

Remi Brensdal Pedersen

# Risk assessment using Hybrid Causal Logic (HCL) modelling

Assessing the collision risk of an unmanned autonomous vessel

Master's thesis in Marine Technology

Supervisor: Ingrid Bouwer Utne

June 2021



Remi Brensdal Pedersen

# **Risk assessment using Hybrid Causal Logic (HCL) modelling**

Assessing the collision risk of an unmanned autonomous vessel

Master's thesis in Marine Technology  
Supervisor: Ingrid Bouwer Utne  
June 2021

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



MASTER THESIS

---

**Risk assessment using Hybrid  
Causal Logic (HCL) modelling -  
Assessing the collision risk of an  
unmanned vessel**

---

Remi Brensdal Pedersen

June 2021

TMR4930

Marine Technology, Master Thesis

DEPARTMENT OF MARINE TECHNOLOGY  
FACULTY OF ENGINEERING





---

## Abstract

Autonomous ships (AS) are currently being developed for use in public waters. One of the requirements for AS is that they should be at least as safe as conventional ships. To obtain this, efficient interaction and communication between software, hardware and humans are critical.

This thesis aims to assess the collision risk of an unmanned autonomous vessel as well as investigate the interaction between the human operators onshore and the ship. The analysis is based on a Hybrid Causal Logic model(HCL), combining event sequence diagrams(ESD) with fault trees and Bayesian Belief Networks(BBN). This allows for analyzing several aspects of the system as a whole instead of only one.

The ESD describes the scenario and models the events that can happen after the initiating event, which was set to be a vessel on a collision course. This includes head-on-, overtaking- and crossing collision. A novel method called Concurrent Task Analysis (CoTA) which describes the different tasks the agent has to perform in order for the events to succeed, has been used to identify the intermediate tasks in the fault trees. The fault trees are further developed based on the IDA model. This divides the failure modes into failures in either information collection, decision making, and action-taking. The fault trees illustrate failure events for both the autonomous system and the human operators. However, in order to further investigate the human failure events, BBN was used. A literature review on Human Reliability Analysis(HRA) and relevant BBN models was conducted to construct the BBN. The BBN's follows the same structure as the fault trees in the sense that one BBN was made for each of the I-D-A phases.

The subject of the risk analysis is a simplified model of a real coastal cargo ship delivering fish food along the coast of Norway. The route was set to be from Brønnøysund to Kristiansund. Quantification of the initiating event in the ESD is based on vessel frequencies and AIS data. Basic events in the fault trees are quantified using data from the literature, critical failure rates from the OREDA handbook, and IMO event frequencies. Data for the input nodes in the BBN's are based on a study that assesses the human-autonomy collaboration for AUVs.

The results from this thesis indicate that the collision probability is higher than comparable studies. However, the compared studies involves other vessel types and a different operational context. Regarding the interaction between the autonomous ship and the human operators, the results showed that the autonomous ship is very reliable. When it comes to the human operators, the results obtained showed a high probability of failure. This is most likely due to a high degree of uncertainty in the values used for quantification, and shows that more research has to be done on the are of human reliability analysis.

---



---

## Sammendrag

Autonome skip utvikles for tiden for bruk i offentlige farvann. Et av kravene til autonome skip er at de skal være minst like sikre som konvensjonelle skip. For å oppnå dette er effektiv samhandling og kommunikasjon mellom programvare, maskinvare og mennesker avgjørende.

Denne oppgaven tar sikte på å vurdere kollisjonsrisikoen til et ubemannet autonomt fartøy, samt undersøke samspillet mellom de menneskelige operatørene på land og skipet. Analysen er basert på Hybrid Causal Logic-modellen (HCL), som kombinerer hendelsessekvensdiagrammer (ESD) med feiltrær og Bayesian Belief Networks (BBN). Dette gjør det mulig å analysere flere aspekter av systemet som en helhet i stedet for bare en.

ESD beskriver scenariet og modellerer hendelsene som kan skje etter den innledende hendelsen, som ble satt til å være et fartøy på kollisjonskurs. Dette inkluderer front-, forbikjøring- og kryssingskollisjon. En ny metode kalt Concurrent Task Analysis (CoTA) som beskriver de forskjellige oppgavene agenten må utføre for at hendelsene skal lykkes, har blitt brukt til å identifisere mellomoppgavene i feiltrærne. Feiltrærne er videreutviklet basert på IDA-modellen. Denne deler sviktmodusene i feil i enten informasjonsinnsamling, beslutningstaking og handling. Feiltrærne illustrerer feilhendelser for både det autonome systemet og de menneskelige operatørene. For å undersøke menneskelige svikthendelser ble BBN imidlertid brukt. En litteraturgjennomgang om menneskelig pålitelighetsanalyse (HRA) og relevante BBN-modeller ble gjennomført for å konstruere BBN modellen. BBN-ene følger den samme strukturen som feiltrærne i den forstand at en BBN ble laget for hver av I-D-A-fasene.

Emnet for risikoanalysen er en forenklet modell av et ekte kystlasteskip som leverer fiskemat langs kysten av Norge. Ruten er satt til gå fra Brønnøysund til Kristiansund. Kvantifisering av den innledende hendelsen i ESD er basert på fartøyfrekvenser og AIS-data. Grunnleggende hendelser i feiltrærne blir kvantifisert ved hjelp av data fra litteraturen, kritiske feilfrekvenser fra OREDA-håndboken og IMO-hendelsesfrekvenser. Data for inngangsnodene i BBN-ene er basert på en studie som vurderer samarbeidet mellom menneskelig og autonomi for AUV-er.

Resultatene fra denne oppgaven indikerer at sannsynligheten for kollisjon er høyere enn sammenlignbare studier. De sammenlignede studiene involverer imidlertid andre fartøystyper og en annen operativ kontekst. Når det gjelder samspillet mellom det autonome skipet og de menneskelige operatørene, viste resultatene at det autonome skipet er veldig pålitelig. Når det gjelder de menneskelige operatørene, ga resultatene høy sannsynlighet for svikt. Dette er mest sannsynlig på grunn av høy grad av usikkerhet i verdiene som ble brukt kvantifisering, og viser at det må gjøres mer forskning innefor menneskelig pålitelighetsanalyse.

---

---

## Preface

This Master Thesis is written as the final delivery at the MSc program in Marine Technology at NTNU and symbolizes the end of a six-year-long journey. The thesis is written within the field of safety and asset management, and it counts as 30 credits. Approval of the Master Thesis results in achieving the title Master of Science in Marine Technology. The thesis presents the results of a study on collision risk and the human-system interaction of an autonomous ship.

It has been an interesting and true learning experience to work with this thesis. However, it has also been very frustrating at times, with several setbacks and unexpected problems. Especially the software Trilith, which has been used in the thesis, has proven to be frustrating at times.

The report builds on the insight gained from the Project Thesis written during the Fall of 2020. Some chapters build on the Project Thesis, especially the part about theory, but they have been expanded and edited in this Master Thesis.

---

---

## Acknowledgment

I would like to express my gratitude to my supervisor Ingrid Bouwer Utne for her guidance and support throughout this process. I would also like to thank Postdoc Christoph Alexander Thieme and Phd student Renan Guedes Maidana for always taking the time to answer my questions.

Trondheim, June, 2021

---

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Background and motivation . . . . .	1
1.2	Objectives . . . . .	2
1.3	Scope and limitations . . . . .	2
1.4	Thesis structure . . . . .	2
<b>2</b>	<b>Risk assessment</b>	<b>5</b>
2.1	Definitions . . . . .	5
2.1.1	Defining risk for autonomous marine systems and operations	6
2.2	Formal Safety Assessment (FSA) . . . . .	6
2.3	HAZID . . . . .	7
2.4	Event Sequence Diagram . . . . .	7
2.5	Fault tree analysis . . . . .	8
2.6	BBN . . . . .	9
2.7	Hybrid Causal Logic (HCL) . . . . .	10
2.8	Level of autonomy and shore control center . . . . .	10
2.8.1	COLREG - Rules on collision avoidance . . . . .	11
2.9	Risk modeling of maritime autonomous surface vessels (MASS) . . . . .	12
<b>3</b>	<b>Human factors</b>	<b>13</b>
3.1	Task Analysis and Concurrent Task Analysis . . . . .	13
3.2	Information-decision-action (IDA) model . . . . .	14
3.3	Human Reliability Analysis and BBN models related to human operators . . . . .	15
3.3.1	Performance Influencing Factors . . . . .	15
3.3.2	Phoenix HRA . . . . .	15

3.3.3	Factors affecting affecting autonomous ships operators performance . . . . .	17
3.3.4	A risk model for autonomous marine systems and operations focusing on human-autonomy collaboration . . . . .	19
<b>4</b>	<b>Method</b>	<b>21</b>
4.1	Modelling event sequence diagram . . . . .	21
4.1.1	ESD flowchart . . . . .	21
4.2	Concurrent task analysis . . . . .	23
4.2.1	Developing a CoTA from an ESD . . . . .	23
4.3	Modelling fault trees . . . . .	26
4.3.1	Generic fault trees . . . . .	26
4.3.2	Generic fault trees for autonomous ships . . . . .	27
4.3.3	Generic fault trees for human operators . . . . .	32
4.4	BBN model development . . . . .	37
4.4.1	GeNie software . . . . .	37
4.5	HCL modelling . . . . .	38
4.6	Quantitative Analysis process . . . . .	40
4.6.1	Trilith: Integrated Risk Information System . . . . .	40
4.6.2	BBN model quantification . . . . .	40
<b>5</b>	<b>System description and hazard identification</b>	<b>45</b>
5.1	Details about the unmanned autonomous ship . . . . .	45
5.2	Control system . . . . .	45
5.2.1	Machinery system . . . . .	47
5.3	External hazards . . . . .	49
5.4	Internal hazards . . . . .	49
5.4.1	System description . . . . .	49
5.4.2	Communication, monitoring and control . . . . .	49
5.4.3	Machinery system . . . . .	51
<b>6</b>	<b>HCL development</b>	<b>53</b>
6.1	Assumptions . . . . .	53
6.2	Scenario development . . . . .	54
6.3	ESD construction . . . . .	54
6.4	Fault tree construction . . . . .	58
6.4.1	Fault trees for the autonomous vessel . . . . .	59
6.4.2	Fault trees for human operators . . . . .	67
6.5	BBN construction . . . . .	72
<b>7</b>	<b>Quantitative assessment</b>	<b>75</b>
7.1	Voyage route and travel time . . . . .	75
7.2	BBN evaluation . . . . .	76
7.3	fault tree evaluation . . . . .	78
7.3.1	Top event probabilities . . . . .	79
7.4	Event sequence diagram evaluation . . . . .	81



7.4.1	Object on collision course . . . . .	81
7.4.2	Collision candidate follows the rules . . . . .	83
7.4.3	HCL final results . . . . .	85
<b>8</b>	<b>Discussion</b>	<b>87</b>
8.1	Model development . . . . .	87
8.2	Quantification process . . . . .	88
8.3	Results . . . . .	89
8.4	Sensitivity analysis for the BBN models . . . . .	89
8.4.1	I-Phase . . . . .	89
8.4.2	D-Phase . . . . .	90
8.4.3	A-phase . . . . .	91
8.5	Sensitivity analysis of the HCL . . . . .	92
<b>9</b>	<b>Conclusion</b>	<b>95</b>
9.0.1	Further work . . . . .	95
<b>A</b>	<b>Additional figures</b>	<b>104</b>
<b>B</b>	<b>Additional tables</b>	<b>120</b>

## List of Figures

2.1	Risk matrix [6]	6
2.2	Types of events and gates in an ESD [16]	8
2.3	Common symbols for FTA [6]	9
2.4	A simple Bayesian network	10
2.5	Different types of collision [16]	11
3.1	IDA model extended for operator and autonomous ship [16]. . . . .	14
4.1	ESD flowchart [16]	22
4.2	CoTA for the autonomous ship [16]	24
4.3	CoTA for the human operators [16]	25
4.4	Top event for generic autonomous failure event [24]	27
4.5	Generic fault tree for the AS failure in collecting necessary data [24]	28
4.6	Generic fault tree for the AS failure in data collection - no data (SDC-N) [24]	29
4.7	Generic fault tree for the AS failure in data collection - incorrect data (SDC-I) [24]	30
4.8	Generic fault tree for the AS failure in communication establishment between SCC and the AS [24]	31
4.9	Generic fault tree for the AS failure in making the correct decision [24]	31
4.10	Generic fault tree for the AS failure in taking the correct action [24]	32
4.11	Generic fault tree for human failure event [24]	33
4.12	Generic fault tree for human failure event in collecting and pre-processing information [24]	34
4.14	Generic fault tree for human failure event in execution to collect information [24]	34

4.13	Generic fault tree for human failure event in decision to collect information [24] . . . . .	35
4.15	Generic fault tree for human failure event in situation assessment and decision-making [24] . . . . .	36
4.16	Generic fault tree for human failure event in taking the correct action (HFA) [24] . . . . .	37
4.17	Overview of the HCL model [24] . . . . .	39
5.1	High level control structure diagram for an autonomous vessel concept [44] . . . . .	46
5.2	The components of the machinery system [44] . . . . .	48
6.1	Case study Event Sequence Diagram . . . . .	56
6.2	Case study Event Sequence Diagram - Transfer Gate: AS fails to detect collision candidate . . . . .	57
6.3	Case study Event Sequence Diagram - Transfer Gate: No collision avoidance plan . . . . .	57
6.4	Fault trees for the failure events: ANS failure, software failure and hardware failure . . . . .	59
6.5	Fault tree for with the top events power supply and generator set failure . . . . .	60
6.6	Fault tree for the AS failure event: Failure in data collection - no data (SDC-N) . . . . .	61
6.7	Fault tree for the AS failure event: Failure in data collection - incorrect data (SDC-I) . . . . .	62
6.8	Fault tree for the AS failure event: Failure in communication establishment . . . . .	63
6.9	Fault tree with the top event satellite failure [8] . . . . .	63
6.10	Fault tree for the AS failure event: Failure to detect collision candidate . . . . .	64
6.11	Fault tree for the AS failure event: Failure to plan collision avoidance route . . . . .	65
6.12	Fault tree for the AS failure event: Failure to implement and execute collision avoidance plan . . . . .	66
6.13	Fault tree with the top event supply system failure [8] . . . . .	67
6.14	Fault tree for the AS failure event: Failure to implement and execute collision avoidance plan by the operator . . . . .	67
6.15	Fault tree for the Human Operator failure event: Failure to detect collision candidate . . . . .	68
6.16	Fault tree for the Human Operator failure event: Failure to respond to alarm . . . . .	69
6.17	Fault tree for the Human Operator failure event: Failure to decide on operational mode . . . . .	70
6.18	Fault tree for the Human Operator failure event: Failure to remotely control AS to safe path . . . . .	70
6.19	Fault tree for the Human Operator failure event: Failure to monitor safe execution . . . . .	71

6.20	BBN for I-Phase . . . . .	72
6.21	BBN for D-Phase . . . . .	72
6.22	BBN for A-Phase . . . . .	73
7.1	Voyage route for the autonomous ship . . . . .	76
7.2	Crossing area . . . . .	84
8.1	Effect of changing the states individually on the probability of adequate I-Phase. . . . .	90
8.2	Sensitivity of the I-Phase node. Darker red charts indicate a higher influence. Grey charts are deterministic. . . . .	91
8.3	Sensitivity of the D-Phase node. Darker red charts indicate a higher influence. Grey charts are deterministic. . . . .	91
8.4	Effect of changing the states individually on the probability of adequate D-Phase. . . . .	92
8.6	Effect of changing the states individually on the probability of adequate A-Phase. . . . .	92
8.5	Sensitivity of the A-Phase node. Darker red charts indicate a higher influence. Grey charts are deterministic. . . . .	93
A.1	Event sequence diagram for the case study . . . . .	104
A.2	Event sequence diagram for the case study . . . . .	105
A.3	Event sequence diagram for the case study . . . . .	105
A.4	Fault tree with the top event failure in data collection from the autonomous ship (no data) . . . . .	106
A.5	Fault tree with the top event failure in data collection from the autonomous ship (incorrect data) . . . . .	107
A.6	Fault tree with the top event failure in communication establishment between the SCC and the autonomous ship . . . . .	108
A.7	Fault tree with the top event ANS failure . . . . .	108
A.8	Fault trees with the top event software failure and hardware failure . . . . .	109
A.9	Fault tree with the top event satellite failure . . . . .	109
A.10	Fault tree with the top event power supply failure . . . . .	109
A.11	Fault tree with the top event generator set failure . . . . .	110
A.12	Fault tree with the top event supply system failure . . . . .	110
A.13	Autonomous ship failure event with the top event failure to detect collision candidate . . . . .	110
A.14	Autonomous ship failure event with the top event failure to plan collision avoidance route . . . . .	111
A.15	Autonomous ship failure event with the top event failure to implement and execute collision avoidance plan . . . . .	111
A.16	Human operator failure with the top event failure in collecting and pre-processing necessary information . . . . .	112
A.17	Human operator failure with the top event failure in situation assessment and making the correct decision . . . . .	113

A.18 Human operator failure with the top event failure in decision to collect information . . . . .	114
A.19 Human operator failure with the top event failure in execution to collect information . . . . .	114
A.20 Human operator failure with the top event failure in taking the correct action . . . . .	115
A.21 Human operator failure event with the top event failure to detect collision candidate . . . . .	115
A.22 Human operator failure event with the top event failure to respond to alarm . . . . .	116
A.23 Human operator failure event with the top event failure to decide on operational mode . . . . .	116
A.24 Human operator failure event with the top event failure to remotely control AS to safe path . . . . .	117
A.25 Human operator failure event with the top event failure to monitor safe execution . . . . .	117
A.26 BBN for the I-phase . . . . .	118
A.27 BBN for the D-phase . . . . .	118
A.28 BBN for the A-phase . . . . .	119

## List of Tables

4.1	ESD flowchart questions [24] . . . . .	22
4.3	Summary of PIFs with proposed states . . . . .	38
4.4	Strength rating associated for the CPT HMI . . . . .	40
4.6	Strength rating associated for the CPT Workload . . . . .	41
4.8	Strength rating associated for the CPT SA . . . . .	41
4.10	Strength rating associated for the CPT I-Phase . . . . .	42
4.12	Strength rating associated for the CPT D-phase . . . . .	42
4.14	Strength rating associated for the CPT A-Phase . . . . .	43
5.1	Main particulars of the unmanned autonomous vessel (based on information from [49]) . . . . .	45
5.2	Components of communication, monitoring and control system (based on information from [44]) . . . . .	50
5.3	Ship information systems (based on information from [51]) . . . . .	51
5.5	Machinery system (based on information from [44], [52]) . . . . .	52
6.1	Scenario ESD questions with answers . . . . .	55
7.1	The autonomous voyage . . . . .	75
7.2	CPT template for building the CPTs for I-Phase, D-Phase and A-Phase [40] . . . . .	76
7.4	Discretized CPT templates for low and high strength of influence. Worst, intermediate and best is a generic representation of the states [40] . . . . .	77
7.6	Event frequency index as defined by IMO [11] . . . . .	78
7.7	Failure probabilities derived from [11] . . . . .	79
7.8	Rounded fault tree top event probabilities for the autonomous ship . . . . .	80

7.10	Rounded fault tree top event probabilities for the human operator . . . . .	81
7.12	Number of collision candidates and probability of being on collision course . . . . .	84
7.14	Collision probability . . . . .	85
8.1	Risk comparison when changing human performance . . . . .	92
B.1	Autonomous ship basic failure events leading to failure in data collection (taken directly from [24]) . . . . .	120
B.2	Autonomous ship basic failure events leading to failure in communication (taken directly from [24]) . . . . .	123
B.3	Autonomous ship basic failure events leading to failure in situation assessment and decision making (taken directly from [24]) . . . . .	125
B.4	Autonomous ship basic failure events leading to failure in action (taken directly from [24]) . . . . .	125
B.5	Operators' basic failure events leading to failure in information gathering and pre-processing (taken directly from [24]) . . . . .	126
B.6	Operators' basic failure events leading to failure in situation assessment and decision making (taken directly from [24]) . . . . .	128
B.7	Operators' basic failure events leading to failure in action (taken directly from [24]) . . . . .	129
B.8	States and values for input nodes in the BBN . . . . .	130
B.10	Calculated failure probabilities . . . . .	131
B.12	IMO frequency categories [67] and corresponding failure probabilities . . . . .	132
B.14	Basic event probabilities and failure rate data source . . . . .	132
B.15	Ship types and route frequencies crossing Rørvik in 2020 [64] . . . . .	135

# Abbreviations

<b>AS</b>	Autonomous ship
<b>AMMS</b>	Autonomous Management System
<b>ANS</b>	Autonomous Navigation System
<b>ARPA</b>	Automatic Radar Plotting Aid
<b>BBN</b>	Bayesian Belief Network
<b>BP</b>	Branch Point
<b>CC</b>	Collision Candidate
<b>CFM</b>	Crew Failure Modes
<b>CoTA</b>	Concurrent Task Analysis
<b>CPT</b>	Conditional Probability Table
<b>DG</b>	Diesel Generator
<b>ESD</b>	Event Sequence Diagram
<b>FT</b>	Fault Tree
<b>FSA</b>	Formal Safety Assessment
<b>HCL</b>	Hybrid Casual Logic
<b>HMI</b>	Human Machine Interface
<b>HRA</b>	Human Reliability Analysis
<b>HSG</b>	Hybrid Shaft Generator
<b>HTA</b>	Hierarchical Task Analysis
<b>IAS</b>	Intelligent Awareness System
<b>IDA</b>	Information, Decision, Action
<b>LoA</b>	Level of Autonomy
<b>MSO</b>	Machinery System Operational mode
<b>ME</b>	Main Engine
<b>MEC</b>	Mechanical
<b>NPP</b>	Nuclear Power Plant
<b>PIF</b>	Performance Influencing Factors
<b>PMS</b>	Power Management System
<b>PTI</b>	Power Take In
<b>PTO</b>	Power Take Out
<b>ROC</b>	Remote Operating Center
<b>SA</b>	Situational Awareness
<b>SC</b>	Ship Control mode
<b>SCC</b>	Shore Control Center
<b>SO</b>	Ship Operation mode
<b>TTA</b>	Tabular Task Analysis



## 1.1 Background and motivation

An important technological trend is the development of maritime autonomous surface ships (MASS). This is due to the potential for increased safety and efficiency, and optimized ship performance [1][2]. Several research projects have already investigated the MASS-concept (REVOLT; MUNIN; YARA), but there are currently no fully autonomous vessels in operation. An operational challenge for MASS is that it may be manned or unmanned [3]. MASS will also influence several aspects of risks in relation to marine stakeholders, the environment and the MASS itself. For conventional ships, collisions and groundings contributes to to most of the risk level [4]. For safe operation the MASS will have to be equipped with collision avoidance systems and sensory equipment. In addition to this, the MASS should also be at least as safe as conventional ships to be acceptable in public oceans [4]; [5].

The aim of a risk assessment is to demonstrate a certain level of risk, and is an important tool for making relevant design decisions [6]. According to [7], who assessed the effect of unmanned vessels, MASS will reduce the collision frequency. However, the severity of the consequences might increase due to the reduced recovery capability. This implies that risk models, implementing technical, human/organizational factors, are needed to reflect the operation of MASS.

Regarding risk research, there has not been conducted much on MASS. In relation to the MUNIN project there has been applied risk-based design methodology which is based on a formal safety assessment. There has also been performed a detailed qualitative and quantitative assessment of the project by Jensen [8]. Apart from that a few risk models specifically related to MASS has been created ([9]; [10]).

---

## 1.2 Objectives

The objective of this thesis will be to develop a risk model assessing the collision risk for an autonomous unmanned cargo vessel sailing along the coast of Norway. The model will be combine an event sequence diagram with fault trees and BBNs, also known as the Hybrid Causal Logic method. The goal with this is to capture and analyze the interaction between the human operators and the autonomous system.

## 1.3 Scope and limitations

To achieve the objective of the thesis a set of tasks has to be performed. These includes to review literature on relevant risk models and theories. Review literature on human reliability analysis and factor affecting human operators in the context autonomous ships. Develop a risk model that represents the collision accident scenario and the interaction between the autonomous ship and the human operator. Quantify the model in order to assess the risk.

The scope in this report is limited to a use-case ship. Only collision probability will be assessed, and critical weather states will not be included.

## 1.4 Thesis structure

The outline of the report can be described as follows:

**Chapter 1** Introduction, including background and motivation, objective, scope and limitations and structure.

**Chapter 2** Relevant theory concerning risk assessment and relevant models. Including information about Level of Autonomy and COLREG.

**Chapter 3** Relevant theory concerning Human Reliability Analysis and factors influencing human operators in the context of autonomous' operations.

**Chapter 4** Description of the method used to develop the model.

**Chapter 5** Description of the system and hazards.

**Chapter 6** The final HCL model with explanations.

**Chapter 7** The quantification process of each model in the HCL and final results.

**Chapter 8** Discussion of the results and the work performed.

**Chapter 9** Conclusion of the thesis and recommendations for further work.

---

---

## 2.1 Definitions

In MSC-MEPC.2/Circ.12/Rev.2, The International Maritime Organization (IMO) defines a *hazard* as: "A potential to threaten human life, health, property or the environment." [11]. In the same document, IMO also defines terms such as *risk*, *accident*, *frequency* and *consequence*. [11].

Risk: "The combination of the frequency and the severity of the consequence."

Accident: "An unintended event involving fatality, injury, ship loss or damage, other property loss or damage, or environmental damage."

Frequency: "The number of occurrences per unit time (e.g. per year)."

Consequence: "The outcome of an accident."

To visualize risk, it can often be useful to use a risk matrix where the risk can be categorized from low risk to high risk. The risk matrix is based on the formula:

$$R = P \cdot C \quad (2.1.1)$$

Where R is the risk, P is the occurrence probability and C the consequences [6]. Figure 2.1 shows that a hazard that is very likely to happen and has catastrophic consequences poses a high, not acceptable risk, whereas one that is not very likely to happen and only leads to minor damages is seen as broadly acceptable. Risks should be kept "As Low As Reasonably Practicable (ALARP)".

Probability/ consequence	1 Improbable	2 Remote	3 Possible	4 Occasional	5 Fairly normal
5 Catastrophic	6	7	8	9	10
4 Severe loss	5	6	7	8	9
3 Major damage	4	5	6	7	8
2 Damage	3	4	5	6	7
1 Minor damage	2	3	4	5	6

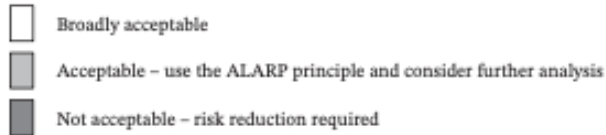


Figure 2.1: Risk matrix [6]

### 2.1.1 Defining risk for autonomous marine systems and operations

As previously stated, the common definition of risk is associated with a hazardous or undesired event, its various causes and consequences, and the probability. Autonomous marine systems are complex systems that add much more uncertainty to the risk associated with them. [12]. [12] proposes a risk perspective consisting of three dimensions; the probability dimension, the knowledge dimension, and surprises (black swans). [13] defines this as;

$$\{a_i, p_i, q\} | k \quad (2.1.2)$$

where  $a$  is a hazardous event,  $c$  is the consequences of  $a$ ,  $q$  is a measure uncertainty and  $k$  is the background knowledge for determining  $a$ ,  $c$  and  $q$ . This implies risk becomes a subjective measure to be quantified in terms of a Bayesian models instead of an objective risk metric [13].

## 2.2 Formal Safety Assessment (FSA)

The FSA proposed by the IMO follows a procedure of five defined steps.

1. hazard identification
2. analysis of risk
3. proposition of risk control options
4. assessment of associated costs and benefits

5. provision of decision-making recommendations based on steps 1-4

This thesis and further work will focus on the two first steps. Several FSAs has been performed by IMO and others. In this thesis the results will be compared with "FSA Navigation Large Passenger Ships" [14] and "Hazard and Risk Assessment of Unmanned Dry Bulk Carriers on the High Seas" [8].

## 2.3 HAZID

HAZID means hazard identification and is a critical stage in a risk assessment process, as a hazard that is not identified in this stage will be excluded from further assessment. A HAZID can be performed in many ways and with different methods, but generally, it is done as a workshop with experts from different fields. However, the objectives of a HAZID are always the same: identification of hazards associated with the defined system and events or sets of circumstances that may cause the hazards and their potential consequences, to generate a list of possible hazards based on those events and circumstances, and lastly, propose a list of possible risk-reducing measures [15].

## 2.4 Event Sequence Diagram

An event sequence diagram is similar to an event tree and can be defined as generalized event trees [16]. It allows for indicating not only the behavior of key process variables but also operator and hardware state changes, enabling it to give a more literal representation of a system state compared to event trees [17]. An ESD represents the possible sequence of events following an initiating event, leading to the possible consequences.

An ESD may contain six types of elements [17]. These are (i) events (observable physical phenomenon); (ii) conditions (binary paths); (iii) gates (connects events); (iv) process parameter set (time and other parameters which affects the system); (v) constraints/boundaries (set of intervals of process parameters which are in competition with the time to occurrence of an event); and (vi) dependency rules (describes the interaction of the set of process parameters. The types of events and gates are illustrated in figure 2.2.

One of the strengths of an ESD is that it can be used to model dynamic systems [17], and thus be used in a dynamic risk analysis of for example an autonomous system. It can also be combined with fault trees, BBNs or a combination of these, in a Hybrid Causal Logic Modeling [18].

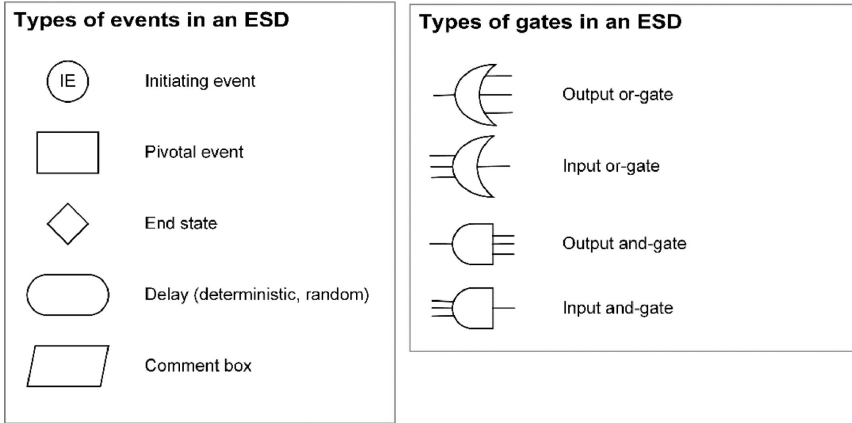


Figure 2.2: Types of events and gates in an ESD [16]

## 2.5 Fault tree analysis

A fault tree is a top-down logic diagram that displays the interrelationships between a potentially hazardous event in a system and the causes of this event [6]. It is the most commonly used method for risk and reliability studies [6], and can be approached both qualitatively and/or quantitatively. The model is deterministic, meaning that when a fault tree is constructed, we know the states of all basic events, the top event, and the states of all the intermediate events. Figure 2.3 shows some of the most commonly used event and gate symbols that are used in fault tree structures.

