tropical environ. accessed: 2022-06-01.

[21] Felix Nobis, Maximilian Geisslinger, Markus Weber, Johannes Betz, and Markus Lienkamp. A deep learning-based radar and camera sensor fusion architecture for object detection. *CoRR*, abs/2005.07431, 2020.

[22] Dietmer Deter. Propulsion and thrusters. https://dynamic-positioning.com/proceedings/dp1997/prop_deter.pdf, 1997. Accessed: 2022-5-10.

[23] Priya Pedamkar. artificial intelligence vs human intelligence. https://www.educba.com/artificial-intelligence-vs-human-intelligence/, 2021. Accessed: 2021-12-05.

[24] Wikipedia. Artificial intelligence. https://en.wikipedia.org/wiki/Artificial_intelligence, 2021. Accessed: 2021-12-05.

[25] Bayesfusion. Bayesian network. https://www.bayesfusion.com/bayesian-networks/, 2021. Accessed: 2021-09-25.

[26] Jidapa Kraisangka and Marek J.Druzdzel. A bayesian network interpretation of the cox's proportional hazard model. *International Journal of Approximate Reasoning*, 103:195–211, December 2018.

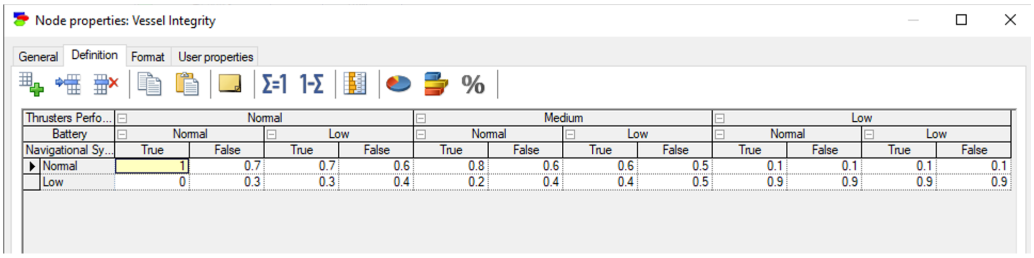
[27] Bayesfusion. Sensitivity analysis in bayesian networks (and influence diagrams). https://support.bayesfusion.com/docs/GeNIe/bn_sensitivitybn.html. Accessed: 2022-05-25.

[28] N. Leveson. *Safety and Security Are Two Sides of the Same Coin.* SpringerLink, 2020.

[29] Bayesfusion. Influence diagram. https://www.bayesfusion.com/influence-diagrams/, July 2018. Accessed: 2021-09-30.

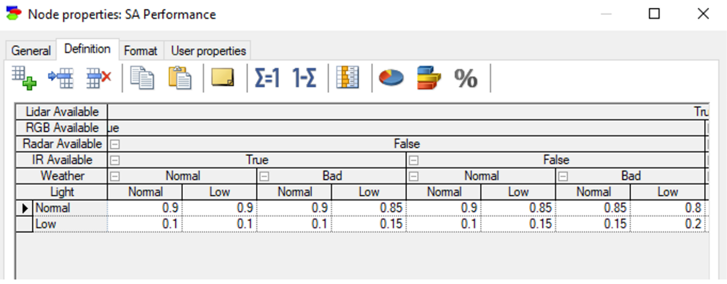
A CPTs for the Models

1.1 Model 1



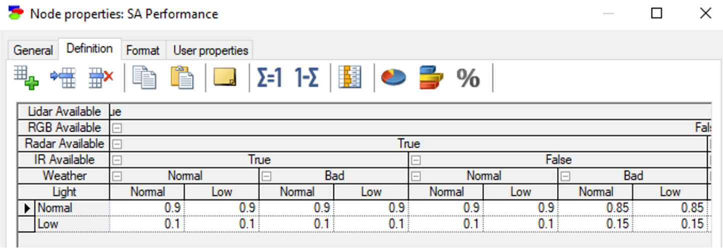
Thrusters Perfo...	Normal				Medium				Low			
Battery	Normal		Low		Normal		Low		Normal		Low	
Navigational Sy...	True	False	True	False	True	False	True	False	True	False	True	False
Normal	1	0.7	0.7	0.6	0.8	0.6	0.6	0.5	0.1	0.1	0.1	0.1
Low	0	0.3	0.3	0.4	0.2	0.4	0.4	0.5	0.9	0.9	0.9	0.9

