Safety Analysis of the Navigation System of Autonomous Ships

Copyright (AUTOSHIP H2020, 2019)

Markella Pikouni

Registration Number: 201642838

Supervisors: Dr Gerasimos Theotokatos & Professor Chengi Kuo

Department of Naval Architecture, Ocean and Marine Engineering

University of Strathclyde, Glasgow

April 17, 2020

ABSTRACT

Autonomous vessels are approaching reality. Before the launching of unmanned and fully autonomous vessels, it is essential that their safety is assessed in order to ensure that they will not pose any security and environmental threat. It is expected that Marine Autonomous Surface Ships (MASS) are likely to experience more hazards with high risk levels than the conventional vessels. One of the systems that requires careful attention is the navigational one. It is important to find ways to enhance the safety of the system and mitigate the risk level of the various hazards.

This report begins by introducing the topic before outlining the main objectives of the project. The current status of the subject is established after conducting critical review. The section provides information to enable the better understanding of MASS as well as safety assurance techniques that are widely used nowadays. Accident data for conventional ships together with collision avoidance systems that have been implemented in various industries are also examined. Areas that require special attention are identified and a research issue is selected for deeper investigation. The research approach and associated strategy for tackling the project are presented before describing the various systems of MASS and the hazards related to their safe operation. The selection of the most appropriate safety assurance method and the conduction of the case study are then given attention. The results are analysed, and conclusions are drawn. Lastly, future developments of the project are proposed together with the practical use of the results.

Based on the research study, the following conclusions are drawn: firstly, the navigation system is more prone to failure during harsh weather conditions if the various system components are developing faults. Secondly, a fully autonomous vessel is more likely to have a greater failure rate than a vessel which has a dynamic level of autonomy that is supervised or remotely controlled by the Shore Control Centre (SCC). The presence of the SCC offers additional redundancy but may expose the vessel to hazards associated with human factors, such as human errors.

DECLARATION

I hereby declare that the dissertation entitled ‘Safety Analysis of the Navigation System of Autonomous Ships’ that I submit at the Department of Naval Architecture, Ocean and Marine Engineering of the University of Strathclyde in Glasgow, is my original work. The information derived from literature has been duly acknowledged in the text and a full list of the references used can be found in the corresponding section of this report.

Markella Pikouni

April 17, 2020

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisors who assisted me to successfully complete this project. Dr Theotokatos provided me with essential guidance since the very beginning of this project and shared some expert advice on the subject, while Victor Bolbot, Research Assistant, was open to discussions about my progress and results.

Professor Kuo guided me in order to organise my project work efficiently following a Systematic Management of Engineering Projects (SMEP) approach. He encouraged me to pay special attention to the presentation of my work. He was always available to give me advice and helped me to gain self-confidence.

TABLE OF CONTENTS

LIST OF FIGURES

Note: The autonomous ship that is depicted in the cover page is subjected to copyright (AUTOSHIP H2020, 2019).

LIST OF TABLES

LIST OF ABBREVIATIONS

AAWA	Advanced Autonomous Waterborne Applications
AEMC	Automated Engine Monitoring and Control
AIS	Automatic Identification System
ARPA	Automatic Radar Plotting Aid
ASC	Autonomous Ship Controller
ASM	Advance Sensor Module
DPS	Dynamic Positioning System
ECDIS	Electronic Chart Display and Information System
ECT	Emergency Control Team
EOSP	End Of Sea Passage
FAOP	Full Ahead On Passage
FMECA	Failure Mode Effects and Criticality Analysis
FTA	Fault Tree Analysis
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GPC	General-Purpose Computer
IMU	Inertial Measurement Unit
LiDAR	LIght Detection And Ranging
LoA	Level of Autonomy
MASS	Marine Autonomous Surface Ship
MUNIN	Marine Unmanned Navigation through Intelligence in Network
NTNU	Norwegian University of Science and Technology
OCT	Onboard Control Team
RMSS	Remote Manoeuvring Support System
SAS	Ship Automation System
SCC	Shore Control Centre
SSS	Short Sea Shipping
STAMP	Systems-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
TRL	Technology Readiness Level
VTS	Vessel Traffic Services

1. INTRODUCTION

Marine Autonomous Surface Ships (MASS) are considered the future of maritime transportation and this is the reason why they are of great interest in the academic as well as the industrial world. Studies have shown that almost 85% of the total number of accidents at sea are caused by inaccurate human decisions and for this reason, the reduction of crew members onboard is expected to have a positive effect on the safe operation of the vessels together with less fatalities and injuries in case of an accident (Illkyun et al., 2018). Therefore, the systems and spaces that are only used by the crew in conventional ships can be removed from the fully autonomous vessels in order to reduce the construction, maintenance and operational costs as well as to free up space that can be used to carry more cargo. Moreover, the autonomous ships will lead to greener shipping and be able to operate in dangerous areas (Ramos et al., 2019).

Automation is implemented gradually on board the ships. During the last few years, most of the systems that are present have been automated, but are not fully autonomous, meaning that the crew is still supervising and taking actions if necessary. It is not expected that fully unmanned and unattended vessels will operate in the near future. Operators in a Shore Control Centre (SCC) will be responsible to supervise or remote control the vessel according to the Level of Autonomy (LoA), in order to provide instantaneous backup in case of a system failure onboard the ship. It is worth noting that MASS may operate with a Dynamic LoA that will change according to the stage of the voyage. It is obvious that since SCC personnel will still affect the safe operation of the ship, MASS will be subjected to human factor (Ramos et al., 2018).

Challenges of the sector:

The main challenge that has to be faced is the reassurance that MASS can operate safely without posing any security and environmental threat. One of the biggest hazards that a MASS may face is the likelihood of communication loss with the SCC. Moreover, maintenance work cannot be undertaken during the voyage because of the absence of crew onboard (Ramos et al., 2019). Sufficient cyber risk management of the systems should also be ensured to reduce the risk of cybersecurity attacks (Bolbot et al., 2019). For the aforementioned reasons, safety analysis of MASS is of great importance and requires attention. However, the quantitative safety analysis is demanding because of the luck of accurate quantitative data due to the novelty of the subject. Therefore, estimations of the risk levels of the various hazardous events have to be made after conducting extensive review and analyzing the findings of previous research and development projects on MASS.

Related past and current work:

There have been numerous projects on MASS, some of which are in their testing phase. Autonomous land vehicles have already been tested and are more developed than ships. Autonomy in the maritime sector is still evolving with the highest degree of autonomy present in the Autonomous Underwater Vehicle, where the absence of traffic makes its operation easier.

In order for the autonomous ship models to be tested and to define hazards associated with their navigation, the first test area for autonomous ships was opened in Trondheim Fjord in 2016 (Fjørtoft, 2017). DNV GL in association with the Norwegian University of Science and Technology (NTNU) are testing a 1:20 scale model of a fully battery power Short Sea Shipping (SSS) vessel (Alfheim et al., 2018, Späth, 2018). A picture of the unmanned vessel DNV ReVolt can be found in Figure 1. NTNU will also test an autonomous ferry in 2020 after completing the testing of a 1:2 scaled model as shown in Figure 2. Note that during the testing phase, people can get onboard in to control the vessel if necessary.

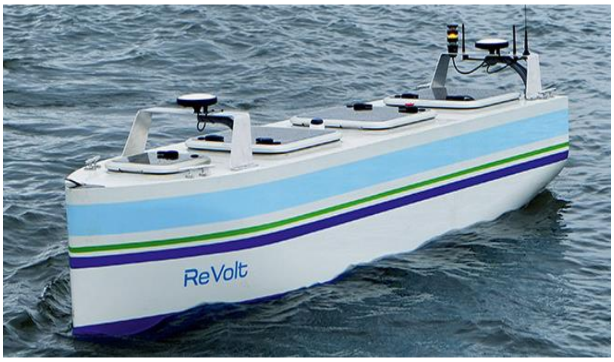


Figure 1 - DNV ReVolt (Späth, 2018)

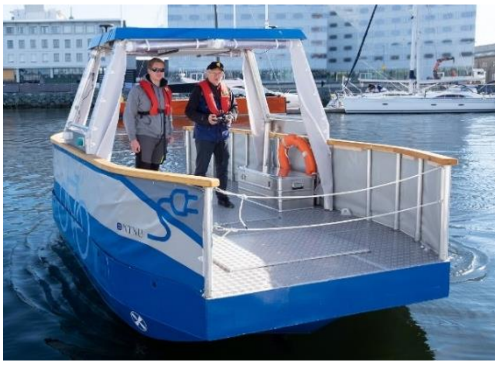


Figure 2 - NTNU Autoferry Photo: Kai Dragland (NTNU, 2018)

Furthermore, Yara and Kongsberg designed the first fully electric and autonomous container vessel with zero emissions that will be launched in 2020 (Skredderberget, 2018). The MUNIN project examined the characteristics of autonomous vessels as well as the obstructions in communication between the vessel and the SCC (Burmeister et al., 2014, MUNIN, 2016). Lastly, Advanced Autonomous Waterborne Applications (AAWA) that is consisted of universities, manufacturers and classification societies aims to improve the detailed design of future autonomous ships (Illkyun et al., 2018).

It has been proven that the majority of accidents of conventional ships are resulted from malfunctioning or failure of the navigation system (EMSA, 2019). The risk level of unsafe navigation of MASS is expected to be increased compared to conventional vessels. Therefore, the failure of the navigation system of MASS requires attention, and this was the reason why it was selected to be analysed.

2. PROJECT AIM AND OBJECTIVES

The aim of the project is to conduct safety analysis and enhancement of the navigational system of a MASS, which is a very novel and important matter concerning the maritime industry.

The main objectives are:

1) To perform literature review in order to establish the subject status.
2) To perform critical review on the methods used to analyse safety of conventional ships and assess their applicability to MASS.
3) To examine hazards associated with the navigation of MASS and estimate their risk level.
4) To conduct safety analysis and propose system enhancements.

3. CRITICAL REVIEW

3.1 WHAT IS A MASS

According to IMO “a MASS is a ship which, to a varying degree, can operate independently of human interaction” (IMO, 2018a). There are various definitions about the terminology of the different Levels of Autonomy (LoA) by multiple authorities and classification societies. However, in this report the different LoA had been defined according to Bureau Veritas and are presented in Table 1. The different LoA are determined according to whether the vessel is manned, the method of control, the authority to make decisions and the initiation of the actions (Bureau Veritas, 2019). When defining the LoA, the vessel should be regarded as a single system with interconnected subsystems covering its overall operation and it is vital that the suggested levels should be confirmed after examining their applicability in real life projects (Zubowicz et al., 2019).

Table 1 - Ship Categories and Level of Autonomy According to BV (Bureau Veritas, 2019)

Ship Category	Level of Autonomy		Manned	Method of Control	Decisions	Actions
Conventional	0	Human operated	Yes	Automated or manual operations under human control	Human	Human
Smart	1	Human directed	Yes/No	Decision Support Human makes decisions & actions	Human	Human
Autonomous	2	Human delegated	Yes/No	Human must confirm decisions	Human	System
	3	Human supervised	Yes/No	System is not expecting confirmation Human is informed of the decisions&actions	Software	System
	4	Fully autonomous	No	System is not expecting confirmation Human is informed in case of emergency	Software	System

Absence of the human element in the system is not the key divergence between the different LoA. The main difference is the ability of the ship to handle data precisely and act, in relation to the decisions that the crew would have made if a similar situation occurred in a conventional vessel (Parasuraman and Sheridan, 2000).

3.2 MASS WITH DYNAMIC LEVEL OF AUTONOMY

It is worth noting that in the foreseeable future autonomous vessels will operate with a dynamic LoA by limiting the fully autonomous operation to deep seas while having crew onboard in heavy traffic areas close to ports. This is preferable in order not to cause any legal problem with the port and coastal state water authorities (MUNIN, 2016). The pilots and “Onboard Control Team” (OCT) will embark the ship before departure from a port and disembark at the pilot station point and “Full Ahead On Passage” (FAOP) respectively. After that, the ship will conduct an unmanned passage with continuous supervision from the SCC, which is going to be notified once the automated systems present onboard are not able to safely handle a situation. In that case, the operators will intervene by remotely controlling the ship and if a major problem occurs the “Emergency Control Team” (ECT) will complete the so called “rendezvous” operation and will embark the vessel with the use of helicopters or shuttle boats. Lastly, the OCT will embark when the vessel reaches the “End Of Sea Passage” (EOSP) to perform duties that are normally executed by the ship crew and pilots will take control in dense traffic areas until port arrival in order to prevent technical and operational problems (Rødseth and Tjora, 2014).

As far as conventional ships are concerned, crew is present onboard at all times and is responsible for the safe operation of the vessel. However, expert pilots are boarding the vessel before port departure and arrival in order to operate the vessel in voyage segments where there is need for additional manoeuvring. In case of an emergency or when the vessel enters canals and restricted areas, emergency crew or pilots board the ship in order to perform their tasks. The aforementioned phases for MASS as well as conventional ships are represented in Figure 3; the upper part corresponds to the phases of MASS and the lower part corresponds to the phases of conventional ships.

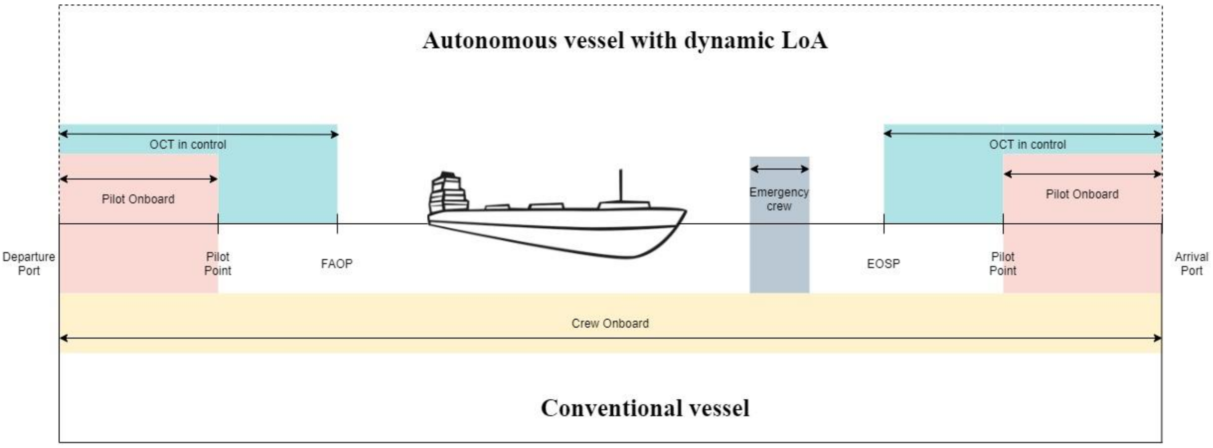


Figure 3 - Voyage phases of a vessel with dynamic LoA and a conventional one (Rødseth and Tjora, 2014)

In the 3rd LoA the SCC will continuously monitor the vessel and the aforementioned teams will embark and disembark whenever necessary as coordinated by the SCC. Vessel Traffic Services (VTS) as well as reporting areas will also be present in order to avoid single point of failure cases. The autonomous ship should have advanced sensors, which are going to be discussed later, in order to detect any potential risks in the vessel's surroundings and it should be able to communicate with other ships as illustrated in Figure 4 (Rødseth and Tjora, 2014). It should be noted that sufficient redundancy should be present in the communication system and the vessel should be programmed to reach the nearest safe location immediately in case of communication failure between the SCC and the ship (MUNIN, 2016).

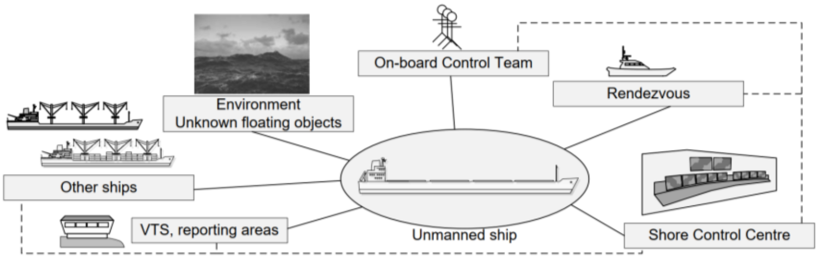


Figure 4 - 3rd LoA Ship Context (Rødseth and Tjora, 2014)

3.3 SAFETY ASSURANCE TECHNIQUES

Since we are approaching a new era in the maritime industry, it is essential that Safety Assurance is performed in order to determine whether the MASS can operate safely. Different safety standards are present in order to either assist the safety guided design or identify the techniques for risk management during operation (Bolbot et al., 2019). ISO 31000 is the most commonly used standard for the operation management of systems (Bolbot et al., 2019, Vara et al., 2016), while IECS 62508 is aligned with the design based on human-machinery interaction and TRL framework focuses on innovative systems design. ISO 31000 is widely used and consists of the following stages: (a) specific hazard identification, (b) risk analysis, (c) risk treatment and (d) risk evaluation (Bolbot et al., 2019).

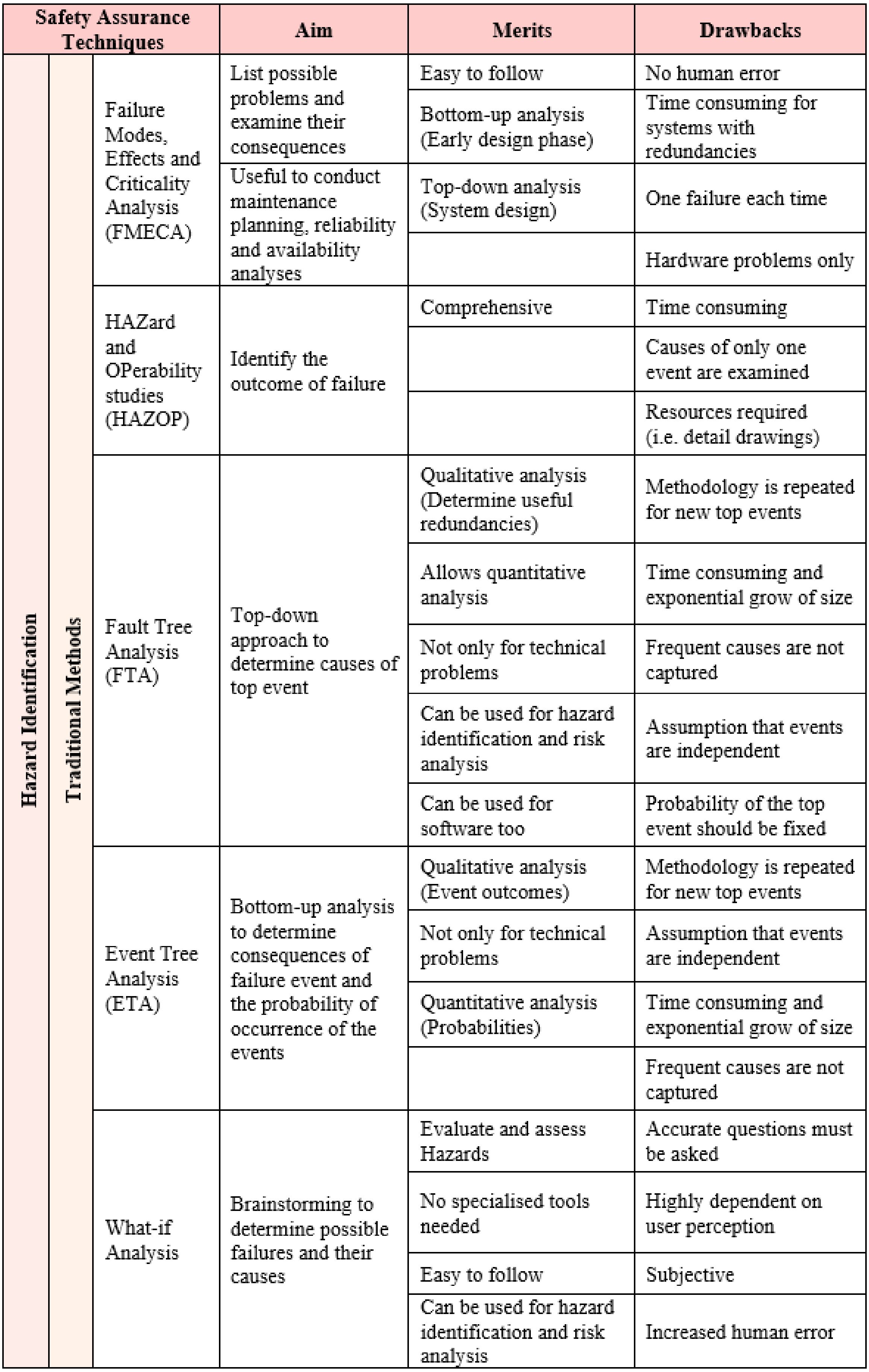
Table 2 presents some of the existing safety assurance methods together with their merits and drawbacks. It is obvious that hazard identification becomes more complex in autonomous systems because of the different hazardous scenarios.