The probability for the TOP event to occur with an AND gate is given by [6]:

$$Q_0(t) = \prod_{i=1}^n q_i(t) \quad (2.5.1)$$

The probability for the TOP event to occur with an OR gate is given by:

$$Q_0(t) = 1 - \prod_{i=1}^n (1 - q_i(t)) \quad (2.5.2)$$



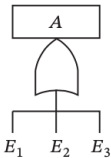
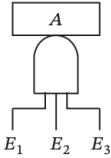





	Symbol	Description
Logic gates	<p>OR-gate</p> 	The OR-gate indicates that the output event $A$ occurs if at least one of the input events $E_i$ occur
	<p>AND-gate</p> 	The AND-gate indicates that the output event $A$ occurs only when all the input events $E_i$ occur at the same time
Input events	<p>Basic event</p> 	The basic event represents an event (typically a basic equipment failure) that requires no further development of failure causes
	<p>Undeveloped event</p> 	The undeveloped event represents an event that is not examined further because information is not available or because its consequence is insignificant
Description	<p>Comment rectangle</p> 	The comment rectangle is for supplementary information
Transfer symbols	<p>Transfer-out</p> 	The transfer-out symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer-in symbol
	<p>Transfer-in</p> 	

Figure 2.3: Common symbols for FTA [6]

## 2.6 BBN

A Bayesian network is a graphical model that shows the causal relationships between key factors (causes) and one or more final outcomes in a system [6], and was first introduced by Pearl in 1986 [19]. The network is made up of nodes and directed arcs. Each node describes a state or a condition, while an arc indicates a direct influence. A Bayesian analysis may be qualitative, quantitative, or both depending on the scope of the analysis. A quantitative network introduces probabilities and aims to find the probability of the outcome. In many ways, Bayesian networks are used for the same purpose as a fault tree, namely investigating the causes leading up to the hazardous event. A significant difference, however, is that Bayesian networks can model probabilistic causation as well as deterministic. There are

---

no international standards for BBN. Figure 2.4 shows the simplest possible BBN where node A is linked to node B. In this case, node A is called a parent node of node B, and node B is called a child node. A node with no parents is a root node.



Figure 2.4: A simple Bayesian network

Bayes theorem is the basis for calculating conditional probabilities in a BBN. Bayes theorem is shown in Equation 2.6.1.

$$P(A | B) = \frac{P(B | A)P(A)}{P(B)} \quad (2.6.1)$$

where,

$$\begin{aligned} P(A) &= \text{Probability of A occurring} \\ P(B) &= \text{Probability of B occurring} \\ P(A | B) &= \text{Probability of A occurring given that B is true} \\ P(B | A) &= \text{Probability of B occurring given that A is true} \end{aligned}$$

## 2.7 Hybrid Causal Logic (HCL)

Hybrid causal logic is a framework for modeling and quantifying accident scenarios. It combines Event sequence diagram/event trees, fault tree, and Bayesian belief networks [6]. The model is a means to get a better understanding of the risk model by separating the different domains into a human, organizational and technical system. The event sequence diagram is used to define the safety context where fault trees are utilized to model the physical/technical system, while BBN is used to capture the human and organizational system.

## 2.8 Level of autonomy and shore control center

Autonomous ships may have functionality with different levels of autonomy (LoA). The LoA impacts the ship's dependency on the operator, planning functionalities, and mission and operation capabilities. One definition of autonomy is: "a system's or sub-system's own ability of integrated sensing, perceiving, analyzing, communicating, planning, decision-making, and acting, to achieve its goals as assigned by its

human operator(s) through designed human-machine interface(HMI)”[13]. There are several different taxonomies proposed to define the different levels of LoA. One of them divides the LoA into four different levels: LoA 1: remote control, LoA 2: Automatic, LoA 3: Constrained autonomous, and LoA 4: Fully autonomous [3]. Even though it is possible to differentiate between different levels of autonomy, a vessel could still change autonomy levels during a voyage. This implies that it may be more reasonable to categorize the LoA depending on both the voyage phase/operation and the ship’s capabilities. The different levels mentioned in this section, except from fully autonomous, require a crew working onshore in a Shore Control Centre (SCC). The role of the SCC will be to monitor unmanned ships and take direct remote control by using available communication technologies.

### 2.8.1 COLREG - Rules on collision avoidance

When it comes to collision, it is said that 80 % of collisions are caused by human error [20]. A collision refers to a contact between two or more vessels, or between a vessel and an object. There are no formal definition for when a ship is on collision course, but it is often stated that a vessel doesn’t change course, it will collide[21]. A collision can be classified into different categories. These are illustrated in figure 2.5.

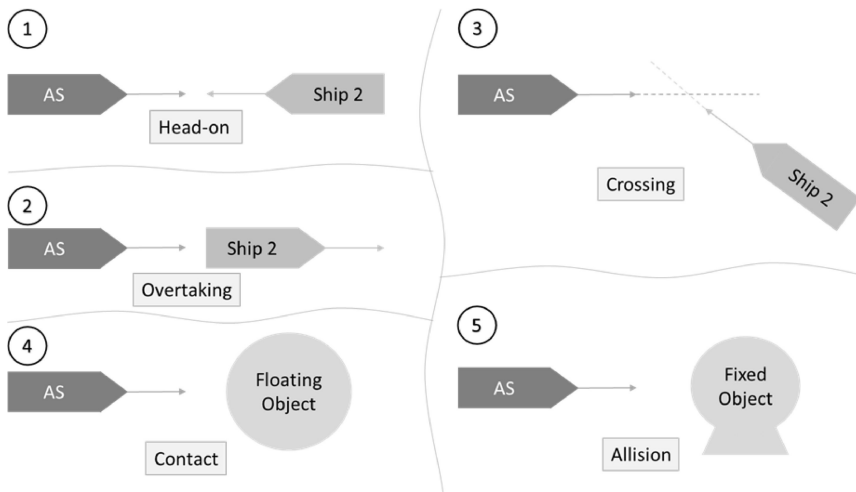


Figure 2.5: Different types of collision [16]

For collision avoidance, there are some rules ships at sea must follow. These are the international rules for collision avoidance- COLREG [22]. For the scenarios in Figure 2.5, the following rules apply (1) Head-on collision, both vessels need to change their course to starboard (rule 14); (2) Overtaking, the autonomous vessel is responsible for avoiding collision (rule 13); (3) Crossing collision, the autonomous vessel is required to have the crossing ship on starboard to alter course and speed

---

to avoid collision (rule 15). In scenarios 4 and 5, the autonomous vessel will have to take action to avoid a collision.

## 2.9 Risk modeling of maritime autonomous surface vessels (MASS)

In the paper *Assessing ship risk model applicability to Maritime Autonomous Surface Ships* [23], the author review and discuss current ship risk models for ship-ship collision, ship-structure collision and groundings, and their applicability to MASS. According to Thieme, none of the risk models reviewed were suitable to be directly used for risk assessment of MASS. There were also no risk models that included software and human operator interaction sufficiently. Some of the models could, however, be used as a basis for further development. Jensen has developed a thorough risk analysis of the MUNIN project[8], but this focuses on hardware failures. One framework, which Thieme does not review, is *A generic approach to analyzing failures in human - System interaction in autonomy* by Ramos [24]. Ramos analyses the humans in relation to autonomous ships by a novel method called the human-system interaction(H-SIA) method, combining Event Sequence Diagrams and a novel method called Concurrent Task Analysis. The collision risk for autonomous vessels exemplifies the model. The H-SIA method used in the model provides a good description of behavior and failures that can occur between the sub-systems and within each sub-system. The method focuses on humans in the loop, but it can also be used to model the behavior between software and hardware. Ramos has also developed a set of generic fault trees related to autonomous- and human failure events based on the IDA model. To further investigate the basic events related to human failures, the author proposes to use BBNs, following the HCL modeling technique.

### 3.1 Task Analysis and Concurrent Task Analysis

Concurrent Task Analysis (CoTA) is a novel method developed in [16]. It is based on Task Analysis (TA) theory and methods and translates the events of the ESD into goals to be achieved. Task Analysis(TA) was initially developed for only analyzing human performance but has since evolved into also covering challenges in the Human-Computer Interaction (HCI)[25]. There are different approaches to developing a TA. Some of them are Hierarchical Task Analysis (HTA), Tabular Task Analysis (TTA), and Cognitive Task Analysis. HTA is a method where complex tasks are analyzed by decomposing goals and re-describing them into sub-goals. These are then organized into plans [26]. The plans state what order in which the sub-goals should be performed. When applied to a system, HTA can be used to understand how the system should behave and how it can fail. The stop-rule determines the re-description of goals into sub-goals. In [27], Ramos developed an HTA for supervising/remotely controlling autonomous ships, which makes use of the operator cognitive model IDA as a stop rule. For the CoTA, the IDA model is used not only as a stop rule for the operator but also for the autonomous ship. The IDA model will be described later in this chapter.

A CoTA is comprised of several HTAs or TTAs, where each task is re-described until basic tasks that can relate to the interaction between the parts of the system are found [16]. The CoTA also has specific *stop-rules*, and includes a new type of task named *parallel task*. Parallel tasks are not directly related to the events in the ESD, but rather supporting tasks necessary for the execution of the other tasks and the interaction between the different parts of the system. Parallel tasks are normally related to gathering data, monitoring, or communication. To develop the CoTA, each task from the ESD is transformed into tasks to be performed by the

agents involved. It thus allows for a more thorough understanding of each task the agents have to perform in order for the events in the ESD to take place.

## 3.2 Information-decision-action (IDA) model

IDA - Information, Decision, and Action is a model initially developed for the human behavior response of a nuclear power plant crew under accident conditions [28]. It consists of three different cognitive phases: I (Information collection and pre-processing); D (decision making and situation assessment); and A (action taking). In [16], Ramos extends the IDA and adapts it for different agents of a system. More specifically, a system consisting of a human operator and an autonomous vessel. This allows for decomposing functions into the same-low level unit of analysis. Figure 3.1 illustrates the elements of the IDA model in an extended version, generalized for an autonomous ship vessel modeling, in addition to operator behavior.

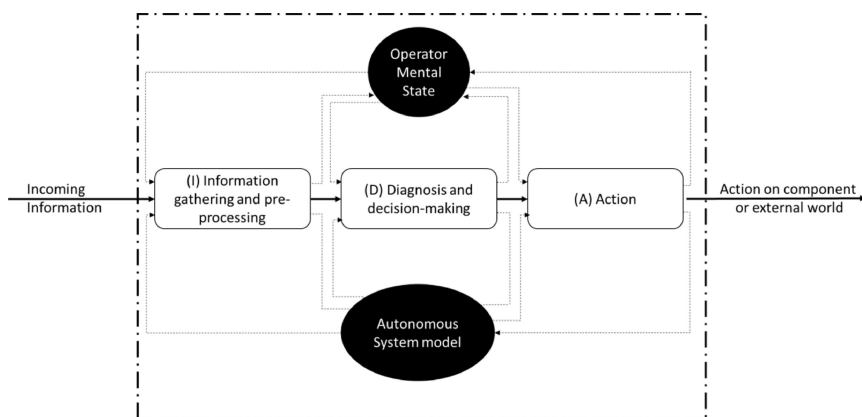


Figure 3.1: IDA model extended for operator and autonomous ship [16].

In the IDA model, the agent receives information from the external world. This may, for instance, be data about the ship trimming and heading for the autonomous vessel or an alarm for the human operator. The information is then received and processed through the (I) block, which includes filtering, comprehension, grouping, and prioritization. The (D) phase relates to the agent's response to the information obtained. These two phases cover situation assessment and response planning. The decisions from the (D) phase are put into action in the (A) phase. For a human operator, the mental state combined with memory represents the cognitive and psychological states. For an autonomous vessel, on the other hand, the AS model includes the programmed behavior, the process models, and the world model of the AS. The interaction between the human operators and the autonomous vessel is a dynamic process of mutual influence where they influence the activities within each of the IDA blocks (dashed lines in Figure 3.1). The goals analyzed in the HTA represent the system's needs as a whole and function as an external reference point in the IDA. A mismatch between these needs and the agent's actions would

be classified as an error. Re-describing the goals as one of the IDA phases allows for identifying errors with respect to the internal reference points. The advantage of identifying the errors within one of the I-D-A phases is that, for the human operator, it can be traced back to the cognitive process leading to the error, while for the system, it can be traced to the responsible component in which the error occurred.

### 3.3 Human Reliability Analysis and BBN models related to human operators

As previously mentioned, BBN's can be used in the HCL method to capture the human and organizational elements of the system. Currently, there are no set of PIFs between HRA methods for humans working in an offshore control center, supervising an autonomous ship [29]. However, many of the HRA studies rely on cognitive science and can thus be relevant for human operators working in an SCC. This is backed by Ramos in her paper *On factors affecting autonomous ships operating in a Shore Control Center*, where she states "...it should have roots on cognitive science..." [29] about developing a PIF set for autonomous ships. One example of a methodology is The Phoenix HRA methodology. It is developed in the context of NPP operations, and uses HCL, and combines BBNs with the FTs to model the influence of Performance Influencing Factors (PIFs) on the failure modes. This method has been applied in several papers ([30], [31]). In *On factors affecting autonomous ships operating in a Shore Control Center*, Ramos [29], provides an initial analysis of factors that have been explored in the autonomous ships' operation. Thieme [23] has also made BBN focusing on human-autonomy collaboration.

#### 3.3.1 Performance Influencing Factors

Performance Influencing Factors(PIFs), are used as a way of representing the context and casual factors influencing human performance in different systems [32]. It can help the analyser identifying *why* the operator can fail, instead of only which failures they can commit.

#### 3.3.2 Phoenix HRA

The Phoenix method is a model-based human reliability analysis methodology based on cognitive science and psychology, experimental results, operating experience from nuclear power plants(NPP) and expert opinions from PRA HRA analysts, plant operators, cognitive scientists and psychologists. The method contains a qualitative and quantitative analysis of the Model-Based HRA methodology with a set of performance influencing factor groups. It also contains a framework for developing Crew failure modes(CFM) to PIFs based on possible causes of failure mechanisms for human error. The CFMs are developed to specify the possible forms of failure in each of the IDA-phases.

---

Ekanem also proposes a Master BBN which shows the relationships between CFMs and all the levels of PIFs defined in his methodology [33]. The model has 19 CFMs and 9 PIF level 1 PIFs. The model also consists of several Level 2 and 3 PIFs which will be described below.

### **Human System Interface (HSI) Group**

This PIF refers to the means and ways of interaction between the crew and the system and covers the quality of the system input and the crew's input to the system. Level 2 PIFs making up this PIF is HSI input and HSI output.

### **Procedures Group**

This PIF refers to the availability and quality of the step-by-step instructions necessary for the crew to perform a task. This PIF is made up of two level 2 PIFs: Procedure quality and Procedure availability, respectively.

### **Resources Group**

This PIF refers to the sufficiency and availability of required resources needed by the crew to aid in completing their assigned tasks. The organization should provide resources. The resource group is made up of two Level 2 PIFs: Tools and Work Place Adequacy. Tools are further made up by Tool quality and Tool availability.

### **Team Effectiveness Group**

This PIF refers to how well the crew harmonizes and their synchronization of the team's overall goals and tasks. This group is made up of two level 2 PIFs: Communication and Team Coordination. Communication is also made up of two level 3 PIFs, communication quality and communication availability, while team coordination is made up of five level 3 PIFs: Leadership, Team Cohesion, Role Awareness, Team composition, and Team Training.

### **Knowledge/Abilities Group**

This PIF refers to the knowledge and abilities of the crew in order to perform assigned tasks. Knowledge is understanding of the system and task to be performed, experience is the knowledge gained over time, while skill is the ability to perform the necessary activities related to the task with little cognitive effort[33]. This group is made up of three level 2 PIFs: Knowledge/Experience/Skill (content), Knowledge/Experience/Skill (access), and Physical Abilities and Readiness. These are in turn comprised of one, one, and zero level 3 PIFs, namely: Task Training and Attention.



### **Bias Group**

This PIF refers to the tendency of the crew to make decisions based on selected pieces of information instead of the whole picture. There are several types of bias, and it may appear in the form of confirmation bias (only selecting the piece of information that supports the hypothesis, belief bias (only selecting the piece of information that already supports your belief, and averaging bias (regression towards the mean). The Bias group is made up of five level 2 PIFs. Morale/Motivation/Attitude, Safety Culture, Confidence in Information, Familiarity with or Recency of Situation, and Competing/Conflicting Goals.

### **Stress group**

This PIF refers to the pressure/tension applied on the crew by their understanding of the situation or their perception of their decisions' consequences and responsibility. It comprises two level 2 PIFs: Stress due to Situation Perception and Stress due to Decision. Stress due to Situation Perception is in turn made up of Perceived Situation Urgency and Perceived Situation Severity.

### **Task Load Group**

This PIF refers to the load applied on the group by the explicit demands required by the task at hand. The task load is increased with the complexity of the task, quantity, importance, and accuracy and can be perceived differently by each crew member depending on the individual's skill level. The PIF group is made up of four level 2 PIFs: Cognitive complexity, Execution Complexity, Extra Workload, and Passive Information Load. Cognitive Complexity and Execution Complexity comprises two level 3 PIFs each: Inherent Cognitive Complexity and Cognitive Complexity due to External Factors, and Inherent Execution Complexity and Execution Complexity due to External Factors.

### **Time constraint group**

This PIF refers to the crew's perception of the time available to perform the task at hand. The time constraint can be perceived differently by each crew member, as there is a *real* duration of completing the task, as well as a *perceived* time.

Each PIF in the BBN will also have two states: *nominal* and *degraded*. Each state describes its influence on the crew's performance. *nominal* implies that the PIFs do not have a significant influence.

### **3.3.3 Factors affecting autonomous ships operators performance**

As the PIFs described in the Phoenix method have been developed for NPP operations, their applicability in the context of autonomous ship operations must be

---

assessed [24]. By comparing these factors to the ones mentioned by Ramos[29], this can be done.

*Information overload* is the fact of receiving too much information. For an operator working in an SCC, information overload can be highly relevant when for example monitoring several vessels at the time. Information overload is mentioned in several HRA studies. In SPAR-H, it is related to the PIF stress [34], while it is modeled as Passive Information Load in Phoenix.

Another factor described by Ramos is *Situational awareness*(SA). This can be defined as "being aware of what is happening around you and understanding what the information means to you now and in the future"[35], and is very important in order to make the correct decisions. In fact, a study on human factors for the MUNIN project with masters mariners and a ship engineer [36] stressed situational awareness as the most critical factor to focus on when moving ship handling from ship to shore. Generally, SA is not in itself analyzed as a PIF in most HRA studies. SA is more of a task of the human operator, which other PIFs can influence. In Phoenix HRA, experience, fatigue(stress), HMI and communication are crucial PIFs for SA.

*Skill degradation* is related to both physical and cognitive loss of skill following disuse[37]. As disuse is an effect of more automated systems, skill degradation is a recognized possible consequence of autonomy. It is also a possible outcome of moving the ship handling from ship to shore [38]. Skill degradation can be analyzed through PIFs related to cognitive and physical skills. In the Phoenix methodology, this could be modeled through knowledge/experience/skill. While in SPAR-H and IDAC, it could be assessed through the PIFs *Experience/training* and *knowledge and experience* respectively [29].

The next factor, *Boredom*, can be defined as "a state of weariness caused by dullness and tedious repetition" [39]. Boredom has been shown to have a negative effect on morale, performance, and quality of work. Related to HRA studies, boredom is usually considered as a factor influencing other PIFs. In SPAR-H, for example, it is related to stress and fitness for duty. In Phoenix, it can be related to stress.

The last factor mentioned in [29], is *Other factors*. These are factors that are mentioned as positive outcomes when shifting from onboard- to onshore operations. In other words, they are factors that have a negative impact on the crew onboard the ship but will not have the same effect in a SCC. The factors mentioned are *sleep deprivation*, *fatigue* and *motion sickness*. Although sleep deprivation and fatigue still may occur, it will not happen with the same severity[29]. Fatigue and sleep deprivation can be analyzed in Phoenix through the PIFs *Physical abilities and readiness* and *Attention*. In SPAR-H, it can be related to the PIFs *Stress* and *fitness for duty*.

### 3.3.4 A risk model for autonomous marine systems and operations focusing on human-autonomy collaboration

Another risk BBN model made is *A risk model for autonomous marine systems and operations focusing on human-autonomy collaboration* [40]. This model is explicitly developed for the interaction between human operators and Autonomous Underwater Vehicles(AUVs). However, many of the nodes in this model related to the human operator are the same or can be related to the nodes described previously in this chapter. The different input nodes used in this model are listed below:

- Communication
- Fatigue
- Feedback from the system
- Etiquette
- Interface design
- Operator's experience
- Operator's training
- Procedures
- Reaction time
- Task load
- Trust
- Workload

---

## 4.1 Modelling event sequence diagram

The method for developing the ESD is based on the flowchart developed by [16], shown in Figure 4.1. The flowchart is developed by analyzing several collision scenarios for autonomous ships and incorporating the human operator and the AS. It involves several Branch Points (BPs) related to the Level Of Autonomy and the system's design. The BPs will be present in the ESD depending on the answer to the questions in Table 4.1, and will thus represent pivotal events. The outcomes of the events may be failure or success and different types of operation - manual or autonomous.

### 4.1.1 ESD flowchart

Table 4.1: ESD flowchart questions [24]

Number	Question
1	Who is primarily responsible for the detection of CC?
2	Can the operators detect the CC from the SCC?
3	Can the operators remotely control the AS from the SCC?
4	Can the operators use other measures to avoid collision?
5	Who is primary responsible for developing the collision avoidance plan?
6	Is there an alarm in the SCC warning about the CC, and are they informed on the plan for collision avoidance?
7	Is the collision candidate a ship?
8	Is there enough time available to re-plan and implement a new plan to avoid collision?

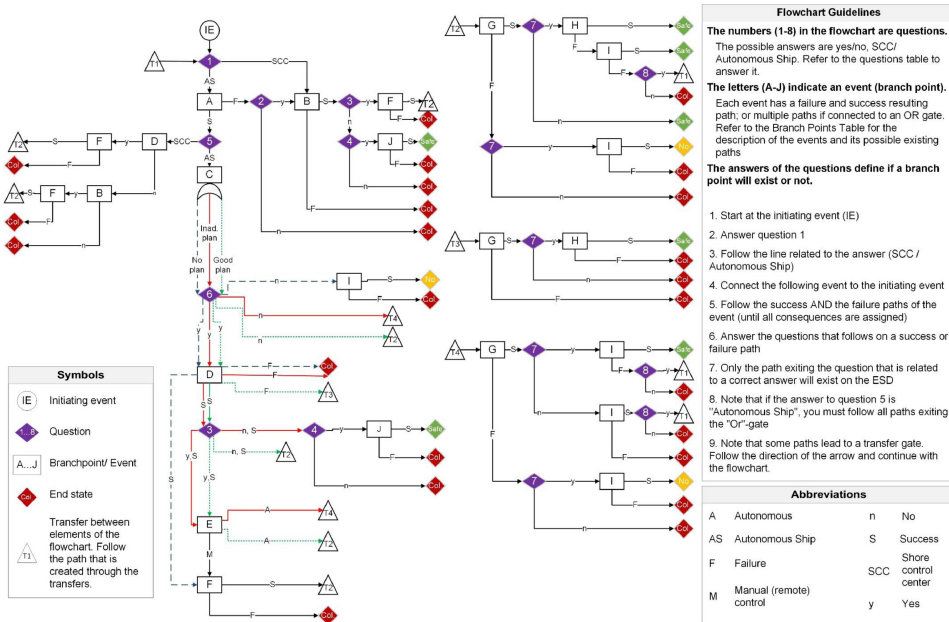


Figure 4.1: ESD flowchart [16]

## 4.2 Concurrent task analysis

The CoTa is developed from the system's ESD, where the events from the ESD are translated into tasks to be performed by the agents. Hence, the ESD presents *what* can happen, while the CoTA details *how* these events come to place.

### 4.2.1 Developing a CoTA from an ESD

Ramos' has come up with five steps on how to develop a CoTA from an ESD [16]:

1. Define the different agents to be analyzed, i.e, operators and AS. Each of the agents will have its own HTA.
2. Define task 0. In this case task 0 is to avoid collision and recover successfully.
3. Analyze each event in the ESD and define which agent is involved: i.e., the AS, the operator or both.
4. Translate each ESD event into a high-level task in the HTA.
5. Identify the tasks that should be executed at all times during the scenario, also known as parallel tasks. These can support the other tasks or be connected to the interaction between the agents, i.e., communication tasks, listening for commands, etc.
6. Use the stop-rule to re-describe tasks. This is done when the tasks: a) are associated with only one of the phases in the IDA model b) represent the interaction with another agent for the dependent tasks. Dependent tasks are tasks that receive input from a task of another agent or sends output to it.

It will not be developed a CoTA from scratch in this thesis. Rather, the CoTAs from [24] will be used as they cover all the events in the ESD. The CoTAs can be found in Figure 4.2 and 4.3.





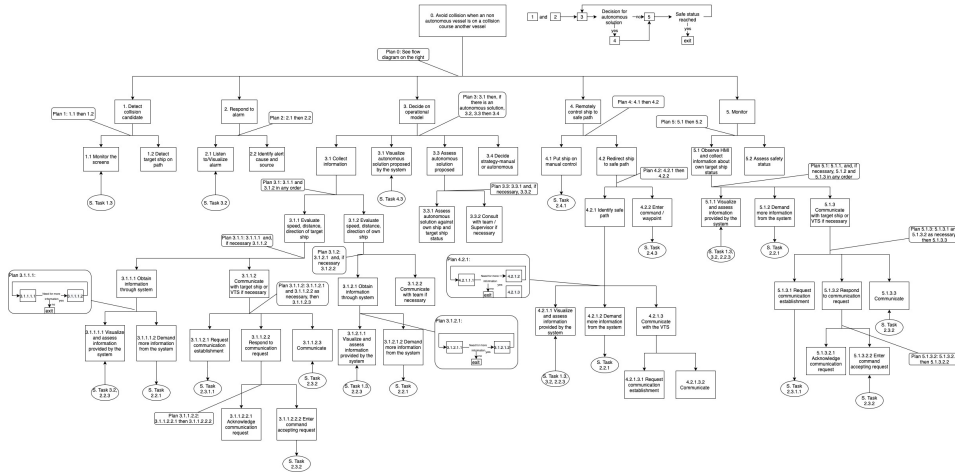


Figure 4.3: CoTA for the human operators [16]

---

## 4.3 Modelling fault trees

The fault trees are based on the IDA structure described in the previous chapter. According to the IDA model, human operators or the autonomous vessel can fail during:

1. Information gathering and pre-processing (I phase), i.e., receiving information from sensors
2. Situation assessment and decision making (D phase), i.e., deciding a collision avoidance plan
3. Action taking (A phase), i.e., sending correct machinery input or sending a command through the HMI

In addition to this, interactions between the system's agents identified in CoTA as interface tasks will be addressed with the FTs. This also includes the parallel tasks. Specifically how the FTs are developed can be summarized as below:

1. Each event of the ESD is re-described in the responsible agent's CoTA.
2. The failure in carry out the event will be the top event of the FT. The failure event can be due to a failure in one of the IDA-phases. An error in action caused by an error in decision-making is defined as a correct action given an incorrect decision.
3. Parallel tasks are modeled through their own FTs, and follows the IDA phases. And- or Or gates connects the parallel tasks to the main FTs.
4. Interface tasks that sends input to the other agent are modeled through their own FTs.
5. Basic events in the FTs can be defined generically if specific features of the system are not defined.

### 4.3.1 Generic fault trees

In [24], Ramos has developed a set of generic fault trees for analyzing the failures related to the autonomous ship and the human operators. The Pheonix HRA method [41] serves as a foundation for the structure of the FTs related to the human operators. The same structure is also applied for the FTs for the autonomous ship where failures concerning information collection, decision-making, and action taking are investigated. And- and Or-gates connects the events in the FTs. Some of the fault trees also include "flags." This indicates that a branch of the FT may be neglected depending on the scenario analyzed. The FTs presented in the next two subsections are developed with the following assumptions in mind: The autonomous ship is unmanned, and the ship may be supervised and/or remotely controlled by operators working in the SCC. A description of the generic basic events can be found in Appendix B.

### 4.3.2 Generic fault trees for autonomous ships

The generic fault tree for autonomous ships might fail due to failure in collecting necessary data, failure in making the correct decision, or failure in taking/executing the correct action. This is visualized in Figure 4.4. According to IEC61508 [42], separating critical safety systems into these three fits the standard for safety-critical systems.

Two parallel tasks are performed by the autonomous ship continuously: *data collection* and *communication*. *Data collection* is crucial for the operation of the ship and involves the collection of all necessary internal and external data. This includes environmental conditions, navigational data, objects in proximity and machinery performance data. There are two ways data collection can fail: The ship may not collect data at all. This may be due to sensor failures, or the ship may collect incorrect or incomplete data.

*Communication* is the communication link between the AS and the SCC as well as other vessels. This involves sending data to the SCC and receiving data/commands from operators. *Communication* will have higher importance if the ship is being monitored or controlled by operators in a SCC. The parallel tasks are abbreviated as SDC-N (ship data collection -NO Data Collected), SDC-I (Ship Data Collection -Incorrect Data Collected), and SCF (Ship Communication Failure).