Figure A.1: CPT of Vessel Integrity from Model 1



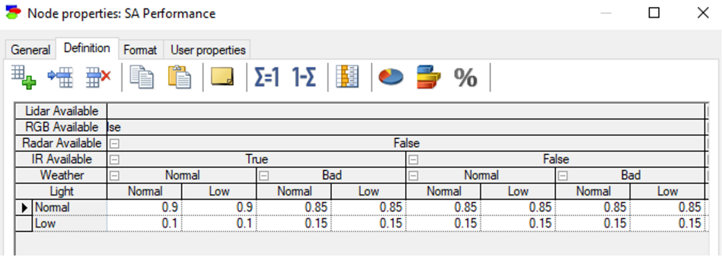
Lidar Available	Tru							
RGB Available	ue							
Radar Available	False							
IR Available	True				False			
Weather	Normal		Bad		Normal		Bad	
Light	Normal	Low	Normal	Low	Normal	Low	Normal	Low
Normal	0.9	0.9	0.9	0.85	0.9	0.85	0.85	0.8
Low	0.1	0.1	0.1	0.15	0.1	0.15	0.15	0.2

Figure A.2: CPT of SA Performance part 2 from Model 1. Lidar Available and RGB Available are True



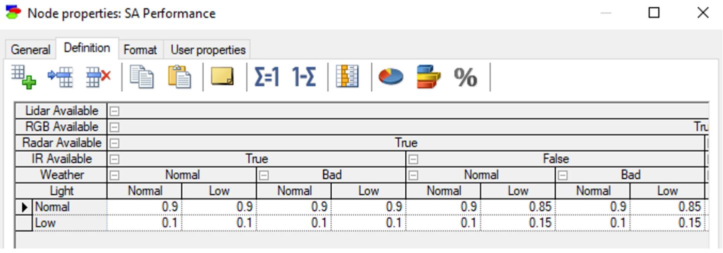
Lidar Available	ue							
RGB Available	Fal							
Radar Available	True							
IR Available	True				False			
Weather	Normal		Bad		Normal		Bad	
Light	Normal	Low	Normal	Low	Normal	Low	Normal	Low
Normal	0.9	0.9	0.9	0.9	0.9	0.9	0.85	0.85
Low	0.1	0.1	0.1	0.1	0.1	0.1	0.15	0.15

Figure A.3: CPT of SA Performance part 3 from Model 1. Lidar Available is true and RGB Available is False



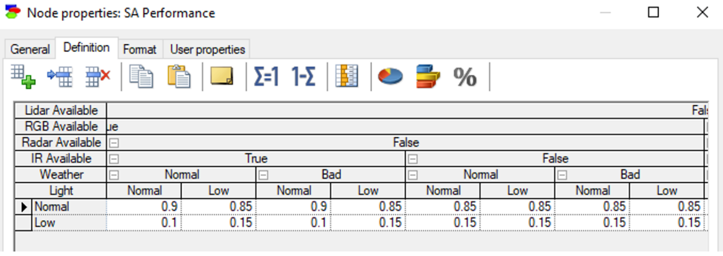
Lidar Available								
RGB Available	lse							
Radar Available	False							
IR Available	True				False			
Weather	Normal		Bad		Normal		Bad	
Light	Normal	Low	Normal	Low	Normal	Low	Normal	Low
Normal	0.9	0.9	0.85	0.85	0.85	0.85	0.85	0.85
Low	0.1	0.1	0.15	0.15	0.15	0.15	0.15	0.15

Figure A.4: CPT of SA Performance part 4 from Model 1. Lidar Available and RGB Available are True