Some of the methods presented in Table 2 can be used for MASS. However, possible amendments might have to be made in order to account for the complex tasks and interconnections between the various sub-systems. These systems introduce new failure modes and discrepancies of the existing methods.

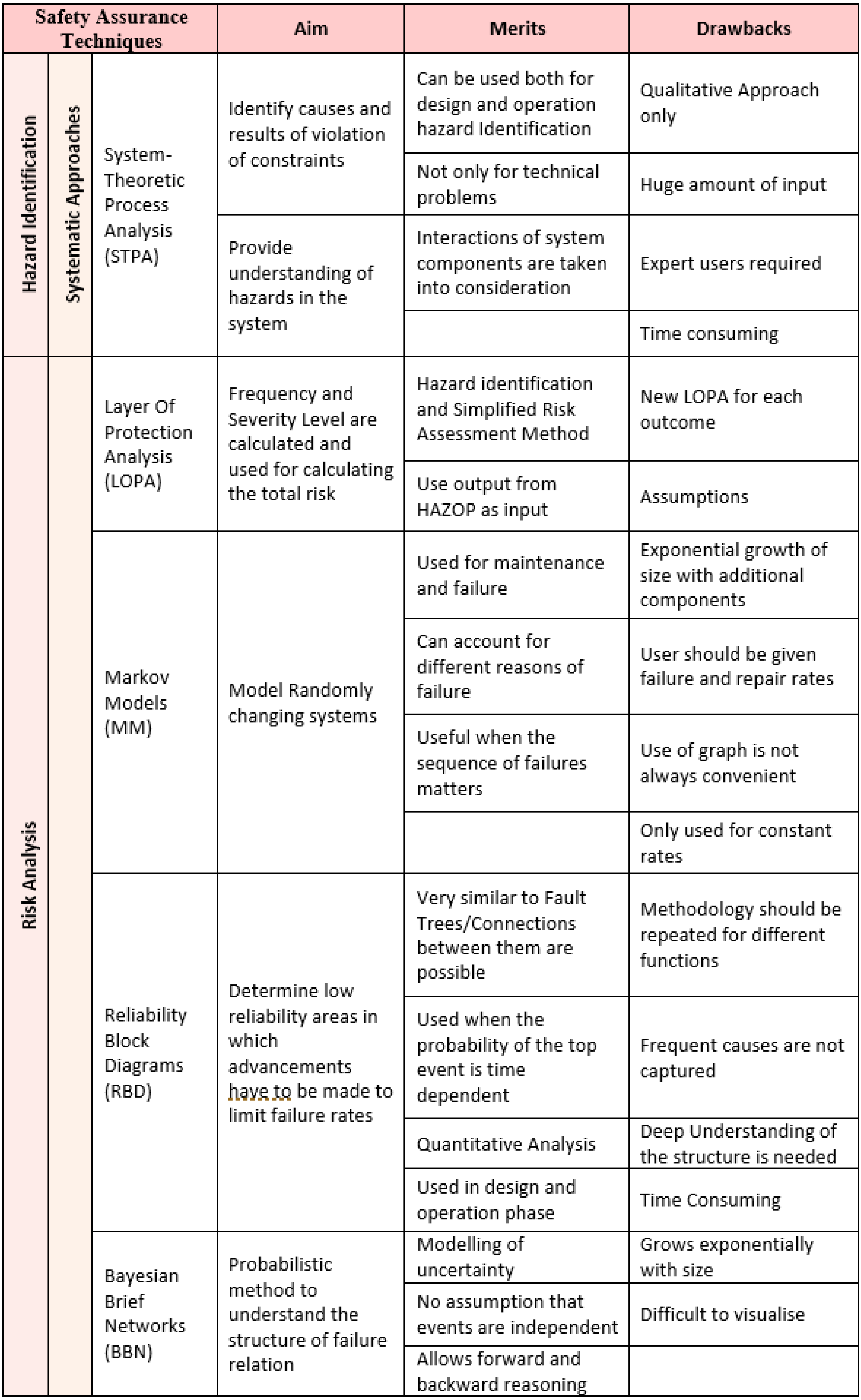
What-if analysis can be used to evaluate the impact of MASS in the maritime industry. Failure Modes, Effects and Criticality Analysis (FMECA) and a modified version of STPA have been used in order to assess the Dynamic Positioning System (DPS) of a vessel and it was concluded that the latter appeared to have more advantages as far as the hazard identification of the system is concerned (Bolbot et al., 2019, Rokseth et al., 2016). The same method had also been used in order to obtain the aim of a test for the vessel’s power management system (Bolbot et al., 2019, Rokseth et al., 2018).

Table 2 will be employed to select the appropriate method in order to conduct the safety analysis in Chapter 7.

Table 2 - Methodologies for Safety Assessment (Bolbot et al., 2019, Pop et al., 2017)



Safety Assurance Techniques			Aim	Merits	Drawbacks
Hazard Identification	Traditional Methods	Failure Modes, Effects and Criticality Analysis (FMECA)	List possible problems and examine their consequences	Easy to follow	No human error
				Bottom-up analysis (Early design phase)	Time consuming for systems with redundancies
			Useful to conduct maintenance planning, reliability and availability analyses	Top-down analysis (System design)	One failure each time
					Hardware problems only
		HAZard and OPerability studies (HAZOP)	Identify the outcome of failure	Comprehensive	Time consuming
					Causes of only one event are examined
					Resources required (i.e. detail drawings)
		Fault Tree Analysis (FTA)	Top-down approach to determine causes of top event	Qualitative analysis (Determine useful redundancies)	Methodology is repeated for new top events
				Allows quantitative analysis	Time consuming and exponential grow of size
				Not only for technical problems	Frequent causes are not captured
				Can be used for hazard identification and risk analysis	Assumption that events are independent
				Can be used for software too	Probability of the top event should be fixed
		Event Tree Analysis (ETA)	Bottom-up analysis to determine consequences of failure event and the probability of occurrence of the events	Qualitative analysis (Event outcomes)	Methodology is repeated for new top events
				Not only for technical problems	Assumption that events are independent
				Quantitative analysis (Probabilities)	Time consuming and exponential grow of size
					Frequent causes are not captured
		What-if Analysis	Brainstorming to determine possible failures and their causes	Evaluate and assess Hazards	Accurate questions must be asked
				No specialised tools needed	Highly dependent on user perception
				Easy to follow	Subjective
				Can be used for hazard identification and risk analysis	Increased human error



Safety Assurance Techniques			Aim	Merits	Drawbacks
Hazard Identification	Systematic Approaches	System-Theoretic Process Analysis (STPA)	Identify causes and results of violation of constraints	Can be used both for design and operation hazard Identification	Qualitative Approach only
				Not only for technical problems	Huge amount of input
			Provide understanding of hazards in the system	Interactions of system components are taken into consideration	Expert users required
					Time consuming
Risk Analysis		Layer Of Protection Analysis (LOPA)	Frequency and Severity Level are calculated and used for calculating the total risk	Hazard identification and Simplified Risk Assessment Method	New LOPA for each outcome
				Use output from HAZOP as input	Assumptions
		Markov Models (MM)	Model Randomly changing systems	Used for maintenance and failure	Exponential growth of size with additional components
				Can account for different reasons of failure	User should be given failure and repair rates
				Useful when the sequence of failures matters	Use of graph is not always convenient
					Only used for constant rates
		Reliability Block Diagrams (RBD)	Determine low reliability areas in which advancements have to be made to limit failure rates	Very similar to Fault Trees/Connections between them are possible	Methodology should be repeated for different functions
				Used when the probability of the top event is time dependent	Frequent causes are not captured
				Quantitative Analysis	Deep Understanding of the structure is needed
				Used in design and operation phase	Time Consuming
		Bayesian Brief Networks (BBN)	Probabilistic method to understand the structure of failure relation	Modelling of uncertainty	Grows exponentially with size
				No assumption that events are independent	Difficult to visualise
				Allows forward and backward reasoning	

3.4 ANALYSIS OF ACCIDENT DATA FOR CONVENTIONAL SHIPS

According to the European Maritime Safety Agency (EMSA), cargo vessels accounted for 43.8% of the marine casualties and incidents for the period 2011-2018, as shown in Figure 5 (EMSA, 2019). For this reason, a cargo vessel was chosen to be examined in the case study of this project.

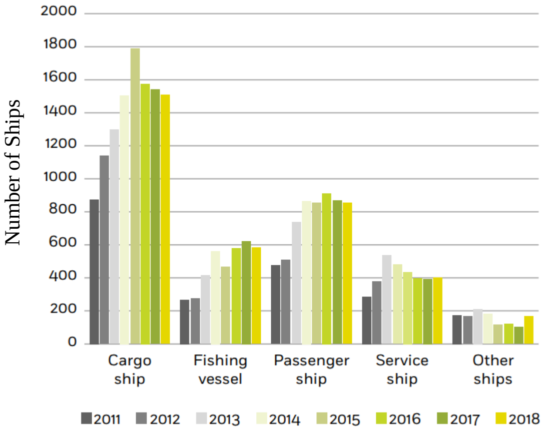


Figure 5 - Distribution of ships involved in a marine casualty or incident by ship type (EMSA, 2019)

Figure 6 indicates that navigational accidents were the majority of casualty events accounting for almost 55% of the total events (EMSA, 2019). Collision is one of the main casualty events for every ship type and it is expected that the risk level of a collision will be increased in autonomous vessels. Therefore, it is essential that the collision avoidance system is examined in detail in order to determine its safety and reliability.

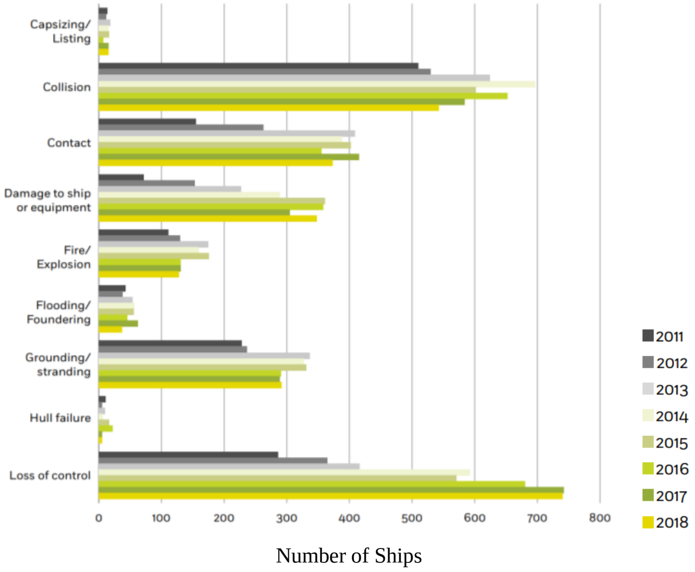


Figure 6 - Distribution of casualty events for the period 2011-2018 (EMSA, 2019)

3.5 COLLISION AVOIDANCE SYSTEM – OTHER INDUSTRIES

The risk level of a possible collision between the MASS and the obstacles present in its surroundings should be assessed and collision avoidance plan and actions should be taken according to COLREGs. The main aim of this system is to prevent or reduce the severity of the outcomes of a collision. Collision avoidance systems have already been well developed in different industries, such as the automotive and aerospace. The review of the collision avoidance system of vehicles and aircrafts is useful in order to enable the improvement of the collision avoidance system of MASS.

Collision Avoidance System – Vehicles

The collision avoidance system has already been employed in autonomous land-based vehicles. One of the most successful implementations was in Stanley Unmanned Ground Vehicle (UGV). The system consists of various sensors (Long/Short/Ultrasound-Range Radar, LiDAR and cameras) in order to map the surroundings and detect obstacles as shown in Figure 7. GPS is widely used in order to provide time and geolocation data. Electronic Control Units are responsible to process the data received from the sensors, and actuators (acceleration and breaking) are following commands of the Adaptive Cruise Control (ACC) component after processing the observation data as well as the safety restrictions imposed.

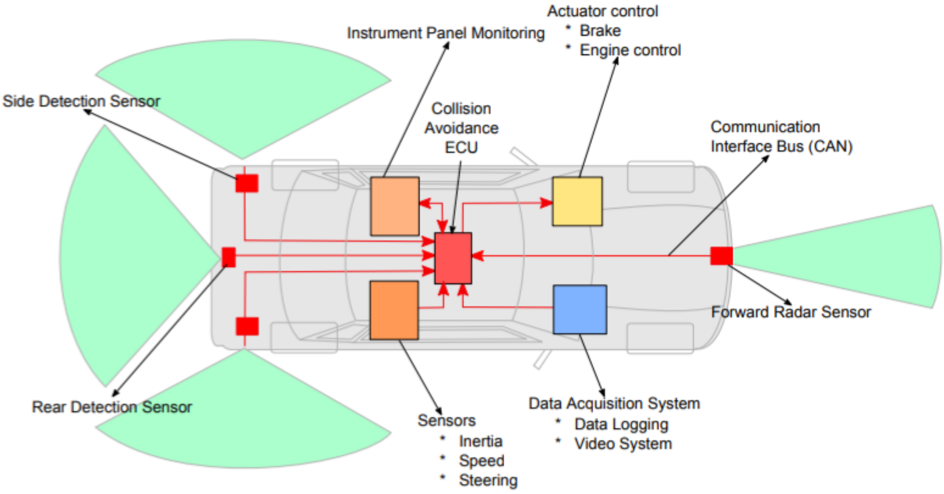


Figure 7 - Collision avoidance system vehicles (Kizheppatt et al., 2014)

Collision Avoidance System – Aircrafts

Traffic Alert and Collision Avoidance System (TCAS) is being employed in order to prevent aircraft collisions. Radar is used to detect, locate and identify targets, while antennas are present in order to receive information about the surroundings as well as transmit the signal and provide up-to-date positioning data. Obstacles are presented on TCAS screen with the use of various symbols that account on the level of threat that they pose. The different notification alerts are diversified as Traffic Advisory (TA) and Resolution Advisory (RA). The former enables the pilots to spot the target and prepare for a potential emergency action, while the latter suggests collision avoidance actions that have to be taken by the pilot (Greeshma, 2012).

The system comprises of TCAS computer unit, antennas and cockpit presentation. The computer unit executes airspace surveillance, threat detection, aircraft tracking, target tracking and Resolution Advisory (RA) manoeuvres. In order for the collision avoidance to be performed, the TCAS Processor fuses data regarding the aircraft status, pressure and radar altitude. The following antennas are widely used: one-directional antenna placed at the top part of the aircraft and one omnidirectional or directional placed at the bottom part. Moreover, two additional antennas are placed on top and bottom of the Mode S transponder. Lastly, the cockpit presents Traffic or Resolution Advisory displays (Камкін, 2015). A schematic representation of the components of the system can be found in Figure 8, while the range of the protection thresholds is presented in Figure 9.

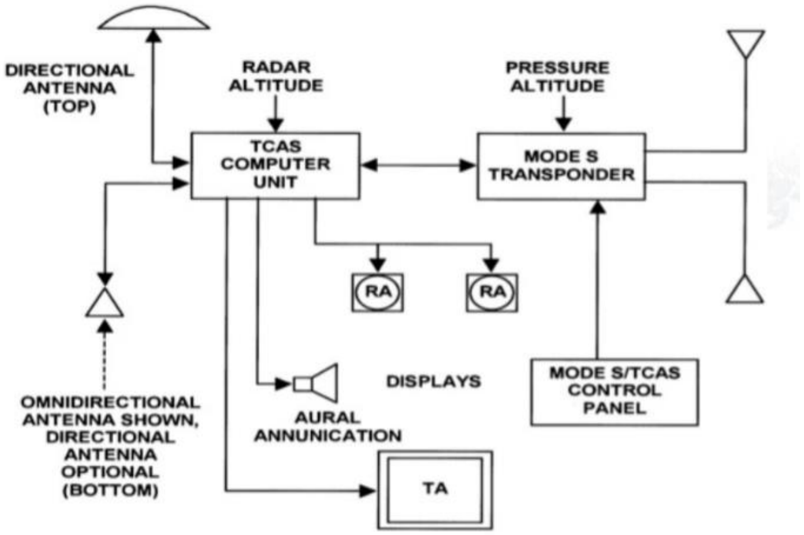

DIRECTIONAL ANTENNA (TOP)
RADAR ALTITUDE
PRESSURE ALTITUDE
TCAS COMPUTER UNIT
MODE S TRANSPONDER
RA
RA
DISPLAYS
MODE S/TCAS CONTROL PANEL
OMNIDIRECTIONAL ANTENNA SHOWN, DIRECTIONAL ANTENNA OPTIONAL (BOTTOM)
AURAL ANNUNICATION
TA

Figure 8 - TCAS Block Diagram (Greeshma, 2012)

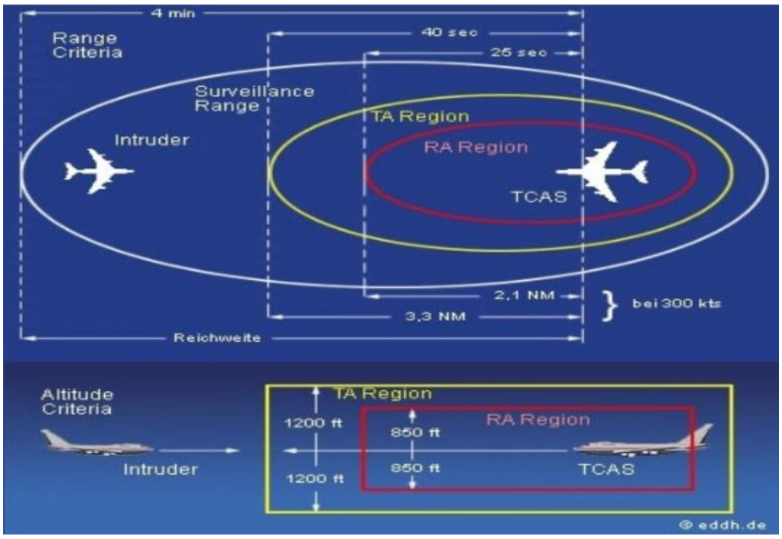


Figure 9- Protection Thresholds (Greeshma, 2012)

The various functions that the collision avoidance system performs in vehicles and aircrafts had been reviewed and the components of the system had been identified. It is worth noting, though, that the exact same systems are not directly applicable to ships, however, their review enabled the broader understanding of the collision avoidance system used in various industries.