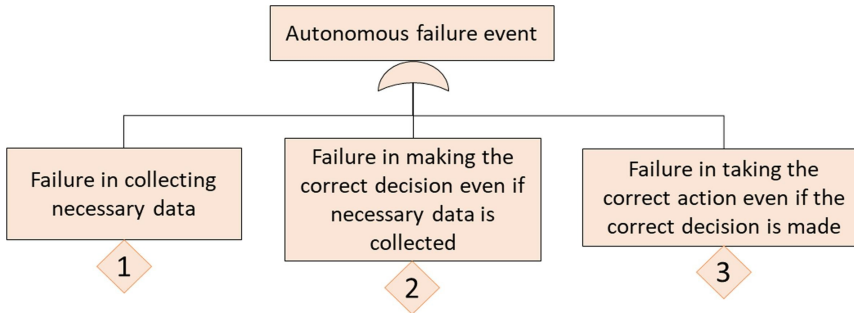


Figure 4.4: Top event for generic autonomous failure event [24]

#### Autonomous ship failure in collecting necessary data - I phase

The AS is equipped with related equipment and sensors for collecting data about its environment and the ship itself. The SCC can also send requests to the autonomous ship for more information or a command. The system may fail in data collection due to Figure 4.5:

- No data is collected (modeled through an OR-gate).
- Incorrect data is collected (modeled through an OR-gate).
- Incorrect or no command is sent by the operators because of:

- Failure in communication establishment with the SCC (modeled through an OR-gate).
- The operator fails to send the correct command or send it in time (HFA).

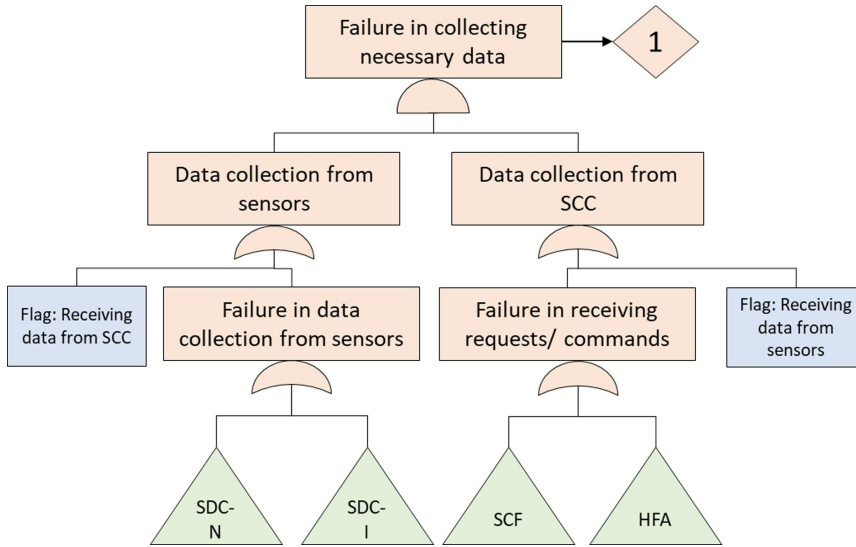


Figure 4.5: Generic fault tree for the AS failure in collecting necessary data [24]

### Autonomous ship failure in data collection - no data collected (SDC-N)

No data being collected may be as a result of (Figure 4.6, Table B.1):

- Failure in collecting raw data due to failures in sensors, databases etc.
- Failure in planning to collect information because of:
  - Inadequacy of the data sampling frequency
  - Data not being identified as needed to be polled
  - Data discounted
- Failure in execution and to collect data because of:
  - Failure in the support system
  - Data failures and data limitations of the system

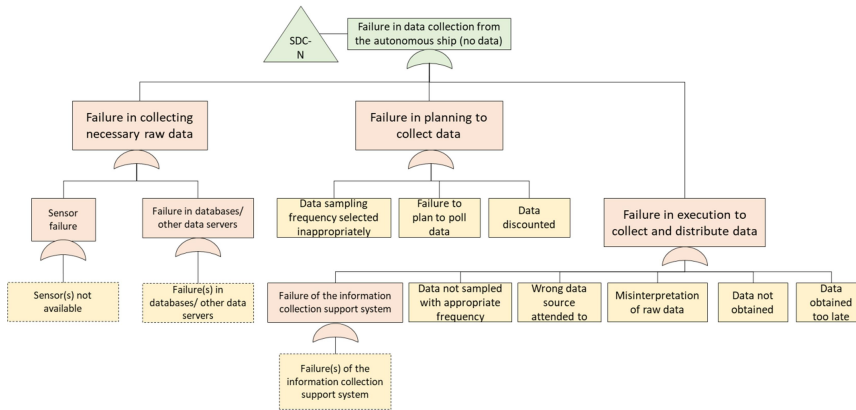


Figure 4.6: Generic fault tree for the AS failure in data collection - no data (SDC-N) [24]

### Autonomous ship failure in data collection - incorrect data collected (SDC-I)

This failure event is very similar to the no data collected. However, the system may collect incorrect data and use it as a basis for further decision-making. The "AND"-gate on the top is the main difference. This ensures that the AS needs to collect incorrect data and not realize it in order to fail. Incorrect data collection may come from failures in sensors, incorrect database entries, decision to collect incorrect data, or a failure in the action of collecting data. The fault tree can be seen in Figure 4.7.

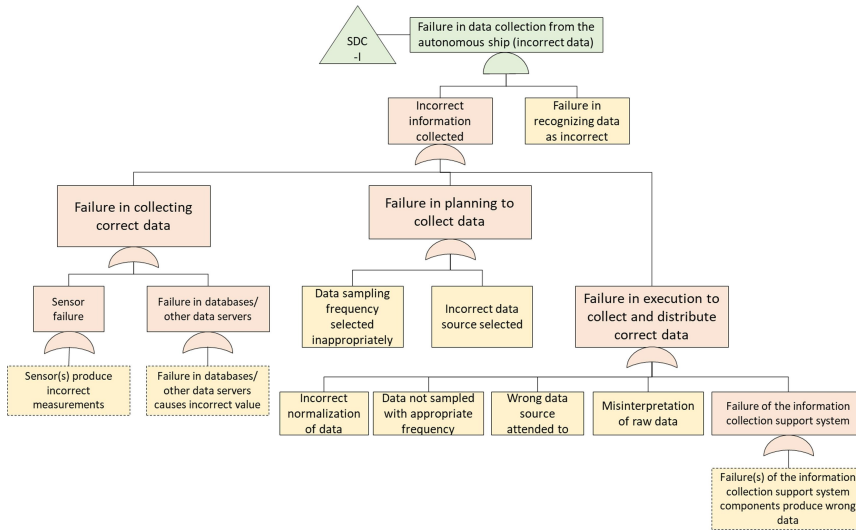


Figure 4.7: Generic fault tree for the AS failure in data collection - incorrect data (SDC-I) [24]

### Autonomous ship failure in communication (SCF)

Failure in communication establishment between the SCC and the autonomous ship is visualized in Figure 4.8 with descriptions of basic events in Table B.2, and may be due to the following events:

- Failure in receiving requests. If there is an error in the information retrieval, the request to establish a communication or data link cannot be received.
- Failures in decision making in conjunction with communication and data transfer. This can happen due to the wrong choice of communication channels or partners, not being able to process and retrieve the necessary information, or prioritizing other actions.
- Failures in hardware or software, incorrect operation of the communication equipment, wrong timing, or incorrect establishing of communication between partners.

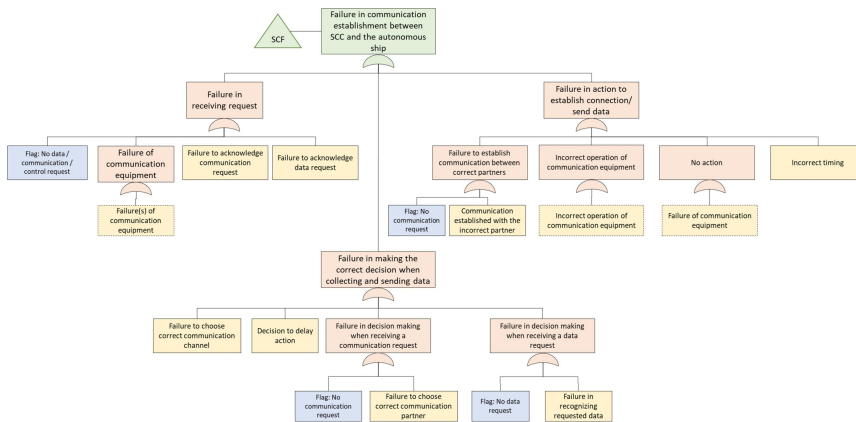


Figure 4.8: Generic fault tree for the AS failure in communication establishment between SCC and the AS [24]

### Autonomous ship failure in situation assessment and decision making - D phase

Failure in situation assessment and decision making is shown in Figure 4.9. This describes the general failures of the autonomous ship to arrive at a sufficient decision on an action in a given situation, and implies that there is a decision that can mitigate or avoid consequences. Descriptions of the basic events are found in Table B.3. The failure may be due to:

- Misdiagnosis of the state of the system and surroundings by the AS.
- Failure in adapting the procedure to the given situation.
- Deciding on an inadequate strategy or delay further action.
- Transfer to an inadequate procedure, i.e. apply the wrong COLREG rule.

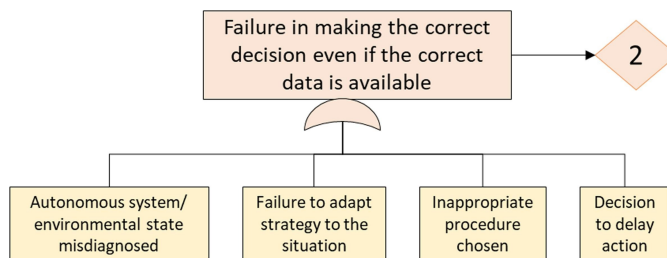


Figure 4.9: Generic fault tree for the AS failure in making the correct decision [24]

---

## Autonomous ship failure - A phase

A failure in making the wrong action may come from failures in the hardware or software. Engaging in the wrong actuators, or the timing of engagement may be basic failure events. Failures can also arise because of inadequate operation of a component or that no action is executed because of a failure of components. The fault tree is shown in Figure 4.10 with descriptions of basic events in Table B.4.

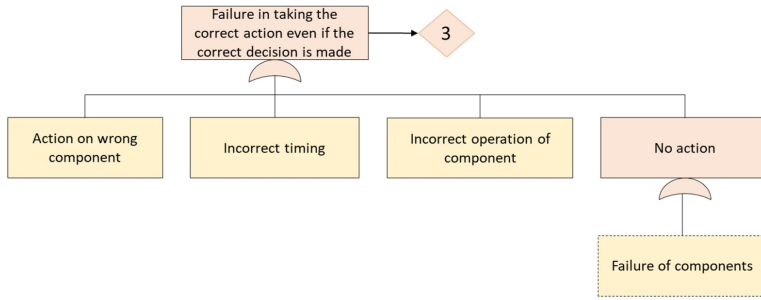


Figure 4.10: Generic fault tree for the AS failure in taking the correct action [24]

### 4.3.3 Generic fault trees for human operators

The Phoenix HRA by Ekanem[41] and the HRA framework by Mosleh [31] serves as the foundation of the generic FTs of the human operators. Even though the FTs were originally developed for operators working in a control room of a NPP, the operations share many similarities with unmanned autonomous systems as it includes monitoring / controlling the system remotely, and sometimes from an offshore control center [36],[27].

The NPP operators and the SCC have some properties they should share; they should be highly trained, have procedures/guidelines for their operation, and possibly work together with other crew members or supervisors. The structure and basic events of the FTs of the Phoenix are in that case applicable for autonomous systems. However, the FTs should be adjusted in order to be applicable for operators interacting an autonomous system. For example, the autonomous ship would be operated remotely, from large distances [43]. Not like other operations in control rooms where the operators can personally interfere in the situation. Therefore, a successful establishment of a communication link is important for the SCC to receive information about the ship and its operational environment. Without this, the operators will not have the opportunity to collect data, make decisions or take actions. As a result of this, four human failure events may occur; failures in the I, D, A phases, but also a failure in communication establishment between the SCC and the autonomous ship (Figure 4.11).

The failure to take the correct action is modeled through its own FT, as it is an interface task. The operators perform an action in the HMI, sending a signal to the autonomous ship. This can, for example, be a change of speed or heading. Thus,



a failure in the operator's actions may result in a human error but also affect the autonomous ship operation. The FT of the HFA is thus connected to both the FTs of human failure event (4.11), and to the FT of autonomous failure event, through a gate in the failure of collecting necessary data (Figure 4.5).

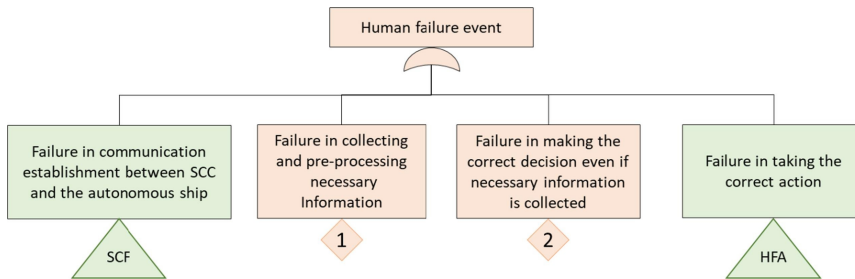


Figure 4.11: Generic fault tree for human failure event [24]

### Operator's failure in information collection and pre-processing - I phase

The operator can fail in collecting and pre-processing information because of (Figure 4.12, Table B.5 ):

- No information is received from the AS. This covers a failure in the HMI, and not the communication establishment.
- Failure in collecting correct and complete data due to a failure in the information source and the failure from the operator to realize that the information is incorrect.
- Failure in decision to collect information (Figure 4.13).
- Failure in execution to collect information (Figure 4.14).

By information sources, this includes all sources the operator could use. All of these needs to fail in order for the failure in information sources to take place. The failure in the decision to collect information may occur when the operator follows a procedure, guideline, or any other written rules as strategy and/or when the operator is following his/her knowledge. In addition, the operator may decide to collect the necessary information but fail in executing it.

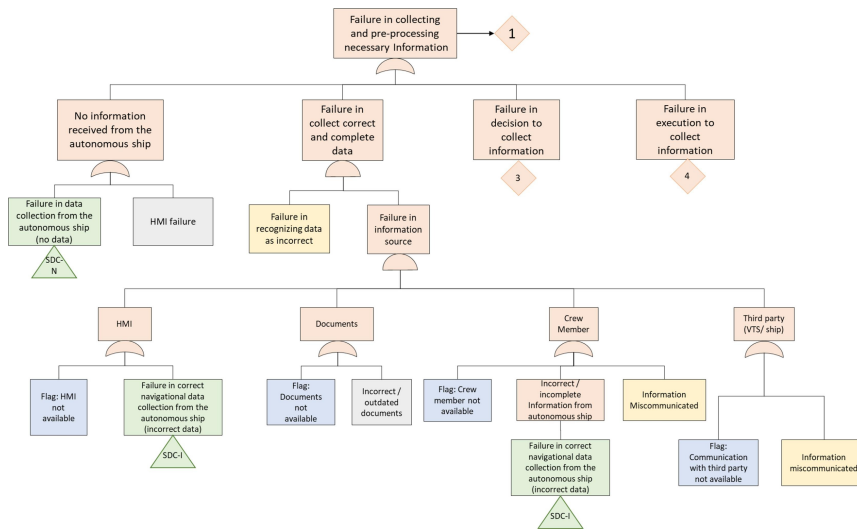


Figure 4.12: Generic fault tree for human failure event in collecting and pre-processing information [24]

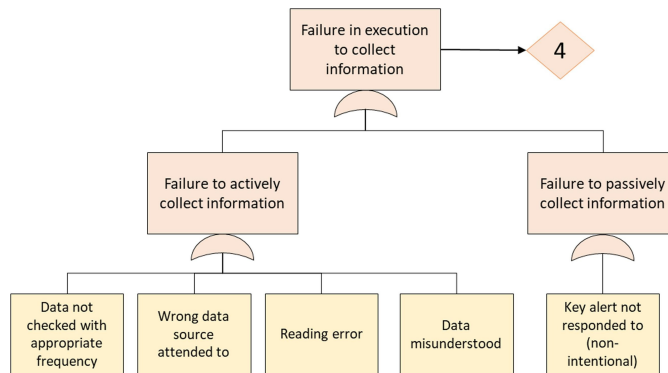


Figure 4.14: Generic fault tree for human failure event in execution to collect information [24]

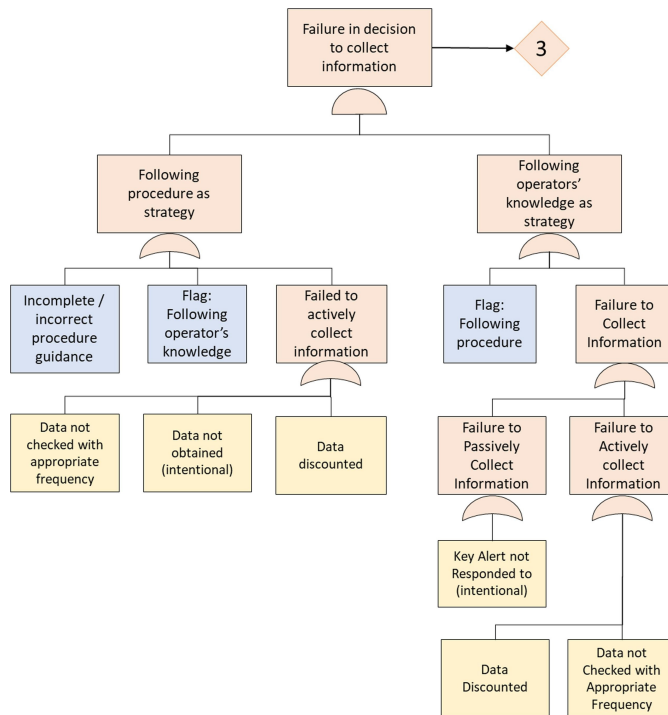


Figure 4.13: Generic fault tree for human failure event in decision to collect information [24]

### Operator's failure in situation assessment and decision making - D phase

Failure in situation assessment and decision-making may happen when the operator follows a procedure/guideline and/or when the operator relies on his/her knowledge. Procedure can be the COLREGS and local rules, but also descriptions of how the operators should interact with the HMI and the autonomous ship (Figure 4.15, Table B.6).

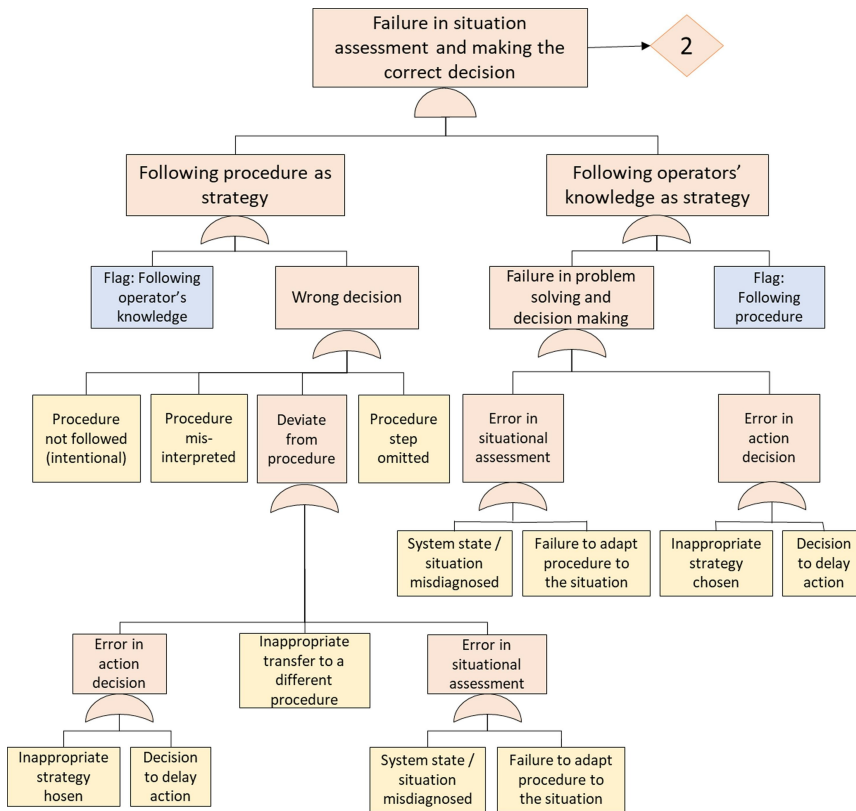


Figure 4.15: Generic fault tree for human failure event in situation assessment and decision-making [24]

### Operator's failure in action - A phase (HFA gate)

The operator may fail in execution even though having made the correct decision. Failure in the A-phase are failures in correctly performing an action that follows a correct decision. The operator may fail due to (Figure 4.16): and B.7.

- Action on the wrong component/object.
- Incorrect timing,
- Incorrect action on the correct component.

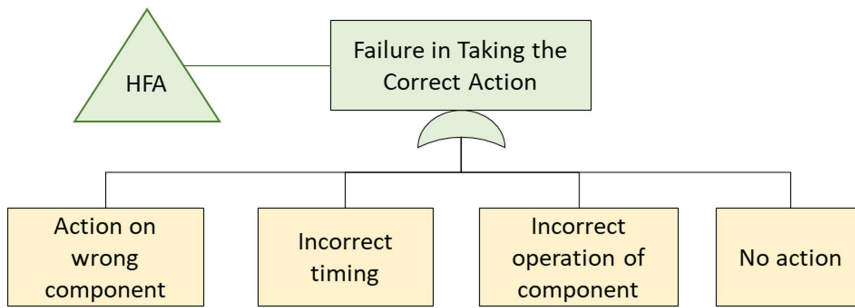


Figure 4.16: Generic fault tree for human failure event in taking the correct action (HFA) [24]

## 4.4 BBN model development

As described in the previous section, Ramos, has made fault trees related to each phase in the IDA model. The same approach will be used here, where the nodes in the Table 4.3 will be used to make three different BBNs. The nodes chosen with proposed states are taken from [40].

### 4.4.1 GeNIe software

GeNIe, a software program will be used to develop and analyze the BBNs. The software allows for graphical creation of network nodes, as well as tools for sensitivity analysis.

---

Table 4.3: Summary of PIFs with proposed states

PIFs	Proposed states
Communication	Low, adequate, high
Etiquette	Disruptive, mediocre, good
Experience	Low, medium, high
Fatigue	High, medium, low
HMI	Poor, mediocre, good
Interface design	Poor, mediocre, good
Number of vehicles per operator	High, medium, low
Procedure	Poor, adequate, good
SA	Low, medium, high
SC-mode	SC1, SC2, SC3
Task load	High, medium, low
Training	Low, adequate, high
Workload	High, medium, low

## 4.5 HCL modelling

Figure 4.17 shows how the different elements of the model will be connected. The events in the ESD serves as tasks to be completed in the CoTA and as failure events in the FTs. The CoTA describes how the task should be performed in order to obtain a successful outcome, while the FTs describe how they can go wrong. For further analysis of the failure events in the FTs related to human failures, BBNs are used.

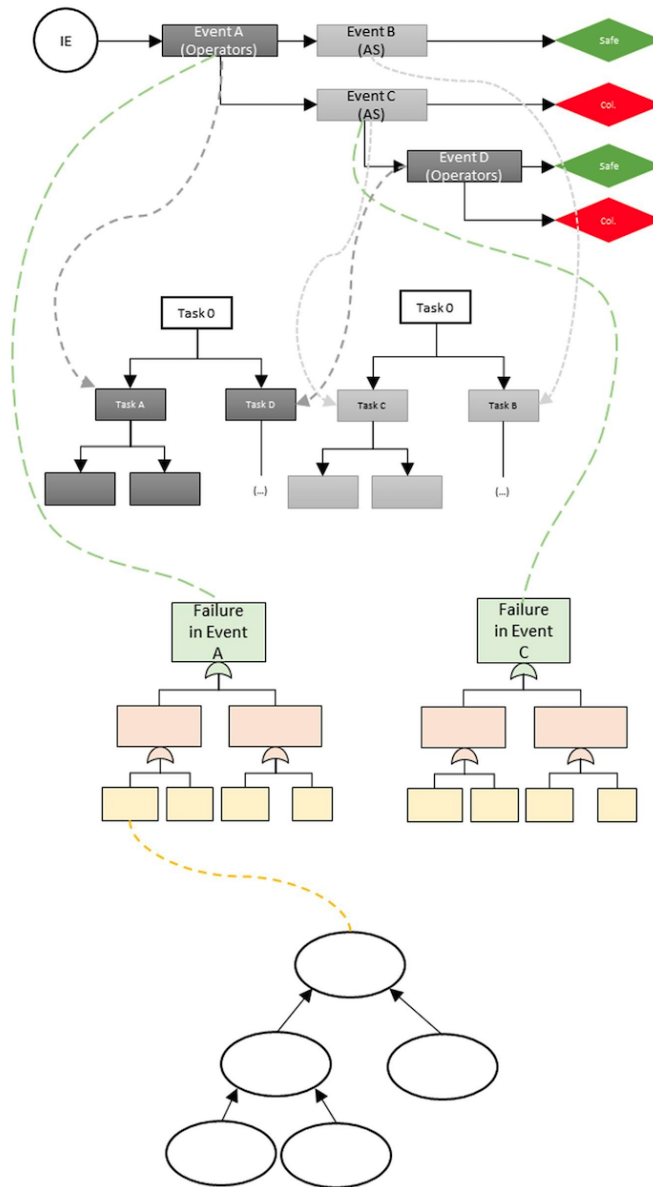


Figure 4.17: Overview of the HCL model [24]

---

## 4.6 Quantitative Analysis process

A quantitative analysis is essential as it provides a basis for evaluating the performance of the autonomous ship and the crew and the interactions. In addition, it also provides possible suggestions for improvement. The qualitative analysis framework has three layers. The chain of events represented by an event sequence diagram forms the top layer. How the different events can fail modeled with fault trees forms the second layer. Basic events related to human operator failure are quantified using a BBN, which forms the third layer.

### 4.6.1 Trilith: Integrated Risk Information System

Trilith is a software for HCL modeling and analysis. It combines Boolean logic risk analysis methods, i.e., ESD, FT, and Bayesian Belief Networks. The benefit lies in using the different tools to model hardware, software, and physical and human, organizational, and regulatory features into different domains.

### 4.6.2 BBN model quantification

The different Conditional Probability Tables (CPT) are related to the operator's failure in the different IDA-phases, information collection and pre-processing (I-Phase), situation assessment and decision making (D-Phase), and action (A-phase). The information in Chapter 3 has been used to determine the nodes relevant for each phase. In order to quantify the conditional probability tables, strength ratings associated with each phase have been developed. This method has been adapted from [44], and can be seen in tables 4.4, 4.6, 4.8, 4.10, 4.12 and 4.14.

Table 4.4: Strength rating associated for the CPT HMI

Parent state	Strength	Reasoning
Etiquette	High	According to research, the way information is presented has a significant influence on the operator [45]
Interface design	High	Physical and virtual quality of the influence the way information is perceived [46]



Table 4.6: Strength rating associated for the CPT Workload

Parent state	Strength	Reasoning
Task load	High	The workload increase with a higher task load
SC-mode	High	According to [35], SC-mode only has a marginal influence on the workload.
Number of vehicles per operator	High	Increasing the number of vehicles per operator will increase the number of tasks [47]

Table 4.8: Strength rating associated for the CPT SA

Parent state	Strength	Reasoning
HMI	High	According to research, the way information is presented has a significant influence on the operator [45]
Fatigue	Low	According to [29], fatigue can have an effect on the situational awareness, but it is not a decisive factor
Communication	Low	Influenced is assumed low, as the information mainly will be communicated through the HMI
Training	High	In order to create an operational picture of the operation, training is very important
Workload	High	According to [48], situational awareness is reduced by a high workload

Table 4.10: Strength rating associated for the CPT I-Phase

Parent state	Strength	Reasoning
HMI	High	Feedback and interaction with the system is very important [45]
Training	High	Training of the operators is very important for the operators to obtain and pre-process correct information
Experience	High	Experience is important for the operators when making decisions and using the equipment to collect information
Fatigue	Low	Fatigue can contribute to the performance of operators, but is not a decisive factor. In addition to this, fatigue should have a reduced effect when moving operations from offshore to onshore [29] [29]

Table 4.12: Strength rating associated for the CPT D-phase

Parent state	Strength	Reasoning
Procedure	High	Procedures will have a high influence in this case as the operators will follow procedures during operation
Workload	High	A high workload can significantly reduce the situational assessment by operators [48]
Training	High	Training is very important in order for the operator to get a good operational picture of the operation
Experience	High	Experience is very important for the operators to perform their tasks efficiently
Fatigue	Low	Fatigue is a contributing factor, but not a decisive one.
SA	High	The situational assessment determines the operator's picture of the operation. It is therefore assessed as highly influential, as it affects what decisions the operators make

Table 4.14: Strength rating associated for the CPT A-Phase

Parent state	Strength	Reasoning
SA(D-Phase)	High	A good situational assessment is very important for the operator to take the correct actions
Training	High	Training is very important for the operators to perform their tasks and take the correct actions
Experience	High	Experience is very important in order for the operator to operate the system efficiently.

---

## System description and hazard identification

### 5.1 Details about the unmanned autonomous ship

A case study is currently ongoing and will be the subject of the risk model developed in this thesis. The system under consideration is a simplified model of a real coastal cargo ship. The main particulars for the ship can be seen in table 5.1. The ship will transport goods along the coast of Norway and can be considered a reference ship for future autonomous cargo ships, with no crew on board, but with human supervisors monitoring and able to take over control from an onshore control center. The existing ship is equipped with a hybrid machinery system, which will be further explained in section 5.2.1.

Table 5.1: Main particulars of the unmanned autonomous vessel (based on information from [49])

Parameter	Symbol	Value
Length	$L_{oa}$	74,70m
Breadth	B	13,6m
Depth	D	5m
Dead Weight tonnage	DWT	1450t
LNG container	$m^3$	110
Cargo tanker	$m^3$	2030

### 5.2 Control system

The concept of an unmanned ship requires a complex network of monitoring and control systems. [44] visualizes the most important systems and their interactions



There are three different modes in this relevant for this; The ship control mode (SC-mode) determines the interactions between the ROC and the ANS system. Ship Operation mode (SO-mode) describes which type of motion control being performed and the. Lastly, there is the Machinery System Operational mode (MSO-mode).

Possible SC-modes:

- Autonomous control
- Supervised autonomous control
- Remote control

Possible SO-modes for the autonomous vessels:

- **Transit mode:** The ship follows a preplanned route and may deviate from the route, i.e., to avoid obstacles and re-plan the route.
- **Maneuvering mode:** The ship position and heading are tracking trajectories, and the speed is low.
- **DP mode:** Station keeping through DP is a particular case for the SO-mode "Maneuvering," in which the heading and position setpoints remain constant.

The different MSO-modes are describes in subsection 5.2.1.