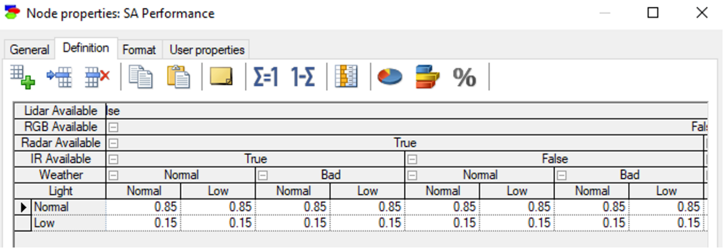
Lidar Available								
RGB Available								Tru
Radar Available	True							
IR Available	True				False			
Weather	Normal		Bad		Normal		Bad	
Light	Normal	Low	Normal	Low	Normal	Low	Normal	Low
Normal	0.9	0.9	0.9	0.9	0.9	0.85	0.9	0.85
Low	0.1	0.1	0.1	0.1	0.1	0.15	0.1	0.15

Figure A.5: CPT of SA Performance part 5 from Model 1. Lidar Available is false and RGB Available is True



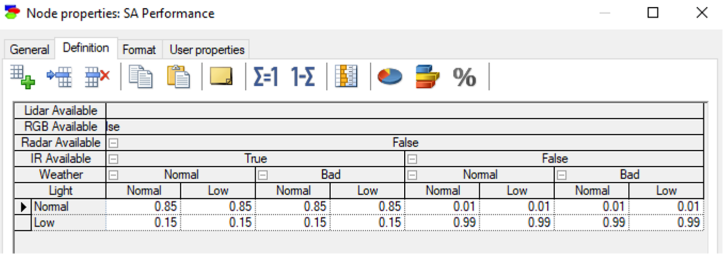
Lidar Available								Fal
RGB Available	ue							
Radar Available	False							
IR Available	True				False			
Weather	Normal		Bad		Normal		Bad	
Light	Normal	Low	Normal	Low	Normal	Low	Normal	Low
Normal	0.9	0.85	0.9	0.85	0.85	0.85	0.85	0.85
Low	0.1	0.15	0.1	0.15	0.15	0.15	0.15	0.15

Figure A.6: CPT of SA Performance part 6 form Model 1. Lidar Available is false and RGB Available is True



Lidar Available	lse							
RGB Available								Fal
Radar Available	True							
IR Available	True				False			
Weather	Normal		Bad		Normal		Bad	
Light	Normal	Low	Normal	Low	Normal	Low	Normal	Low
Normal	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85
Low	0.15	0.15	0.15	0.15	0.15	0.15	0.15	0.15

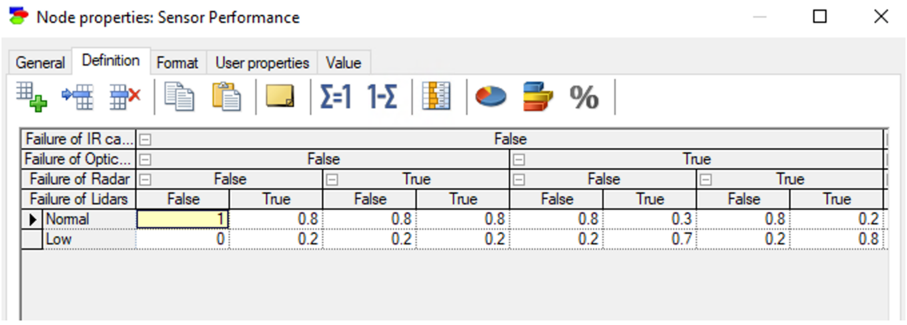
Figure A.7: CPT of SA Performance part 7 form Model 1. Lidar Available and RGB Available are False



Lidar Available								
RGB Available	lse							
Radar Available	False							
IR Available	True				False			
Weather	Normal		Bad		Normal		Bad	
Light	Normal	Low	Normal	Low	Normal	Low	Normal	Low
Normal	0.85	0.85	0.85	0.85	0.01	0.01	0.01	0.01
Low	0.15	0.15	0.15	0.15	0.99	0.99	0.99	0.99

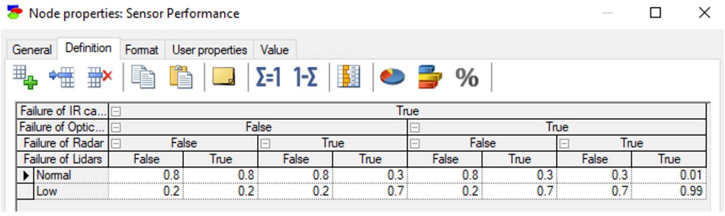
Figure A.8: CPT of SA Performance part 8 from Model 1. Lidar Available and RGB Available are False