4. SELECTION OF RESEARCH TOPIC

After establishing the subject status in the critical review, it was concluded there are five topics that deserve research study. Navigation of MASS was the initial selection after only considering the personal interest. However, it was essential to assess whether this was an over dominating criterion, and this is the reason why a Selection Thinking Aided Matrix (STAM) was used. It should be noted, though, that STAM is not a selection tool and that it was only used to check the selection (Kuo, 2018). The merit of this approach is that it enables several criteria to be incorporated and can be readily used. The numerical values assigned for the comparison of the relative importance of the different topics requires some previous experience. This experience is best gained by regular practice in using STAM in decision making for everyday matters such as selection of food, travelling destinations, outfit etc. For example, when one tries to decide how to travel to work, some of the choices are to use their car, to cycle or to walk. The dominate criterion is usually their safety. However, STAM can be used in order to check whether the choice is influenced by other criteria such as the time taken to get there, health benefits, reduction of emissions, psychological benefits etc. Once sufficient practise is performed, one builds up an accurate feel when assigning the various numerical values.

The main topics that had been considered for this project are the following:

Topic 1: Risk Assessment of MASS

Topic 2: Formal Safety Assessment of MASS

Topic 3: Recommendations for MASS Safety Assurance Framework

Topic 4: Safety assurance of the Navigational System of MASS

Topic 5: Effects of cybersecurity on MASS

The aforementioned topics were assessed using personal interest plus the five more criteria:

Criterion 1: Personal interest

Criterion 2: Ability to conduct the project in the available time

Criterion 3: Novelty of the topic - Contribution

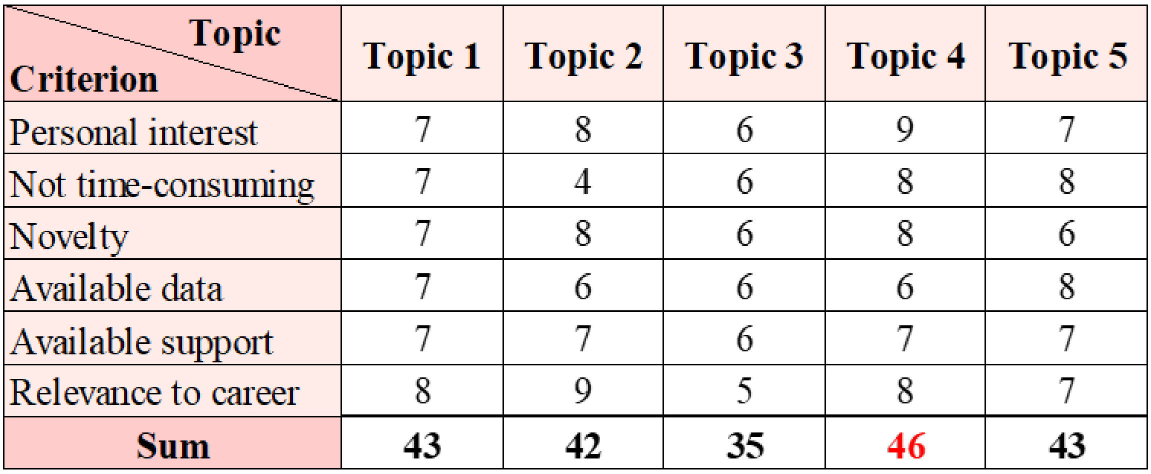
Criterion 4: Availability of data

Criterion 5: Availability of support

Criterion 6: Relevance to future career

Weighting scale from 1 (least important) to 10 (most important) was used in order to compare the relative importance of the topics for a given criterion. The results are shown in Table 3. The findings supported the initial choice.

Table 3 - STAM for checking the suitability of the selected of topic



Topic Criterion	Topic 1	Topic 2	Topic 3	Topic 4	Topic 5
Personal interest	7	8	6	9	7
Not time-consuming	7	4	6	8	8
Novelty	7	8	6	8	6
Available data	7	6	6	6	8
Available support	7	7	6	7	7
Relevance to career	8	9	5	8	7
Sum	**43**	**42**	**35**	**46**	**43**

5. RESEARCH APPROACH AND STRATEGY

In order to complete a challenging project, it is important to follow a strategy. It should always be ensured that the objectives are met after conducting several tasks and reaching the milestones on time. As Professor Kuo states 'Tackling a project is very challenging because it requires going from little knowledge about a topic or problem to greater and broader understanding in finite amount of time' (Kuo, 2018).

The different steps that had been followed in order to complete the project were as follows:

Step 1: Critical review

Research on the topic and critical review, aiming to obtain a broader understanding about MASS as well as identify the merits and drawbacks of the different safety assurance techniques that are widely used nowadays, before deciding the most appropriate method for the particular project.

Step 2: Analysis of accident data for conventional ships

Analysis of accident data for conventional ships and identification of the major hazards leading to accidents nowadays.

Step 3: Reference system and components

Selection of the reference system and creation of a block diagram including the various components after analysis of their functions.

Step 4: Selection of safety assurance technique

Selection of the most appropriate safety assurance method in order to conduct the particular analysis.

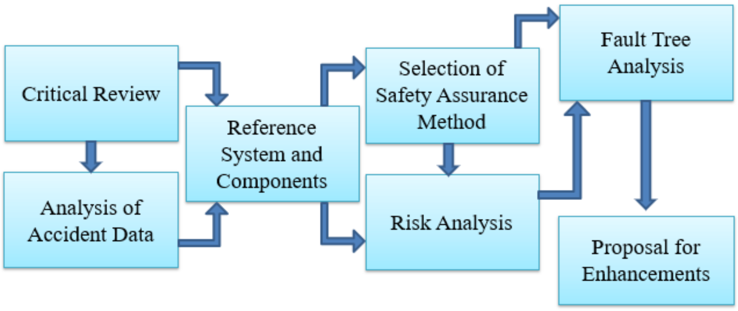
Step 5: Risk Analysis and Fault Tree Analysis

Conduction of Risk Analysis for the identification of potential hazards to the system. Estimation of their risk levels in order to enable the approximation of the failure rates of the various events that had been used as input in the method used. It is worth noting that in the current stage, the collection of quantitative data was challenging. This is justifiable considering the novelty of the project. The estimation of the risk levels for the approximation of the various failure rates can be assumed to be acceptable for a fourth-year project.

<u>Step 6</u>: Safety Enhancement

Identification of the critical failures as well as the combinations of failures that can result in potential failure of the system and proposal for safety enhancement solutions in order to mitigate the critical hazards.

A flow diagram of the strategy that was followed during the project is presented in Figure 10.



Critical Review
Analysis of Accident Data
Reference System and Components
Selection of Safety Assurance Method
Risk Analysis
Fault Tree Analysis
Proposal for Enhancements

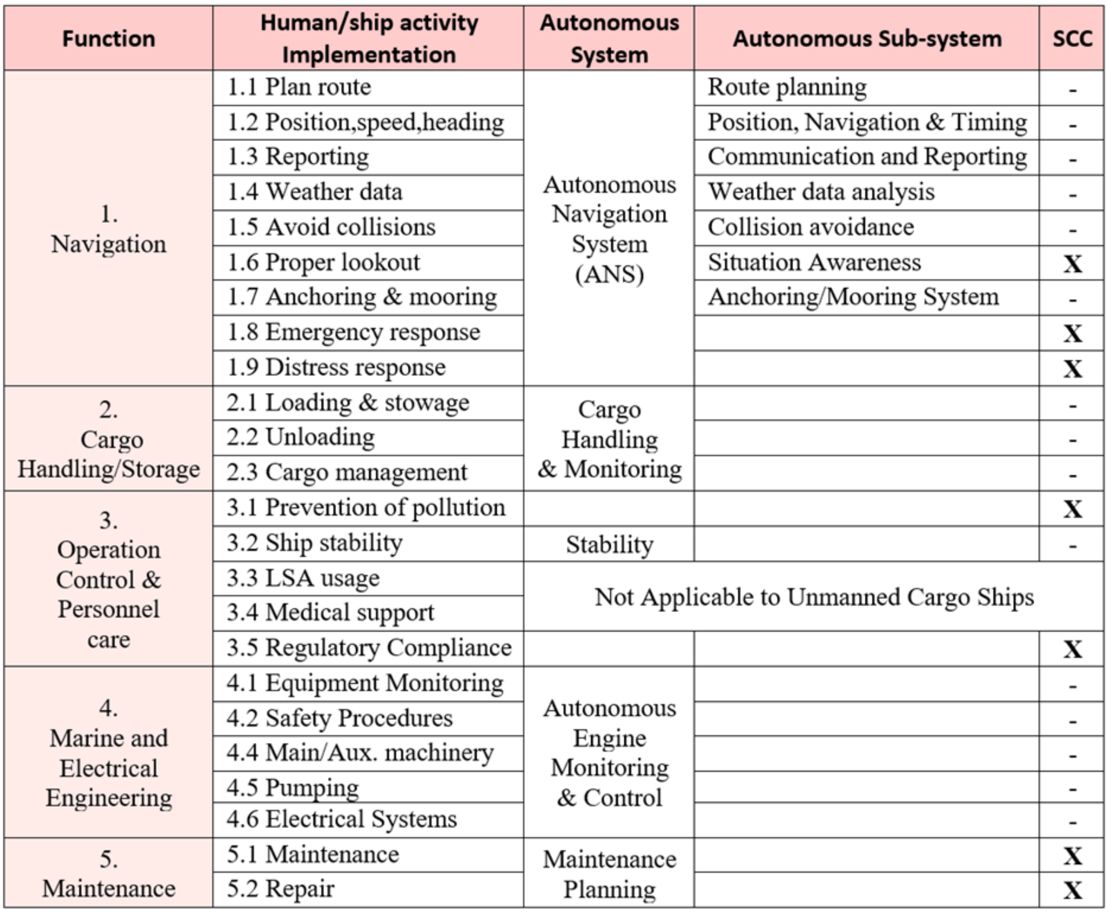
Figure 10 - Flow diagram of the research strategy followed

Note that the theory associated with the methodology used is presented in Chapters 6 and 7, while detailed analysis and results are presented in Chapters 8 to 11.

6. MASS SYSTEM DESCRIPTION

In the particular project, the ship can be represented by a sum of multiple systems and sub-systems that perform the various functions. Table 4 summarises the implemented functions and the systems that perform them in vessels with dynamic LoA. It is worth noting that vessel with dynamic LoA consists of the same systems that are present in fully autonomous vessels, however, the Shore Control Centre (SCC) is also present in order to execute some of the functions and monitor the operation of the ship.

Table 4 – Ship with dynamic LoA: functions and systems



Function	Human/ship activity Implementation	Autonomous System	Autonomous Sub-system	SCC
1. Navigation	1.1 Plan route	Autonomous Navigation System (ANS)	Route planning	-
	1.2 Position,speed,heading		Position, Navigation & Timing	-
	1.3 Reporting		Communication and Reporting	-
	1.4 Weather data		Weather data analysis	-
	1.5 Avoid collisions		Collision avoidance	-
	1.6 Proper lookout		Situation Awareness	X
	1.7 Anchoring & mooring		Anchoring/Mooring System	-
	1.8 Emergency response			X
	1.9 Distress response			X
2. Cargo Handling/Storage	2.1 Loading & stowage	Cargo Handling & Monitoring		-
	2.2 Unloading			-
	2.3 Cargo management			-
3. Operation Control & Personnel care	3.1 Prevention of pollution			X
	3.2 Ship stability	Stability		-
	3.3 LSA usage	Not Applicable to Unmanned Cargo Ships		
	3.4 Medical support			
	3.5 Regulatory Compliance			X
4. Marine and Electrical Engineering	4.1 Equipment Monitoring	Autonomous Engine Monitoring & Control		-
	4.2 Safety Procedures			-
	4.4 Main/Aux. machinery			-
	4.5 Pumping			-
	4.6 Electrical Systems			-
5. Maintenance	5.1 Maintenance	Maintenance Planning		X
	5.2 Repair			X

A diagram representing the various systems and functions of a vessel with dynamic LoA is included Figure 11.

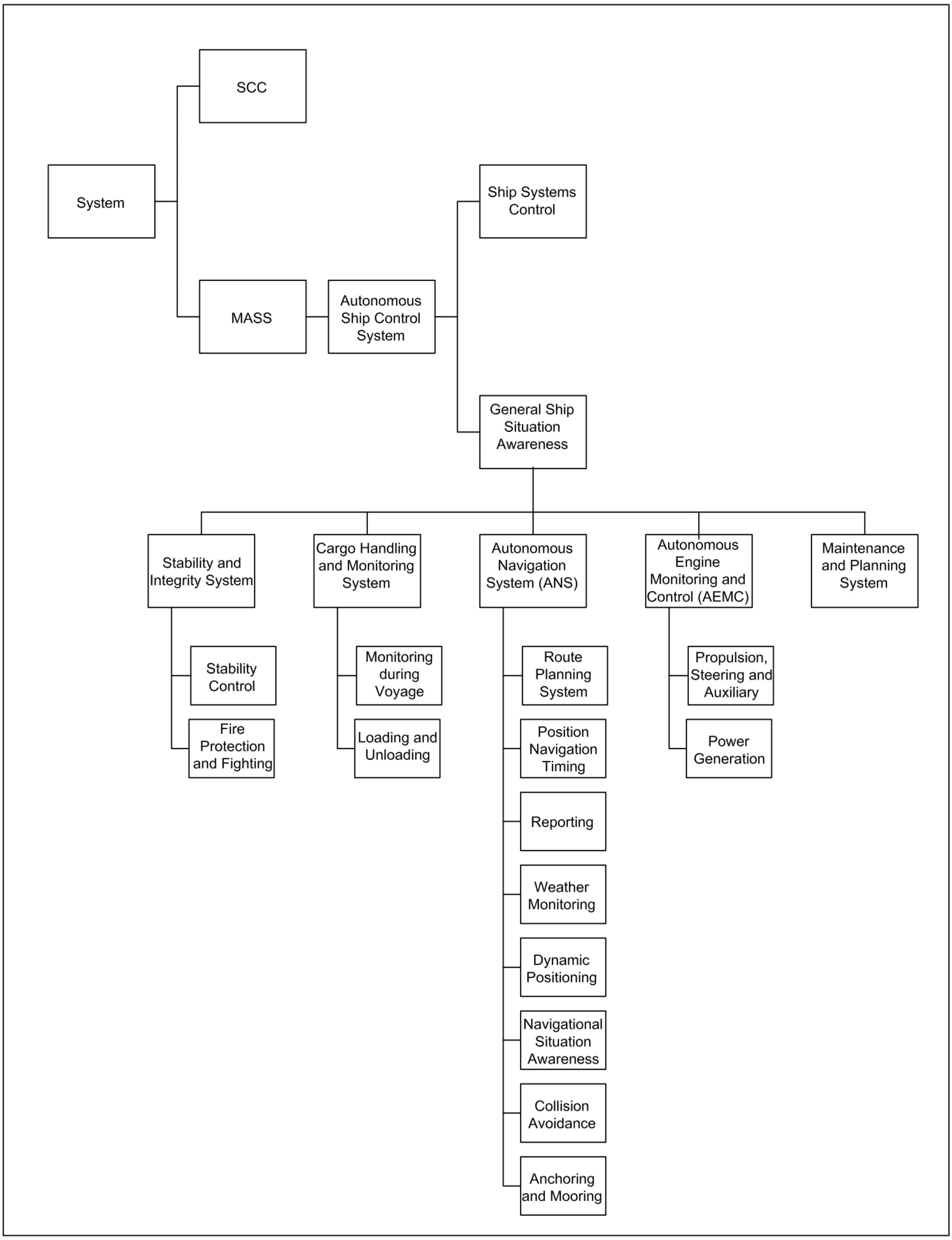

System
SCC
MASS
Autonomous Ship Control System
Ship Systems Control
General Ship Situation Awareness
Stability and Integrity System
Cargo Handling and Monitoring System
Autonomous Navigation System (ANS)
Autonomous Engine Monitoring and Control (AEMC)
Maintenance and Planning System
Stability Control
Fire Protection and Fighting
Monitoring during Voyage
Loading and Unloading
Route Planning System
Position Navigation Timing
Reporting
Weather Monitoring
Dynamic Positioning
Navigational Situation Awareness
Collision Avoidance
Anchoring and Mooring
Propulsion, Steering and Auxiliary
Power Generation

Figure 11 - Systems and functions of a MASS with dynamic LoA

The Shore Control Centre (SCC) sends information such as the voyage plan, weather forecasts, risk parameters etc. to the Autonomous Ship Control System (ASCS). The particular system is responsible to control the rest of the systems that are present onboard. The route planning subsystem generates a route plan based on the information received from the SCC as well as the fused sensor data. Positioning, Navigation and Timing System (PNT) continuously sends information to the different systems present onboard. It is essential that the route planning system updates the route plan in accordance with the information received by the PNT system.

The weather monitoring and interpretation system fuses sensor data and combines them with the information sent from shore. After that, weather data are sent to the route planning system and navigational situation awareness system. The latter, fuses sensor, camera, radar etc. data in order to map the surroundings of the vessel. In case that an obstacle is detected, the aforementioned means are used in order to identify it. If collision is regarded as a possible scenario, data is sent to the collision avoidance system.

The collision avoidance system is one of the most important sub-systems of the Autonomous Navigation System (ANS) because it generates the collision avoidance plan that alters the route plan in order to minimise the risk of collision. Information about the vessel's performance is continuously sent from the different subsystems to the reporting and communication subsystem that sends it to the Autonomous Ship Control System (ASCS) and the Shore Control Centre (SCC).

Communication between the MASS and ships that are operating nearby is also possible via the communication system. However, in a distress situation (e.g. inevitable collision) the SCC intervenes and takes control of the vessel with the use of the Remote Manoeuvring Support System (RMSS).

The aforementioned flow of information between the various systems and sub-systems of a vessel with dynamic LoA is presented in Figure 12.