### 5.2.1 Machinery system

The machinery system consists of a power management system (PMS) and a set of power sources, actuators, a hybrid shaft generator (HSG), and an electrical distribution system. The main engine (ME) is LNG-fueled and is connected to the main propeller through a gearbox. The gearbox is also connected to a hybrid shaft generator (HSG) which can function both as a generator, providing electrical power to a DC-bus, and as a motor, providing mechanical power to the propeller shaft from the DC-bus. There are two AC-buses that can be connected and can feed the DC-bus. Each AC-bus is connected to an auxiliary diesel generator (Aux 1 and Aux 2), and AC-bus 2 is connected to the hotel loads and deck loads. The DC-bus power two tunnel thrusters (TT1 and TT2). In addition, an emergency generator and an emergency AC distribution are connected to the second AC bus. Figure 5.2 shows a single-line diagram of the machinery system.

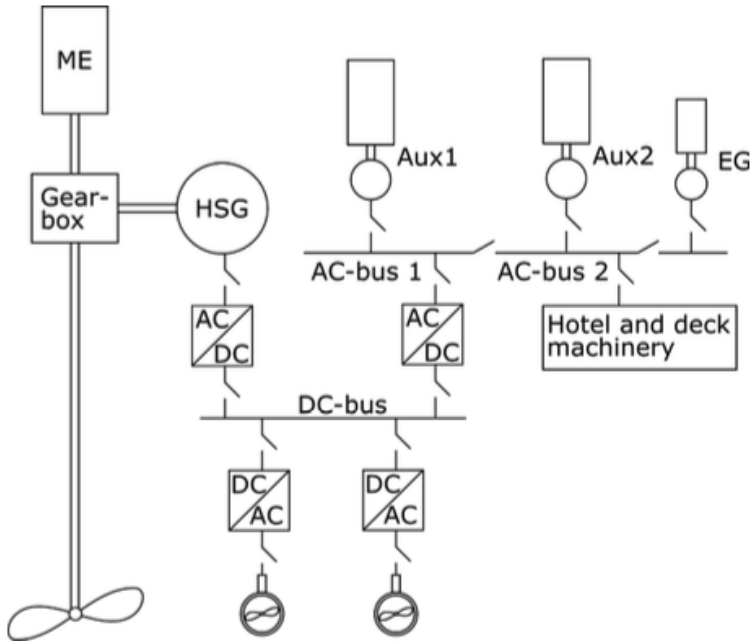


Figure 5.2: The components of the machinery system [44]

The machinery system can be operated in the following three machinery system operating modes (MSO-modes) during normal sailing [50]:

- **MSO-mode 1 - Power Take Out (PTO):** The main engine is responsible for both the main propulsion and the electrical loads of the ship. Power is distributed to the main propeller and the electrical system through the gear-box. In this operating mode, the hybrid shaft generator (HSG) is operated as a generator, transforming mechanical power from the main engine shaft to electrical power on the main electrical bus.
- **MSO-mode 2 - Mechanical (MEC):** The main engine is responsible for the propulsion, while one of the diesel generators is used for electrical power generation for the electrical loads of the ship. In this case, the HSG is offline.
- **MSO-mode 3 - Power Take In (PTI):** The main engine is offline while both diesel generators are online and provides power for both the electrical loads of the ship and propulsion. The HSG is operated as an electrical motor, providing torque for the propeller shaft through the gearbox.

It is assumed that the AMMS determines the MSO-mode and that the ANS determines the SO-mode for the system. The ROC can override both.

The control action "Thrust capacity reservation" from the ANS to the AMMS in figure 5.1, is how the ANS can communicate future capacity needs to the AMMS



based on the situation at hand. The ANS also has the capability of requesting from the AMMS that the machinery system should be configured to obtain a certain level of robustness, which is defined as the machinery system's ability to withstand abnormal or unexpected events or conditions without losing its ability to make the ship follow the motion control objectives.

## 5.3 External hazards

External hazards that the ship may experience along the coast of Norway can be:

- Other ships or objects
- Narrow fairways
- Harsh weather conditions
- Jamming or spoofing of AIS and GPS signals

Only collision with other ships will be considered in this report. As the autonomous ship is to be transporting fish feed to fish farms along the coast of Norway, there are many potential collision candidates. Leisure craft, tankers, and other service vessels are potential collision candidates to be aware of.

Jamming or spoofing of the AIS and GPS signals is also something to aware of and may lead to errors in navigation and communication.

## 5.4 Internal hazards

### 5.4.1 System description

In this thesis the human operators at the SCC is considered as a part of the internal system. In order to identify internal hazards, the system is broken down into subsystems. This is based on the control structure diagram in Figure 5.1:

- Shore-control-center
- Communication, monitoring and control system
- Navigation system: radar, satellite, AIS etc.
- Machinery system
- Propulsion system: main engine, propeller, auxiliary engines etc.
- Tanks and cargo holds: cargo, ballast, bunker (fuel, lube oil)

### 5.4.2 Communication, monitoring and control

The communication, monitoring, and control system have already been briefly explained in section 5.2. The system is characterized by many interactions between

the system components as well as with other components that lie outside of the boundaries of this system, such as the SCC. Its most important entities are listed in Table 5.2 together with their functions.

Table 5.2: Components of communication, monitoring and control system (based on information from [44])

Functional entity	function
Remote Operating Center (ROC)	monitoring and supervising Remote control (dependent on SC-mode) Plan journeys
Autonomous Navigation System (ANS)	Collision avoidance Docking Route planing Weather states Data collection from AMMS and IAS
Autonomous Machinery Management System AMMS (AMMS)	Controls states and capacity of machinery system
Intelligent Awareness System (IAS)	Navigational states of obstacles Classification of objects Weather lookout
Machinery system	Control forces

Table 5.3 shows the most important means of communication and navigation that can be found onboard the ship.

Table 5.3: Ship information systems (based on information from [51])

System	Component
Navigation	Radar
	AIS
	CCTV
	Inertial Measurement Unit (IMU)
	Speed log
	ARPA
	Compass
	Echo Sonar
Ship to shore communication	DSC
	4G
	GALILEO
	VHF
Satellite systems	Satellite equipment
	Ship station equipment
	Satellite control equipment
	Ground station equipment

A significant difference between an autonomous ship and a conventional vessel is the decision-making process. While the ship information systems are used as guidance for the master's navigational decisions at a conventional ship, they are used as a basis for decision-making in an autonomous vessel.

### 5.4.3 Machinery system

The use-case ship has a propulsion system which is described in subsection 5.2.1. Table 5.5 gives an overview of the most important elements of the propulsion and power generation systems.

As previously described, the engine on-board is LNG-fueled which can be related to several potential different hazards.

LNG is an eco-friendly bunker fuel with many advantages, like decreasing the emissions of  $SO_x$  and particulate materials (PM) and meeting the international maritime organization (IMO) MARPOL Annex VI requirements on  $NO_x$  emissions, and economic benefits compared to heavy fuel oil (HFO) [53].

LNG is neither corrosive nor toxic [54], so it will not pose as a threat as long as it is not ignited. On the other hand, the leakage of LNG fuel serves as a threat to the safety of LNG-fueled vessels due to its inflammable and explosive characteristics. Sources of ignition could be heat, sparks, and flames. Other sources

---

Table 5.5: Machinery system (based on information from [44], [52])

Component	Functional purpose
Main engine	Provide power to turn the propeller
Fuel system	Provide fuel to run the main engine
Cooling water system	Cooling of engine parts
Lubrication oil system	Lubrication of engine parts
Propeller	Generate thrust
Propeller shaft	Transmit power
Auxiliary engines	Generate power
Emergency generator	Generate power
Hybrid shaft generator	Generate electrical and mechanical power
Gearbox	Control power output
Tunnel thrusters	Generate thrust

of ignition could be static electricity and mechanical/electrical equipment such as the engine.

A LNG-fueled power system consists of numerous pipes, flange connectives, and valves. According to [54], the leakage of LNG occurs in these places, as well as in the storage tank itself. [53] has also identified possible causes for a LNG leak which can be breach or crack due to fatigue, among others.

## HCL development

The model has been developed in the following manner:

1. The event sequence diagram has been constructed with the method described in section 4.1
2. Fault trees has been constructed using the CoTAs in Figure 4.2 and 4.3, and the applicable branches from the generic fault trees described in subsection 4.3.1.
3. The BBN has been developed using the method described in section 4.4

The event sequence diagram describes how the scenario unfolds from the initiating event to an end state which is either *No collision* or *Collision*. The purpose of the fault trees is to calculate the occurrence probability of the events, while the BBN's on the other hand, serves to calculate the occurrence probability of the basic events related to human operators.

### 6.1 Assumptions

The model has been developed with the following assumptions in mind:

- Many of the intermediate failure events in the fault trees are related to software and hardware failures. Especially failures related to the decision phase as this is based on software[24]. In this case, the relevant subsystems in the control system have been identified. I.e., the ANS is, among others, responsible for route planning. A failure in making the correct decision on applicable rules and routes will therefore result from an ANS failure.
- The collision avoidance plan generated by the AS will either be labeled as *No plan* or *successful*. This implies that when the operator decides on operational

---

mode, a "wrong" action will be to remotely control the AS if it has already generated a successful plan.

- The initiating event will not cause changes in the fault trees or the BBN's.

## 6.2 Scenario development

The ESD has been developed with the following assumptions in mind:

1. The ship is in SC mode Supervised autonomous control. This means that the AS is unmanned during all phases of the operation, but is supervised by a human operator in the SCC.
2. The ship operation mode is Transit mode. This means that the AS is following a pre-planned route, but may deviate to avoid obstacles/other ships and re-plan the route.
3. The initiating event is set to be AS on collision course. This can be either head-on, overtaking or crossing collision.
4. The collision candidate (CC) is another vessel.
5. The crew on the SCC has the possibility to establish direct contact with the CC.
6. The AS is main responsible for generating a collision avoidance plan and avoiding collision
7. The AS can send a sonorous and/or visual alarm to the SCC in case it detects another vessel as a CC.
8. The crew on the SCC consists of teams monitoring several vessels at a time.
9. There are two different possible end states: "No collision" and "Collision". In the framework, three methods are proposed; Collision, no collision and safety. In this cases safety and no collision has been merged into the same end state.
10. The Human operators will follow procedure as strategy.

## 6.3 ESD construction

The ESD flowchart questions with answers based on the case study are presented in Table 6.1. The resulting ESDs are presented in Figure 6.1, 6.2 and 6.3. The ESD in this thesis is the same as the one in [24], except from the details described in the scenario development.

Table 6.1: Scenario ESD questions with answers

Number	Question	Answer
1	Who is the primary responsible for detection of the CC?	AS
2	Can the operators detect the CC from the SCC?	Yes
3	Can the operators remotely control the AS from the SCC	Yes
4	Can the operators use extreme measures to avoid collision	No
5	Who is primary responsible for developing collision avoidance plan?	AS
6	Is there an alarm in the SCC warning about the CC, and are they informed on the plan for collision avoidance?	Yes
7	Is the collision candidate a ship?	Yes
8	Is there enough time available to re-plan and implement a new plan to collision avoidance	No

The resulting ESDs are shown in Figures 6.1, 6.2 and 6.3. The initiating event is that the autonomous ship is on a collision course. This includes overtaking-, head-on- and crossing collision. ESDs 6.2 and 6.3 are connected to the ESD in Figure 6.1 through transfer gates (hereby addressed as Transfer 1 and Transfer 2). According to the scenario, it will move to transfer 1 if the autonomous ship does not detect the collision candidate, which is another vessel, in this case. The scenario will move to transfer 2 if the operators decide to take manual control over the ship. The events will be described more in detail in the next subsection.

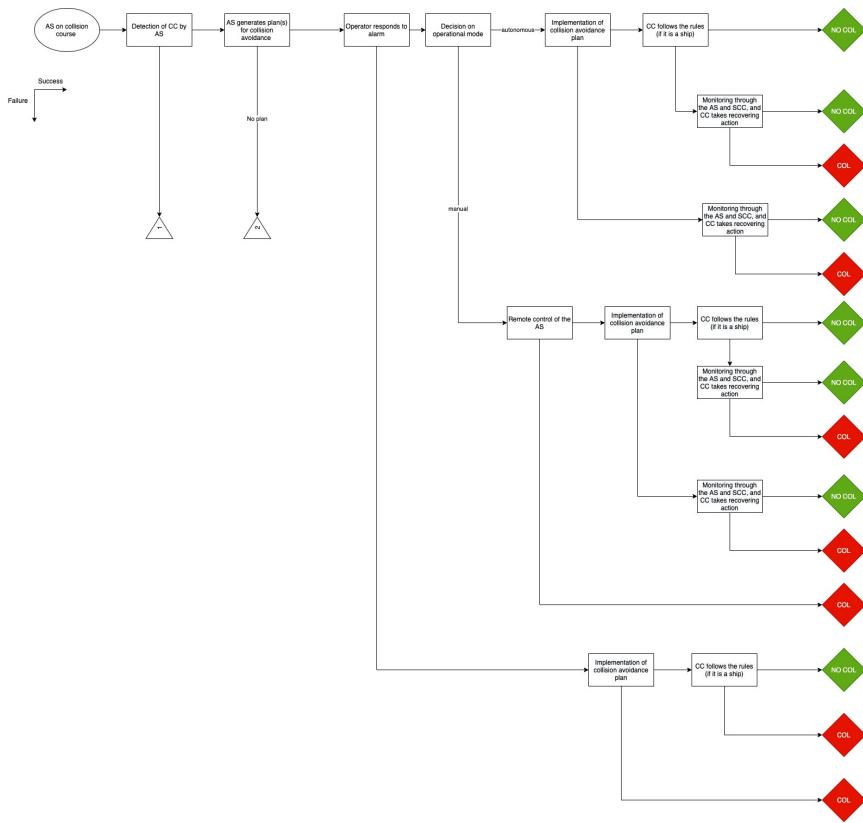


Figure 6.1: Case study Event Sequence Diagram



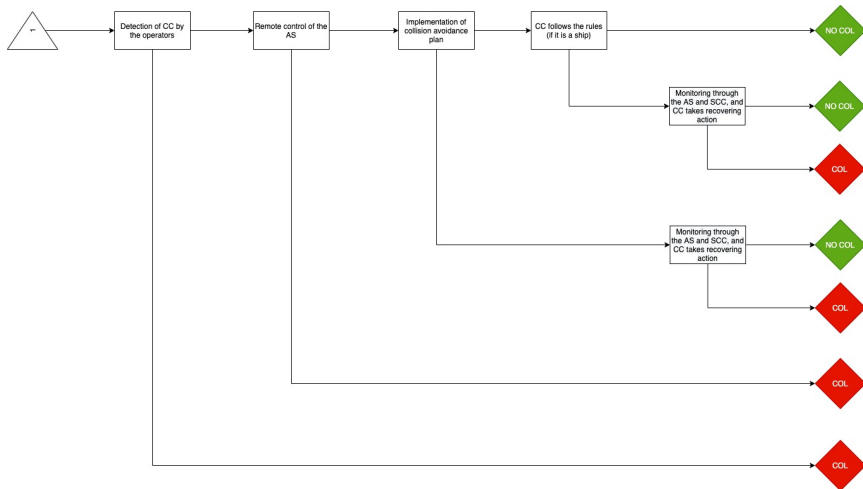


Figure 6.2: Case study Event Sequence Diagram - Transfer Gate: AS fails to detect collision candidate

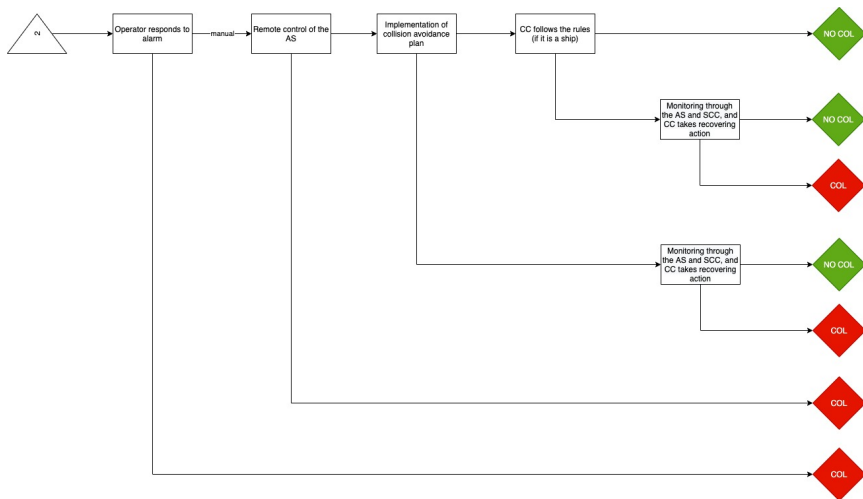


Figure 6.3: Case study Event Sequence Diagram - Transfer Gate: No collision avoidance plan

---

## 6.4 Fault tree construction

As previously described, the fault trees are based on the CoTA and the applicable branches from the generic fault trees. The CoTA explains how tasks can succeed in the case of both the AS and the human operator. The goal of the fault tree will thus be to determine how these tasks can fail. Basic events have been reached using a top-down approach until basic events with known probabilities are reached. When it comes to maintenance, which is a combination of both technical and human failure, it is assumed that maintenance is not possible during the voyage. To further develop the applicable branches, relevant literature has been used. Fault trees developed in the master thesis by Jensen: *Hazard and Risk Assessment of Unmanned Bulk Carriers on the High Seas*[8] which is a risk assessment of the MUNIN project, has also been used when applicable.

From the ESD and CoTA, the current failures applies for the autonomous vessel:

- Failure in data collection (parallel task)
- Failure in communication (parallel task)
- Failure to detect collision candidate
- Failure to generate collision avoidance route
- Failure to implement and execute collision avoidance plan

For the human operators:

- Failure to respond to alarm
- Failure to decide on operational mode
- Failure to take remote control of the autonomous vessel
- Failure to implement and execute collision avoidance route
- Failure to monitor safe execution

### 6.4.1 Fault trees for the autonomous vessel

Several of the intermediate events in the following fault trees are connected to the transfer gate *ANS failure*. ANS is responsible for the decision-making in the autonomous ship and data collection from the other functional entities as shown in Figure 5.1. The fault tree is further connected to the fault trees *hardware failure* and *software failure*. This is shown in Figure 6.4. The FTs for hardware- and software failure are based on [8] (fault trees figure A.12). Software failure can happen due to incorrect programming, random breakdown, or hacking. Hardware can fail due to a failure of the computer. Redundancy in the ANS is accounted for by an AND-gate and the intermediate events A and B.

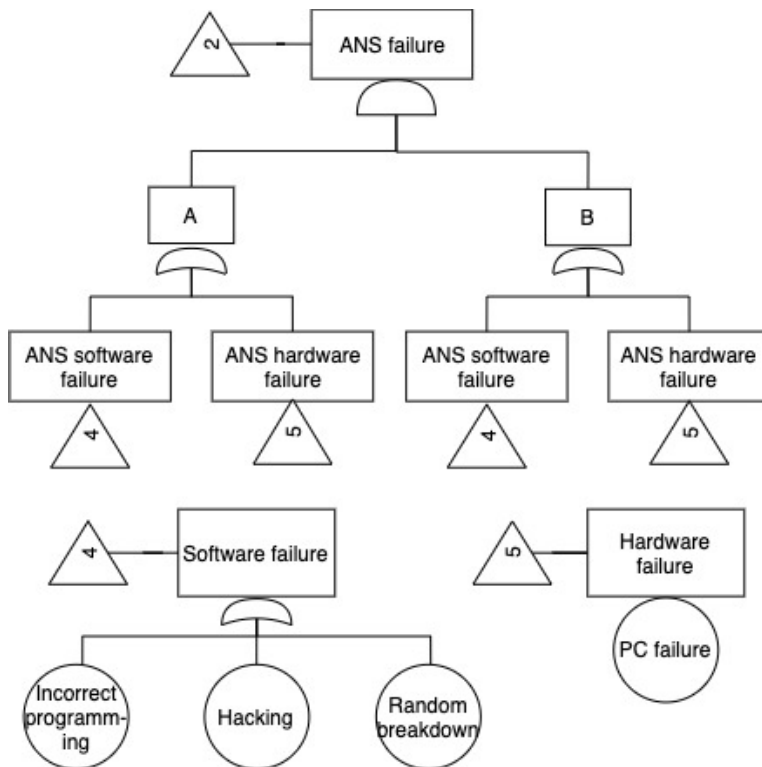


Figure 6.4: Fault trees for the failure events: ANS failure, software failure and hardware failure

---

## Autonomous failure event: Failure in data collection

The generic fault trees for how the autonomous ship can fail during data collection have been modified to fit the actual system and scenario. The fault trees have already been described in Section 4.3.1. The branch for the intermediate events *AIS failure* and *CCTV failure* is based on the analysis by Jensen ([8], fault tree in figure 7.11). Even though the fault trees are similar, there are some differences. Regarding sensor failure, there is a difference between jamming and spoofing. While jamming can lead to no data being collected from the AIS, spoofing can lead to false signals KILDE. Regarding the CCTV, the complete failure can be due to hardware failure or due to damages from waves/wind. Bad visibility can lead to inadequate images. There is also a difference in the intermediate failure *Failure in the information collection support system*. For the FT *no data* this can occur due to a power supply failure(transfer gate7, Figure 6.5) or a failure in the network. Power supply failure can occur due to a switchboard without power or if the generator sets generate no power. The intermediate event *switchboard without power* is derived from [55](fault tree page 114), while the generator set failure is based on the system description. In the FT *incorrect data* the basic event *PMS* failure is included. This does not necessarily lead to a complete blackout but can lead to some systems losing power due to overloading the system [56].

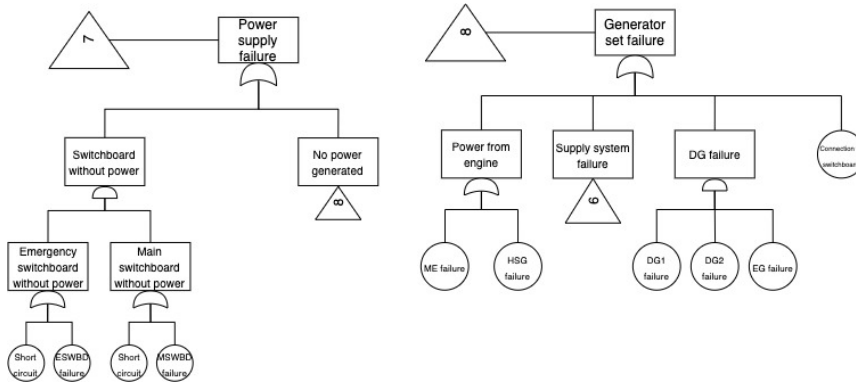


Figure 6.5: Fault tree for with the top events power supply and generator set failure

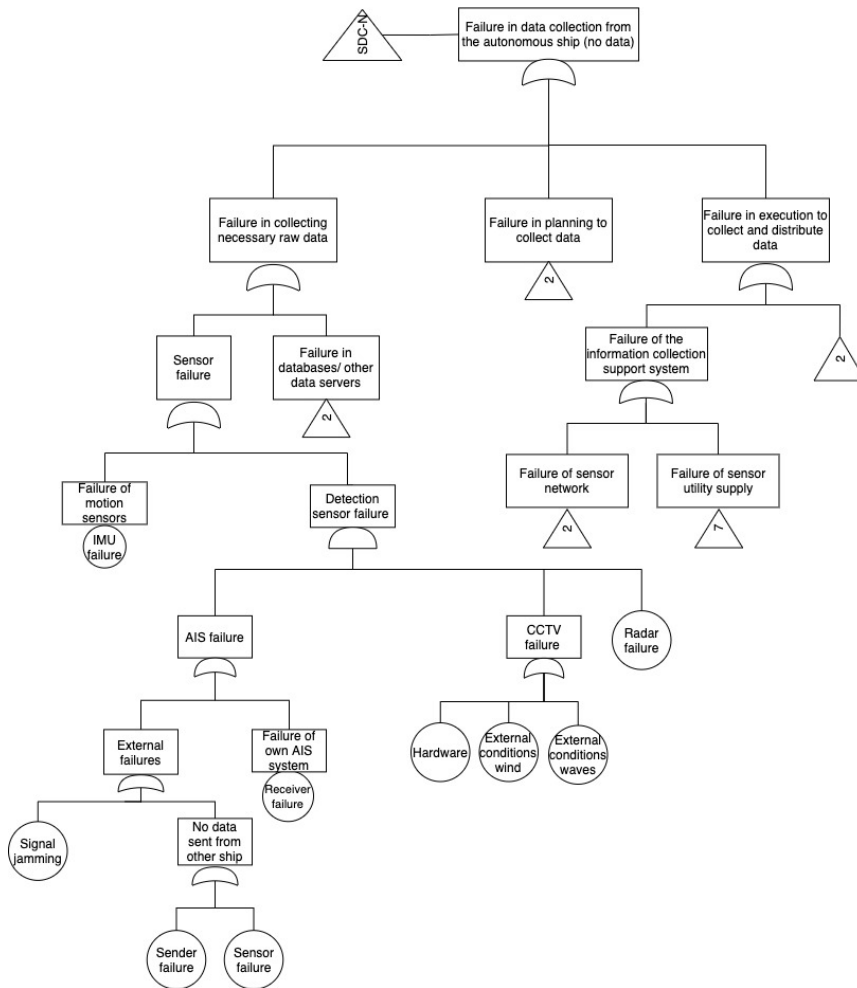


Figure 6.6: Fault tree for the AS failure event: Failure in data collection - no data (SDC-N)

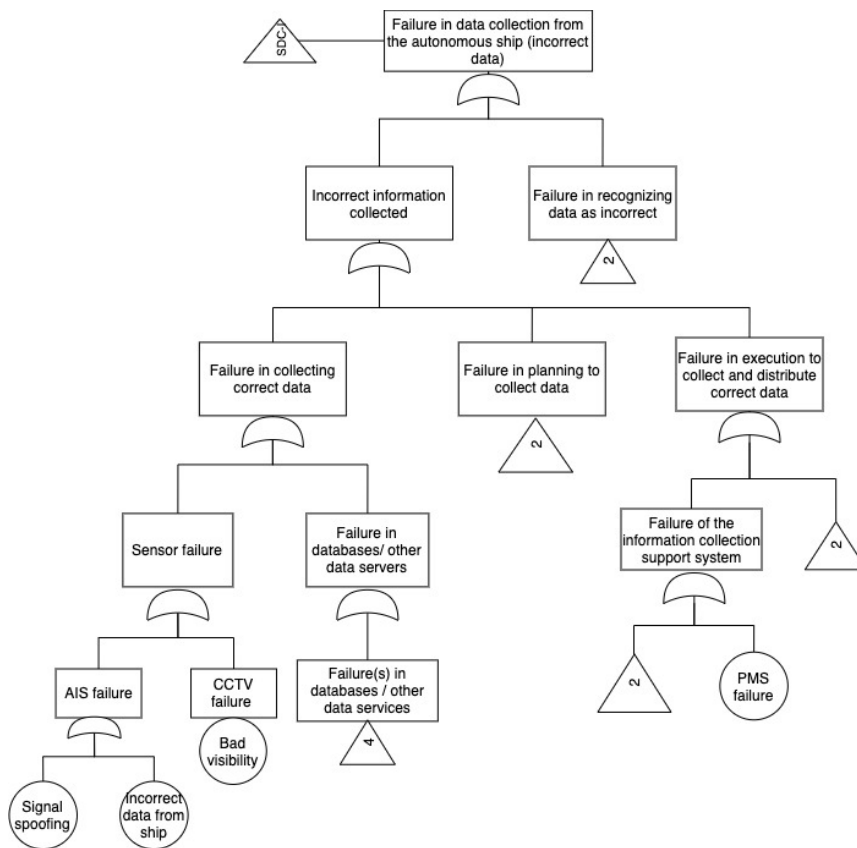


Figure 6.7: Fault tree for the AS failure event: Failure in data collection - incorrect data (SDC-I)

### Failure in communication establishment between the SCC and the autonomous ship

The FT *Failure in communication establishment between the SCC and the autonomous ship* (Figure 6.8) has been developed by adjusting the generic fault tree shown in Figure 4.8 to fit the system. The intermediate events can all fail due to a failure in the ANS. Further, the intermediate event failure in communication equipment can fail due to the satellite ground station's failure or a failure in the satellite stations onboard the ship. The fault tree for the satellite stations is based on [8](fault tree Figure A.13) and can fail due to damage on the antenna or the antenna motor (Figure 6.9).

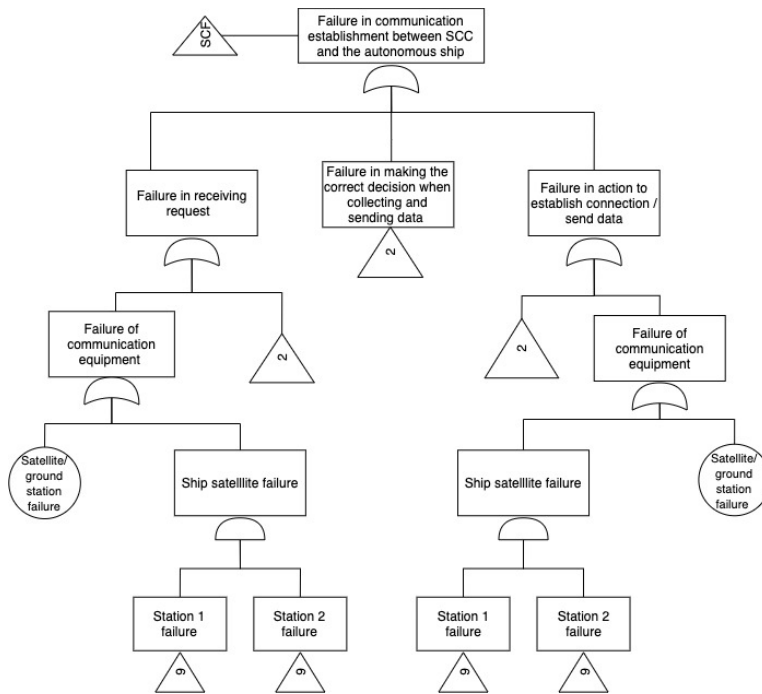


Figure 6.8: Fault tree for the AS failure event: Failure in communication establishment

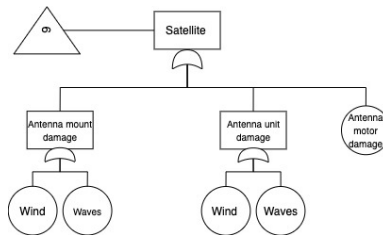


Figure 6.9: Fault tree with the top event satellite failure [8]

---

### Autonomous failure event: Failure to detect collision candidate

The fault tree with the top event *Autonomous failure event: Failure to detect collision candidate* is shown in Figure 6.10.