1.2 Model 2



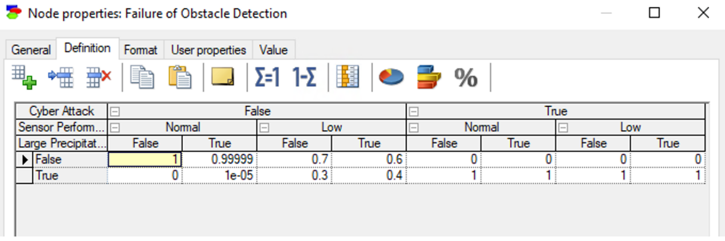
Failure of IR ca...	False							
Failure of Optic...	False				True			
Failure of Radar	False		True		False		True	
Failure of Lidars	False	True	False	True	False	True	False	True
Normal	1	0.8	0.8	0.8	0.8	0.3	0.8	0.2
Low	0	0.2	0.2	0.2	0.2	0.7	0.2	0.8

Figure A.9: CPT of Sensor Performance part 1 from Model 2.



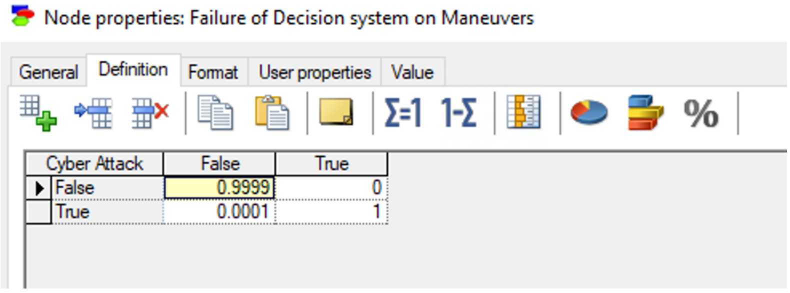
Failure of IR ca...	True							
Failure of Optic...	False				True			
Failure of Radar	False		True		False		True	
Failure of Lidars	False	True	False	True	False	True	False	True
Normal	0.8	0.8	0.8	0.3	0.8	0.3	0.3	0.01
Low	0.2	0.2	0.2	0.7	0.2	0.7	0.7	0.99

Figure A.10: CPT of Sensor Performance part 2 from Model 2.



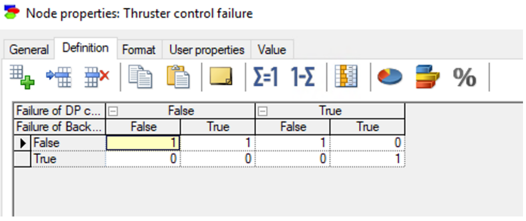
Cyber Attack	False				True			
Sensor Perform...	Normal		Low		Normal		Low	
Large Precipitat...	False	True	False	True	False	True	False	True
False	1	0.99999	0.7	0.6	0	0	0	0
True	0	1e-05	0.3	0.4	1	1	1	1

Figure A.11: CPT of Failure of Obstacle Detection.



Cyber Attack	False	True
False	0.9999	0
True	0.0001	1

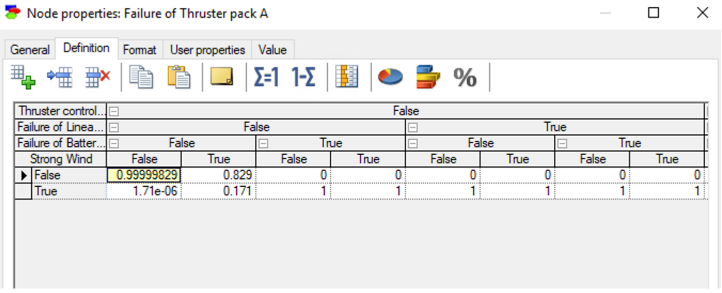
Figure A.12: CPT of Failure of Decision system on Maneuvers.