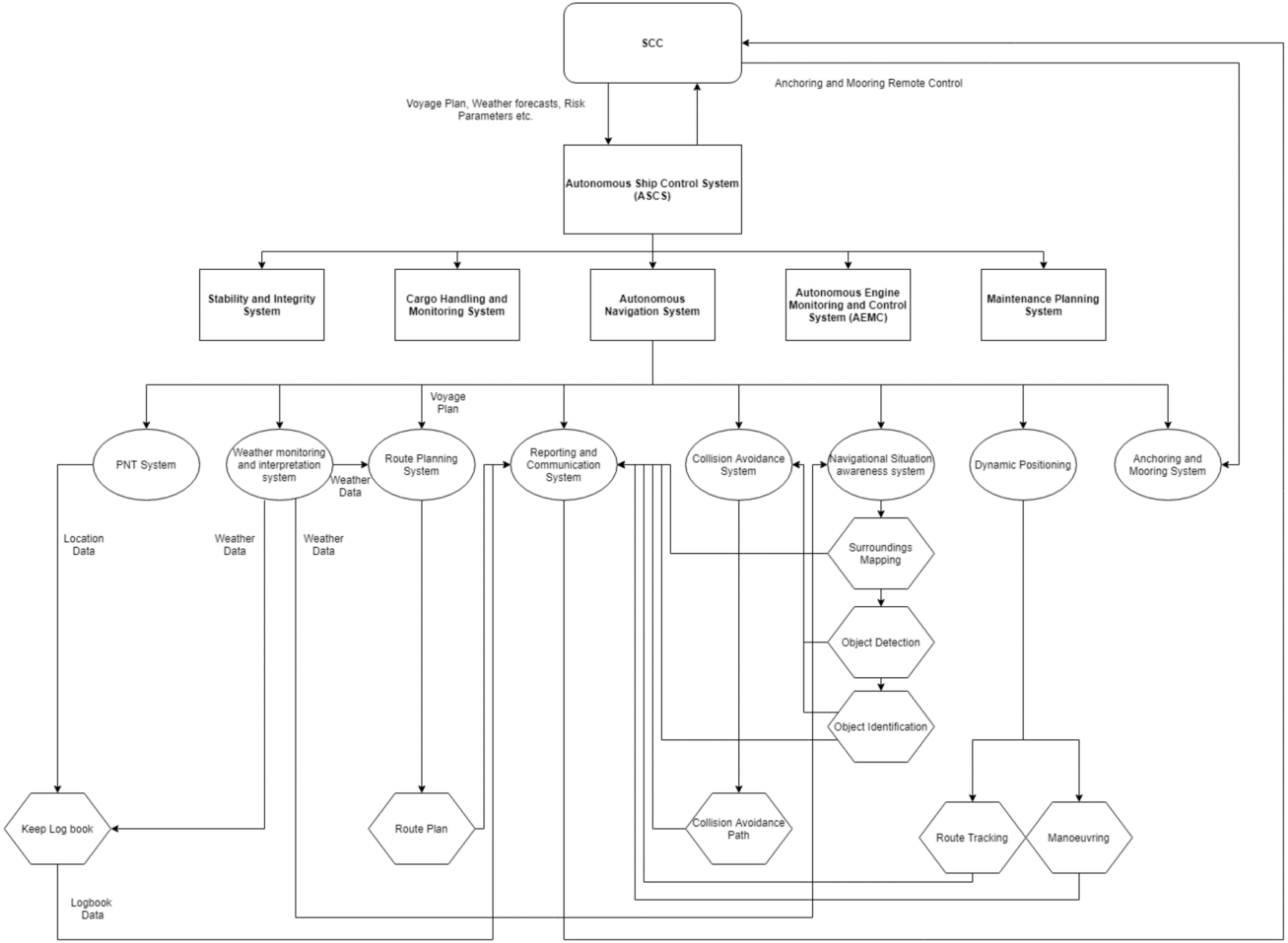

SCC
Anchoring and Mooring Remote Control
Voyage Plan, Weather forecasts, Risk Parameters etc.
Autonomous Ship Control System (ASCS)
Stability and Integrity System
Cargo Handling and Monitoring System
Autonomous Navigation System
Autonomous Engine Monitoring and Control System (AEMC)
Maintenance Planning System
Voyage Plan
PNT System
Weather monitoring and interpretation system
Weather Data
Route Planning System
Reporting and Communication System
Collision Avoidance System
Navigational Situation awareness system
Dynamic Positioning
Anchoring and Mooring System
Location Data
Weather Data
Weather Data
Surroundings Mapping
Object Detection
Object Identification
Keep Log book
Route Plan
Collision Avoidance Path
Route Tracking
Manoeuvring
Logbook Data

Figure 12 - Information flow diagram between the systems of a vessel with dynamic LoA

6.1 COLLISION AVOIDANCE SYSTEM

The collision avoidance system of a ship estimates the collision risk level and determines actions that have to be taken in order to minimise or even eliminate it.

First of all, during the observation stage, data is received from the various sensors and equipment in order to map the surroundings of the ship. Obstacles are recognised and navigational information of the vessel is obtained. During the decision stage, the aforementioned data are fused, and the level of collision risk is calculated in order to determine whether collision avoidance actions have to be taken. The optimal route is estimated using the collision avoidance algorithm. If required, collision avoidance control performs collision avoidance plan according to the decision stage and the autopilot is actuated to the optimal route. (Kang et al., 2010).

Since human look-out will be absent in order to assess the risk level of collision it is essential that an Advance Sensor Module (ASM) is present in order to detect and classify targets (Bruhn et al., 2014).

Real-time navigational information such as geolocation and magnitude of speed are obtained by the Global Navigation Satellite Systems (GNSS) together with the depth transducer and speed log, whereas, the compass indicates the heading of the vessel. GNSS receives latitude, longitude, altitude and time information and indicates the location, speed and heading of the vessel. On the other hand, the compass, uses the angle to north as raw data and features the heading of the ship, while the depth transducer measures the depth in order to create the seafloor contour.

For accuracy enhancement and redundancy purposes an Inertial Measurement Unit (IMU) is also present in order to determine the heading, speed and acceleration of the vessel. It is usually consisted of gyroscopes, magnetometers and electromechanical accelerometers in order to be able to determine the location of the vessel accurately (Bruhn et al., 2014).

Information from the Electronic Chart Display and Information System (ECDIS) is used in order to identify navigational hazards and enable the vessel to follow a route that aims in reaching its destination cost-effectively and safely. In order to achieve this, weather forecasts and observations by METOCEAN services are sent from the SCC and are compared with data fused by the various environmental sensors, such as wind speed and direction, air temperature and pressure, wave characteristics etc.

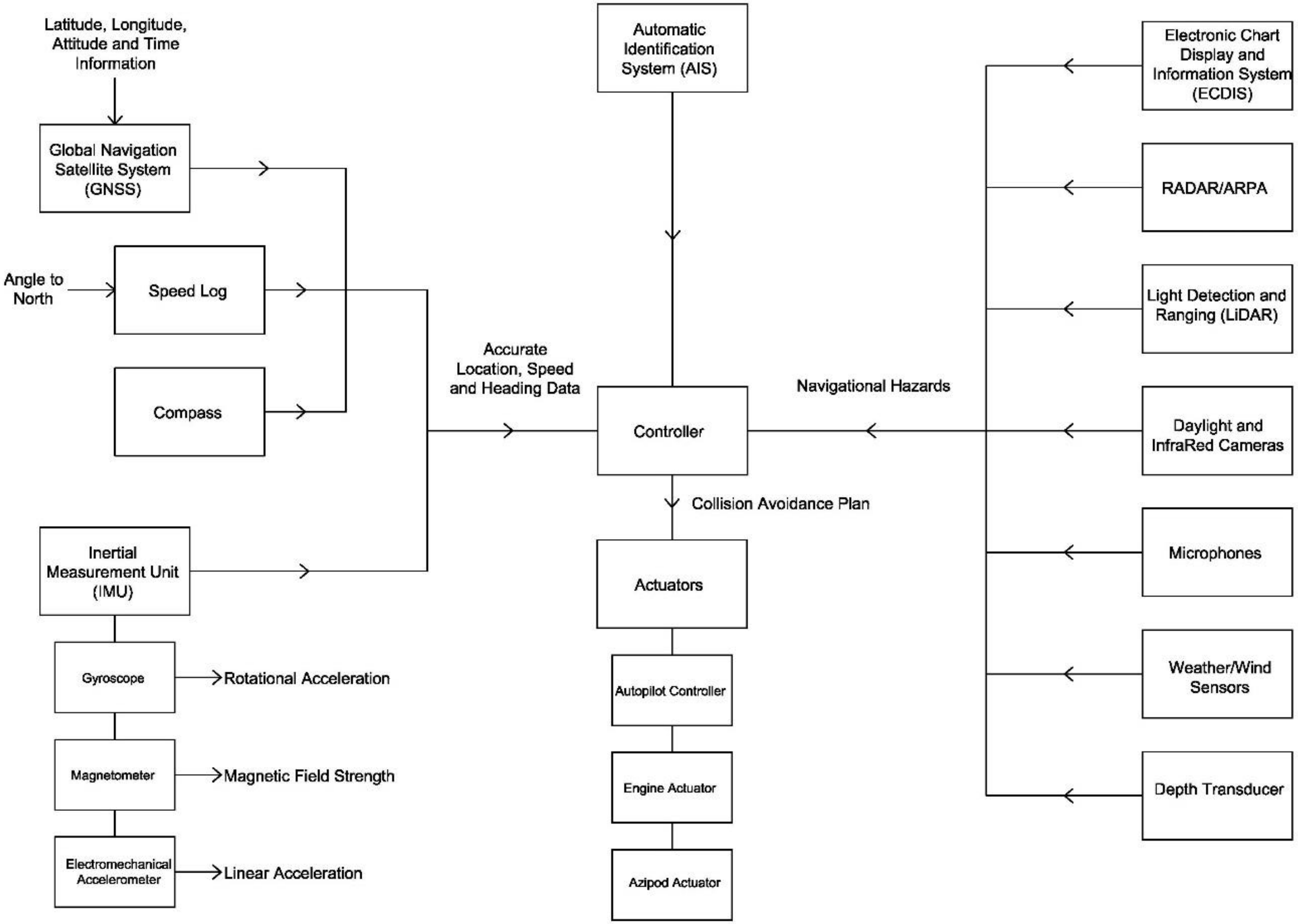
Moreover, Radar and Automatic Radar Plotting Aids (ARPA) enable the detection of fixed and moving targets using electromagnetic energy pulses. However, for autonomous vessels it is essential that additional sensors are present for redundancy purposes and to map the shadow regions of the Radar. Light Detection and Ranging (LiDAR) produces light pulses enabling the detection and accurate recognition of objects within a range of approximately half a kilometre.

Automatic Identification System (AIS) is used in order to share information about the specifications and the navigational status of the vessel for safety purposes as well as to establish communication with the shore. AIS utilises ship data in order to estimate the traffic situation. The Situation Awareness and Sensor Fusion (SASF) system merges information from the different sensors and sources in order to determine the position and speed of nearby obstacles. Data from the SASF is used as input for the collision avoidance system.

Therefore, obstacles are spotted and tracked after the fusion of data from different sensors of the AIS, the pulse RADAR, LiDAR, microphones and electro-optical daylight and infrared cameras in order to provide redundancy and overcome the blind zone of the Radar (Son and Kim, 2018). It is worth noting though, that some objects require human identification and for this reason, in case that the system is not able to perform target identification or issue a collision avoidance plan, data from the situational awareness sensors are sent to the SCC to take immediate action.

The autonomous ship controller performs computations after fusing the aforementioned data and executes instructions. The output of the collision avoidance system is used by the actuators in order to take adequate actions to avoid the collision. Sound and light alarms are also generated to warn nearby vessels (Johansen et al., 2016).

The flow diagram of the aforementioned information inside the system is presented in Figure 13, while Figure 14 presents the information flow and the system components selected for the particular case study.



Latitude, Longitude, Attitude and Time Information
Global Navigation Satellite System (GNSS)
Angle to North
Speed Log
Compass
Inertial Measurement Unit (IMU)
Gyroscope
Rotational Acceleration
Magnetometer
Magnetic Field Strength
Electromechanical Accelerometer
Linear Acceleration
Accurate Location, Speed and Heading Data
Automatic Identification System (AIS)
Controller
Collision Avoidance Plan
Actuators
Autopilot Controller
Engine Actuator
Azipod Actuator
Navigational Hazards
Electronic Chart Display and Information System (ECDIS)
RADAR/ARPA
Light Detection and Ranging (LiDAR)
Daylight and InfraRed Cameras
Microphones
Weather/Wind Sensors
Depth Transducer

Figure 13 - Collision avoidance system of MASS

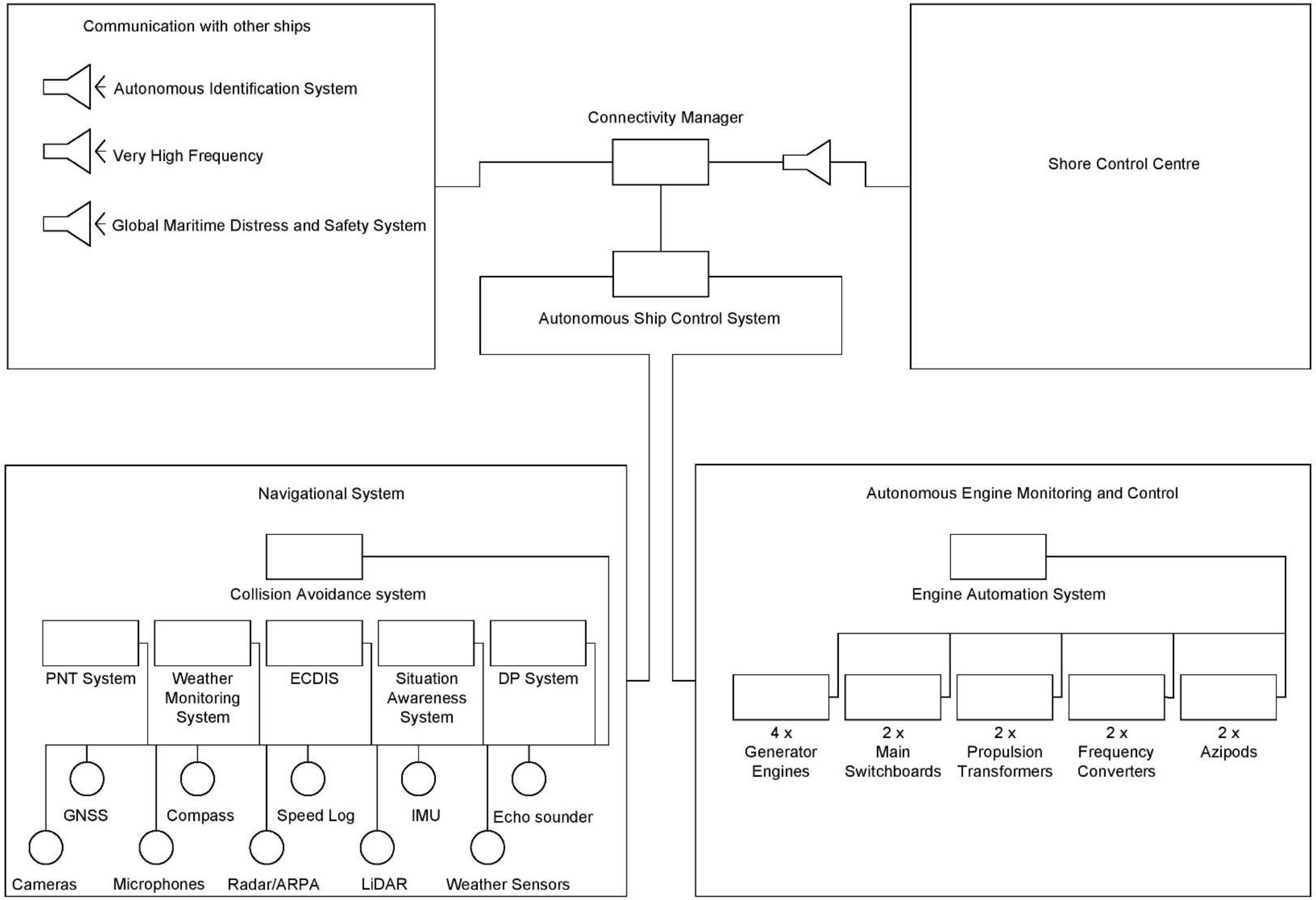


Figure 14 – MASS system components and information flow

The components that enable the collision avoidance of a vessel with a dynamic LoA are going to be examined in this section. First of all, a Global Navigation Satellite System (GNSS) consisted of antennas and receivers will be present in order to provide positioning, course and timing information of the vessel. For the accurate estimation of the speed of the vessel, the speed log will be consisted of two transducers (one forward and one aft).

As already mentioned, an Inertial Measurement Unit (IMU) will also be present for redundancy reasons. It will be consisted of three accelerometers, three gyroscopes, three magnetometers as well as Digital signal processing hardware and communication hardware. The Automatic Identification System (AIS) will enable both the estimation of the location and heading of the particular vessel as well as the navigational status of the surrounding vessels. It will be consisted of antennas, VHF transmitters and receivers, a Central Processing Unit (CPU) together with interface to heading and speed devices.

Cameras of various types are going to be present in order to enhance the situational awareness and enable the classification of the various objects by capturing the vessel's surroundings. HD Cameras are able to help in the classification of objects by separating them from their background using colour information. However, infrared (IR) cameras will also be required in order to perform the imaging of the surroundings in total darkness (Long Wave infrared-LWIR) and low light conditions using reflected radiation signal instead of thermal (Short Wave infrared-SWIR).

However, cameras are malfunctioning during harsh weather conditions and it is not easy to extract the distance information of the obstacle. For these reasons, data obtained only from cameras is not reliable. Distance and velocity information can be provided by LiDAR. However, similarly to cameras, their efficiency and accuracy is highly dependent on the weather conditions.

Radar is used in order to assist the object detection and is also operating during harsh conditions, when cameras mail fail. It is the most efficient means to determine the distance of the target from the vessel. The main components of the Radar are the transmitter, the receiver, the scanner as well as the display. There are various types of radar bands. Type S- and X- band radars cannot be used to perform collision avoidance because they do not have adequate resolution. However, Short Range radar (SR radar) like type Ka- and W- band radars are very efficient in obstacle detection compared to traditional ship radars. These types of radar have already been used in automotive. However, they enable the detection of objects within a limited range.

Information of radar, AIS, GNSS, speed log and other sensors are used in order to depict the actual traffic situation around the vessel with the use of the ECDIS. Lastly, the General-Purpose Computer (GPC) creates the collision avoidance plan after fusing the data from the different situational awareness sensors. It is consisted of an input device, a central processing unit, an output device and a memory.

Table 5 presents a matrix including a rating for the various characteristics of the main situational awareness sensors. The rating scale varies from 1 to 6, where 1 indicates that the design feature is not well satisfied and 6 indicates that the design feature is very well satisfied. The rating does not represent absolute values but an estimation that has been made after conducting the aforementioned research.