A failure in this event may be due to a failure in collecting necessary data, a failure in making the correct decision based on the collected data, or failing to notify the SCC about the CC. All IDA phases are included in the FT, and the intermediate events all end up in transfer gates. The ANS is responsible for making the correct decision on the obstacle status. When it comes to notifying the SCC, timing is essential. Too late will lead to the operators not being able to respond due to lack of time.

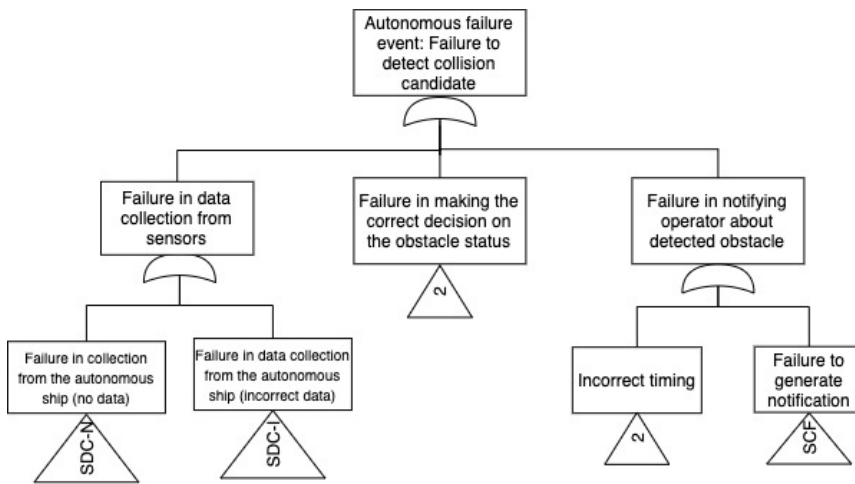


Figure 6.10: Fault tree for the AS failure event: Failure to detect collision candidate

### Autonomous failure event: Failure to plan collision avoidance route

The AS can fail to plan the collision avoidance route by either failing to make the correct decision on applicable rules and routes or as indicated in the CoTA, informing the operator about the planned strategy. The ANS is responsible for making the decision about applicable rules and routes. The ARPA is also a device that plots routes to avoid obstacles or other ships [57], which is why this is a basic event. Regarding informing the operator about the strategy, this relies on establishing communication between the AS and the SS and the ANS. The fault tree is shown in figure Figure 6.11.



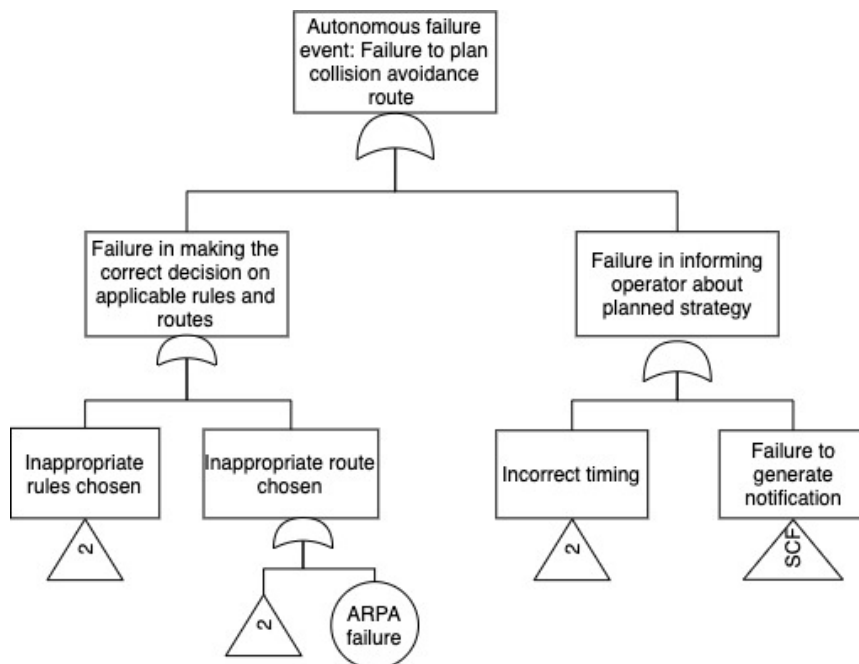


Figure 6.11: Fault tree for the AS failure event: Failure to plan collision avoidance route

### AS failure event: Failure to implement and execute collision avoidance plan

There are two versions of this fault tree depending on whether the operators take remote control of the ship or not. This is shown in the ESDs.

Figure 6.12 shows the fault tree with the top event *Autonomous failure event: Failure to implement and execute collision avoidance plan*. A failure in this event can happen due to a failure in deciding what input to send to the machinery or in sending the input to the machinery. As described in the system description, the ANS is responsible for deciding on the input, while the AMMS is responsible for performing it. The fault tree for the AMMS is modeled in the exact same way as for the ANS. Regarding the execution of the collision avoidance plan, it is also crucial that the propulsion system, or backup propulsion system is working. As described in SEC5.2.1, the ship has three different machinery modes; PTO, MEC, and PTI. In order for the propulsion system to fail, all of these have to fail. According to [50], loss of propulsion power in PTO mode can only happen as a result of the main engine failure. This also applies to the MEC mode. In PTI mode, two diesel generators are responsible for the propulsion power. It is assumed that one DG can provide enough power in case one of them should fail. Hence, to get a loss in propulsion power, both the DGs and the HSG must fail. The intermediate failure

event *failures of steering system* and *supply system failure* (Figure 6.13 is adapted from [8] (fault tree figures A.8 and A.9) . Failure modes for the LNG engine are derived from [53].

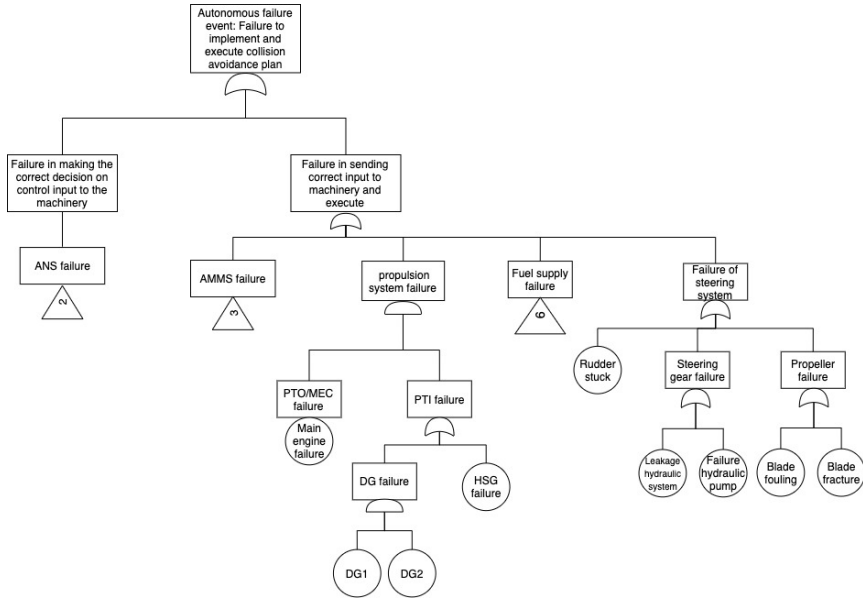


Figure 6.12: Fault tree for the AS failure event: Failure to implement and execute collision avoidance plan

If the operators decide to take remote control over the ship, the intermediate events *Failure in making the correct decision on control input to the machinery* and *Failure in sending correct input to machinery and execute* will change. Instead of this being a task for the ANS and AMMS, it will now have to be performed by the operators in the SCC. The changes are visualized in Figure 6.14.

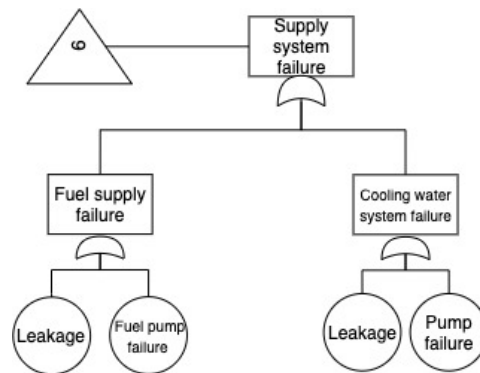


Figure 6.13: Fault tree with the top event supply system failure [8]

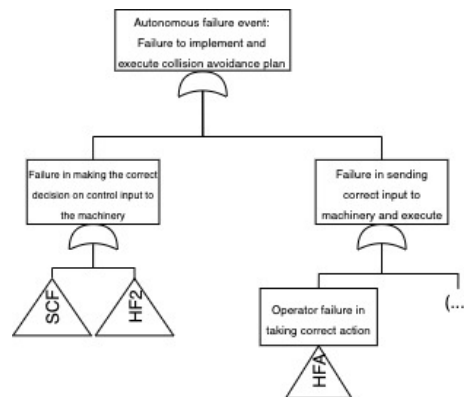


Figure 6.14: Fault tree for the AS failure event: Failure to implement and execute collision avoidance plan by the operator

### 6.4.2 Fault trees for human operators

The fault trees for the human operator events are developed based on the CoTA and by using the applicable paths of the generic FTs described in Section 4.3.1. The FTs have not been changed much. However, according to the scenario, the operators are supposed to follow procedure as strategy. The fault tree with the top event *Failure in communication establishment between the SCC and the AS* is also connected to all of the FTs. Without communication between the ship and the operators, the operators will not be able to take action or collect information from the ship. The final FTs for the human operator events *Failure in collecting and pre-processing necessary information*, *Failure in situation assessment and making the correct decision*, *Failure in decision to collect information*, *Failure in execution to collect information* and *Failure in taking the correct action* can be found in Appendix A.

---

### Human failure event: Failure to detect collision candidate

The fault tree with the top event *Failure to detect collision candidate* is shown in Figure 6.15 . Two transfer gates serve as a connection to other fault trees: *Failure in communication establishment between SCC and the autonomous ship* and *Failure in pre-processing necessary information*. This event concerns the human operator detecting the collision candidate in case the AS fails to do so. In order to do so, the human operator needs to have continuous communication establishment with the AS as well as being able to collect and pre-process the information, so s/he can detect potential collision candidates.

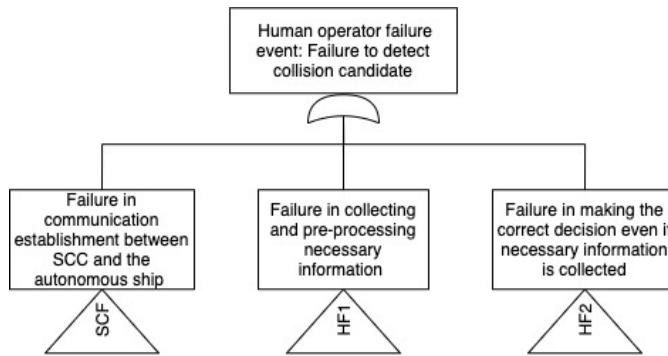


Figure 6.15: Fault tree for the Human Operator failure event: Failure to detect collision candidate

### Human failure event: Failure to respond to alarm

Figure 6.16 shows the fault tree with the top event *Failure to respond to alarm*. The event concerns the operator responding to an alarm sent by the AS, and involves both visualization and understanding of its source. I.e., the operator must understand that it concerns a potential collision and the identification of a potential collision object. The fault tree is connected to three transfer gates with the top event, which further explains how the operator could fail: *Failure in communication establishment between the SCC and the autonomous ship*, *Failure in the collection and pre-processing necessary information* and *Failure in making the correct decision even if necessary information is collected*.

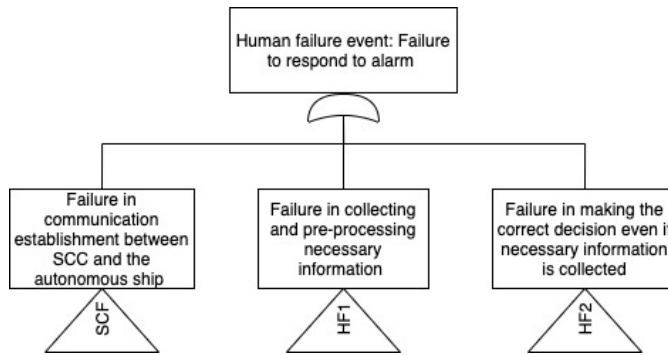


Figure 6.16: Fault tree for the Human Operator failure event: Failure to respond to alarm

### Human failure event: Failure to decide on operational mode

The fault tree with the top event *Failure to decide on operational mode* is shown in Figure 6.17. This event is related to whether the SCC should take manual control over the AS or not and has thus, according to Ramos[16], two outcomes, namely autonomous- or manual remote control. However, as mentioned, the outcome of the event *AS generates plan for collision avoidance* only has two different outcomes; no plan or successful plan. In this event, the operator should already be aware of the CC and the plan generated. If the plan generated by the AS is successful, the operator would be wrong to decide on manual remote control. For the sake of this thesis, a failure in deciding operational mode would therefore be to decide on manual control of the AS. The operator can fail by either failing to establish a connection with the AS, fail to collect and pre-process information or fail in situation assessment and making the correct decision.

### Human failure event: Failure to remotely control AS to safe path

Figure 6.18 shows the fault tree with the top event *Failure to remotely control AS to safe path*. This event can fail if the operator fails in taking the correct action or

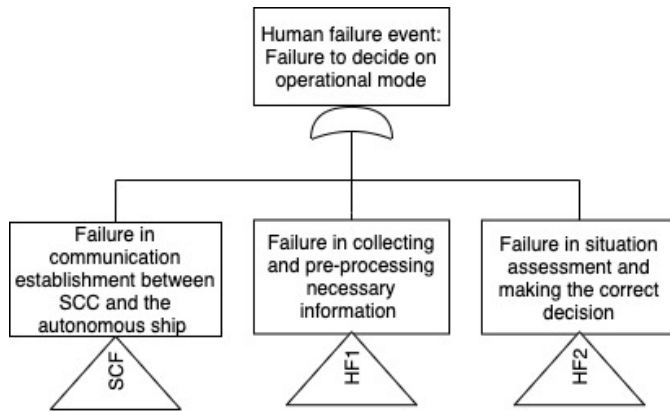


Figure 6.17: Fault tree for the Human Operator failure event: Failure to decide on operational mode

fails to correctly assess the situation and make the correct decisions. This event is only relevant if the operator has decided to operate the AS manually.

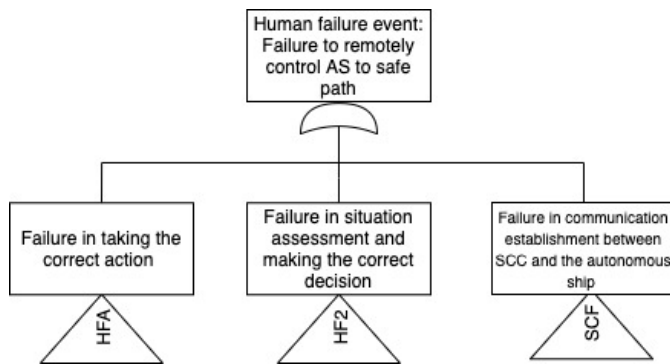


Figure 6.18: Fault tree for the Human Operator failure event: Failure to remotely control AS to safe path

**Human/AS failure event: Failure to monitor safe execution**

This event concerns the operators in the SCC to monitor through the AS and identify if the maneuvers taken by the AS are sufficient to avoid a collision. This involves both monitoring the route of the AS and the CC. In the CoTA, this event is assigned to both the AS and the operators. is shown in Figure 6.19. If they are not sufficient, the operator can warn the CC.

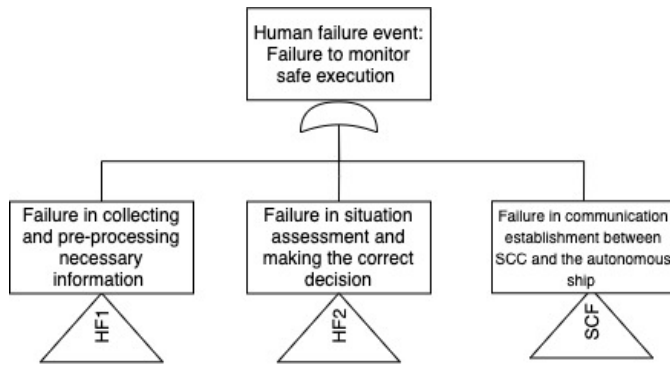


Figure 6.19: Fault tree for the Human Operator failure event: Failure to monitor safe execution

---

## 6.5 BBN construction

Figure 6.20, 6.21 and 6.22, shows the BBNs developed for the I-phase, D-phase and A-phase respectively. The connection of the nodes has already been explained in the strength rating tables in the previous chapter.

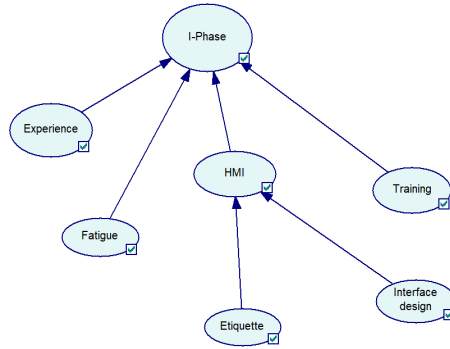


Figure 6.20: BBN for I-Phase

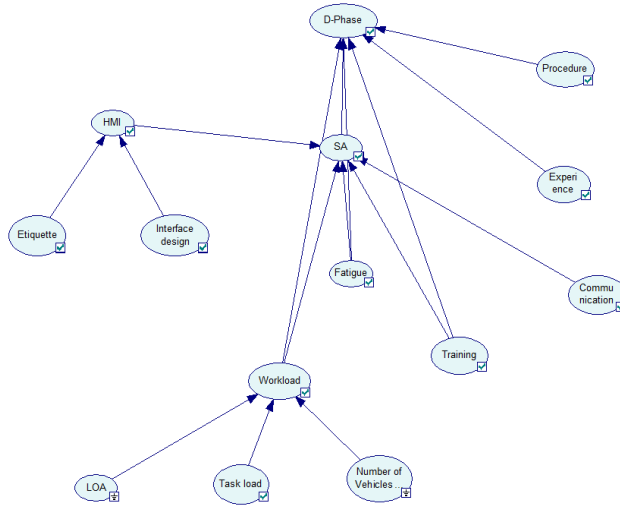


Figure 6.21: BBN for D-Phase



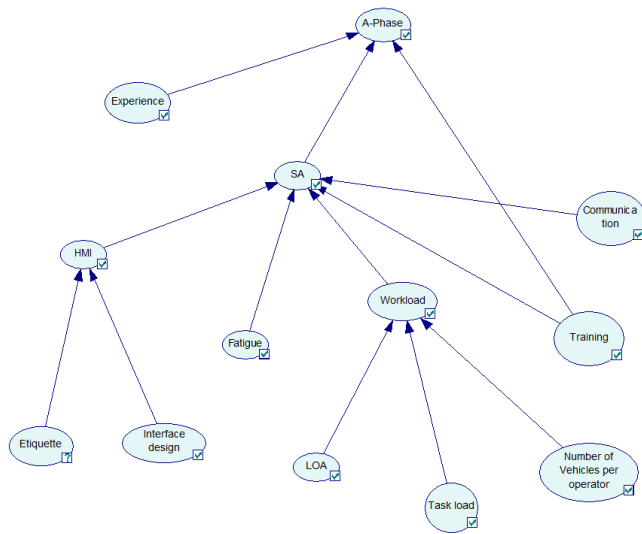


Figure 6.22: BBN for A-Phase

---

## Quantitative assessment

### 7.1 Voyage route and travel time

The use cape ship to be evaluated is operated along the coast of Norway. The ship has several stops along the way, unloading fish food, but in order to limit the scope, this thesis will only focus on the voyage south, after unloading fish food, from Brønnøysund to Kristiansund. The details can be found in Table 7.1

Table 7.1: The autonomous voyage

point	coordinates
Start	N65°28'21.63 E012°12'12.47
End	N63°06'51.25 E007°44'59.65

The route was created with Marinetraffic, and the vessel will travel at a constant speed along the route. The maximum speed of the vessel is 15kn [49], but a speed of 14kn is more realistic. The total distance sailed between Brønnøysund and Kristiansund is 195,7nm, yielding a total number of voyage days:

$$T_{\text{voyage}} = \frac{1}{24h/\text{days}} \cdot \frac{195,7nm}{14nm/h} = 0.58\text{days} \quad (7.1.1)$$

For this case, it is assumed that the vessels makes this trip two times a week when it's operational. According to [58], 270 sailing days can be assumed for one year. This means that the vessel will be able to sail  $2\text{times}/\text{week} \cdot 52\text{weeks} \cdot \frac{270\text{days}/\text{year}}{356\text{days}/\text{year}} = 76.93 \approx 77$  trips each year.



Figure 7.1: Voyage route for the autonomous ship

## 7.2 BBN evaluation

The process of quantifying the different CPTs, is adapted from [40], which is adapted and simplified from [59]. This process involves defining a template used for CPT elicitation. Table 7.2 shows the CPT template used for the IDA nodes, while Table 7.4 shows the CPT templates for the assessment of the child nodes.

Table 7.2: CPT template for building the CPTs for I-Phase, D-Phase and A-Phase [40]

Child state	Parent state	
Low	Inadequate	0.90
	Adequate	0.10
Medium	Inadequate	0.10
	Adequate	0.90
High	Inadequate	0.01
	Adequate	0.99

Table 7.4: Discretized CPT templates for low and high strength of influence. Worst, intermediate and best is a generic representation of the states [40]

Parent's state	Child's states	Low strength template	High strength template
Worst	Worst	0.60	0.90
	Intermediate	0.30	0.09
	Best	0.10	0.01
Intermediate	Worst	0.20	0.05
	Intermediate	0.60	0.90
	Best	0.20	0.05
Best	Worst	0.10	0.01
	Intermediate	0.30	0.09
	Best	0.60	0.90

The strength of influence defines the spread in the template. In this thesis, low and high are used. A high influence template has a lower spread over the range of states compared to a low influence template. Worst, intermediate and best denotes the range of states and corresponds to all of the states in Table 4.3 except from the PIF fatigue. The next step in the quantification process involves determining the strength of influence each parent node has on the child node. Own opinions and relevant models determine the strength of influence. The weight of each parent node is also determined based on the strength of influence. A low strength of influence is given the weight 1, while a high is given the weight 3. The weights for each parent node are then normalized with the total sum of all weights. To build the CPT, the templates for each parent node are multiplied with their normalized weight. The weighted templates for a given combination of the parent node's states are then added together and inserted into the respective column of the child node's CPT.

The value for each input node can be found in Table B.8.

---

### 7.3 fault tree evaluation

In order to successfully quantify fault trees, failure probabilities of the basic events are necessary. Exact failure probabilities can sometimes be hard to determine, so approximate probabilities have to be estimated in some of the cases. In addition to this, equipment failure data is often given in terms of failure rate per time. To obtain probability values of failure occurrence, it is possible to use an exponential distribution that describes the possibility of a component failure in the time interval from 0 to  $t$ .

$$q_i(t) = 1 - e^{-(\lambda_i t)} \approx \lambda_i t \quad (7.3.1)$$

As previously mentioned, it is assumed that maintenance only can be performed in port. The time will therefore be put as the total time of the voyage.  $\frac{195,7nm}{14nm/h} = 13,97h \approx 14h$

In the OREDA handbook, critical failure rates are used. The critical failure rate is then multiplied with a factor that considers the contribution of the relevant elements to the critical failure mode. The factor is taken from [8], where hardware systems in an autonomous ship is analyzed with the same approach.

The IMO event frequencies classification can be useful for estimating failure rates. In [11], four different categories are defined which can be seen in Table 7.6. By applying formula 7.3.1 with  $t=14h$ , and assuming 270 effective sailing days per year [58], the different IMO frequency categories can be used to calculate failure probabilities. These values are listed in Table 7.7.

Table 7.6: Event frequency index as defined by IMO [11]

Frequency	Definition	F(per ship year)
Frequent	Likely to occur once per month on one ship	10
Reasonably probable	Likely to occur once per year in a fleet of 10 ships	0.1
Remote	Likely to occur once per year in a fleet of 1,000 ships	$10^{-3}$
Extremely remote	Likely to occur once in the lifetime (20 years) of a world fleet of 5,000 ships	$10^{-5}$

Table 7.7: Failure probabilities derived from [11]

Frequency	Event frequency (per year and per ship)	Failure probability
Frequent	10	2.1E-02
Reasonably probable	0.1	2.2E-04
Remote	0.001	2.2E-06
Extremely remote	0.00001	2.2E-08

### 7.3.1 Top event probabilities

Top events are calculated using Trilith and is based on the Formulas 2.5.1 and 2.5.2. Table 7.8 presents the values for top events related to the autonomous ship, while Table 7.10 shows the values for the top events related to the human operators. The probability is given per critical course.

---

Table 7.8: Rounded fault tree top event probabilities for the autonomous ship

Top event	Failure probability [per critical course]
Failure in data collection from the AS (no data)	1.31E-03
Failure in data collection from the AS (incorrect data)	2.14E-02
Failure in communication establishment between the SCC and the AS	5.20E-03
Failure in detecting CC	3.82E-02
Failure in generating collision avoidance plan	6.06E-03
Failure in implementing and executing collision avoidance plan	6.88E-03
ANS/AMMS failure	5.90E-04
Hardware failure	8.54E-04
Software failure	5.90E-04



Table 7.10: Rounded fault tree top event probabilities for the human operator

Top event	Failure probability [per critical course]
Failure in collecting and pre-processing necessary information	9.93E-01
Failure in situation assessment and making the correct decision	9.68E-01
Failure in decision to collect information	8.43E-01
Failure in execution to collect information	9.54E-01
Failure in taking the correct action	9.77E+00
Failure to detect collision candidate	1.00E+00
Failure to respond to alarm	1.00E+00
Failure to decide on operational mode	1.00E+00
Failure to remotely control the AS to safe path	9.99E-01
Failure to monitor safe execution	1.00E+00
Failure in implementing and executing collision avoidance plan	9.99E-01

## 7.4 Event sequence diagram evaluation

The quantitative assessment of the event sequence diagram is based on the calculated occurrence probabilities of the fault tree top events and those quantified with other methods. The initial event *AS on collision course* will be calculated in the following section and includes head-on, overtaking, and crossing collision.

### 7.4.1 Object on collision course

The probability for a vessel to be on collision course will be calculated in line with IALA IWRAP Mk2.

According to [60], the yearly number of collision candidates, is defined as  $N_a$  times a causation probability factor  $P_c$ :

$$N_a \cdot P_c = N_{ship-ship} \quad (7.4.1)$$

---

Data from havbase.no [61] was used in order to identify relevant shipping routes and types of ships affecting the autonomous ship. The ships are distributed along the routes using normal distribution, where the value  $\mu$  indicates the distance from the middle of the channel to the ship's route. By looking at ship traffic data on marinetransport, this distance was found to be 190.9m. This distance will be the same for the whole route. The standard deviation,  $\sigma$ , can be calculated with the factor

$$\sigma = 3.65B \quad (7.4.2)$$

This factor corresponds to a 96% probability of a ship being within  $\pm 7.5B$  of the planned route, which is also the zone that an operator considers being a safe zone [62]. Considering that different ships travel along the route, an average breadth is calculated. This will be used in order to calculate  $\sigma$ . The average breadth is calculated with the formula:

$$B_{average} = \frac{\sum_{j=1}^n f_j \cdot B_j}{\sum_{j=1}^n f_j} \quad (7.4.3)$$

Where  $f_j$  is the frequency of vessel type  $j$  with breadth  $B_j$  of all  $n$  vessels operating on the route.

By extracting AIS data from havbase.no, it was possible to identify each ship type and their frequency crossing a line just outside Rørvik. It was not possible to obtain a frequency for the specific route. However, as Rørvik is almost right in the middle of Brønnøysund and Kristiansund, this estimate is considered adequate for this report. Ship dimensions of existing ships will be used. An overview of the characteristics can be found in Table B.15.

Formulas 7.4.4 and 7.4.5 will be used for calculating the number of collision candidates,  $N_a$  for the different collision types [60].

$$N_G^{\text{head-on/overtaking}} = LW \sum_{i,j} P_{Gi,j}^{\text{head-on/overtaking}} \frac{V_{ij}}{V_i^{(1)} V_j^{(2)}} \left( Q_t^{(1)} Q_j^{(2)} \right) \quad (7.4.4)$$

$$N_G^{\text{crossing}} = \sum_{i,j} \frac{Q_i^{(1)} Q_j^{(2)}}{V_i^{(1)} V_j^{(2)}} D_{tj} V_{ij} \frac{1}{\sin \theta} \quad (7.4.5)$$

Where:

- $Q_t^{(1)}$  and  $Q_j^{(2)}$  is the traffic frequencies on route 1 and 2
- $V_i^{(1)}$  and  $V_j^{(2)}$  is the vessel speeds
- $V_{ij} = V_i^{(1)} + V_j^{(2)}$  is the relative velocity for head-on collision

- $V_{ij} = V_i^{(1)} - V_j^{(2)}$  is the relative velocity overtaking collision
- $V_{ij} = \sqrt{\left(V_i^{(1)}\right)^2 + \left(V_j^{(2)}\right)^2 - 2V_i^{(1)}V_j^{(2)} \cos \theta}$  is the relative speed for crossing collision
- $L_W$  is the set encounter length
- $\bar{B}_{ij} = \frac{B_i^{(1)} + B_j^{(2)}}{2}$  is the mean breadth
- $\sigma_{ij} = \sqrt{\left(\sigma_i^{(1)}\right)^2 + \left(\sigma_j^{(2)}\right)^2}$  is the standard distribution of the joint distribution
- $\mu_{ij} = \mu_i^{(1)} + \mu_j^{(2)}$  is the mean distance between the two vessels

Traffic distribution plays a part in head-on and overtaking collision. Obviously, if  $V_{ij} < 0$ , then vessel  $i$  will not be able to overtake vessel  $j$ . The mean distance  $\mu$  will therefore have to be replaced with  $\mu_{ij} = \mu_i^{(1)} - \mu_j^{(2)}$  in Equation(7.4.6) for overtaking collision. Crossing collision on the other hand, is dependent on a geometric collision diameter (7.4.7).

$$P_{G_{i,j}^{\text{head-on/overtaking}}} = \Phi\left(\frac{\bar{B}_{ij} - \mu_{ii}}{\sigma_{tj}}\right) - \Phi\left(-\frac{\bar{B}_{ij} + \mu_{ij}}{\sigma_{tj}}\right) \quad (7.4.6)$$

$$D_{ij} = \frac{L_i^{(1)}V_j^{(2)} + L_j^{(2)}V_i^{(1)}}{V_\psi} \sin \theta + B_j^{(2)} \left\{ 1 - \left( \sin \theta \frac{V_i^{(1)}}{V_{ij}} \right)^2 \right\}^{1/2} + B_i^{(2)} \left\{ 1 - \left( \sin \theta \frac{V_j^{(2)}}{V_{ij}} \right)^2 \right\}^{1/2} \quad (7.4.7)$$

The probability for being on a head-on or collision course can be taken directly from Formula 7.4.6, while the probability of being on a crossing collision course can be calculated with the formula:

$$P = N_{\text{candidates/year}} \cdot \frac{\frac{0.02h}{\text{collision situation}}}{\frac{98.8m}{7.2m/s} \cdot 77 \text{voyages/year} \cdot \frac{98.8m}{5.2m/s} \cdot 884 \text{voyages/year}} \quad (7.4.8)$$

This probability is calculated with the assumption that the collision situation has a duration of 0.02 hrs. This is because the AS takes approximately 2 minutes to cross the geometric diameter which was calculated to be 98.9m.