Node properties: Thruster control failure

Failure of DP c...	False		True	
Failure of Back...	False	True	False	True
False	1	1	1	0
True	0	0	0	1

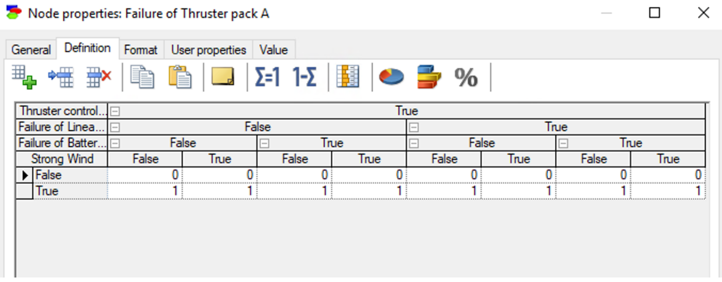
Figure A.13: CPT of Thruster control Failure.



Node properties: Failure of Thruster pack A

Thruster control...	False							
Failure of Linea...	False				True			
Failure of Batter...	False		True		False		True	
Strong Wind	False	True	False	True	False	True	False	True
False	0.99999829	0.829	0	0	0	0	0	0
True	1.71e-06	0.171	1	1	1	1	1	1

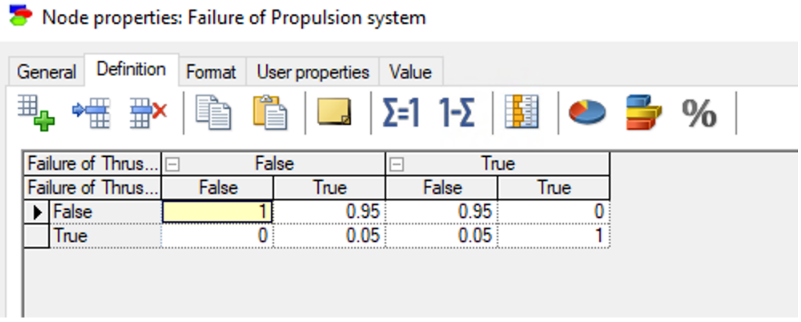
Figure A.14: CPT of Filure of Thruster pack A.



Node properties: Failure of Thruster pack A

Thruster control...	True							
Failure of Linea...	False				True			
Failure of Batter...	False		True		False		True	
Strong Wind	False	True	False	True	False	True	False	True
False	0	0	0	0	0	0	0	0
True	1	1	1	1	1	1	1	1

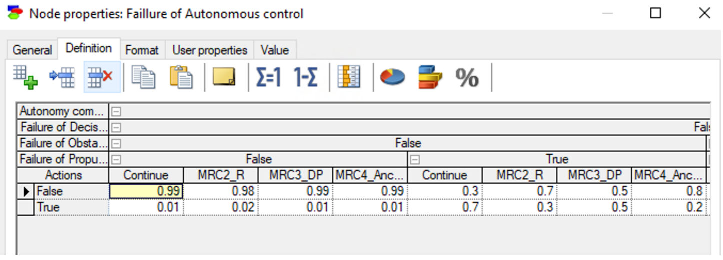
Figure A.15: CPT of Filure of Thruster pack A.



Node properties: Failure of Propulsion system

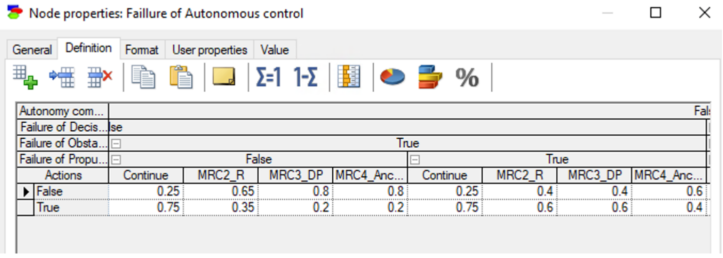
Failure of Thrus...	False		True	
Failure of Thrus...	False	True	False	True
False	1	0.95	0.95	0
True	0	0.05	0.05	1

Figure A.16: CPT of Filure of Propulsion system pack A.