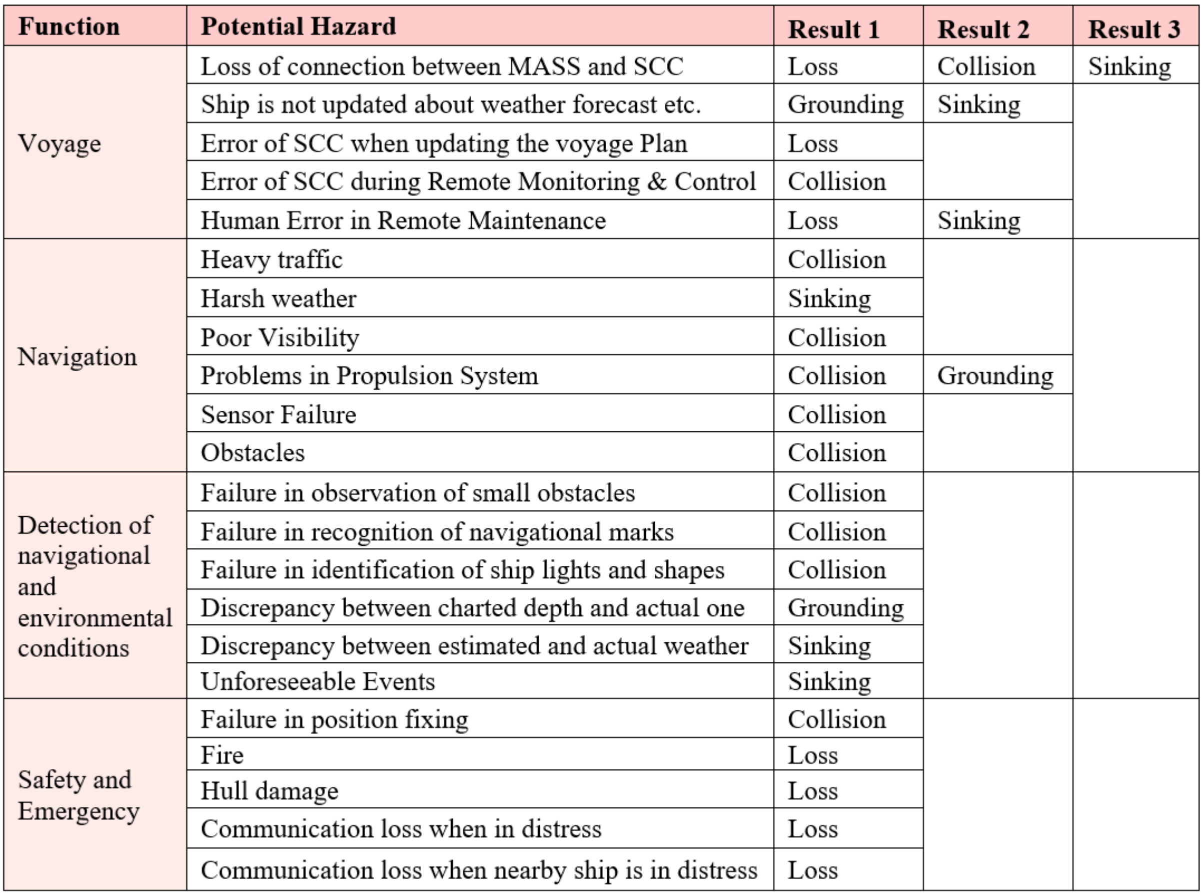
Table 5 - Rating Matrix for the characteristics of the main situational awareness sensors

Type of sensor **Characteristic**	**LiDAR**	**Ship Radar**	**SR Radar**	**HD Cameras**	**IR Cameras**	**Sound**
Range	4	6	3	2	2	3
Tracking of object distance	4	6	6	2	2	1
Object identification	4	5	5	6	3	2
Spatial Accuracy	5	3	3	4	3	1
Reasonable amount of data	1	5	5	1	1	2
Tolerance to Bad Weather	2	5	5	2	2	3
Marine Robustness	2	4	3	4	4	3

6.2 HAZARDS ASSOCIATED WITH MASS SYSTEMS

In order to assess the safety of the autonomous vessels and achieve the aim of this project, it is vital to identify the potential hazards associated with MASS and assess their risk levels. For this to be performed, the ship is regarded as a combination of various systems onboard and onshore executing the various functions. Each operation is associated with different threats that have to be taken into consideration when assessing the safety of the ship as shown in Table 6.

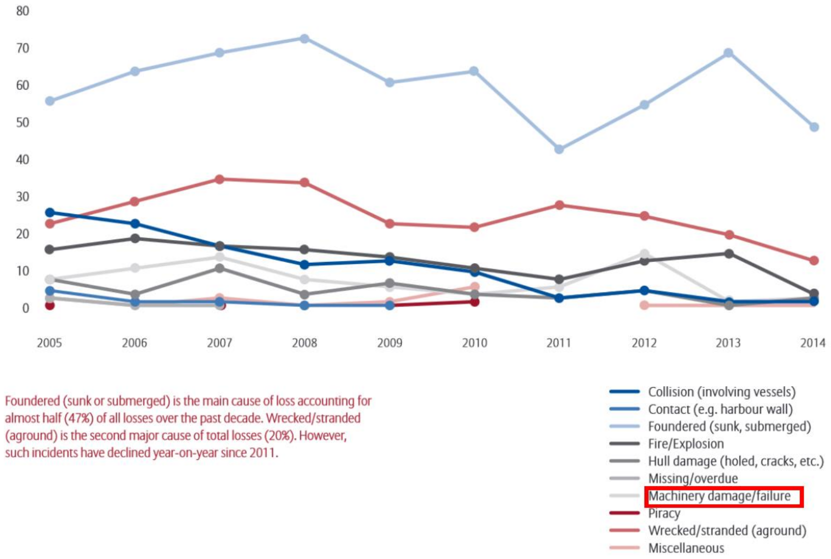
Table 6 - Hazard Identification and Results for different functions of MASS (Bureau Veritas, 2019)



Function	Potential Hazard	Result 1	Result 2	Result 3
Voyage	Loss of connection between MASS and SCC	Loss	Collision	Sinking
	Ship is not updated about weather forecast etc.	Grounding	Sinking	
	Error of SCC when updating the voyage Plan	Loss		
	Error of SCC during Remote Monitoring & Control	Collision		
	Human Error in Remote Maintenance	Loss	Sinking	
Navigation	Heavy traffic	Collision		
	Harsh weather	Sinking		
	Poor Visibility	Collision		
	Problems in Propulsion System	Collision	Grounding	
	Sensor Failure	Collision		
	Obstacles	Collision		
Detection of navigational and environmental conditions	Failure in observation of small obstacles	Collision		
	Failure in recognition of navigational marks	Collision		
	Failure in identification of ship lights and shapes	Collision		
	Discrepancy between charted depth and actual one	Grounding		
	Discrepancy between estimated and actual weather	Sinking		
	Unforeseeable Events	Sinking		
Safety and Emergency	Failure in position fixing	Collision		
	Fire	Loss		
	Hull damage	Loss		
	Communication loss when in distress	Loss		
	Communication loss when nearby ship is in distress	Loss		

Investigation of the hazards with high risk level can be performed after examining the probability of occurrence and severity of their results. If the autonomous vessel is regarded as a system of interconnected sub-systems, the possible failures that can occur are: failure of a component, network or power which can lead to severe consequences. Therefore, failure analysis should be conducted in order to identify and evaluate the consequences of every failure.

Figure 15 shows that foundering is the main cause of loss during the period shown, followed by grounding, fire and collisions. Technical problems happen frequently but are not one of the main causes for total loss of conventional ships, however, it is expected that they will cause severe problems to MASS. Therefore, the monitoring, maintenance and redundancy of the machinery systems are essential. Fire and explosion incidents will be limited for MASS because they are usually initiated by human activity. On the other hand, unattended machinery systems without proper maintenance can cause fires onboard the ships. However, extinguishing systems can be more efficient when the vessel is unmanned (Kretschmann et al., 2012).



Foundered (sunk or submerged) is the main cause of loss accounting for almost half (47%) of all losses over the past decade. Wrecked/stranded (aground) is the second major cause of total losses (20%). However, such incidents have declined year-on-year since 2011.

Figure 15 - Total Ship Losses from 2005 until 2014 (Kretschmann et al., 2012)

It is worth noting that collision avoidance and weather routing are of high importance because traffic and harsh weather are the two most serious hazards and can cause foundering, submerging, sinking and total loss of the vessel.

7. SELECTION OF SAFETY ASSURANCE METHOD

The selection of the appropriate safety assurance method was one of the most challenging tasks that had to be conducted while tackling this project. Extensive research on the various methods and consideration of their merits and drawbacks as presented in Chapter 3.3 led to the conclusion that either STPA or FTA could have been used for the particular study.

It is worth noting that after conducting critical review on the safety assurance techniques, STPA was considered the most suitable method for this project because it can be used to analyse complex systems and consider the interconnections of the various components. It has also been used for the acquisition of verification objectives and hazardous scenarios and it is proven that it is suitable to be used for MASS (Thieme et al., 2018). However, a possible use of the particular method would not have provided any novelty in this project because similar publications are already available. Therefore, the selection of a common method instead, can make an actual contribution while focusing on the system configuration and its physical failures and using critical thinking for the estimation of the risk levels of the various hazardous events.

Fault Tree Analysis (FTA) can be used to identify potential hazards that result in Unsafe Navigation and calculate the probability of occurrence of this undesirable event. The particular method does not capture the interactions between the various elements, but it focuses on physical failures and enables the identification of critical components for the safety of the ship. The method is widely used for the assessment of reliability and risk in all fields of engineering. The FTA follows a top-down approach and converts the real system into a Boolean logical diagram representing the various combinations of events that can lead to an undesirable event (Ehiagwina et al., 2015).

A Selection Thinking Aiding Matrix (STAM) was used again in order to verify that the FTA was the most appropriate method to be used for the case study, after considering various criteria (Kuo, 2018). It is worth mentioning that STAM is not a selection tool but can be used in order to ensure that the choice of method was not dominated by personal preference and that other criteria had also been examined as explained in detail in Chapter 4. Note that, that the numerical values used are not absolute values and they were assigned as an indication of the ability of the method to fulfil the various criteria. The numbers were decided after conducting critical review.

A weighting scale from 1 (unsuitable) to 10 (ideal) was used in order to compare the relative importance of the methods for a given criterion. The results are shown in Table 7 and the findings supported the aforementioned statements.

The selection criteria that had been considered where the following:

Criterion 1: Ability to conduct quantitative analysis

Criterion 2: Ability to conduct qualitative analysis

Criterion 3: Applicability

Criterion 4: Ease of use

Criterion 5: Understandability

Criterion 6: Effectiveness

Criterion 7: Novelty of its use for the safety analysis of MASS

Criterion 8: Not enough expertise on the method required

Criterion 9: Ability to conduct the analysis in the available time

Table 7 – STAM for assistance in the selection of Safety Assurance method

Method **Criterion**	**STPA**	**FTA**
Quantitative analysis	0	10
Qualitative analysis	10	10
Applicability	9	7
Ease of use	7	8
Understandability	7	9
Effectiveness	8	7
Novelty	4	7
No expertise needed	3	6
Not time consuming	5	6
Sum	**53**	**70**

7.1 FTA THEORY

It was assumed that the failure rate of the various events that can lead to the top event was fixed. Logic gates (AND, OR etc.) are used in order to illustrate how the various events are interconnected. A Legend of the various symbols that had been used for the Fault Trees of this project is presented in Table 8.

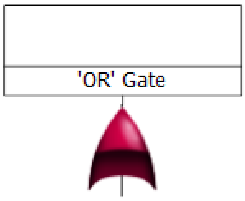
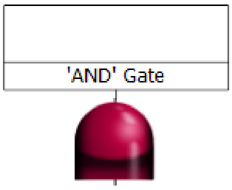
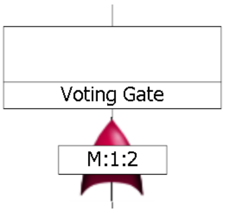
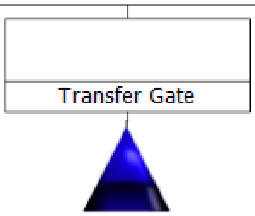
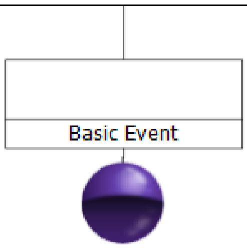
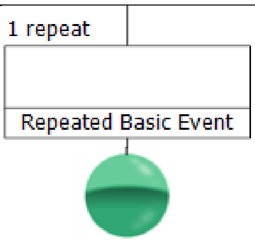
It is worth noting, that the probability of the output event of a logic gate is dependent on the probability of the input events. According to statistics, the probability of an ‘OR’ gate is calculated after considering the union of the input events (i.e. A and B), while the probability of an ‘AND’ gate is calculated after considering the intersection of the input events, as follows:

$$\boldsymbol{P(A\ or\ B) = P(A \cup B) = P(A) + P(B) - P(A \cap B) = P(A) + P(B) - P(A) \times P(B)}$$

$$\boldsymbol{P(A\ and\ B) = \ P(A \cap B) = P(A) \times P(B)}$$

Careful consideration should be taken when using commercial software in order to conduct FTA. Over-reliance on the software should be avoided at all times and independent verification should be made after examining the physical interpretation of the results and ensuring that the results of the various gates had been calculated in accordance with the aforementioned equations.

Table 8 - Fault Tree Legend

Symbol	Description
	The output event occurs when any of the input events occur.
	The output event occurs only if all of the input events occur.
	The output event occurs when at least 1 of the 2 input events occur.
	A supressed tree that is extended in another figure.
	A basic event with known frequency and failure rate.
	A basic event that has been repeated in another branch of the fault tree.

7.2 ANALYSIS OF IMPORTANT METRICS

Analysis of the important metrics enables the detection of critical components whose failure can result in the malfunctioning of the system examined. They contribute in the identification of weaknesses of the particular design and therefore indicate where there should be upgrades in order to enhance the reliability of the system.

The importance measures that had been examined in the case study were the following:

Birnbaum: It is a measure of the rate of change in the failure rate of the top gate due to the change in availability of the event examined.

Criticality: It is a measure to indicate the contribution that the failure of the event examined has in the failure of the top gate. It enables the identification of the components that should be prioritized for modification in order to increase the reliability of the system.

Fussel-Vessely: It is a measure to determine the contribution of the event examined in the failure of the top gate, without considering whether it is the most critical one.

8. CASE STUDY

The safety analysis was implemented for a Short Sea Shipping (SSS) cargo vessel having a dynamic LoA. The choice of this type of vessel lies on the fact that long international voyages imply stricter safety regulations as well as extensive autonomous operation that would have made the study more complex. The vessel was dealt as a single system with interconnected subsystems covering its overall operation as explained earlier.

The collision avoidance system of the vessel, as described in Chapter 6.1, together with the communication and the actions taken from the SCC, had been considered for the conduction of the case study and the safety analysis of the overall navigation system of the ship.

After describing the system and its components, risk analysis had been conducted in order to estimate the risk levels of the various hazardous events for different weather and light scenarios (i.e. day and good weather, harsh weather as well as night and good weather scenarios). The location and number of sensors were decided after assuming that the vessel is around 100m in length and has a deadweight of 2000t. The risk levels and the probabilities that some sensors can malfunction during harsh weather conditions had been estimated after taking into consideration the climate in the Norwegian Coasts, where the vessel is assumed to be operating. The frequency of military exercises taking place in the aforementioned region was also taken into consideration in order to estimate the probability that the GNSS will not be operating.

The outcomes of this analysis enabled the approximation of the failure rates of the various events that affect the safe navigation of the vessel. It is worth noting that hazards associated with cybersecurity had not been taken into consideration for the particular study. After that, the Fault Trees had been constructed for the various scenarios after considering the functions of the system. The estimations of the various failure rates had been used as input for the different basic events of the fault tree. This enabled the quantitative safety analysis and the probability of unsafe navigation had been calculated for the various scenarios.

As an additional step, it was decided to conduct safety analysis of a fully autonomous vessel and compare the results. The outcomes of the various analyses enabled the identification of the components that have a great effect in the safety of the system. Lastly, safety enhancement solutions had been proposed in order to increase the reliability of the vessel for the various scenarios and LoA.

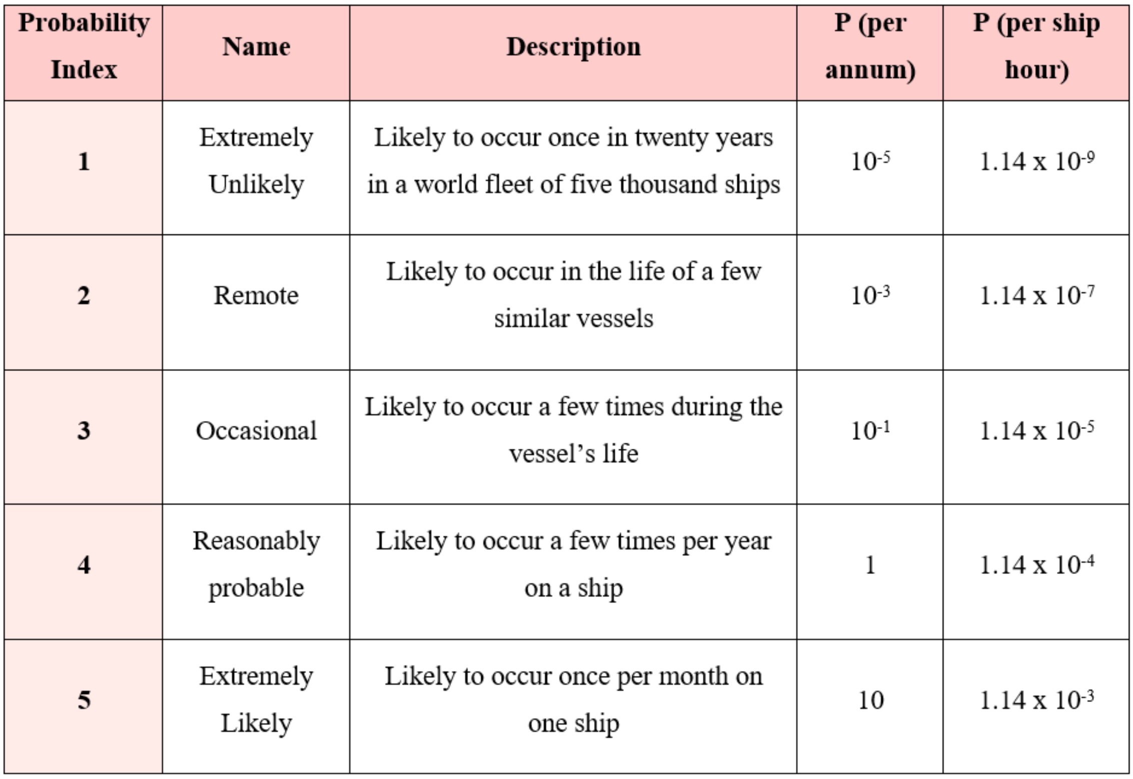
9. RISK ANALYSIS

A qualitive method was used in order to estimate the risk level of the various hazardous events by using a risk matrix approach. It was essential to examine the probability of occurrence and the consequence of every basic event that can result in unsafe navigation. It is worth noting that the risk can be calculated after the multiplication of the consequence of the event and its probability of occurrence:

$$\boldsymbol{Risk}\ (\boldsymbol{R}) = \boldsymbol{Consequence}\ (\boldsymbol{C}) \times \boldsymbol{Probability\ of\ Occurence}\ (\boldsymbol{P})$$

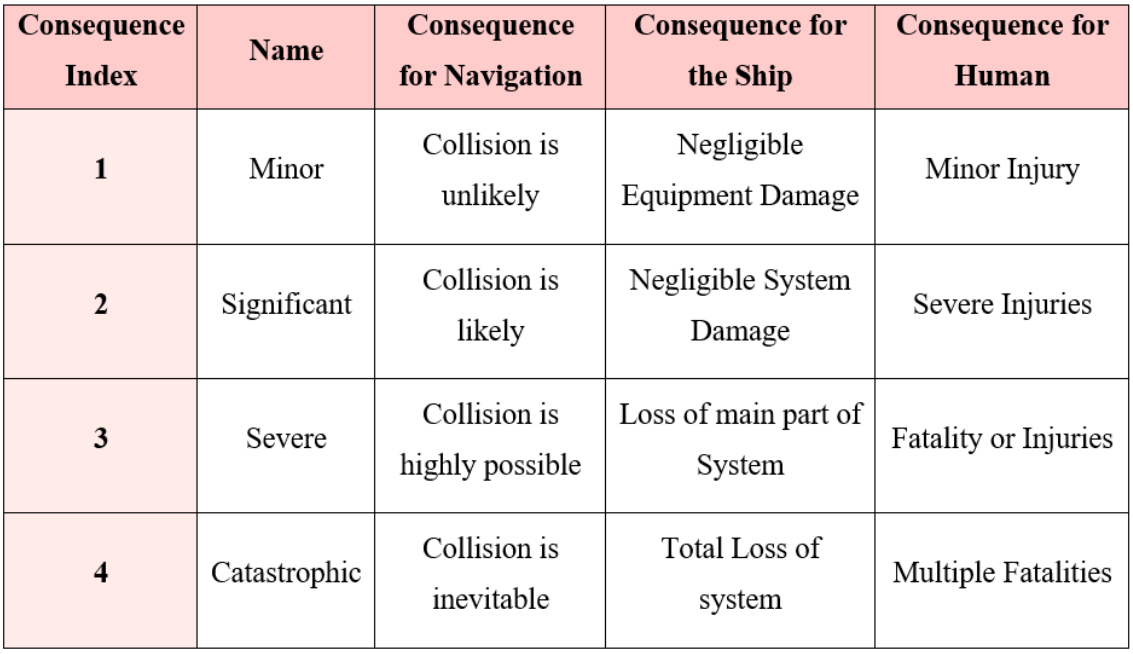
The Risk Matrix in Table 12 represents the ranking of the risk with regards to the relation between the probability of occurrence and the consequence of the event. The classification of rankings is presented in the Tables 9 and 10:

Table 9 - Probability of occurrence index of basic events (IMO, 2018b, Lazakis et al., 2012)



Probability Index	Name	Description	P (per annum)	P (per ship hour)
1	Extremely Unlikely	Likely to occur once in twenty years in a world fleet of five thousand ships	10^{-5}	1.14×10^{-9}
2	Remote	Likely to occur in the life of a few similar vessels	10^{-3}	1.14×10^{-7}
3	Occasional	Likely to occur a few times during the vessel's life	10^{-1}	1.14×10^{-5}
4	Reasonably probable	Likely to occur a few times per year on a ship	1	1.14×10^{-4}
5	Extremely Likely	Likely to occur once per month on one ship	10	1.14×10^{-3}

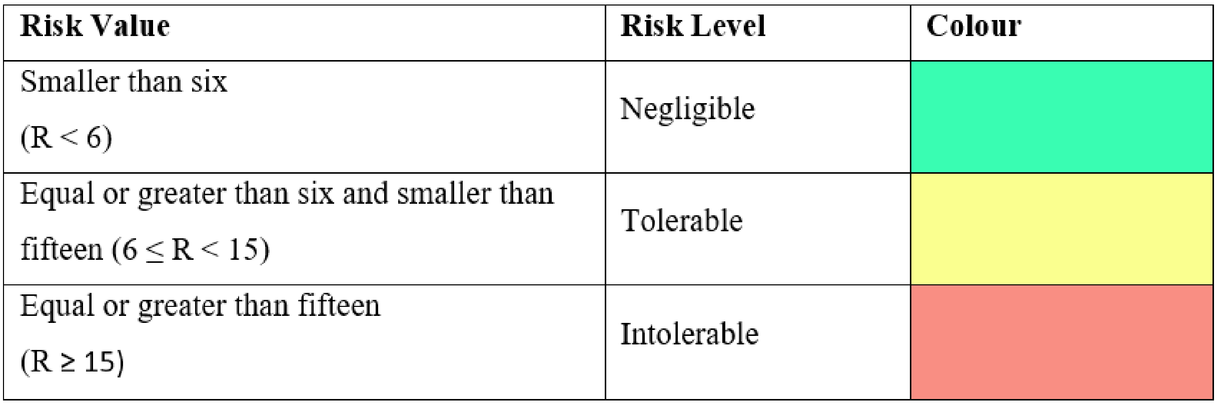
Table 10 - Consequence Index of Basic Events (IMO, 2018b, Lazakis et al., 2012)



Consequence Index	Name	Consequence for Navigation	Consequence for the Ship	Consequence for Human
1	Minor	Collision is unlikely	Negligible Equipment Damage	Minor Injury
2	Significant	Collision is likely	Negligible System Damage	Severe Injuries
3	Severe	Collision is highly possible	Loss of main part of System	Fatality or Injuries
4	Catastrophic	Collision is inevitable	Total Loss of system	Multiple Fatalities

The rankings of the risk are dependent on the value that occurs after the multiplication of the corresponding index for Probability of occurrence (P) and Consequence (C). The colours represent the various risk levels as shown in Table 11.

Table 11 - Risk level according to risk value (Kuo, 2007)



Risk Value	Risk Level	Colour
Smaller than six (R < 6)	Negligible	🟩
Equal or greater than six and smaller than fifteen (6 ≤ R < 15)	Tolerable	🟨
Equal or greater than fifteen (R ≥ 15)	Intolerable	🟥

Table 12 - Risk Matrix (IMO, 2018b, Lazakis et al., 2012)

Risk Matrix (R)			**Probability of Occurrence (P)**				
			Extremely Unlikely	Remote	Occasional	Reasonably Probable	Definite
			1	**2**	**3**	**4**	**5**
Consequence (C)	Catastrophic	**4**	4	8	12	16	20
	Severe	**3**	3	6	9	12	15
	Significant	**2**	2	4	6	8	10
	Minor	**1**	1	2	3	4	5

The different hazards that can result in unsafe navigation had been examined and their risk level was estimated in order to enable the quantitative analysis of the Fault Tree. Three different scenarios had been examined; Unsafe navigation during: (a) Day and good weather, (b) Harsh weather and (c) Night and good weather.

In all three scenarios, the lack of power supply to the various equipment can result by the failure of the low voltage system together with the Uninterruptible Power Supply (UPS) and the probability of occurrence of such an event was set to be equal to 2 due to the increased redundancy.

Moreover, it is expected that the SCC will fail to update the software of the different equipment that will be present on board the vessel a few times during the lifetime of the ship, and therefore, the probability of occurrence of such an event was set to be equal to 3 for the three cases. Human failure of SCC personnel associated with improper lookout, stress and fatigue etc. is expected to take place almost every 1000 hours according to literature. In the Fault Tree Analysis results that are presented later, it is shown that according to the assumptions made, human failure happens at a rate of almost 0.0023, a number that complies with the expected value. As far as the equipment failure is concerned, for the majority of the cases it was set as 3. Same applies to the equipment that is being used for the propulsion of the ship apart from generators that according to literature they are expected to fail more frequently.

HD cameras cannot operate during the night, so the probability of their malfunction is assumed to be definite. However, as already mentioned, the LiDAR and cameras are malfunctioning during the harsh weather conditions and their range is significantly reduced. For this reason, their probability of failure was set to be equal to 4, since it is expected that it will take place a few times per year. The anemometer that will be used in harsh weather conditions is also prone to failure and the probability was set to be equal to 4.

It is also expected that the communication between the SCC and the vessel will be lost a few times during the lifetime of the vessel and more frequently during harsh weather conditions. It is definite that ships that are not obliged to have an AIS will be encountered very frequently and therefore, the probability was set to 5. Lastly, the GNSS might not have signal during military exercises. This can happen a few times per year, depending on the location that the vessel is operating.

As far as the consequence of the different events is concerned, the failure of GNSS is one of the most catastrophic events that may take place for the navigation system because it is used to obtain various information, such as location and heading as well as the speed of the vessel if the speed log is not operating. The failure of the speed log was set to be equal to 3 because in the unlikely event that there is a failure, it is possible to calculate the speed of the ship by measuring the distance that the vessel has completed in a given amount of time and divide it by the aforementioned duration. The consequence of the failure or malfunctioning of the IMU is also assumed to be severe.

The consequence of the failure of ECDIS was set to be equal to 4, because it provides information about the location and heading as well as depth clearance according to chartered depth at a specific location. Since the chartered depth can usually be assumed accurate enough in deep seas, the failure of the Eco-Sounder can be partially solved by using the depth provided by ECDIS. Consequently, the Eco-Sounder failure is assumed to be severe and not catastrophic.

The anemometer is a very crucial equipment during harsh weather conditions and a possible fault in its operation can be catastrophic for the estimation of the wind direction and speed. The decision and action operations are undertaken by the General-Purpose Computer (GPC) and the propulsion equipment respectively. The malfunction or failure of the aforementioned equipment can be proved catastrophic for the safe navigation of the vessel.

Furthermore, a failure of the AIS and GMDSS systems is assumed to be catastrophic for the navigation, while the VHF failure was set to be equal to 3. The safe navigation of a MASS with a dynamic LoA is highly dependent on the accurate and timely actions taken by the SCC. Consequently, the failure of the SCC to remote control or communicate with the vessel is assumed to be catastrophic for the safety of the latter.

During the day, infrared cameras are only present in order to assist the operation of HD cameras and LiDAR. For this reason, there will be a minor consequence in the safe navigation in case of their failure. On the other hand, the picturing of the surroundings is highly dependent on Infrared cameras during the night operation and a possible failure is assumed to be catastrophic.

The LiDAR and cameras are assisting the operation of each other. Because of the increased redundancy, the consequence value for both of them was set to be equal to 3. Last but not least, Radar is the only equipment that can be used in order to obtain the accurate distance of the various targets from the ship and therefore, a possible malfunction or failure can be catastrophic for the safe navigation of the ship.

The aforementioned rankings for the three different scenarios are presented in Appendix 1, while Figure 16 illustrates the risk levels of various events that either show a great variance in the different scenarios or have intolerable risk values as explained earlier.

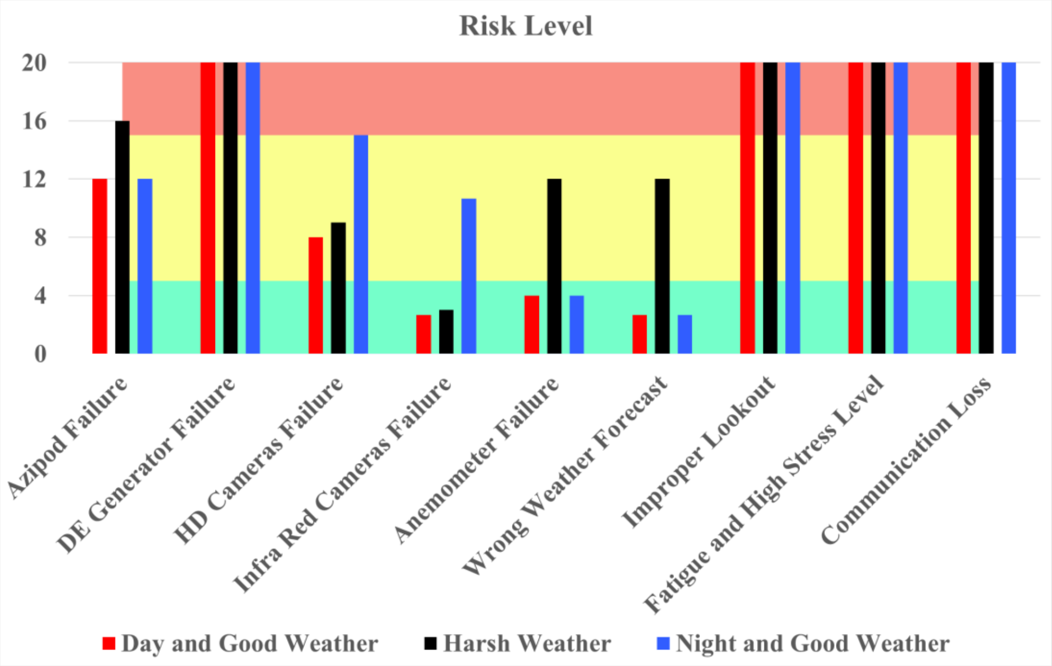


Figure 16 - Risk Level of various Hazardous Events for different scenarios

10. FAULT TREE ANALYSIS

Fault Tree Analysis was performed in order to present the events that can result in unsafe navigation. PTC Windchill Quality Solutions software was used in order to assist the quantitative analysis of the fault tree. It is worth mentioning, though, that over-reliance on software should always be avoided and two additional steps should be followed in order to ensure that the results are realistic; a) Independent verification of the results and b) Physical interpretation of the results. The first step has been achieved by conducting hand calculations in order to find the failure rates of the various events after following the theory associated with FTA that is presented in Chapter 7.1. The second step has been achieved after analysing the results and ensuring that they are realistic as presented in Chapter 11.

The three different top events that had been examined were ‘Unsafe navigation during the day with good weather conditions’, ‘Unsafe navigation during harsh weather conditions’ and ‘Unsafe navigation during the night’. It is worth noting that for this project, ‘Failure of a system’ can be defined as the situation when the system is not operating or is malfunctioning.

In all three scenarios, unsafe navigation can result when the ship does not produce and follow a correct collision avoidance plan and the SCC cannot intervene and remote control the vessel safely and in time.

Global Navigation Satellite System (GNSS) may malfunction due to the satellite and receiver clock errors, signal propagation errors (such as the sagnac effect, multipath errors as well as ionosphere and troposphere errors) together with signal spoofing and other reasons.

The reasons why the echosounder might not display the correct depth are related to the pitch motion of the vessel, the shallow water reflecting effect that can cause the signal to be received more than once as well as the error in the orientation of the transducer and the rotational speed of the stylus. However, this is of great importance in shallow waters and it is assumed that weather conditions and ship motions are not affecting the measurement during the voyage segment examined. The speed log might malfunction due to the rolling and pitching motions of the vessel as well as the orientation of the transducer.

The compass variation and deviation due to the earth’s and vessel’s magnetic fields should be taken into consideration when deriving the heading of the ship. Distortions of the magnetic field due to the presence of the ship and latency errors between the time received from the GNSS and IMU are also affecting the accuracy of the Inertia Measurement Unit (IMU).

The main problem that the LiDAR might face is the difficulty in subtracting their background from the targets, while the Radar has a blind sector in which targets are not displayed. Another limitation of the radar is that it cannot discriminate between two objects that have the same bearing and slightly different range and vice versa, and may report them as a single obstacle.

Failure to obtain depth clearance at a specific location can occur when the echosounder fails together with the GNSS and ECDIS Systems and therefore, it is not possible to obtain the required data from the charts. Failure to obtain speed and acceleration can only occur when the speed log fails together with the GNSS and the IMU. In the event that both the speed log and the IMU fail, the position shift in a specific amount of time that is obtained from the GNSS can be used in order to calculate the speed of the ship.

A number of sensors will be used for the detection of the surrounding ships and obstacles. Radar will be used in order to spot and calculate the distance of nearby vessels and LiDAR will map the surroundings of the ship. Communication between the vessel and nearby ships will also be present in order to establish communication during distress situations. Cameras will enable the capturing of the surroundings. It is vital for infrared cameras to be present in order to operate during low or no-light conditions and provide redundancy in case that HD cameras fail during the day.

10.1 SCENARIOS AND ASSUMPTIONS

The first top event examined was the ‘Unsafe navigation during the day with good weather conditions (G1)’. In this scenario, there is no risk associated with the failure of the weather sensors or the failure of the SCC to provide accurate weather forecast. Moreover, infrared cameras are present in order to provide sufficient redundancy in case HD cameras fail. Lastly, sensors and communications that are prone to malfunctioning due to bad weather conditions are not in the risk of failure. The main reasons why this top event can occur are related to equipment failure, out-of-date software as well as lack of power to the corresponding components of the subsystems. It is worth mentioning that it is assumed that an action failure can occur when there is a failure of 3 out of 4 DE generators or both switchboards, propulsion transformers, frequency converters or azipods. It is assumed that one generator during these conditions suffices for the safe operation of the ship.

The second top event examined was the ‘Unsafe navigation during harsh weather conditions (G2)’. In this scenario, weather estimation is very critical and communication between the SCC and the ship should also include the exchange of the correct weather forecast. The proper function of the weather sensors and anemometer is of great importance in this case. The overall system is very prone to malfunctioning and failures due to the bad weather conditions. It is worth mentioning that an action failure is assumed to occur when there is a failure of 2 out of 4 generators or 1 out of 2 switchboards, propulsion transformers, frequency converters or azipods. It is assumed that at least two generators are required for the navigation and manoeuvring of the vessel during such conditions.

The last top event examined was the ‘Unsafe navigation during the night with good weather conditions (G3)’. This scenario is very similar to the first one, however, possible failure of the infrared cameras will affect the safety because of the reduced lighting conditions that do not permit the use of HD cameras.

The first three levels of the Fault Tree Diagram for the Unsafe navigation during the day with good weather conditions are presented in Figure 17 below, while the full diagrams for the three different scenarios are presented in Appendices 2A-2C. A legend of the various symbols used in the fault tree is presented in Table 8 of Chapter 7.1.

It is worth noting that for the coding system of the events and gates, ‘G’ was used to indicate a gate and ‘E’ was used to indicate an event.

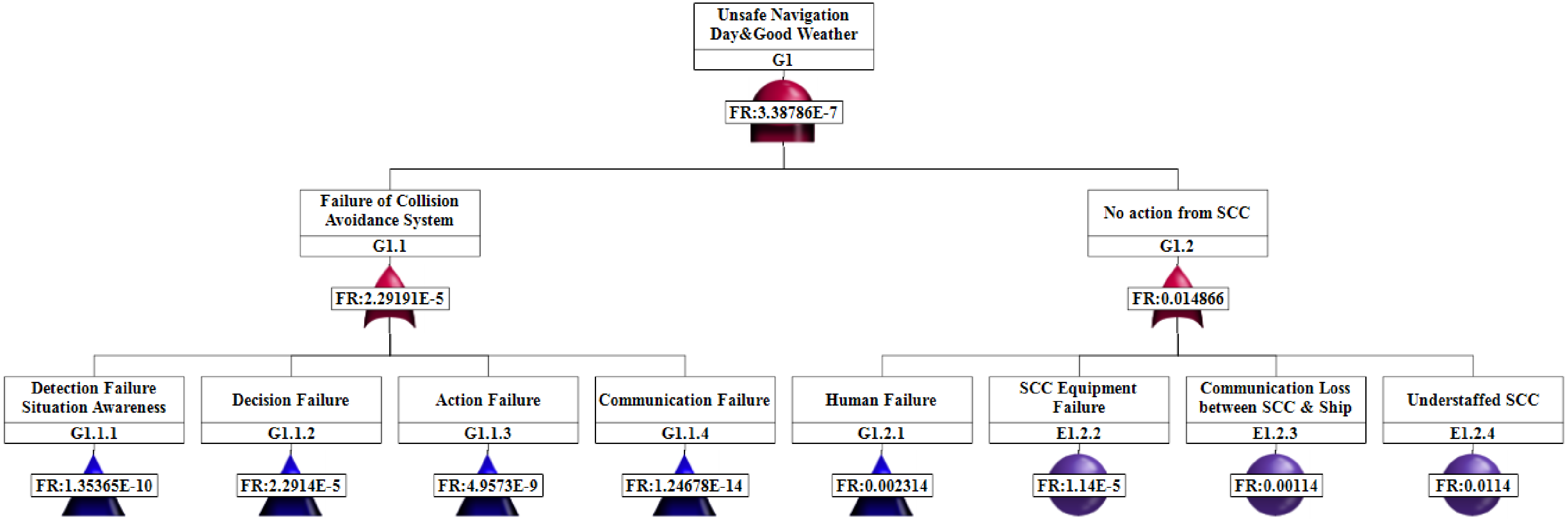


Figure 17 - FT Diagram: Day and good weather (First 3 levels)

10.2 FULLY AUTONOMOUS SCENARIO

As a further step, it was decided to analyse the navigational system of a fully autonomous ship, with no presence of a SCC and compare the results with the ones obtained for a vessel with dynamic level of autonomy. This was achieved after considering the 'Failure of collision avoidance system' as the topmost gate. Three different weather and light scenarios were examined as previously.

It is worth mentioning, though, that the vessel was assumed to have the same systems and subsystems as before. However, it was expected that in this configuration, no sufficient redundancy was present and therefore, a modified system has also been examined with increased redundancy in the systems that could result in single point failures as explained in the next chapter.