## 7.4.2 Collision candidate follows the rules

As the collision candidate in this thesis is another ship, it can execute its own maneuvers in case the AS fails to implement and execute the collision avoidance

Table 7.12: Number of collision candidates and probability of being on collision course

	Collision candidates N	Probability of being on collision course
Head-on collisions	2.19	1.04E-08
Overtaking collisions	18532,48	0,16
Crossing collisions	1395453	0,0016
Total	1413987.68	0.16

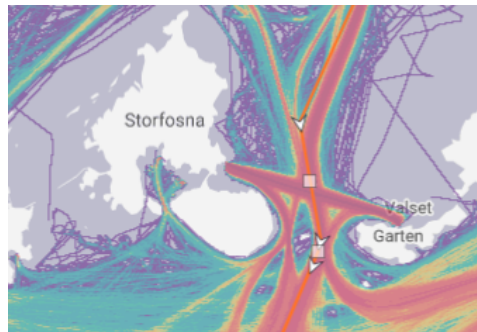


Figure 7.2: Crossing area

plan or the human operators fail to take remote control of the AS. If the maneuvers performed by the CC is compliant with the traffic rules, it is assumed that the scenario will result in a "safe" end-state. According to [63], 56% of major maritime collision includes violation of COLREGs. Since 1983 there has been recorded 14 collision accidents [64]. This yields a collision frequency of 0.37 per year. This means that  $0.37 \cdot 0.56 = 0.21$  of these accidents included a violation of COLREGs. From Table??, the total frequency of ships along the route is 1868 ships/year. This includes all the ships sailing north and south and the ferries from the crossing fairway. The probability that the CC follows the rules can then be calculated as  $1 - \frac{0.21}{1868} = 0.99$  percent.

### 7.4.3 HCL final results

The final model obtains a probability of colliding of  $1.53E - 04$  per trip. With 77 trips per year, the ship will collide every 85th year.

The results are compared with the collision probability from Jensen[8] and DNV[14]. The comparison is shown in Table 7.14.

Table 7.14: Collision probability

---

---

	HCL model	Jensen,2015	DNV, 2003
Collision probability per critical course	1.53E-04	1.4E-07	8.60E-06

---

---

The complete model can be found in Appendix A.

---

## 8.1 Model development

The system of the unmanned autonomous vessel consists of several subsystems, components, and interactions both with its surroundings and human operators. This level of complexity is tough to reproduce when at the same time trying to make the analysis manageable. The system has therefore been simplified. One risk by doing this is that potential important components and failure modes get neglected. One simplification made in this thesis was that the failures related to decision making and system interaction in the AS were reduced to the failure ANS failure. This failure concerned both hardware and software failure, but at a high level. The reason for this simplification is the lack of failure data related to software and hardware systems. It can also be hard to determine the different basic events for software and hardware failures, as a failure in the software can lead to hardware failures and vice versa.

The model in this thesis follows the HCL methodology. One of the advantages of the HCL methodology is that it can separate the different domains into technical and human/organizational factors, allowing for a better understanding of the risk picture. At least in the near future, autonomous ships will still have to rely on human operators for monitoring and intervening when necessary. So to fully assess the risk picture, the interaction between the system and the humans have to be considered. The IDA model, which the fault trees in this thesis are built upon, divides the operation into three different phases; Information collection, decision making, and action-taking. This has previously only been done concerning human reliability analysis. One benefit of the IDA model is that it is flexible because it provides a structure independent of the system architecture. This allows for extending this method to the autonomous system. Another benefit of this approach is that it leads to cut sets that may not otherwise be included. Using traditional risk analysis methods can be easy to only focus on one part of the system. For

---

example, when analyzing the operator's failure in detecting collision candidates using only HRA, the cut sets would typically not include basic failure events related to communication or data collection.

The ESD in this thesis was made using a flowchart. This ensures traceability and that every critical event related to the AS and the human operator is considered. Regarding the FTs, they were derived based on a CoTA for collision avoidance. The CoTA described how the tasks of the ESD could successfully be performed. One negative aspect of this approach is that possible failure events such as performing an unexpected task will not be identified.

The input nodes for the BBN models are mainly based on studies related to NPP and AUVs and not autonomous ships. However, the selected nodes rely on literature related to human-autonomy interaction and cognitive science. It is, therefore, reasonable to assume that they can be applied to this case as well. Regardless of what type of operation, the human operators have to solve the same general tasks: gathering information, making decisions about what type of information to gather, and then putting this information into action. This corresponds well with the IDA framework, which has been used throughout the thesis. One negative aspect by making a BBN for each of the phases in IDA, is that it makes it difficult in separating between the different CFMs. This makes it harder to analyse the results and identify the basic events with the most negative contribution. In hindsight, it would have been better to make a BBN for each CFM, although this would require more research on HRA related to autonomous operations.

## 8.2 Quantification process

The initiating event, probability of being on collision course, was calculated based on registered traffic data. The standard deviation of the normal distribution of the traffic were calculated with the use of an approximation formula. Detailed AIS data would typically be used to get a correct picture of the traffic situation.

The reliability of the failure probabilities chosen for the different basic events should also be discussed. Many of the failure probabilities are assumed based on the IMO frequencies, and even though this can give a decent indication, it does not give an entirely correct picture. Failure rates for components were chosen on the basis of existing failure rate data. Adjusting failure rate data to fit the system is something that should be handled with care. The failure rates were converted to failure probabilities for the end of the trip. In other words, the results obtained show a conservative view.

The numbers and data-set used for the input nodes in the BBN's were based on a human/AUV operation. Even though they share many similarities, there are still significant differences in supervising a ship compared to a small autonomous underwater vehicle. Primarily related to the navigation part, but also the severity of the consequences if something goes wrong. The BBN models put much emphasis on training and experience. These numbers have been adapted directly from an AUV



operation, where it makes sense that the operators do not have much training and experience. The same can be argued when looking at autonomous ship operations. Even though the operators are likely to have experience in navigation and ship-handling, they will not have experience supervising and monitoring an autonomous ship, as it is an entirely new field. The probability of an inadequate state would therefore be high.

### 8.3 Results

The failure probabilities for the fault trees related to human failure events ranged between 99-100%. This is unrealistically high. However, this can be explained by the fact that each BBN was developed to model each phase in the IDA model instead of each crew failure mode. With this approach, the failure probability of each CFM will be significantly overestimated as the BBN in some way covers all the tasks.

Risk assessments often rely on historical data, and with that in mind, there will always be many insecurities involved when trying to model the risk of an autonomous ship. As described in the introduction, autonomous ships should be as least as safe as conventional ships. In this thesis, the results showed that for this specific course, this was not the case. However, the studies that this model was compared with involves other types of ship and a different operational context. In addition to this, they do not include human failure events to the same extent as in this thesis. The calculated probability of being on a collision course was significantly higher in this thesis than what was the case for the compared studies. As this was set to be the initiating event, this will significantly impact the end results.

Even though some of the fault trees related to human errors were calculated to a failure probability of almost 100%, the collision probability was still reasonably low. As far as this can prove anything, it shows that the technical systems included in this case are very reliable and that the autonomous ship does not necessarily have to rely on human operators.

### 8.4 Sensitivity analysis for the BBN models

A sensitivity analysis was conducted through GeNIe with the built in sensitivity analysis function. This shows how the different nodes influence the outcome. A higher sensitivity would mean that there is low uncertainty in the node. A sensitivity analysis was conducted for all the three BBN models.

#### 8.4.1 I-Phase

Figure 8.2 shows the results for the I-Phase. Darker red charts indicate a higher influence, while grey charts are deterministic and based on the specific case. The sensitivity of these are therefor not assessed. The most influential nodes are Experience, Training and HMI. Figure 8.1 shows the effects of changing each state

individually on the probability of the adequate state. On the top, the case study is shown as a reference value. The figure also shows the worst and best case where all input nodes were set to their worst and best states respectively. If all input nodes are put to their best state, the probability of an adequate I-Phase is 98%. On the other hand, if all input nodes are set to their worst state, the probability drops to 12%. The most influential individual nodes are Training and Experience. They both reduce the probability of an adequate I-Phase with 8%. When put to their best state, they improve the probability with 18%. The least influential states were Interface design, Etiquette and Fatigue. Interface and Etiquette improve the probability with only 2%, while Fatigue improves the probability with 1%. However, they decrease the probability with 9% and 8%, which is the same, or even more than what Training and Experience did.

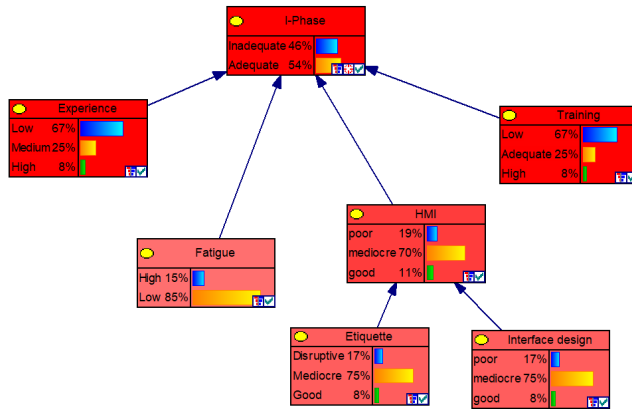


Figure 8.1: Effect of changing the states individually on the probability of adequate I-Phase.

### 8.4.2 D-Phase

Figure 8.3 shows the sensitivity analysis for the D-Phase. The most influential nodes are Training, Experience, Procedure and Workload. If all input nodes are set to their best state, the probability of an adequate D-phase is 93%. When set to their worst states, the probability becomes 23%. The most influential individual input nodes are Training, Experience and Procedures. They increase the probability of an adequate state with 15%, 12% and 1% respectively when set to their best states. Their worst states reduce the probability with 6%, 5% and 16%. Etiquette, Interface design and communication has the least influence, with Etiquette and Interface design only improving/reducing with 1%. Communication does not change the probability at all. Figure 8.4 shows the effects of changing each state individually on the probability of the adequate state.

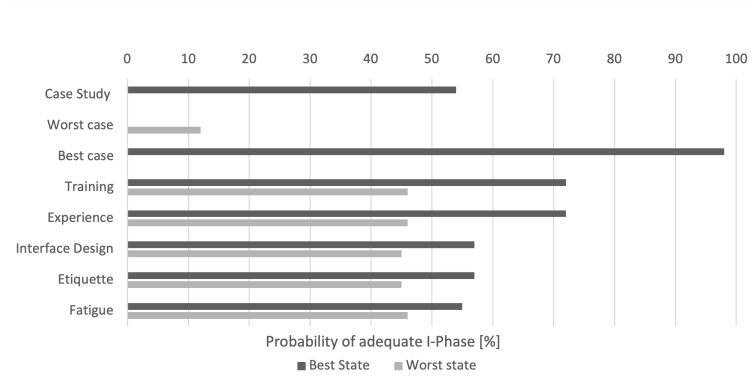


Figure 8.2: Sensitivity of the I-Phase node. Darker red charts indicate a higher influence. Grey charts are deterministic.

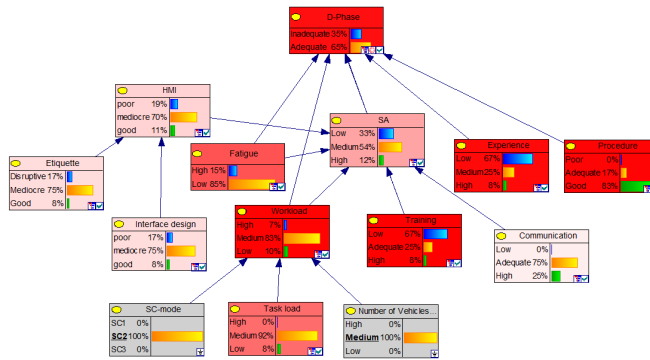


Figure 8.3: Sensitivity of the D-Phase node. Darker red charts indicate a higher influence. Grey charts are deterministic.

### 8.4.3 A-phase

Figure 8.5 shows the sensitivity analysis for the A-Phase. The most influential nodes are Training and Experience. If all input nodes are set to their best state, the probability of an adequate A-phase is 90%. When set to their worst states, the probability becomes 17%. The most influential individual input nodes are Training and Experience. They increase the probability of an adequate state with 26% and 25% respectively when set to their best states. Their worst states reduce the probability with 11% and 2%. Etiquette, Interface design, Task load and communication has the least influence, with Etiquette, Interface design and Task load only improving/reducing with 1%. Communication also improves the probability of an adequate state with 1% when set to it's best state, but does not reduce it when it's set to it's worst state. Figure 8.6 shows the effects of changing each state individually on the probability of the adequate state.

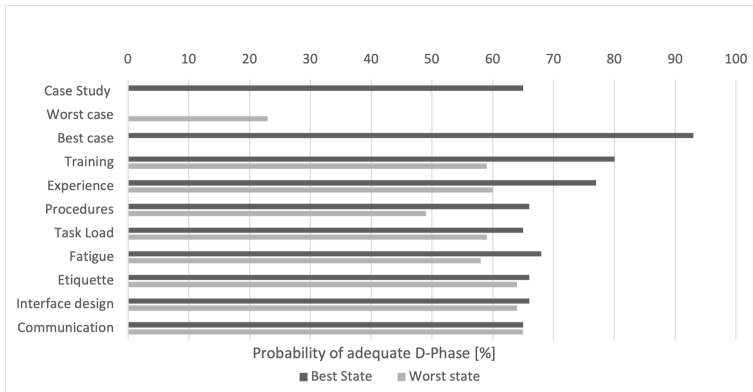


Figure 8.4: Effect of changing the states individually on the probability of adequate D-Phase.

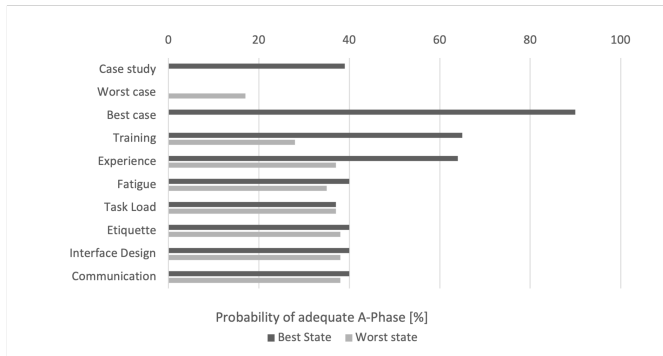


Figure 8.6: Effect of changing the states individually on the probability of adequate A-Phase.

## 8.5 Sensitivity analysis of the HCL

To investigate how the the human performance impact the collision probability, a sensitivity analysis was conducted. The value of an inadequate state when all input nodes were put to their best state was used as the failure probability of the human basic events. Table 8.1 shows how it affected the probability.

Table 8.1: Risk comparison when changing human performance

	Calculated performance	Best performance
Collision probability per critical course	1.53E-04	8.41E-01

The collision frequency increased with better human performance. This can be explained by the fact that the probability of failure for the human operators are still very high. They vary between 53% and 63% even when put to their best state. Compared to the original case where the failure probabilities of the human operators were  $\approx 100\%$ , the operators are now much more involved in the scenario.

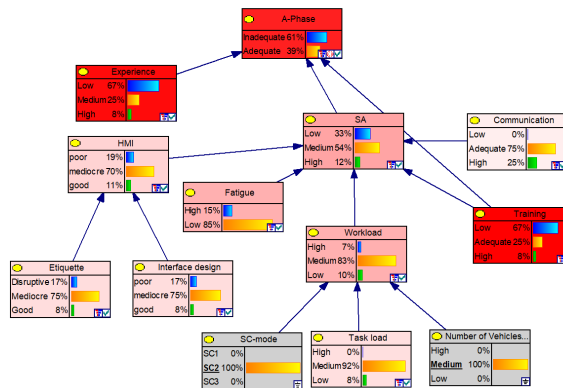


Figure 8.5: Sensitivity of the A-Phase node. Darker red charts indicate a higher influence. Grey charts are deterministic.

the failure probabilities between the human operators and the autonomous ship makes for uncertain results. A BBN made for each CFM with a higher level of accuracy regarding the input values is needed to obtain a more realistic result. It is expected that with a more accurate quantification of the CFMs, the failure probabilities of the human failure events will go down, resulting in a lower collision probability.

These results show that an inadequate operator can impact the autonomous operation in a negative way. With few events that have to fail before reaching a collision, it could be wise to consider putting extra safety measures into place. For example, solutions monitoring the human operator and not only the autonomous ship.

---

This thesis has investigated the collision risk for an unmanned autonomous ship sailing along the coast of Norway from Brønnøysund to Kristiansund. A literature review covering the specific aspects of the case was conducted. This includes, among others, relevant risk models and human reliability analysis. A Hybrid Causal Logic model for the collision accident scenario was developed. The HCL comprises of an Event Sequence Diagram, Fault Trees, and BBN's. The model was quantified using relevant data from the literature as well as collision frequency calculations.

The calculated collision probability was  $1.53E - 04$ . This is a bit higher than the studies compared to in this thesis. However, the context and scenario in this thesis are completely different from the other studies.

This thesis has also investigated the interaction between human operators and the autonomous ship. The results showed that even with a high probability of human failure, the ship is still reliable. The results obtained for the human failure events shows that more research on human reliability analysis related to autonomous operations is important.

### **9.0.1 Further work**

Several assumptions were made in this thesis, which impacts the results and makes them more uncertain. A more detailed focus on software and hardware errors and their failure modes is important to improve the adequacy of the results. Critical weather situations and detailed assessment of the risk related to LNG as fuel should also be evaluated for a complete risk assessment. Most importantly, more research has to be done on human reliability analysis related to autonomous operation, especially when it comes to quantification. This is critical to obtain a realistic and adequate risk assessment.

---



## Bibliography

- [1] D. M. Authority, “ANALYSIS OF REGULATORY BARRIERS TO THE USE OF AUTONOMOUS SHIPS”, Tech. Rep., Sep. 2017, p. 141. [Online]. Available: <https://www.dma.dk/Documents/Publikationer/Analysis%20of%20Regulatory%20Barriers%20to%20the%20Use%20of%20Autonomous%20Ships.pdf>.
- [2] DNVGL, *Remote-controlled and autonomous ships, DNVGL group technology & research, position paper 2018 in the maritime industry*, 2018. [Online]. Available: <https://www.dnvgl.com/maritime/publications/remote-controlled-autonomous-ships-paper-download.html>.
- [3] Ø. J. Rødseth and H. Nordahl, *Definitions for Autonomous Merchant Ships*, 2017.
- [4] P. T. Pedersen, “Review and application of ship collision and grounding analysis procedures”, en, *Marine Structures*, vol. 23, no. 3, pp. 241–262, Jul. 2010. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0951833910000213> (visited on 12/18/2020).
- [5] IMO, “Report of a survey on what maritime professionals think about autonomous shipping, REGULATORY SCOPING EXERCISE FOR THE USE OF MARITIME AUTONOMOUS SURFACE SHIPS (MASS)”, International Maritime Organization, London, UK, Tech. Rep., 2018.
- [6] M. Rausand and S. Haugen, *Risk Assessment, 2nd Edition*, eng, 2nd ed. Wiley, 2020.
- [7] K. Wróbel, J. Montewka, and P. Kujala, “Towards the assessment of potential impact of unmanned vessels on maritime transportation safety”, en, *Reliability Engineering & System Safety*, vol. 165, pp. 155–169, Sep. 2017. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0951832016303337> (visited on 12/18/2020).

- 
- [8] F. Jensen, “Hazard and Risk Assessment of Unmanned Dry Bulk Carriers on the High Seas”, Master of Science Thesis, Hamburg University of Technology, Hamburg, 2015.
- [9] I. B. Utne, B. Rokseth, A. J. Sørensen, and J. E. Vinnem, “Towards supervisory risk control of autonomous ships”, en, *Reliability Engineering & System Safety*, vol. 196, p. 106757, Apr. 2020. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0951832018308160> (visited on 08/18/2020).
- [10] K. Wróbel, P. Krata, J. Montewka, and T. Hinz, “Towards the Development of a Risk Model for Unmanned Vessels Design and Operations”, *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 10, pp. 267–274, Jul. 2016.
- [11] IMO, *REVISED GUIDELINES FOR FORMAL SAFETY ASSESSMENT (FSA) FOR USE IN THE IMO RULE-MAKING PROCESS*, Sep. 2018. [Online]. Available: [https://wwwcdn.imo.org/localresources/en/OurWork/HumanElement/Documents/MS-Circ.12-Rev.2%20-%20Revised%20Guidelines%20For%20Formal%20Safety%20Assessment%20\(Fsa\)For%20Use%20In%20The%20Imo%20Rule-Making%20Proces...%20\(Secretariat\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/HumanElement/Documents/MS-Circ.12-Rev.2%20-%20Revised%20Guidelines%20For%20Formal%20Safety%20Assessment%20(Fsa)For%20Use%20In%20The%20Imo%20Rule-Making%20Proces...%20(Secretariat).pdf).
- [12] T. Aven, “Practical implications of the new risk perspectives”, en, *Reliability Engineering & System Safety*, vol. 115, pp. 136–145, Jul. 2013. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0951832013000550> (visited on 11/16/2020).
- [13] I. B. Utne, A. J. Sørensen, and I. Schjøberg, “Risk Management of Autonomous Marine Systems and Operations”, en, American Society of Mechanical Engineers Digital Collection, Sep. 2017. [Online]. Available: <https://gasturbinespower.asmedigitalcollection.asme.org/OMAE/proceedings/OMAE2017/57663/V03BT02A020/280986> (visited on 06/20/2021).
- [14] DNV GL, *FSA Navigation Large Passenger Ships*, 2003.
- [15] W. Røed and J. E. Vinnem, *Offshore Risk Assessment Vol. 1: Principles, Modelling and Applications of QRA Studies*, eng, 4th ed. 2020, ser. Springer Series in Reliability Engineering. London: Springer London, Limited, Springer London, 2019.
- [16] M. A. Ramos, C. A. Thieme, I. B. Utne, and A. Mosleh, “Human-system concurrent task analysis for maritime autonomous surface ship operation and safety”, en, *Reliability Engineering & System Safety*, vol. 195, p. 106697, Mar. 2020. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0951832018313085> (visited on 12/22/2020).
- [17] S. Swaminathan and C. Smidts, “The Event Sequence Diagram framework for dynamic Probabilistic Risk Assessment”, en, *Reliability Engineering & System Safety*, vol. 63, no. 1, pp. 73–90, Jan. 1999. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0951832098000271> (visited on 12/22/2020).
- [18] W. Røed, A. Mosleh, J. E. Vinnem, and T. Aven, “On the use of the hybrid causal logic method in offshore risk analysis”, en, *Reliability Engineering*
-

- System Safety*, vol. 94, no. 2, pp. 445–455, Feb. 2009. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S095183200800135X> (visited on 12/22/2020).
- [19] J. Pearl, “Fusion, propagation, and structuring in belief networks”, *Artificial Intelligence*, vol. 29, no. 3, pp. 241–288, 1986.
- [20] M. Minami and R. Shoji, “Estimation of the Collision Risk on Planned Route”, *Lecture Notes in Civil Engineering*, vol. 65 LNCE, pp. 516–532, 2021.
- [21] S. Li, Q. Meng, and X. Qu, “An Overview of Maritime Waterway Quantitative Risk Assessment Models”, *Risk Analysis*, vol. 32, no. 3, pp. 496–512, 2012.
- [22] T. Statheros, G. Howells, and K. McDonald-Maier, “Autonomous ship collision avoidance navigation concepts, technologies and techniques”, *Journal of Navigation*, vol. 61, no. 1, pp. 129–142, 2008.
- [23] C. A. Thieme, I. B. Utne, and S. Haugen, “Assessing ship risk model applicability to Marine Autonomous Surface Ships”, en, *Ocean Engineering*, vol. 165, pp. 140–154, Oct. 2018. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0029801818313210> (visited on 09/08/2020).
- [24] M. A. Ramos, C. A. Thieme, I. B. Utne, and A. Mosleh, “A generic approach to analysing failures in human – System interaction in autonomy”, en, *Safety Science*, vol. 129, p. 104808, Sep. 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0925753520302058> (visited on 04/27/2021).
- [25] J. Annett and N. A. Stanton, *Task Analysis*, en. CRC Press, Jun. 2000.
- [26] A. Shepherd, *Hierarchical task analysis*, English. London; New York: Taylor & Francis, 2001.
- [27] A. Ramos, T. Varum, and J. Matos, “Integrated multilayer yagi antenna for 5G”, 2019, pp. 33–34.
- [28] C. Smidts, S. Shen, and A. Mosleh, “The IDA cognitive model for the analysis of nuclear power plant operator response under accident conditions. Part I: Problem solving and decision making model”, *Reliability Engineering and System Safety*, vol. 55, no. 1, pp. 51–71, 1997.
- [29] M. A. Ramos, I. B. Utne, and A. Mosleh, “On factors affecting autonomous ships operators performance in a Shore Control Center”, en, *Los Angeles*, p. 12, 2018.
- [30] M. A. Ramos, E. L. Drogue, A. Mosleh, M. d. C. Moura, and M. R. Martins, “Revisiting past refinery accidents from a human reliability analysis perspective: The BP Texas City and the Chevron Richmond accidents”, en, *The Canadian Journal of Chemical Engineering*, vol. 95, no. 12, pp. 2293–2305, 2017. [Online]. Available: <https://www.onlinelibrary.wiley.com/doi/abs/10.1002/cjce.22996> (visited on 04/22/2021).
- [31] A. Mosleh, J. Forester, R. Boring, S. Hendrickson, A. Whaley, S.-H. Shen, D. Kelly, J. Chang, V. Dang, J. Oxstrand, and E. Lois, *A Model-Based Human Reliability Analysis Framework*. Jun. 2010.
- [32] K. M. Groth and A. Mosleh, “A data-informed PIF hierarchy for model-based Human Reliability Analysis”, en, *Reliability Engineering & System*

- 
- Safety*, vol. 108, pp. 154–174, Dec. 2012. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0951832012001561> (visited on 05/27/2021).
- [33] N. J. Ekanem, “A MODEL-BASED HUMAN RELIABILITY ANALYSIS METHODOLOGY (PHOENIX METHOD)”, en, 2013. [Online]. Available: <https://drum.lib.umd.edu/handle/1903/14831> (visited on 04/27/2021).
- [34] D. Gertman, H. Blackman, J. Marble, C. Smith, and R. Boring, *The SPAR-H human reliability analysis method*. Jan. 2004.
- [35] M. R. Endsley, *Designing for Situation Awareness: An Approach to User-Centered Design, Second Edition*, 2nd. USA: CRC Press, Inc., 2011.
- [36] Y. Man, M. Lundh, T. Porathe, and S. MacKinnon, “From Desk to Field - Human Factor Issues in Remote Monitoring and Controlling of Autonomous Unmanned Vessels”, *Procedia Manufacturing*, vol. 3, pp. 2674–2681, 2015.
- [37] R. Parasuraman, T. Sheridan, and C. Wickens, “A model for types and levels of human interaction with automation”, *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 30, no. 3, pp. 286–297, May 2000, Conference Name: IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans.
- [38] M. Wahlström, J. Hakulinen, H. Karvonen, and I. Lindborg, “Human Factors Challenges in Unmanned Ship Operations – Insights from Other Domains”, en, *Procedia Manufacturing*, 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015, vol. 3, pp. 1038–1045, Jan. 2015. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2351978915001687> (visited on 05/23/2021).
- [39] M. Cummings, C. Mastracchio, K. Thornburg, and A. Mkrtchyan, “Boredom and Distraction in Multiple Unmanned Vehicle Supervisory Control”, en, *Interacting with Computers*, vol. 25, no. 1, pp. 34–47, Jan. 2013. [Online]. Available: <https://academic.oup.com/iwc/article/775106/Boredom> (visited on 05/23/2021).
- [40] C. A. Thieme and I. B. Utne, “A risk model for autonomous marine systems and operation focusing on human–autonomy collaboration”, eng, *446-464*, 2017. [Online]. Available: <https://ntnuopen.ntnu.no/ntnu-xmliu/handle/11250/2450091> (visited on 05/24/2021).
- [41] N. Ekanem, A. Mosleh, and S.-H. Shen, “Phoenix–A model-based human reliability analysis methodology: Qualitative analysis procedure”, *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 1–15, 2015.
- [42] I. E. Commission, “Functional safety of electrical/electronic/programmable electronic safety related systems”, *IEC 61508*, 2000. [Online]. Available: <https://ci.nii.ac.jp/naid/10020953356/#cit> (visited on 04/22/2021).
- [43] R. Kari, H. Gaspar, A. Gausdal, and M. Morshedi, “Human Interactions Framework for Remote Ship Operations”, 2018, pp. 581–587.
- [44] B. Rokseth, *Autonomous ship safety - STPA workshop in the ORCAS project*, en, Jul. 2019.
-

- [45] R. Parasuraman and C. Miller, “Trust and etiquette in high-criticality automated systems”, *Commun. ACM*, vol. 47, pp. 51–55, Apr. 2004.
- [46] T. Sheridan and R. Parasuraman, “Human-Automation Interaction”, *Reviews of Human Factors and Ergonomics*, vol. 1, pp. 89–129, Jun. 2005.
- [47] E. de Visser, T. Shaw, A. Mohamed-Ameen, and R. Parasuraman, “Modeling Human-Automation Team Performance in Networked Systems: Individual Differences in Working Memory Count”, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 54, pp. 1087–1091, Sep. 2010.
- [48] H. A. Ruff, S. Narayanan, and M. H. Draper, “Human Interaction with Levels of Automation and Decision-Aid Fidelity in the Supervisory Control of Multiple Simulated Unmanned Air Vehicles”, en, *Presence: Teleoperators and Virtual Environments*, vol. 11, no. 4, pp. 335–351, Aug. 2002. [Online]. Available: <https://direct.mit.edu/pvar/article/11/4/335-351/18417> (visited on 06/02/2021).
- [49] Eidsvaag AS, *MV Eidsvaag Pioneer – Eidsvaag AS*, Oct. 2021. [Online]. Available: <https://eidsvaag.no/mv-eidsvaag-pioneer/> (visited on 06/23/2021).
- [50] B. Rokseth and I. B. Utne, “A Risk-Based Control System for Mode Control of a Hybrid-Electric Machinery System for an Autonomous Ship”, en, 2020.
- [51] T. Johansen, *System description, case ship, Trondheim*, Mar. 2021.
- [52] Kim Idar Giske, *Eidsvaag Pioneer (07/2013)*, nb, Jul. 2013. [Online]. Available: <https://maritimt.com/nb/batomtaler/eidsvaag-pioneer-072013> (visited on 06/04/2021).
- [53] S. Fu, X. Yan, D. Zhang, C. Li, and E. Zio, “Framework for the quantitative assessment of the risk of leakage from LNG-fueled vessels by an event tree-CFD”, en, *Journal of Loss Prevention in the Process Industries*, vol. 43, pp. 42–52, Sep. 2016. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0950423016301140> (visited on 10/22/2020).
- [54] P. Raj and T. Lemoff, “Risk analysis based LNG facility siting standard in NFPA 59A”, *Journal of Loss Prevention in the Process Industries*, vol. 22, no. 6, pp. 820–829, 2009.
- [55] R. de Boer, *Zuverlässigkeitstechnische Systemanalyse für schiffstechnische Systeme am Beispiel der elektrischen Energieversorgung*. Aachen: Shaker Verlag, 2004. [Online]. Available: <https://www.consumerstore.com/de/bucher/fachbucher/ingenieurwissenschaften/zuverlassigkeitstechnische-systemanalyse-fur-schiffstechnische-systeme-am-beispiel-der-elektrischen-energieversorgung-berichte-aus-der-energietechnik.html> (visited on 06/12/2021).
- [56] Wärtsilä, *Wärtsilä Power Management System*, 2021. [Online]. Available: <https://www.wartsila.com/marine/build/electrical-and-power-systems/hybrid-automation/wartsila-power-management-system> (visited on 06/24/2021).
- [57] Kongsberg, *ARPA radar*, no, Jun. 2021. [Online]. Available: <https://www.kongsberg.com/no/maritime/products/bridge-systems-and-control-centres/navigation-system/arpa-radar/> (visited on 06/24/2021).