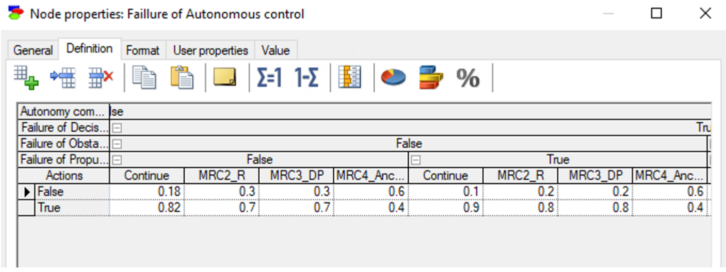
Autonomy com...	⊟							
Failure of Decis...	⊟ Fal							
Failure of Obsta...	⊟ False							
Failure of Propu...	⊟ False				⊟ True			
Actions	Continue	MRC2_R	MRC3_DP	MRC4_Anc...	Continue	MRC2_R	MRC3_DP	MRC4_Anc...
▶ False	0.99	0.98	0.99	0.99	0.3	0.7	0.5	0.8
True	0.01	0.02	0.01	0.01	0.7	0.3	0.5	0.2

Figure A.17: CPT of Filure of Autonomous control part 1. Autonomy computer Failure is False and Failure of Decision system on Maneuvers is False



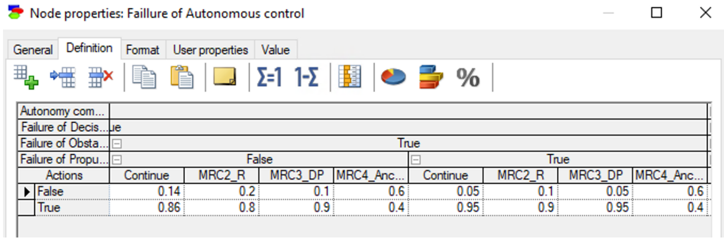
Autonomy com...	Fal							
Failure of Decis...	lse							
Failure of Obsta...	⊟ True							
Failure of Propu...	⊟ False				⊟ True			
Actions	Continue	MRC2_R	MRC3_DP	MRC4_Anc...	Continue	MRC2_R	MRC3_DP	MRC4_Anc...
▶ False	0.25	0.65	0.8	0.8	0.25	0.4	0.4	0.6
True	0.75	0.35	0.2	0.2	0.75	0.6	0.6	0.4

Figure A.18: CPT of Filure of Autonomous control part 1. Autonomy computer Failure is False and Failure of Decision system on Maneuvers is False



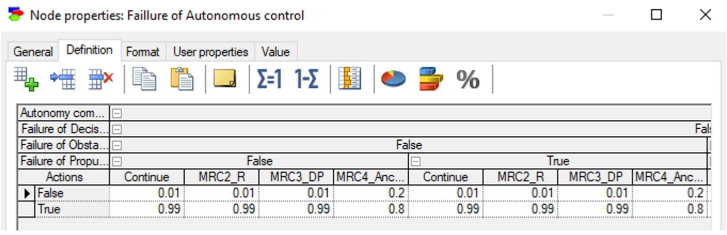
Autonomy com...	lse							
Failure of Decis...	⊟ Tru							
Failure of Obsta...	⊟ False							
Failure of Propu...	⊟ False				⊟ True			
Actions	Continue	MRC2_R	MRC3_DP	MRC4_Anc...	Continue	MRC2_R	MRC3_DP	MRC4_Anc...
▶ False	0.18	0.3	0.3	0.6	0.1	0.2	0.2	0.6
True	0.82	0.7	0.7	0.4	0.9	0.8	0.8	0.4

Figure A.19: CPT of Filure of Autonomous control part 1. Autonomy computer Failure is False and Failure of Decision system on Maneuvers is True



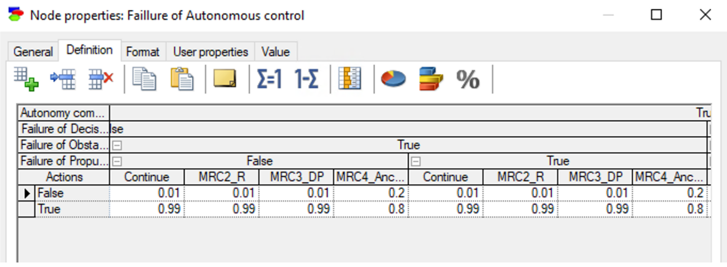
Autonomy com...								
Failure of Decis...	ue							
Failure of Obsta...	⊟ True							
Failure of Propu...	⊟ False				⊟ True			
Actions	Continue	MRC2_R	MRC3_DP	MRC4_Anc...	Continue	MRC2_R	MRC3_DP	MRC4_Anc...
▶ False	0.14	0.2	0.1	0.6	0.05	0.1	0.05	0.6
True	0.86	0.8	0.9	0.4	0.95	0.9	0.95	0.4