11. ANALYSIS OF FINDINGS

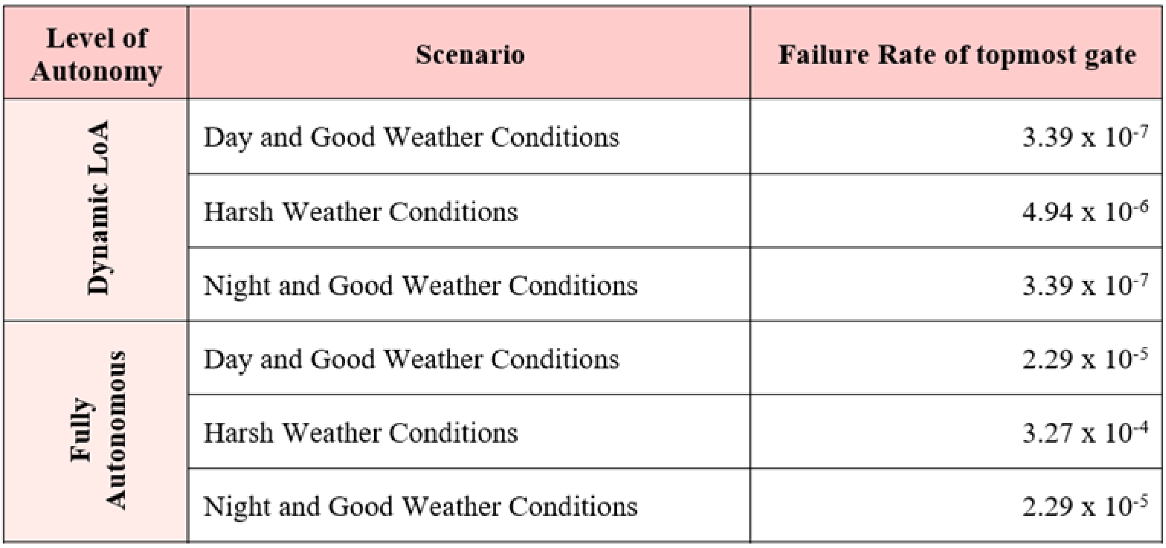
11.1 SUMMARY OF KEY FINDINGS

After conducting critical review and identifying potential hazards as well as their risk levels, the different fault trees had been constructed. PTC Windchill software was used in order to assist the quantitative analysis of the fault tree. It was decided to include as input the estimated failure rates of the various basic events in order to calculate the failure rate of the topmost gate that was the 'Unsafe Navigation' for various scenarios. It is worth noting failure rate is defined as 'the probability of failure per ship hour' and it was assumed to be fixed. The values of the failure rates for the various basic events had been decided after transforming the various rankings into probabilities per ship hour as explained in Table 9 of Chapter 9.

The failure rates of the basic events that had been used as input can be found on the corresponding basic events of the Fault Trees that are present in Appendices 2A-2C together with the calculated failure rates for the various gates for the three different scenarios. Table 13 indicates that the most critical scenario amongst the three was the one in harsh weather conditions for both the Short Sea Shipping vessel with the dynamic LoA and the fully autonomous one. However, for the fully autonomous vessel, the failure rates are significantly increased. This is the case because of the assumption of this analysis that the fully autonomous ship has exactly the same systems and subsystems as the one with the dynamic LoA. The only difference is the absence of the SCC that cannot supervise or remote control the vessel in case of emergency. It is expected that in order for fully autonomous ships to be implemented, modifications and redundancies will have to be included as explained later.

The failure rates of the top gate for the day and night with good weather scenarios are the equal for the two different types of vessel. It was expected that they would have the same result because their only difference is the malfunctioning of the HD Cameras during the night. However, as shown at the Fault Trees in Appendices 2A-2C, the camera failure occurs if both the infrared and HD cameras fail. The visualization failure occurs if the LiDAR or both types of cameras fail. Therefore, the failure rate of the visualization 'OR' gate is calculated after addition of the corresponding failure rates of the cameras and the lidar as explained in Chapter 7.1. However, the failure rate of LiDAR is much greater than the simultaneous failure of the cameras and this is the reason why the visualization failure rate and therefore the navigation failure rate does not vary significantly for the two different scenarios.

Table 13 - Failure Rates of topmost event for different scenarios



Level of Autonomy	Scenario	Failure Rate of topmost gate
Dynamic LoA	Day and Good Weather Conditions	3.39×10^{-7}
	Harsh Weather Conditions	4.94×10^{-6}
	Night and Good Weather Conditions	3.39×10^{-7}
Fully Autonomous	Day and Good Weather Conditions	2.29×10^{-5}
	Harsh Weather Conditions	3.27×10^{-4}
	Night and Good Weather Conditions	2.29×10^{-5}

Critical thinking is of vital importance in order to verify the results obtained and avoid over-reliance on the software. The physical interpretation of the results as well as the reassurance that they are realistic had been taken into consideration. Specifically, it is very reasonable that the navigation system of the fully autonomous vessel has a much higher failure rate than that of a vessel with dynamic LoA. Similarly, harsh weather scenario was expected to be the most critical one from the assumptions taken in the case study. The results that are presented in Table 13 indicate that failure of the navigation system for a fully autonomous ship is expected to take place a few times during the vessel’s life, while it is expected to take place a few times during the life of similar vessels with dynamic LoA, based on Table 9 of Chapter 9. The results are very reasonable.

Minimal cut sets are defined as ‘the unique combinations of simultaneous failures that can result in the failure of the top event’, i.e. in unsafe navigation. The minimal cut sets with an order less than three are presented in Appendix 3 for the various scenarios. It is always important to ensure that a failure of a single component does not result in the failure of the whole system. Therefore, the system was designed in such a way in order to have sufficient redundancy and avoid single point failures. However, for the fully autonomous ship a possible failure or malfunctioning of the General-Purpose Computer can result in unsafe navigation. In harsh weather conditions a failure of 1 out of 2 switchboards, propulsion transformers, frequency converters or azipods, or a failure to obtain the weather forecast can be proved critical and this was the reason why a modified fault tree has been created to avoid single point failures as explained in Chapter 11.2.

Reliability importance metrics are used in order to locate critical components that require attention, as explained in Chapter 7.2. The importance measures had been analysed in order to find the top critical failures for the different scenarios. The metrics are presented in Appendix 4 and are sorted with descending criticality values. It was concluded that the most critical events for the vessel with the dynamic LoA were the ones that are associated with humans, such as the understaffed SCC, improper lookout, fatigue, inadequate training etc. Communication loss is one of the very important aspects that have to been taken into consideration for both types of vessel. As far as equipment failures are concerned, propulsion equipment and SCC equipment have the highest criticality values. Radar/ARPA and LiDAR are the components with the highest criticality values onboard the vessel, followed by ECDIS, echosounder and GNSS. Modifications and additional redundancy had to considered in order to increase the safety of the ship as discussed in the following chapter.

11.2 SAFETY ENHANCEMENT

The aim of this project was to propose safety enhancements for MASS after identifying hazards with the highest risk levels from the Risk Analysis and events with highest criticality metrics from the Fault Tree Analysis that had been conducted.

The system can be enhanced by reducing the risk level of some hazards. This can be achieved by either reducing the probability of occurrence or the consequence. It is worth noting, though, that the reduction of the probability index is very difficult to be achieved, whereas the consequence index is more expensive. For this reason, it is always preferable to reduce both the probability and consequence indexes.

Both analyses indicated that the most critical hazards were associated with the presence of human element, such as the improper lookout, high stress levels and/or fatigue, inadequate training and human errors related to the update of the weather forecast and software. The most efficient way to eliminate the risk of hazards caused by humans for the vessel with the dynamic LoA, is the reassurance that the SCC is not understaffed and the adequate training of SCC personnel. The workplace wellness is of vital importance in order to create a healthy working environment and increase the productivity of employees.

As addressed earlier, loss of communication between the vessel and the SCC or nearby ships is one of the barriers that should be overcome. It was observed that in all scenarios and autonomy levels that had been examined, communication loss is one of the main critical scenarios. The importance of the presence of additional equipment to provide redundancy in the communication is vital. It should be noted that cybersecurity will have a great impact on the malfunctioning or failure of communication and in reality, the risk of such an event will be much higher if cybersecurity is taken into consideration.

Some of the critical components onboard the vessel include the Radar/ARPA, LiDAR, Anemometer, ECDIS and GNSS. It is proposed to increase the redundancy of the system by including additional components. However, it is worth mentioning that as far as ECDIS is concerned, vessels without AIS will not be displayed even if additional equipment are present onboard. An enhancement of the GNSS is to use data from two different sources (GALILEO and GLONASS) in order to provide accurate estimation of the location of the vessel. However, in the event that military exercises are taking place in the particular location, positioning data will not be obtained.

The importance measures for all scenarios as well as the risk indexes, indicate that equipment that is associated with the propulsion of the vessel is very prone to failure. However, it is assumed that for the particular project, the main focus is on equipment concerning the detection, decision and communication functions undertaken for the safe navigation of the ship.

A failure of the GPC in the fully autonomous scenario resulted in a failure of the overall collision avoidance system, due to the fact that SCC personnel are not present in order to intervene and decide of the best collision avoidance plan that has to be followed. Therefore, a modified fully autonomous system was also examined, having additional redundancy in the GPC in order to avoid single point failure. It is worth noting, that in the modified fully autonomous scenario, the additional redundancy in the GPC equipment had a great effect in the reduction of the failure rate of the top gate for the day and night with good weather scenarios. However, this was not the case for the harsh weather one, because the action failure can result by a failure of at least one of the azipods, switchboards, propulsion platformers or frequency converters, or 2 out of 4 DE Generators. Therefore, the action failure rate is much bigger and affects greatly the failure rate of the top event. For this reason, an additional fully autonomous modified scenario was also examined for the harsh weather conditions with an additional assumption that there is adequate reliability of the propulsion equipment and therefore, only if a malfunctioning of both azipods, switchboards, propulsion platformers or frequency converters, or 3 out of 4 DE Generators occurs, a failure of the overall system can occur (just like the good weather scenario). The fault tree diagrams for all the scenarios of the fully autonomous modified vessels are presented in Appendices 2D-2G, with the corresponding Cut-sets and Importance Measures present in Appendices 3 and 4, respectively.

Table 14 summarises the failure rates of the Navigation System for the various scenarios and levels of autonomy that had been examined. Once again, careful consideration has been given in the reassurance that the results obtained by the software were realistic. The modified fully autonomous scenario with the increased redundancy in the GPC resulted in a reduction of the failure rate of the navigation system apart from the harsh weather scenario, where a possible failure of the propulsion equipment could lead in single point failure because of the assumptions that had been taken in the initial modified scenario. However, the results of the modified harsh weather scenario with the additional assumption that the reliability of the propulsion equipment is sufficient, displayed a reduction of the failure rate of the navigation system.

Table 14 – Failure Rate variation with different assumptions and scenarios

Level of Autonomy	Scenario	Failure Rate of topmost gate
Dynamic LoA	Day and Good Weather Conditions	3.39 x 10^{-7}
	Harsh Weather Conditions	4.94 x 10^{-6}
	Night and Good Weather Conditions	3.39 x 10^{-7}
Fully Autonomous	Day and Good Weather Conditions	2.29 x 10^{-5}
	Harsh Weather Conditions	3.27 x 10^{-4}
	Night and Good Weather Conditions	2.29 x 10^{-5}
Fully Autonomous (Modified)	Day and Good Weather Conditions	5.62 x 10^{-9}
	Harsh Weather Conditions	3.04 x 10^{-4}
	Harsh Weather Conditions & Assumption	1.51 x 10^{-7}
	Night and Good Weather Conditions	5.87 x 10^{-9}

Last but not least, the location of the various sensors and especially cameras that are used for the detection of targets is of great importance. Overlapping of their ranges provides increased redundancy. HD and infrared cameras should be located next to each other for redundancy reasons. Cameras should have a range of 180° and be able cover a range of 270° by being flexible in rotational motion. In a configuration as the one shown in Figure 18, a failure occurs when there is malfunctioning of at least two nearby cameras (e.g. fore and starboard cameras). During increased light situations, infrared cameras can also be used in case HD cameras fail, however, during the night only the infrared cameras can be used.

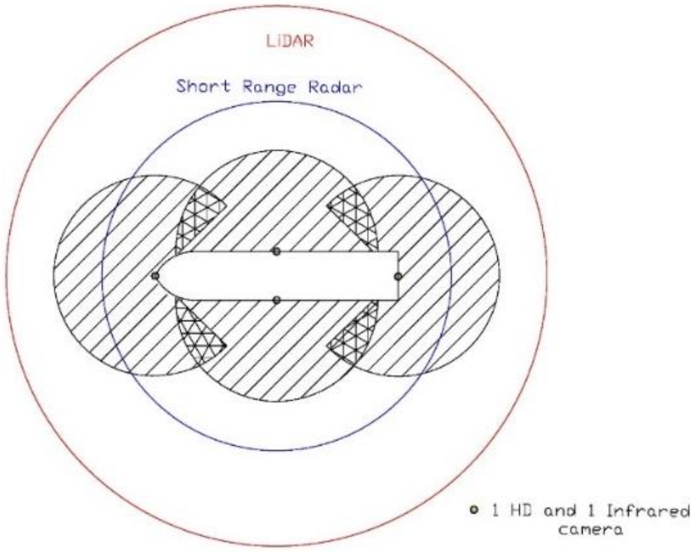


Figure 18 - Sensor Range

11.3 PRACTICAL USE OF RESULTS

The practical application of the outcomes of the particular project are the following:

Providing background information

Any further work on the subject can be benefited from the critical review that has been conducted in order to establish the subject status. Moreover, the analysis that has been followed can be reviewed in order to obtain background information about the safety assurance of the navigation system of MASS. The list of references that have been used during the project are beneficial in order to gain a broader understanding of the subject. Last but not least, the background information and outcomes of the thesis can be used to stimulate the education of people in the maritime industry about MASS and can be amended into teaching material for academic purposes.

As ready reference for industrial use

The quantitative data that had been used for the risk and safety analysis had been decided upon extensive research due to the lack of data associated with the novelty of the topic. The estimated values can be reviewed by people who have knowledge on ship operation and management in order to provide a better approximation because of their experience in the field and contribute in the future development of the project.

12. DISCUSSION

12.1 EXPERIENCE GAINED

Tackling a demanding project with lack of previous relevant experience was very challenging but provided a great foundation in order to develop life-long skills that will be used to meet objectives efficiently and effectively.

Importance of proper time and resource management

The importance of proper time and resource management had been perceived since the very beginning of the project. Various tasks had to be performed and the Systematic Management of Engineering Project (SMEP) enabled the organisation of information as well as the efficient planning of the project.

Importance of a well-structured report

The presentation of the findings is of vital importance in order to make them appealing and straightforward to the reader. It is worth mentioning that a compromise between the presentation of the big picture and the amount of details provided should be found in order to make the report reader friendly.

Development of critical thinking

Important decisions had to be made throughout the project, demonstrating critical ability and self-confidence after obtaining wider knowledge of the subject. Over-reliance on software should be avoided by all means, and validation of the results should always be made in order to examine whether they are realistic or not.

12.2 FUTURE WORK

There is potential for further improvement of this analysis. Several aspects had been addressed but not examined due to the finite amount of time that was available for the completion of this project.

Hazards associated with cybersecurity

Hazards associated with cybersecurity should be taken into consideration as they are expected to have high risk levels and affect the safe operation of the vessel. The confidentiality, integrity and availability of the ship will be highly dependent upon cyber risk. Therefore, cyber risk assessment should also be executed.

Safety assurance of MASS having various LoA

The safety assurance that had been conducted in this project focused only on a vessel with dynamic LoA and a fully autonomous one. As a future work, the same procedure can be followed for all the different LoA in order to calculate and compare the variation that might occur in the safety of their safety levels.

Safety assurance using different methods

Different safety assurance techniques can be used in order to conduct safety analysis of the same system. After considering the merits and drawbacks of the various methods, as presented in this report, a combination of them can be found in order to consider the all functions of MASS and produce efficient and effective results.

12.3 MY CONTRIBUTION

The project made a contribution in the following areas:

Estimation of data for quantitative analysis

The main contribution of this project is the estimation of the risk levels and failure rates of the various hazards associated with the navigation system of MASS. The collection of quantitative data is challenging at the current stage and this project is a good starting point for the quantitative safety analysis of the navigation system of such vessels.

Identification of critical components

The quantitative analysis enabled the identification of critical components of the navigation system of MASS that require special attention. These findings can be used during the designing and building phase of scaled models or full-scaled MASSs in order to enhance their safety.

Reference for future work

This project can enhance the understanding and academic knowledge about autonomous ships as well as the potential navigational hazards that are associated with their operation. Future projects can benefit from this thesis in order to obtain an understanding of the subject after reviewing the report and the references used.

13. CONCLUSION

The main conclusions that had been drawn from the study are the following:

1) Weather conditions have a great influence on the safe navigation of marine autonomous surface ships, regardless of the level of autonomy of the vessel. The underlying reason is that some of the components are prone to failure or malfunctioning during harsh weather conditions.
2) Unsafe navigation is less probable for a vessel with a dynamic level of autonomy because of the existence of the shore control centre and its ability to intervene and take remote control in case of emergencies. However, in this case the ship may be imposed to additional high-risk level hazards due to the effects of human factors, such as human error.
3) The safety of the navigation system can be enhanced by introducing additional redundancy in the components that had the highest risk levels according to the analysis. This can reduce the likelihood of the failure of the system.

REFERENCES

ALFHEIM, H. L., MUGGERUD, K., BREIVIK, M., BREKKE, E. F., EIDE, E. & ENGELHARDTSEN, Ø. 2018. Development of a Dynamic Positioning System for the ReVolt Model Ship. *IFAC-PapersOnLine,* 51**,** 116-121.

AUTOSHIP H2020 2019. Autonomous Shipping Initiative for European Waters.

BOLBOT, V., THEOTOKATOS, G., BUJORIANU, L. M., BOULOUGOURIS, E. & VASSALOS, D. 2019. Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. *Reliability Engineering & System Safety,* 182**,** 179-193.

BRUHN, W., BURMEISTER, H.-C., MORÆUS, J. & LONG, M. 2014. *Conducting look-out on an unmanned vessel: Introduction to the advanced sensor module for MUNIN's autonomous dry bulk carrier*.

BUREAU VERITAS. 2019. *Guidelines for Autonomous Shipping* [Online]. Available: http://erules.veristar.com/dy/data/bv/pdf/641-NI_2019-10.pdf [Accessed 27 September 2019].

BURMEISTER, H.-C., BRUHN, W., RØDSETH, Ø. J. & PORATHE, T. 2014. Autonomous Unmanned Merchant Vessel and its Contribution towards the e-Navigation Implementation: The MUNIN Perspective. *International Journal of e-Navigation and Maritime Economy,* 1**,** 1-13.

EHIAGWINA, F., AFOLABI, L. & KEHINDE, O. 2015. Fault Tree Model for Assessing the Failure Rate of a Locally Developed and Fabricated Dark Detector. *UroToday International Journal Engineering,* 6**,** 2278-4209.

EMSA. 2019. *Annual Overview of Marine Casualties and Incidents 2019* [Online]. EMSA. Available: http://www.emsa.europa.eu/news-a-press-centre/external-news/item/3734-annual-overview-of-marine-casualties-and-incidents-2019.html [Accessed February 2020].

FJØRTOFT, K. 2017. *Test Areas Autonomous Vessels* [Online]. SINTEF Ocean. Available: https://www.sintef.no/globalassets/project/trine2018/seminar-2018/kay-fjortoft_nettverksgruppe-autonome-testomrader.pdf [Accessed 26 December 2019].