- 
- [58] M. Hansen, S. Randrup-Thomsen, T. Askeland, M. Ask, L. Skorpa, S. Hillestad, and J. Veie, “Bridge crossings at Sognefjorden – Ship collision risk studies”, in, May 2013, pp. 9–17.
- [59] J. E. Vinnem, R. Bye, B. A. Gran, T. Kongsvik, O. M. Nyheim, E. H. Okstad, J. Seljelid, and J. Vatn, “Risk modelling of maintenance work on major process equipment on offshore petroleum installations”, en, *Journal of Loss Prevention in the Process Industries*, vol. 25, no. 2, pp. 274–292, Mar. 2012. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0950423011001781> (visited on 06/02/2021).
- [60] P. Friis-Hansen, *Predicting Collision Frequencies - IWRAP*, Mar. 2008. [Online]. Available: [https://www.iala-aism.org/wiki/iwrap/index.php/Predicting\\_Collision\\_Frequencies](https://www.iala-aism.org/wiki/iwrap/index.php/Predicting_Collision_Frequencies) (visited on 05/15/2021).
- [61] MarineTraffic, *MarineTraffic: Global Ship Tracking Intelligence — AIS Marine Traffic*, en, May 2021. [Online]. Available: <https://www.marinetraffic.com/en/ais/home/centerx:-17.9/centery:49.6/zoom:5> (visited on 06/06/2021).
- [62] P. Friis-Hansen, *Lateral Traffic Distribution - IWRAP*, Mar. 2008. [Online]. Available: [https://www.iala-aism.org/wiki/iwrap/index.php/Lateral\\_Traffic\\_Distribution](https://www.iala-aism.org/wiki/iwrap/index.php/Lateral_Traffic_Distribution) (visited on 06/04/2021).
- [63] L. Du, O. A. Valdez Banda, F. Goerlandt, Y. Huang, and P. Kujala, “A COLREG-compliant ship collision alert system for stand-on vessels”, en, *Ocean Engineering*, vol. 218, p. 107 866, Dec. 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0029801820308349> (visited on 06/05/2021).
- [64] Havbase, *Havbase*, Jun. 2021. [Online]. Available: <https://havbase.no/> (visited on 06/23/2021).
- [65] C. Thieme, “Development of a Risk Management Process for NTNU’s REMUS 100 AUV”, eng, 105, 2014, Accepted: 2014-12-19T12:13:04Z Publisher: Institutt for marin teknikk. [Online]. Available: <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/239188> (visited on 06/23/2021).
- [66] SINTEF. and S. f. I. o. T. Forskning, *OREDA: Offshore Reliability Data Handbook*. OREDA Participants, 1997. [Online]. Available: [https://books.google.no/books?id=a\\_nPtQEACAAJ](https://books.google.no/books?id=a_nPtQEACAAJ).
- [67] M. 83/INF.2, *Formal Safety Assessment: Consolidated text of the Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process(MSC/Circ.1023-MEPC/Circ.392*, 2007.
- [68] Center for Chemical Process Safety, “CCPS Generic Failure Rate Data Base”, en, in *Guidelines for Process Equipment Reliability Data with Data Tables*, John Wiley & Sons, Ltd, 1989, pp. 127–212. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470938355.ch5> (visited on 06/17/2021).
- [69] M. Asami and F. Kaneko, “Development of a vessels collision model based on Naturalistic Decision Making model”, *Journal of the Japan Society of Naval Architects and Ocean Engineers*, vol. 15, no. 0, 2012. [Online]. Available: <https://trid.trb.org/view/1281153> (visited on 06/17/2021).
-

- [70] Ørnulf Jan Rødseth and B. Kvamstad, *D4.3:Evaluation of ship to shore communication links*, Dec. 2012.
- [71] MarineTraffic, *BOW SANTOS*, en, Jun. 2021. [Online]. Available: <https://www.marinetraffic.com/en/ais/details/ships/shipid:314879/mmsi:259887000/imo:9303651/vessel:BO%20SANTOS> (visited on 06/23/2021).
- [72] BalticShipping.com, *BW MAGELLAN*, en, Jun. 2021. [Online]. Available: <https://www.balticshipping.com> (visited on 06/24/2021).
- [73] Egil Ulvan Rederi AS, *Kristian With*, 2021. [Online]. Available: <https://ulvan-rederi.no/fartoyene/kristian-with/> (visited on 06/23/2021).
- [74] Sjøhistorie, *M/T Fjellstrøm*, Jun. 2021. [Online]. Available: <https://www.sjohistorie.no/no/skip/1013513/> (visited on 06/23/2021).
- [75] MarineTraffic, *HOEGH TRACER*, en, Jun. 2021. [Online]. Available: <https://www.marinetraffic.com/en/ais/details/ships/shipid:10582/mmsi:0/imo:7924841/vessel:HOEGH%20TRACER> (visited on 06/23/2021).
- [76] RoyalArcticLine, *Siwana Arctica*, Jun. 2021. [Online]. Available: <https://www.ral.dk/sejlpplaner/bygdeskibe/siuana-arctica/> (visited on 06/24/2021).
- [77] Solstad, *Far Spica*, en-US, Jun. 2021. [Online]. Available: <https://www.solstad.com/vessel/far-spica/> (visited on 06/23/2021).
- [78] Knut W. Vadseth, *Frøy Valkyrien (11/2017)*, nb, Jan. 2017. [Online]. Available: <https://maritimt.com/nb/batontaler/froy-valkyrien-112017> (visited on 06/19/2021).
- [79] MarineTraffic, *MELINE*, en, Jun. 2021. [Online]. Available: <https://www.marinetraffic.com/en/ais/details/ships/shipid:5100432/mmsi:912577124/imo:0/vessel:MELINE> (visited on 06/23/2021).
- [80] Fiskeriportalen, *FREKØY*, Jun. 2021. [Online]. Available: <https://www.fiskeriportalen.no/fiskebater/frekoy-m-0149f> (visited on 06/24/2021).
- [81] KnutsenGroup, *Hilda Knutsen*, Jun. 2021. [Online]. Available: <https://knutsenoas.com/ship/hilda-knutsen/> (visited on 06/24/2021).
- [82] Kystekspresen, *MS Tyrhaug*, no, Jun. 2021. [Online]. Available: <http://m.fosennamsos.no/sor-i-trondelag-more-og-romsdal/ms-tyrhaug-article2673-930.html> (visited on 06/23/2021).
- [83] Hurtigruten, *MS Kong Harald*, no, Jun. 2021. [Online]. Available: <https://www.hurtigruten.no/skip/ms-kong-harald/> (visited on 06/23/2021).
- [84] MarineTraffic, *NIDAROS II*, en, Jun. 2021. [Online]. Available: <https://www.marinetraffic.com/en/ais/details/ships/shipid:305737/mmsi:257277400/imo:5132626/vessel:NIDAROS%20II> (visited on 06/19/2021).

## Additional figures

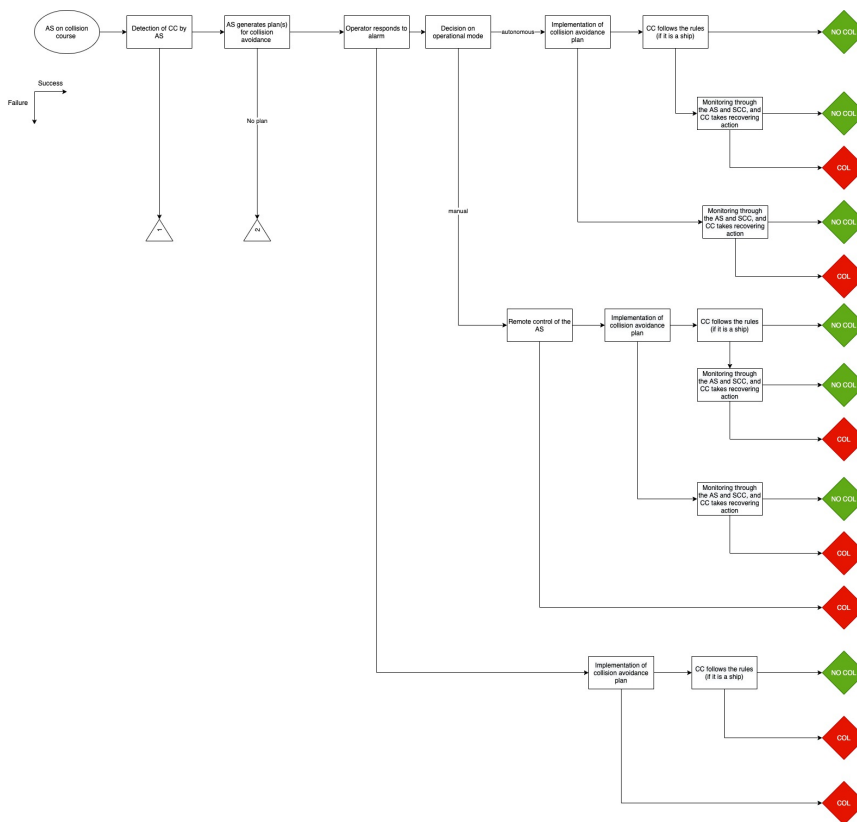


Figure A.1: Event sequence diagram for the case study



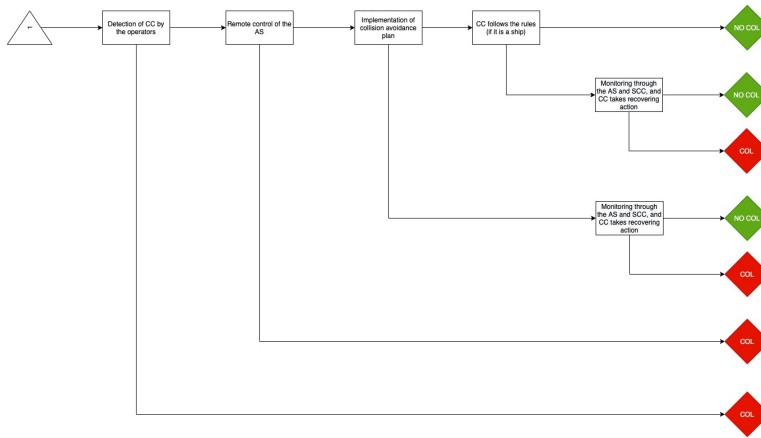


Figure A.2: Event sequence diagram for the case study

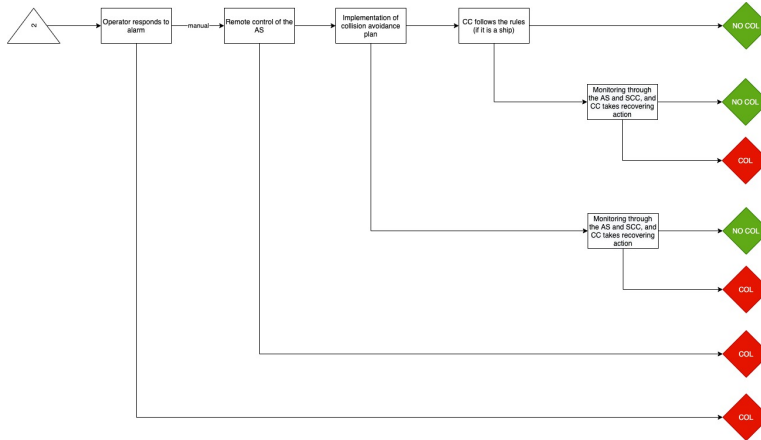


Figure A.3: Event sequence diagram for the case study

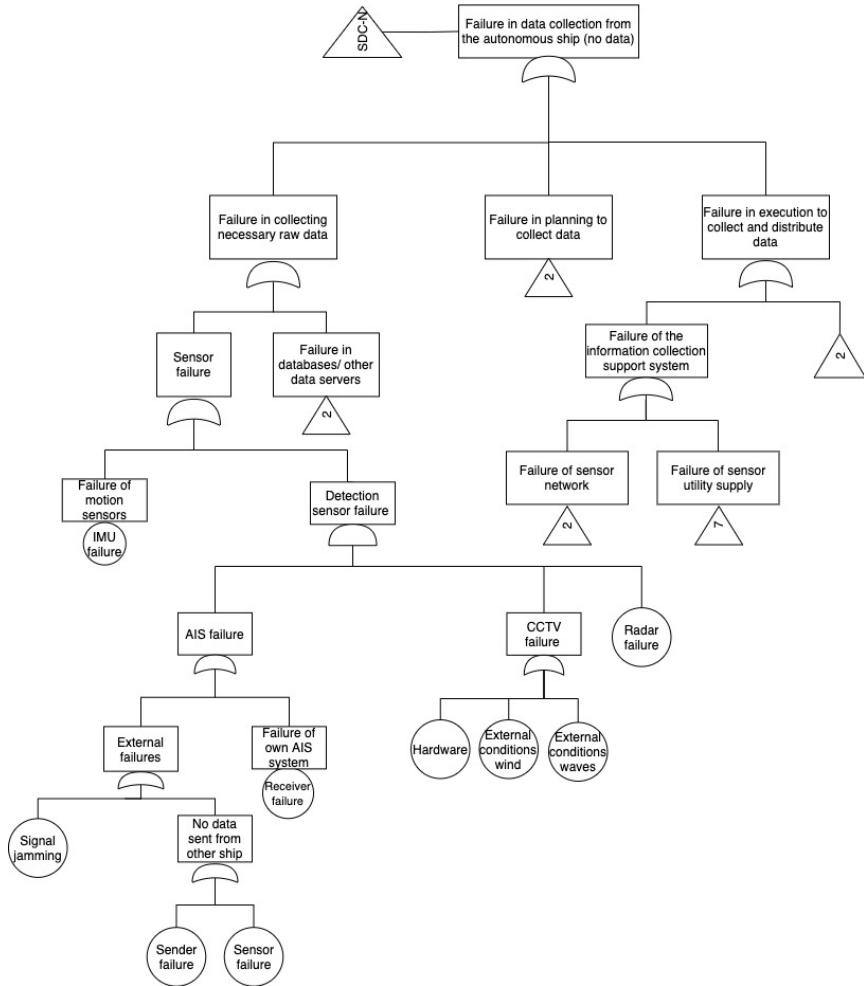


Figure A.4: Fault tree with the top event failure in data collection from the autonomous ship (no data)

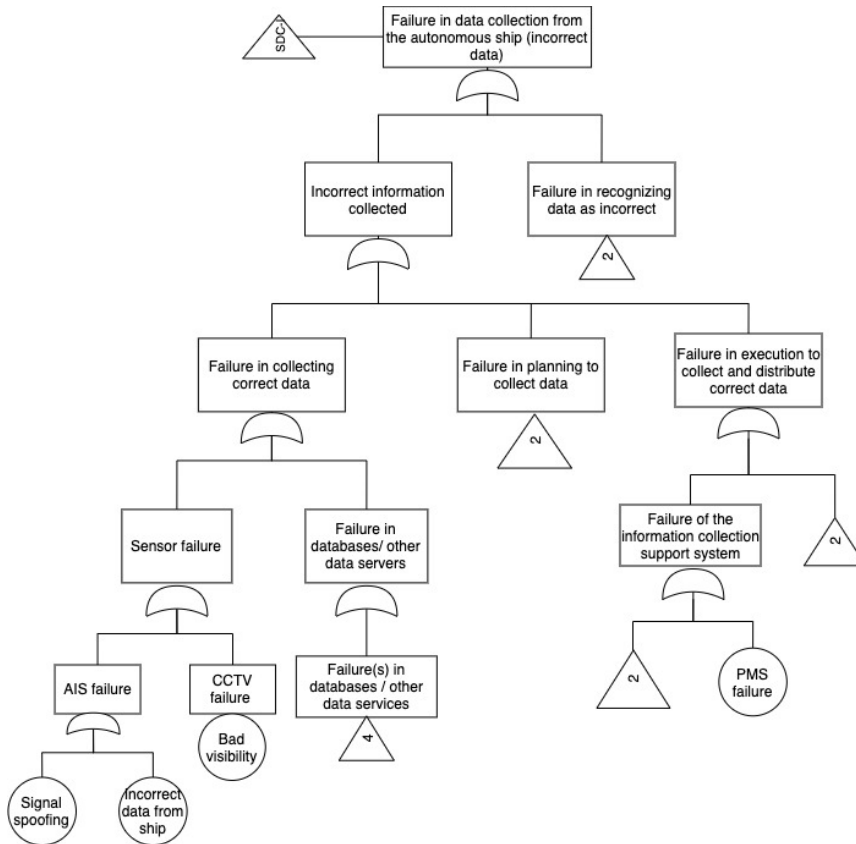


Figure A.5: Fault tree with the top event failure in data collection from the autonomous ship (incorrect data)

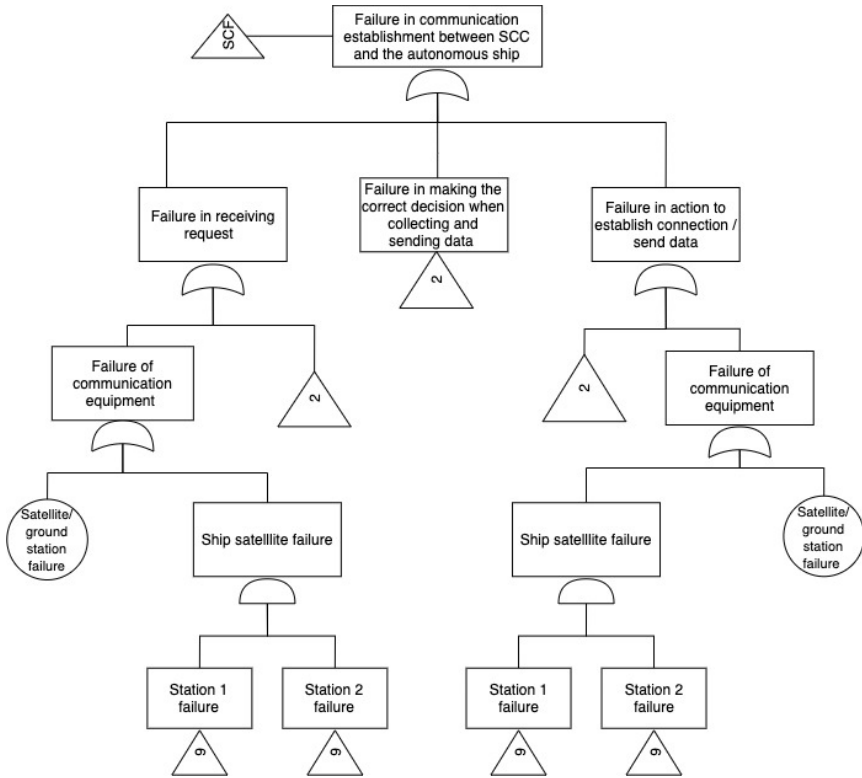


Figure A.6: Fault tree with the top event failure in communication establishment between the SCC and the autonomous ship

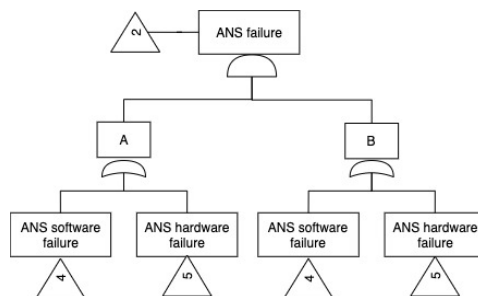


Figure A.7: Fault tree with the top event ANS failure

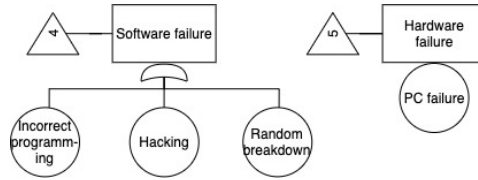


Figure A.8: Fault trees with the top event software failure and hardware failure

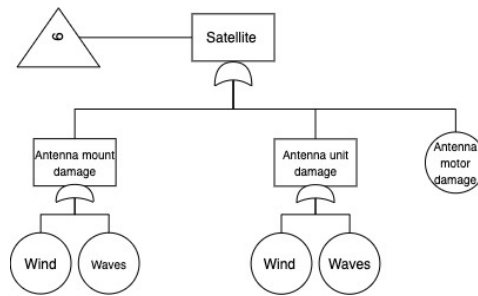


Figure A.9: Fault tree with the top event satellite failure

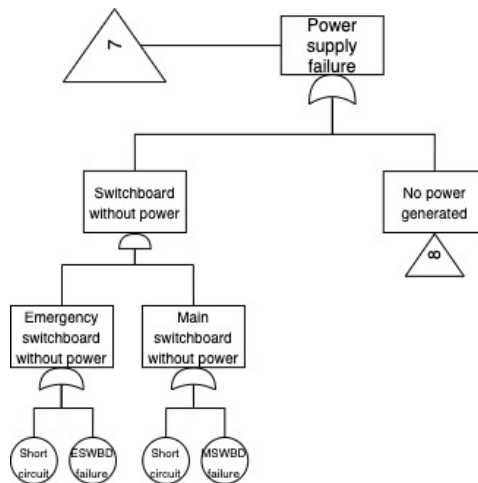


Figure A.10: Fault tree with the top event power supply failure

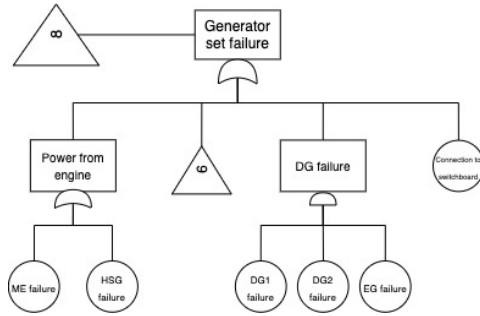


Figure A.11: Fault tree with the top event generator set failure

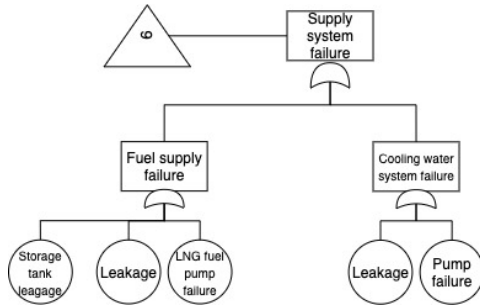


Figure A.12: Fault tree with the top event supply system failure

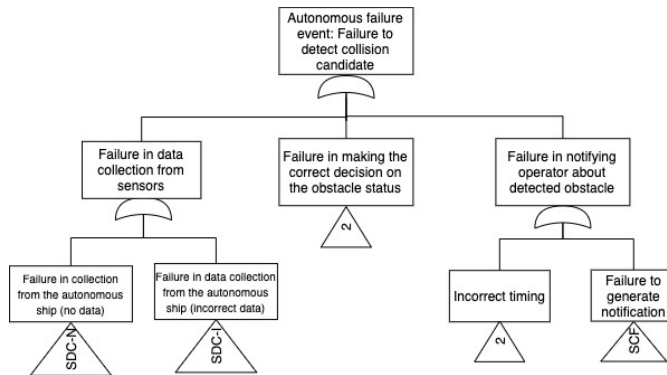


Figure A.13: Autonomous ship failure event with the top event failure to detect collision candidate

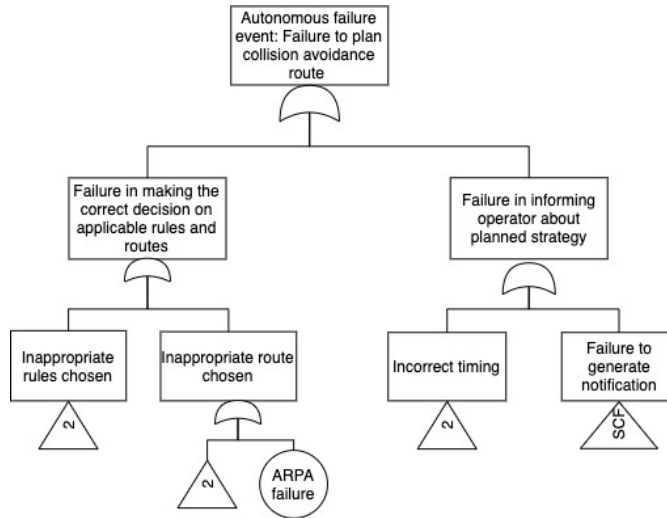


Figure A.14: Autonomous ship failure event with the top event failure to plan collision avoidance route

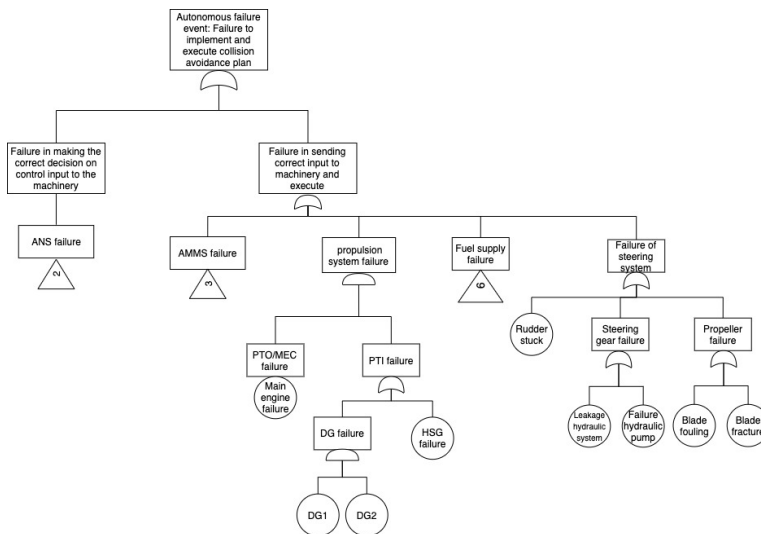


Figure A.15: Autonomous ship failure event with the top event failure to implement and execute collision avoidance plan

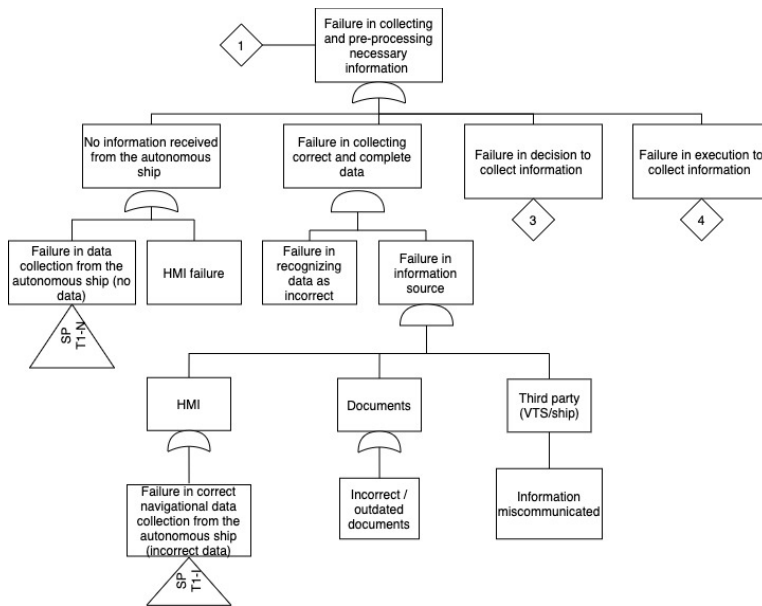


Figure A.16: Human operator failure with the top event failure in collecting and pre-processing necessary information