Figure A.20: CPT of Filure of Autonomous control part 1. Autonomy computer Failure is False and Failure of Decision system on Maneuvers is True



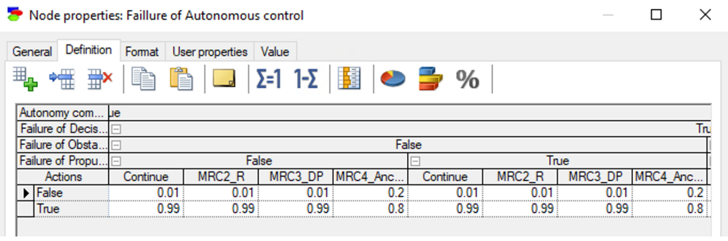
Autonomy com...	⊟							
Failure of Decis...	⊟							Fal
Failure of Obsta...	⊟ False							
Failure of Propu...	⊟ False				⊟ True			
Actions	Continue	MRC2_R	MRC3_DP	MRC4_Anc...	Continue	MRC2_R	MRC3_DP	MRC4_Anc...
False	0.01	0.01	0.01	0.2	0.01	0.01	0.01	0.2
True	0.99	0.99	0.99	0.8	0.99	0.99	0.99	0.8

Figure A.21: CPT of Filure of Autonomous control part 1. Autonomy computer Failure is True and Failure of Decision system on Maneuvers is False



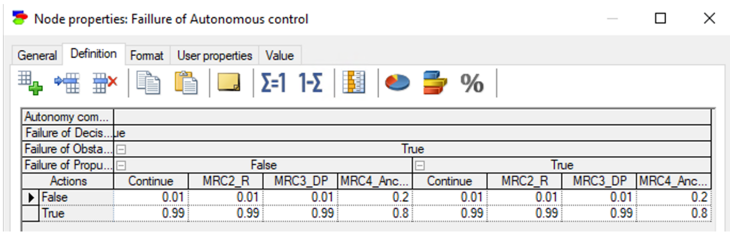
Autonomy com...								Tru
Failure of Decis...	lse							
Failure of Obsta...	⊟ True							
Failure of Propu...	⊟ False				⊟ True			
Actions	Continue	MRC2_R	MRC3_DP	MRC4_Anc...	Continue	MRC2_R	MRC3_DP	MRC4_Anc...
False	0.01	0.01	0.01	0.2	0.01	0.01	0.01	0.2
True	0.99	0.99	0.99	0.8	0.99	0.99	0.99	0.8

Figure A.22: CPT of Filure of Autonomous control part 1. Autonomy computer Failure is True and Failure of Decision system on Maneuvers is False



Autonomy com...	ue							
Failure of Decis...	⊟							Tru
Failure of Obsta...	⊟ False							
Failure of Propu...	⊟ False				⊟ True			
Actions	Continue	MRC2_R	MRC3_DP	MRC4_Anc...	Continue	MRC2_R	MRC3_DP	MRC4_Anc...
False	0.01	0.01	0.01	0.2	0.01	0.01	0.01	0.2
True	0.99	0.99	0.99	0.8	0.99	0.99	0.99	0.8

Figure A.23: CPT of Filure of Autonomous control part 1. Autonomy computer Failure is True and Failure of Decision system on Maneuvers is True



Autonomy com...								
Failure of Decis...	ue							
Failure of Obsta...	⊟ True							
Failure of Propu...	⊟ False				⊟ True			
Actions	Continue	MRC2_R	MRC3_DP	MRC4_Anc...	Continue	MRC2_R	MRC3_DP	MRC4_Anc...
False	0.01	0.01	0.01	0.2	0.01	0.01	0.01	0.2
True	0.99	0.99	0.99	0.8	0.99	0.99	0.99	0.8

Figure A.24: CPT of Filure of Autonomous control part 1. Autonomy computer Failure is True and Failure of Decision system on Maneuvers is True

NTNU

Norwegian University of
Science and Technology