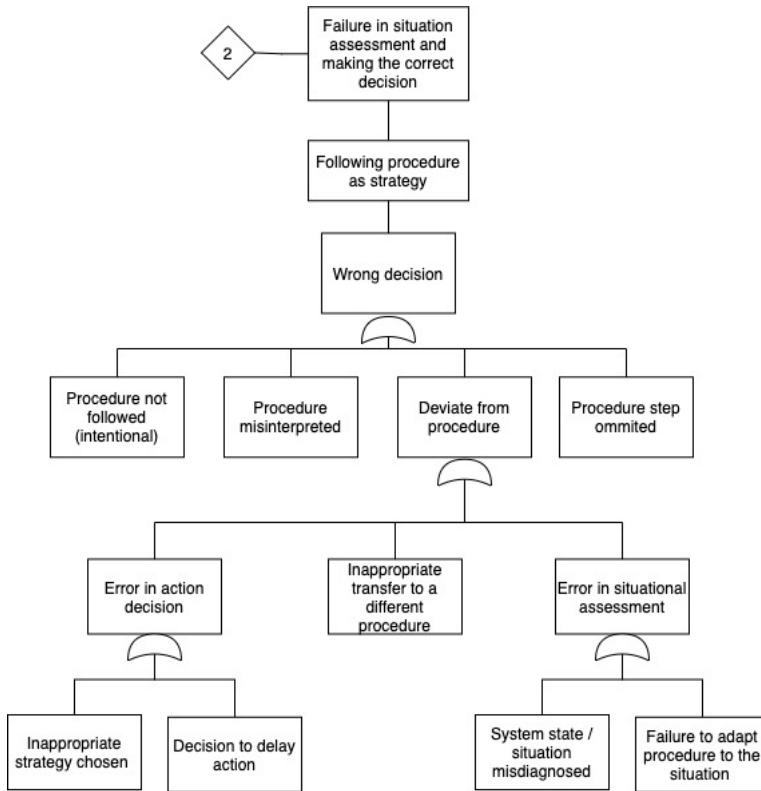


Figure A.17: Human operator failure with the top event failure in situation assessment and making the correct decision

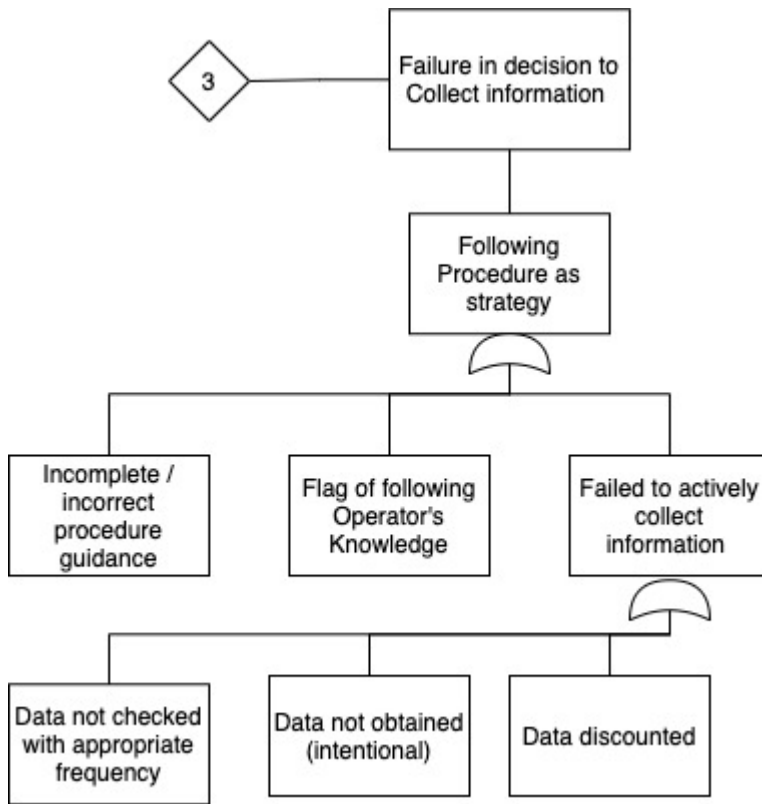


Figure A.18: Human operator failure with the top event failure in decision to collect information

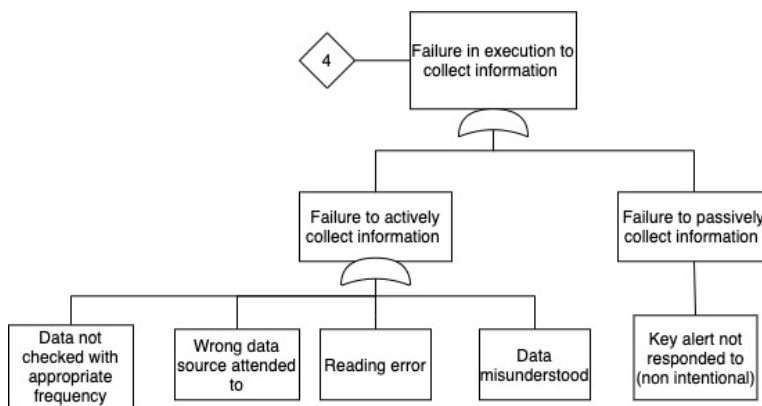


Figure A.19: Human operator failure with the top event failure in execution to collect information

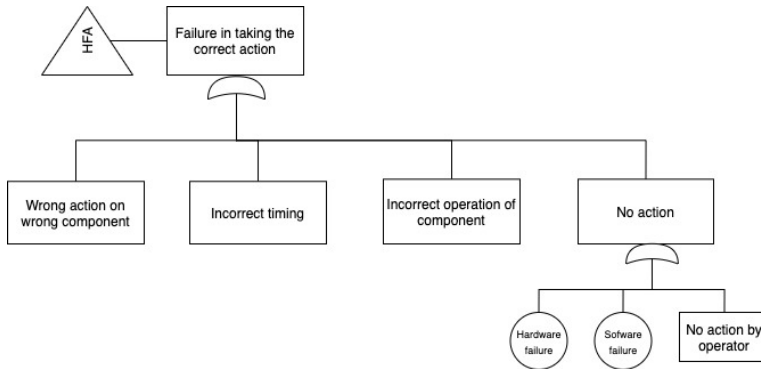


Figure A.20: Human operator failure with the top event failure in taking the correct action

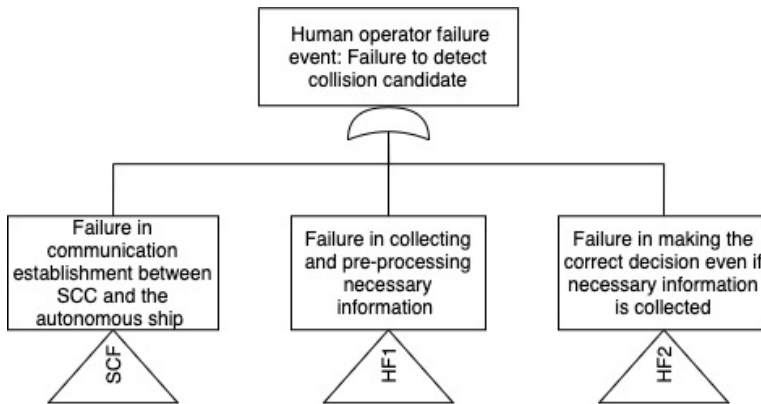


Figure A.21: Human operator failure event with the top event failure to detect collision candidate

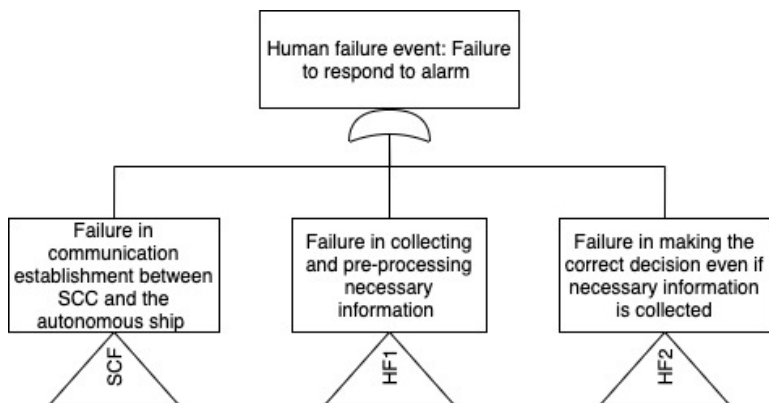


Figure A.22: Human operator failure event with the top event failure to respond to alarm

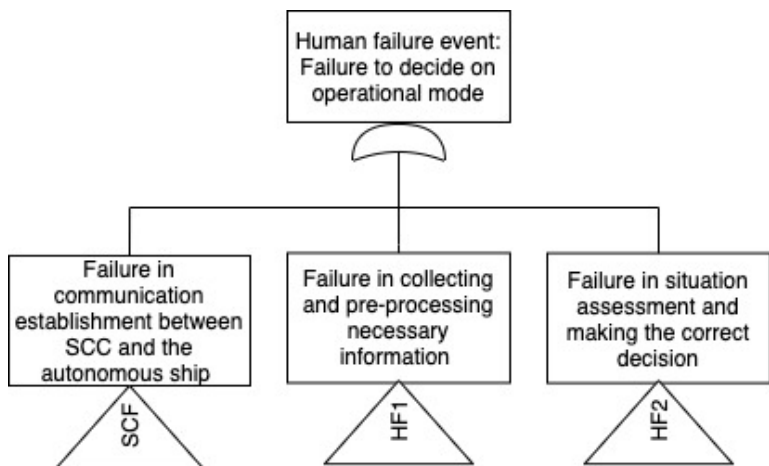


Figure A.23: Human operator failure event with the top event failure to decide on operational mode

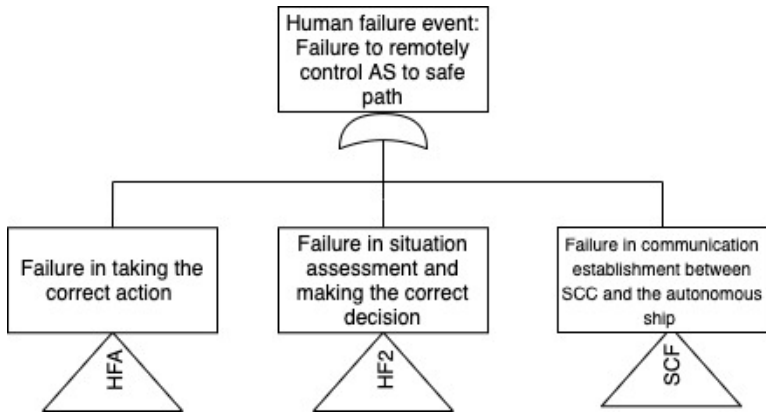


Figure A.24: Human operator failure event with the top event failure to remotely control AS to safe path

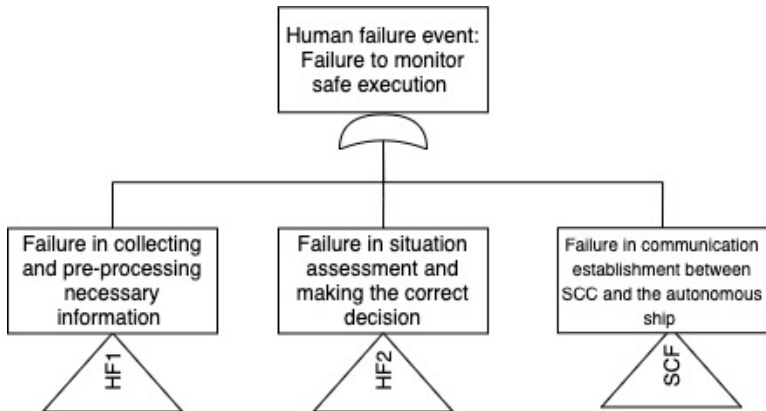


Figure A.25: Human operator failure event with the top event failure to monitor safe execution

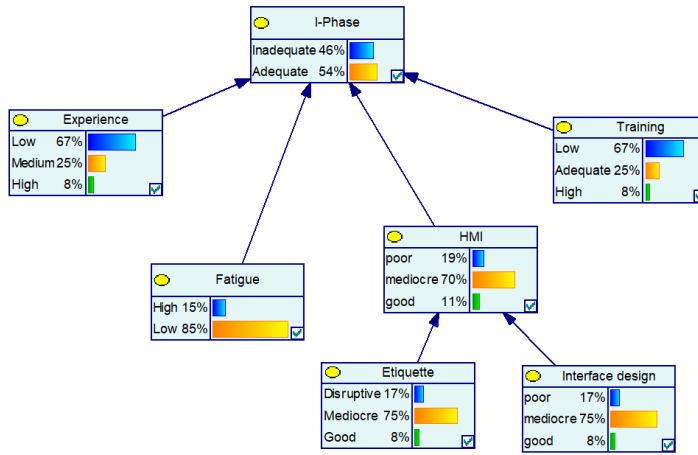


Figure A.26: BBN for the I-phase

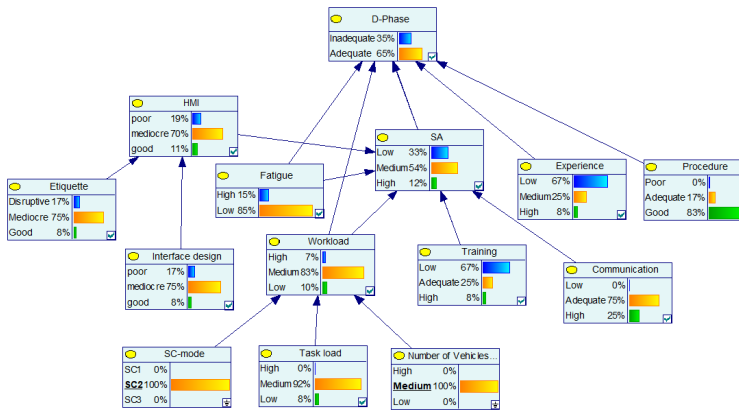


Figure A.27: BBN for the D-phase

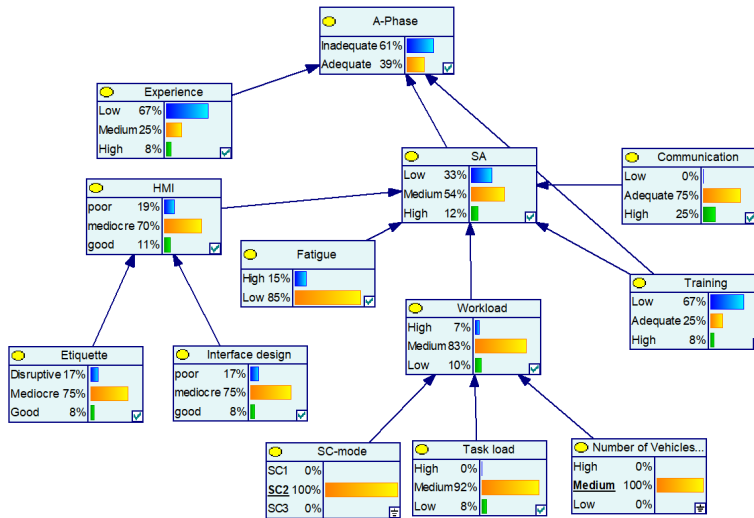


Figure A.28: BBN for the A-phase



## Additional tables

Table B.1: Autonomous ship basic failure events leading to failure in data collection (taken directly from [24])

Basic Failure Event	Description
Sensor(s) not available or Sensor(s) produce incorrect measurements	One or several sensors fails and either produce no output (SDC-N) or an incorrect output (SDC-I). The sensors involved and the logical connection of these are highly dependent on the situation of concern. Sensor failures may range from optical sensors, to cameras, over radar, or accelerometers
Failure(s) in databases/other data servers	Data that is not provided or incorrectly provided may also a failure source for failure of data collection. Similar to the Sensor failure described above, these are highly context specific failures that may have several sub events



<b>Basic Failure Event</b>	<b>Description</b>
Data sampling frequency selected inappropriately	Depending on the situation, the frequency may be too low, no data is available, since it was not collected yet, or the data was not updated yet. Another example are adaptive sampling algorithms that may decide not to collect information when necessary or too late
Failure to plan to poll data (for SDC-N)	Failure of the system to collect data when this is needed. The data in this case is of sporadic type and not collected continuously. An example of such data could be the weather forecast data that is not polled when an update is available
Data discounted (for SDC-N)	The ship makes the decision to not use available data. This may happen due to some failure in voting, or erroneous weights
Incorrect data source selected (for SDC-I)	In this case a failure is caused by the system deciding to collect data from the wrong source. Examples and causes may be, weighing of information sources
Failure of the information collection support system	This is a collective event that may include several basic events that are connected through different logic gates. This basic event refers to these failures in the data collection system that are caused through failed support systems. Events may include failure(s) in the network, loose or broken cables, a (partial) blackout, etc.

Basic Failure Event	Description
Data not sampled with the appropriate frequency	<p>This basic failure event may also cause both failures leading to no data, or failures leading to incorrect data. This FM, in comparison to Data sampling frequency selected inappropriately describes the failure of the ship to collect data with the appropriate sampling frequency. Reasons and causes may be found in a network overload or a software-hardware system that cannot process the amount of data fast enough</p>
Wrong data source attended to	<p>This basic failure event may also lead to no data or incorrect data being collected. Instead of collecting the data from the correct source, another source is used for obtaining that information. That source may not contain the information or have incorrect information. An example may be the retrieval of information from a data server instead of directly from the sensor network</p>
Misinterpretation of raw data	<p>This basic failure event describes a failure where the obtained raw data is encoded in one data type, but the ship interprets the data as another datatype. This may lead to the case that the information cannot be interpreted (SDC- N), or that the information is transferred into another value and hence incorrect (SDC-I)</p>
Data not obtained (for SDC-N)	<p>The autonomous ship polls for information does not obtain the information back. An example may be, if the system asks for a specific variable name, but this variable name is different from the variable name, the data is associated with</p>

Basic Failure Event	Description
Data obtained too late (SDC-N)	The system collects the data too late to execute to current action correctly. Similar to the inadequate frequency this may be caused by an overload of the network, or insufficient processing capabilities
Incorrect normalization of data (SDC-D)	The data that is supposed to be used is processed incorrectly and hence leads to a failure
Failure in recognizing data as incorrect (SDC-I)	This event summarizes the detection capabilities of a failure during data collection for the event under consideration. Such features may cover only a part of the possible failures described above. Such systems may include validity checks, probabilistic reasoning, etc.

Table B.2: Autonomous ship basic failure events leading to failure in communication (taken directly from [24])

Basic Failure Event	Description
Failure(s) of communication equipment	This basic failure event is a set of events connected through logic gates. These failures represent the failure of different communication equipment, e.g., satellites, mobile network, satellite receiver, etc.
Failure to acknowledge communication request	The ship receives a request for communication. However, the ship does not realize the request, e.g., it does not realize that it is the ship called over radio
Failure to acknowledge data request	The ship does not realize that it is required to send data although the request has been received. This may be caused by a failure to understand the request

Basic Failure Event	Description
Failure to choose correct communication channel	The ship chose a communication channel that is inadequate for the current situation. E.g., using radio or the mobile network to reach the shore base while being on the high seas
Decision to delay action	The ship decides to delay further action, due to prioritization of other tasks
Failure to choose correct communication partner	The ship does not identify the correct communication partner, e.g., it identifies wrongly the calling vessel and informs the operator about the wrong calling vessels
Failure in recognizing requested data	The ship fails to identify the requested data. This may be due to a request for data with an unknown variable name
Communication established with the incorrect partner	The ship established the communication with the wrong partner, i.e., it calls upon the wrong vessel through a satellite phone connection
Incorrect operation of communication equipment	The vessel fails in operating the communication equipment as required. Possible failures include, use of incorrect encryption/encoding of the information, or use of an inadequate frequency in radio
Failure of communication equipment	Equipment for communication has a failure and is not operable. This may be caused through software or hardware related failures, such as, failure of antennas, partial blackout, failure of transponder
Incorrect timing	The ship executes the requested action with respect to communication at the wrong time. In most cases, too late will be the basic failure event

Table B.3: Autonomous ship basic failure events leading to failure in situation assessment and decision making (taken directly from [24])

<b>Basic Failure Event</b>	<b>Description</b>
System/environmental state misdiagnosed	The ship and its algorithms cannot assess the state of the ship and/or its environment correctly. This may be the position of ship in relation to objects and other ships, or the wave and wind load that may alter the course of the ship
Failure to adapt strategy to the situation	A strategy planned by the ships algorithms is insufficient for the present situation. A strategy in this article is related to “learned” and adaptive behavior of the system. Examples may be found in a self-learned algorithm for trajectory prediction, or the self-learned collision avoidance strategy that is insufficient in the current situation
Inappropriate procedure chosen	A procedure followed by the ship is inadequate in the current situation. Procedure in this article refers to directly implemented rules and behaviors in the algorithms of the ship. Examples are turning in the wrong direction, or action if no action is required by the ship
Decision to delay action	The system may delay further action, e.g., prioritizing other actions
Decision to delay action	The ship decides to delay further action, due to prioritization of other tasks

Table B.4: Autonomous ship basic failure events leading to failure in action (taken directly from [24])

<b>Basic Failure Event</b>	<b>Description</b>

<b>Basic Failure Event</b>	<b>Description</b>
Action on wrong component	The intended action is not carried out by the intended component. For the ship, this maybe actuation of the wrong thruster. Failure causes for this event may be found in interaction failures, software failure, hardware failure, etc.
Incorrect timing	The intended action is not carried out in the right time. This may be too early, but in most cases a delay will be a relevant failure cause
Incorrect operation of components	The action is not carried out as expected. This may be too much thrust from the thruster, or too little pitch of the rudder
Failure of components	A physical failure of one or several components leads to failure of the action. The basic events are collected below an or-gate but may be connected through other logic gates. Examples are the failure of a thruster, failure of an engine, failure in the gear box, etc.

Table B.5: Operators' basic failure events leading to failure in information gathering and pre-processing (taken directly from [24])

<b>Basic Failure Event</b>	<b>Description</b>
Failure in recognizing data as incorrect	The operator receives incorrect data and fails to recognize it
Information miscommunicated	During communication between the operator at the SCC and team member or a third party there may be a miscommunication, in which the information is not complete or in incorrect, or it is sent to the wrong person or at a wrong time

Basic Failure Event	Description
Data not checked with appropriate frequency	This event is particularly relevant during monitoring tasks. For instance, if the system operates with a high LoA and the operator should take over control in case of a problem, the operator must be checking the HMI with an appropriate frequency. If s/he fails to do so, s/he may miss an important shift in one variable, or a variable that is out of the expected range
Data not obtained (intentional)	The operator intentionally fails to collect a data needed for the operation. S/he may believe, for instance, that the data at hand about the environmental conditions suffices and decides to not collect an additional piece of data that would complete their assessment
Data discounted	The operator gathers particular data s/he needs but decides to discard it afterwards. S/he may assume the data is not relevant for the situation. For example, s/he may see at their screens that there is an object approaching the ship, but believe the paths will not cross, and discard this information when performing situation assessment
Key alert not responded to	A key alert should alert the operator about a crucial status of the system, and their response to it should put them in the path of a successful outcome. For instance, it is expected that in certain LoAs the operator will be able to override the system, or shut it down in case of an emergency, among other situations

<b>Basic Failure Event</b>	<b>Description</b>
Wrong data source attended to	The operator is aware of a needed information but collect it from a wrong source. This failure event can be particularly relevant in case the operator is monitoring more than one ship at a time
Reading error	The operator performs an error during reading a piece of information. This may be an information from the HMI or from a written guideline /procedure. They may, for instance, incorrectly read a speed number
Data misunderstood	The operator gathers data but incorrectly internally processes it

Table B.6: Operators' basic failure events leading to failure in situation assessment and decision making (taken directly from [24])

<b>Basic Failure Event</b>	<b>Description</b>
Procedure not followed	The operator intentionally does not follow the procedures or guidelines. S/he decide to follow their own knowledge instead, whereas following the procedure /guidelines would put lead to success
Procedure misinterpreted	The operator is following the procedure or guidelines but incorrectly interprets it
Procedure step omitted	The operator is following the procedure but omits one step of it. This may be due to, for instance, a perceived lack to available time to follow the procedure, or a confidence that certain steps are not necessary



<b>Basic Failure Event</b>	<b>Description</b>
Inappropriate strategy chosen	The operator correctly diagnoses the situation but chooses an inappropriate strategy to deal with it. For instance, s/he may recognize a potential collision scenario involving the autonomous ship but decide to avoid the collision by lowering the speed when the correct strategy would be to change the ship course
Decision to delay action	The operator decides to delay an action. This may be because s/he believes that the information at hand is not sufficient and s/ he waits for gathering more information
Inappropriate transfer to a different procedure	The operator transfers to another guideline when it is inappropriate. For example, s/he transfers to a local rule that is not appropriate for the situation in hand
System state/situation misdiagnosed	The operator misdiagnoses the situation in hand. For instance, s/he may visualize a ship approaching the autonomous ship, but assess that, given its speed and direction, it will not be on collision course
Failure to adapt procedure to the situation	The operator is following a certain procedure but does not understand how to adapt it to the situation at hand

Table B.7: Operators' basic failure events leading to failure in action (taken directly from [24])

<b>Basic Failure Event</b>	<b>Description</b>
Action on wrong component	The operator performs a correct and needed action, but on the wrong component. The component may be a ship component or a component of the HMI

Basic Failure Event	Description
Incorrect timing	The operator executes the decision in a bad timing – too late or too early
Incorrect operation of component	The operator operates the correct component in an incorrect manner
No action	The operator fails to take the action, despite having previously decided to take it. This may be due to external factors

Table B.8: States and values for input nodes in the BBN

Node	States			Source
	Worst	Intermediate	Best	
Communication	0.001	0.749	0.250	[65]
Etiquette	0.167	0.750	0.083	[65]
Interface design	0.167	0.750	0.083	[65]
SC-mode		SC-2		[44]
Number of ships per operator	0	1	0	Scenario
Experience	0.667	0.250	0.083	[65]
Training	0.667	0.250	0.083	[65]
Procedure	0.001	0.166	0.833	[65]
Task load	0.001	0.016	0.083	[65]

Table B.10: Calculated failure probabilities

Component	Failure rate	Factor	Failure rate · factor	$F(t) = 1 - \exp(-\lambda t)$	Source
CLU - software	1.23E-042	0.2187 [8]	2.69E-05	3.77E-04	[66], pages 262, 263, 267, 269
CLU - hardware	1.23E-04	0.4948 [8]	6.09E-05	8.52E-04	[66], pages 262, 263, 267, 268
Pumps	2.18E-04	0.6632 [8]	1.45E-04	2.02E-03	[66], pages 104, 106, 108
Component	1.05E-05	1	1.05E-05	1.40E-04	[55], page 40
Main engine	1.80E-04	1	1.80E-04	2.52E-03	[50]
Diesel generator	5.04E-04	1	5.04E-04	7.03E-03	[50]
HSG	3.60E-04	1	3.60E-04	5.03E-03	[50]

Table B.12: IMO frequency categories [67] and corresponding failure probabilities

Frequency categories	per ship year	Per hour (6480 operational hrs in one year)	$F(t) = 1 - \exp(-\lambda t)$
Frequent	10	$1.50E - 03$	$2.1E - 02$
Reasonably probable	0.1	$1.50E - 05$	$2.2E - 04$
Remote	0.001	$1.50E - 07$	$2.2E - 06$
Extremely remote	0.00001	$1.50E - 09$	$2.2E - 08$

Table B.14: Basic event probabilities and failure rate data source

Basic Event	Failure probability	Failure rate data source
Antenna motor	3.9E-03	[68], page 138
Antenna mount - waves	2.2E-04	Assumed based on [67] - reasonably probable
Antenna mount - wind	2.2E-06	Assumed based on [67] - remote
Antenna unit - waves	2.2E-04	Assumed based on [67] - reasonably probable
Antenna unit - wind	2.2E-06	Assumed based on [67] - remote
ARPA failure	8.52E-04	[66], pages 262, 263, 267, 269
Blade fouling	2.2E-04	Assumed based on [67] - reasonably probable
Blade fracture	2.2E-06	Assumed based on [67] - remote
Camera damage - waves	2.2E-04	Assumed based on [67] - reasonably probable
Camera damage - wind	2.2E-06	Assumed based on [67] - remote
Camera hardware	1.4E-04	[55]

<b>Basic Failure Event Probabilities</b>	<b>Failure probability</b>	<b>Failure rate data source</b>
Connection to switchboard	1.40E-04	[55]
Cooling water leakage	2.2E-06	Assumed based on [67] - remote
Diesel generator failure	7.03E-03	[50]
Fuel supply leakage	1.0E-07	[53]
Hacking	2.2E-04	Assumed based on [67] - remote
HMI failure	8.52E-04	[66], pages 262, 263, 267, 26
HSG failure	1.4E-06	[50]
Hydraulic pump failure	2.02E-03	[66], pages 104, 106, 108
IMU failure	8.52E-04	[66], pages 262, 263, 267, 269
Incorrect data from ship	2.2E-04	Assumed based on [67] - remote
Incorrect programming	0	Set
Leakage hydraulic system	1.0E-07	[53]
LNG fuel pump failure	2.02E-03	[66], pages 104, 106, 108
Main engine failure	2.52E-03	[44]
No image - bad visibility	3.1E-03	[8]
PC failure	8.52E-04	[66], pages 262, 263, 267, 269
PMS failure	3.77E-04	[66], pages 262, 263, 267, 269
Pump failure	2.02E-03	[66], pages 104, 106, 108
Radar failure	1.7E-02	[69], page 52
Random breakdown	3.77E-04	[66], pages 262, 263, 267, 269
Rudder stuck	2.2E-06	Assumed based on [67] - remote
Sender failure	1.4E-04	[55]

---

<b>Basic Failure Event Probabilities</b>	<b>Failure probability</b>	<b>Failure rate data source</b>
Sensor failure	1.4E-04	[55]
Short circuit	2.20E-06	Assumed based on [67] - remote
Signal jamming	5.0E-04	[70]
Signal spoofing	2.2E.04	Assumed based on [67] - remote
Storage tank leakage	5.0E-06	[53]
Switchboard failure	2.20E-04	Assumed based on [67] - remote

---

Table B.15: Ship types and route frequencies crossing Rørvik in 2020 [64]

Ship type	B [m]	V [kn]	Frequency		Reference ship
			S	N	
Chemical tankers	24.23	7.70	19	16	[71]
Gas tankers	36.60	16.30	4	4	[72]
Bulk carriers	12.80	12.00	25	20	[73]
Cargo vessel	13.60	14.00	25	20	[49]
Tankers	16.72	15.00	4	5	[74]
RoRo	29.40	15.80	6	7	[75]
Reefer ship	16.00	11.10	23	20	[76]
Offshore supply ship	18.00	12.00	10	12	[77]
Tugs	13.00	9.00	2	2	[78]
Pleasure craft	5.00	25.00	49	43	[79]
Fishing vessel	8.00	6.00	106	121	[80]
Oil tankers	46.03	5.50	11	10	[81]
Passenger vessel	10.80	34.00	68	66	[82]
Cruise ship	19.20	15.00	7	6	[83]
Ferry(crossing)	13.60	10.10	442	442	[84]