GREESHMA. 2012. *Traffic alert and Collision Avoidance System (TCAS)* [Online]. Available: https://www.slideshare.net/greeshma6225/traffic-alert-and-collision-avoidance-system [Accessed February 2020].

ILLKYUN, I., DONGRYEOL, S. & JONGPIL, J. 2018. Components for Smart Autonomous Ship Architecture Based on Intelligent Information Technology. *Procedia Computer Science,* 134**,** 91-98.

IMO. 2018a. *IMO MSC 99, 16-25 May 2018* [Online]. Available: http://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx [Accessed].

IMO. 2018b. *Revised Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process* [Online]. Available: http://www.imo.org/en/OurWork/Safety/SafetyTopics/Documents/MSC-MEPC%202-Circ%2012-Rev%202.pdf [Accessed].

JOHANSEN, T. A., CRISTOFARO, A. & PEREZ, T. 2016. Ship Collision Avoidance Using Scenario-Based Model Predictive Control. *IFAC-PapersOnLine,* 49**,** 14-21.

KANG, J., JIN, M. & PARK, D. 2010. A study on application of sensor fusion to collision avoidance system for ships.

KIZHEPPATT, V., SHANKER, S., FAHMY, S. & EASWARAN, A. 2014. *Mapping Time-Critical Safety-Critical Cyber Physical Systems to Hybrid FPGAs*.

KRETSCHMANN, L., FULLER, B. S., ØRNULF, R., NOBLE, H., HORAHAN, J. & MCDOWELL, H. 2012. *MUNIN D9.3: Quantitative assessment* [Online]. Available:

http://www.unmanned-ship.org/munin/wp-content/uploads/2015/10/MUNIN-D9-3-Quantitative-assessment-CML-final.pdf [Accessed 24 December 2019].

KUO, C. 2007. *Safety Management and its Maritime Application,* The Nautical Institute.

KUO, C. 2018. The SMEP approach for tackling a project.

LAZAKIS, I., TURAN, O. & ROSENDAHL, T. 2012. *Risk assessment for the installation and maintenance activities of a low-speed tidal energy converter*.

MUNIN. 2016. *MUNIN – Maritime Unmanned Navigation through Intelligence in Networks* [Online]. Available: http://www.unmanned-ship.org/munin/ [Accessed 21 September 2019].

NTNU. 2018. *Autoferry – Autonomous all-electric passenger ferries for urban water transport* [Online]. Available: https://www.ntnu.edu/autoferry [Accessed 19 December 2019].

PARASURAMAN, R. & SHERIDAN, T. 2000. A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans,* 30.

POP, P., SCHOLLE, D., ŠLJIVO, I., HANSSON, H., WIDFORSS, G. & ROSQVIST, M. 2017. Safe cooperating cyber-physical systems using wireless communication: The SafeCOP approach. *Microprocessors and Microsystems,* 53**,** 42-50.

RAMOS, M., UTNE, I., VINNEM, J. E. & MOSLEH, A. 2018. Accounting for human failure in autonomous ship operations.

RAMOS, M. A., THIEME, C. A., UTNE, I. B. & MOSLEH, A. 2019. Human-system concurrent task analysis for maritime autonomous surface ship operation and safety. *Reliability Engineering & System Safety,* 195**,** 106697.

RØDSETH, Ø. & TJORA, Å. 2014. *A system architecture for an unmanned ship*.

ROKSETH, B., UTNE, I. B. & VINNEM, J. E. 2016. A systems approach to risk analysis of maritime operations. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* 231**,** 53-68.

ROKSETH, B., UTNE, I. B. & VINNEM, J. E. 2018. Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis. *Reliability Engineering & System Safety,* 169**,** 18-31.

SKREDDERBERGET, A. 2018. *The first ever zero emission, autonomous ship* [Online]. Available: https://www.yara.com/knowledge-grows/game-changer-for-the-environment/ [Accessed 19 December 2019].

SON, N.-S. & KIM, S.-Y. 2018. *On the sea trial test for the validation of an autonomous collision avoidance system of unmanned surface vehicle, ARAGON*.

SPÄTH, N. 2018. *Setting the standards for the future of shipping: DNV GL releases autonomous and remotely operated ship guideline* [Online]. Available: https://www.dnvgl.com/news/setting-the-standards-for-the-future-of-shipping-dnv-gl-releases-autonomous-and-remotely-operated-ship-guideline-128471 [Accessed 19 December 2019].

THIEME, C., UTNE, I. & HAUGEN, S. 2018. Assessing Ship Risk Model Applicability to Marine Autonomous Surface Ships. *Ocean Engineering,* 165.

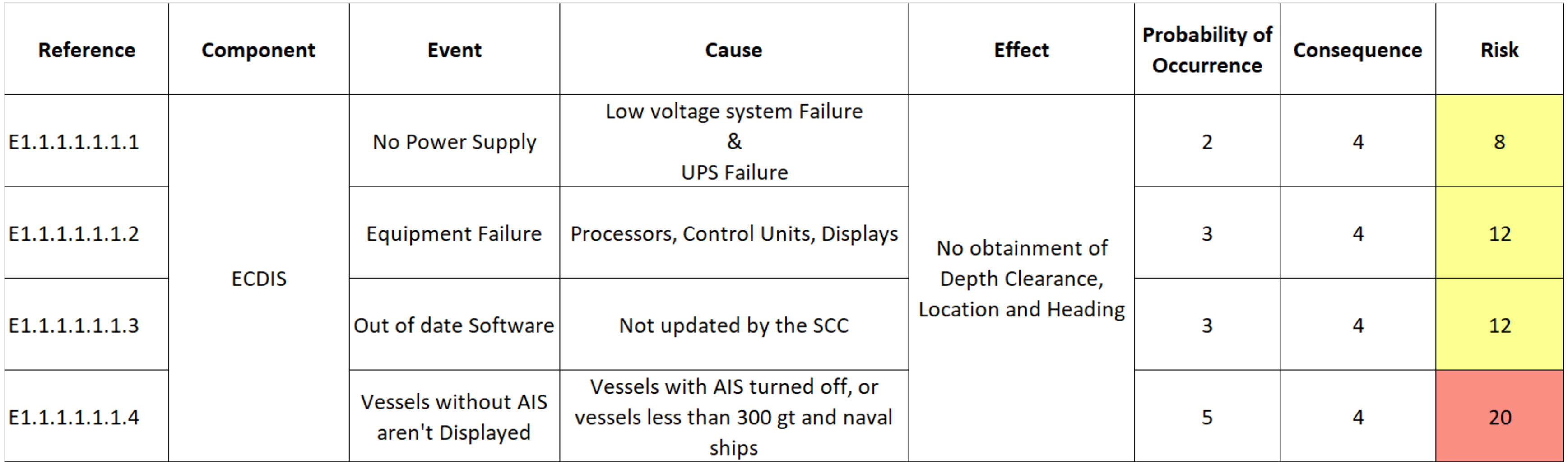
VARA, J. L. D. L., BORG, M., WNUK, K. & MOONEN, L. 2016. An Industrial Survey of Safety Evidence Change Impact Analysis Practice. *IEEE Transactions on Software Engineering,* 42**,** 1095-1117.

ZUBOWICZ, T., ARMIŃSKI, K., WITKOWSKA, A. & ŚMIERZCHALSKI, R. 2019. Marine autonomous surface ship - control system configuration. *IFAC-PapersOnLine,* 52**,** 409-415.

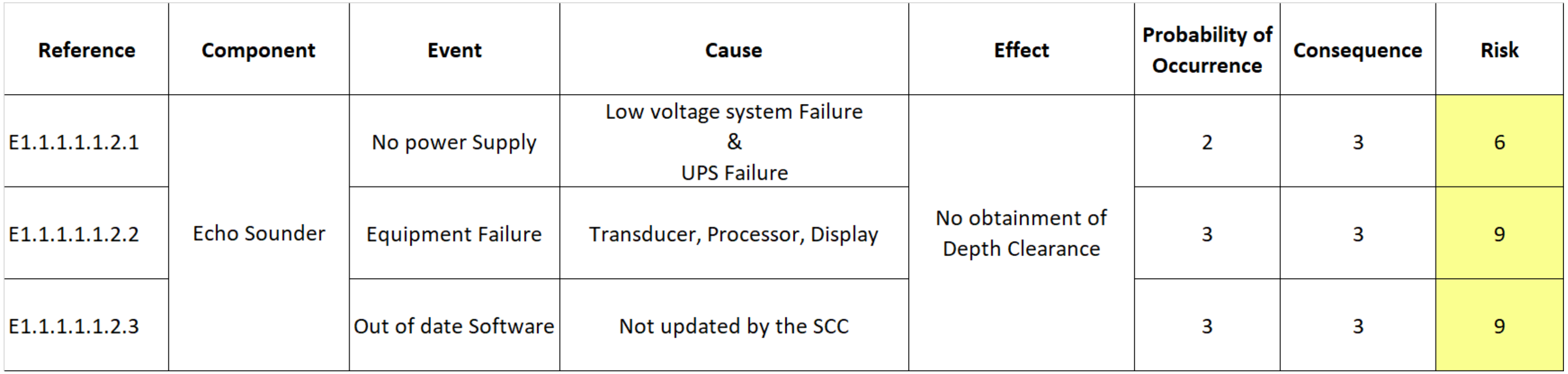
КАМКІН, І. 2015. *Traffic alert and collision avoidance system* [Online]. Available: https://www.slideshare.net/ssuser95aded/tcas-48886109 [Accessed February 2020].

APPENDIX 1. HAZARD IDENTIFICATION AND RISK RANKING

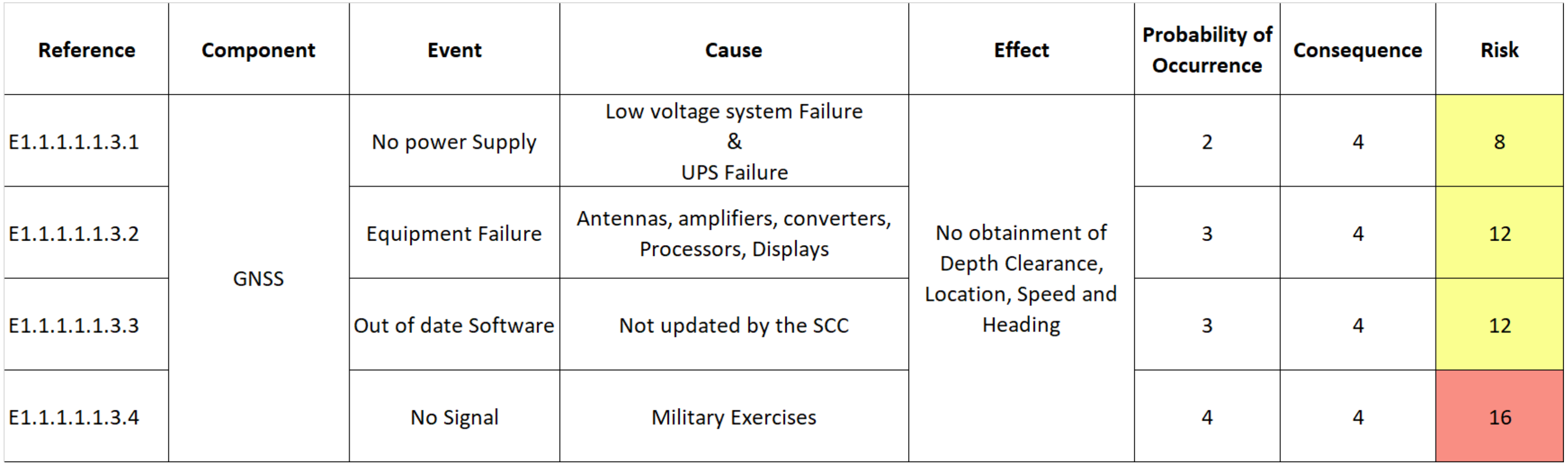
APPENDIX 1A. DAY AND GOOD WEATHER SCENARIO



Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.1.1.1.1.1	ECDIS	No Power Supply	Low voltage system Failure & UPS Failure	No obtainment of Depth Clearance, Location and Heading	2	4	8
E1.1.1.1.1.1.2		Equipment Failure	Processors, Control Units, Displays		3	4	12
E1.1.1.1.1.1.3		Out of date Software	Not updated by the SCC		3	4	12
E1.1.1.1.1.1.4		Vessels without AIS aren't Displayed	Vessels with AIS turned off, or vessels less than 300 gt and naval ships		5	4	20



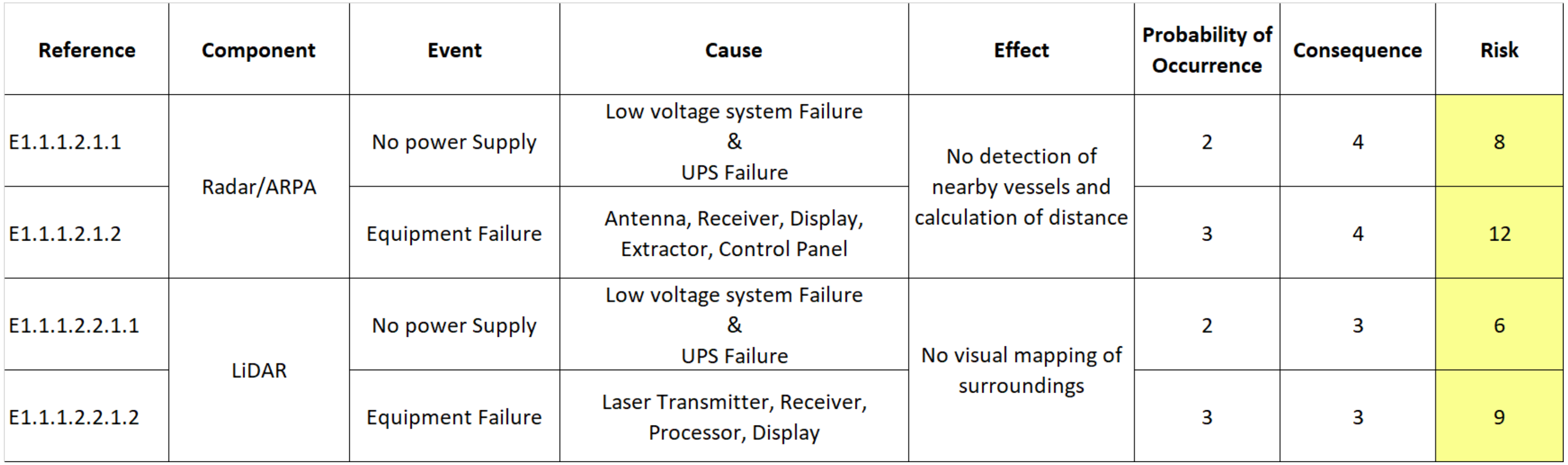
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.1.1.1.2.1	Echo Sounder	No power Supply	Low voltage system Failure & UPS Failure	No obtainment of Depth Clearance	2	3	6
E1.1.1.1.1.2.2		Equipment Failure	Transducer, Processor, Display		3	3	9
E1.1.1.1.1.2.3		Out of date Software	Not updated by the SCC		3	3	9



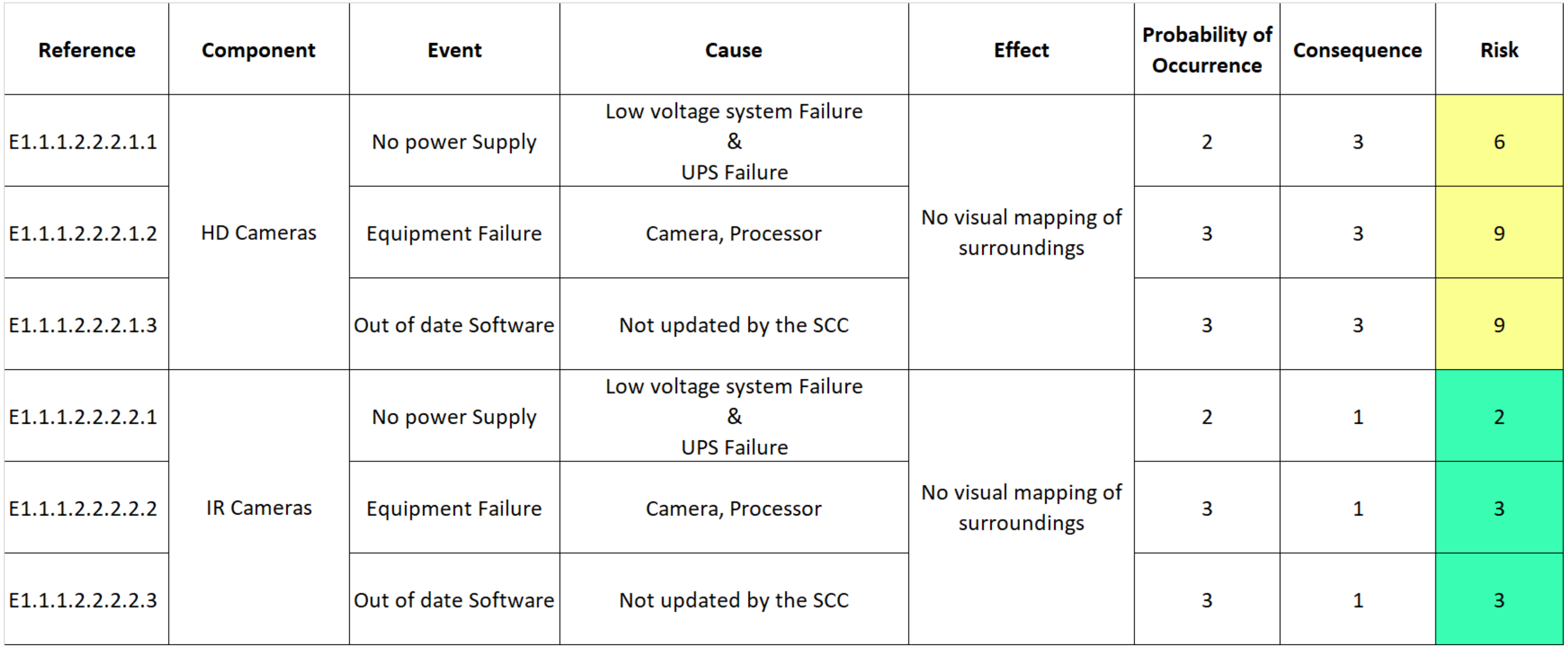
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.1.1.1.3.1	GNSS	No power Supply	Low voltage system Failure & UPS Failure	No obtainment of Depth Clearance, Location, Speed and Heading	2	4	8
E1.1.1.1.1.3.2		Equipment Failure	Antennas, amplifiers, converters, Processors, Displays		3	4	12
E1.1.1.1.1.3.3		Out of date Software	Not updated by the SCC		3	4	12
E1.1.1.1.1.3.4		No Signal	Military Exercises		4	4	16

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.1.1.2.2.1	Speed Log	No power Supply	Low voltage system Failure & UPS Failure	No obtainment of Speed	2	2	4
E1.1.1.1.2.2.2		Equipment Failure	Transducer, Processor, Display		3	2	6
E1.1.1.1.2.2.3		Out of date Software	Not updated by the SCC		3	2	6

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.1.1.2.3.1	IMU	No power Supply	Low voltage system Failure & UPS Failure	No obtainment of Heading and Acceleration	2	3	6
E1.1.1.1.2.3.2		Equipment Failure	Accelerometer, Magnetometer, Gyroscope, Converter, Processor, Display		3	3	9
E1.1.1.1.2.3.3		Out of date Software	Not updated by the SCC		3	3	9
E1.1.1.1.3.2	Compass	Equipment Failure	Processor, Dimmer Unit, Display	No obtainment of Heading	3	4	12



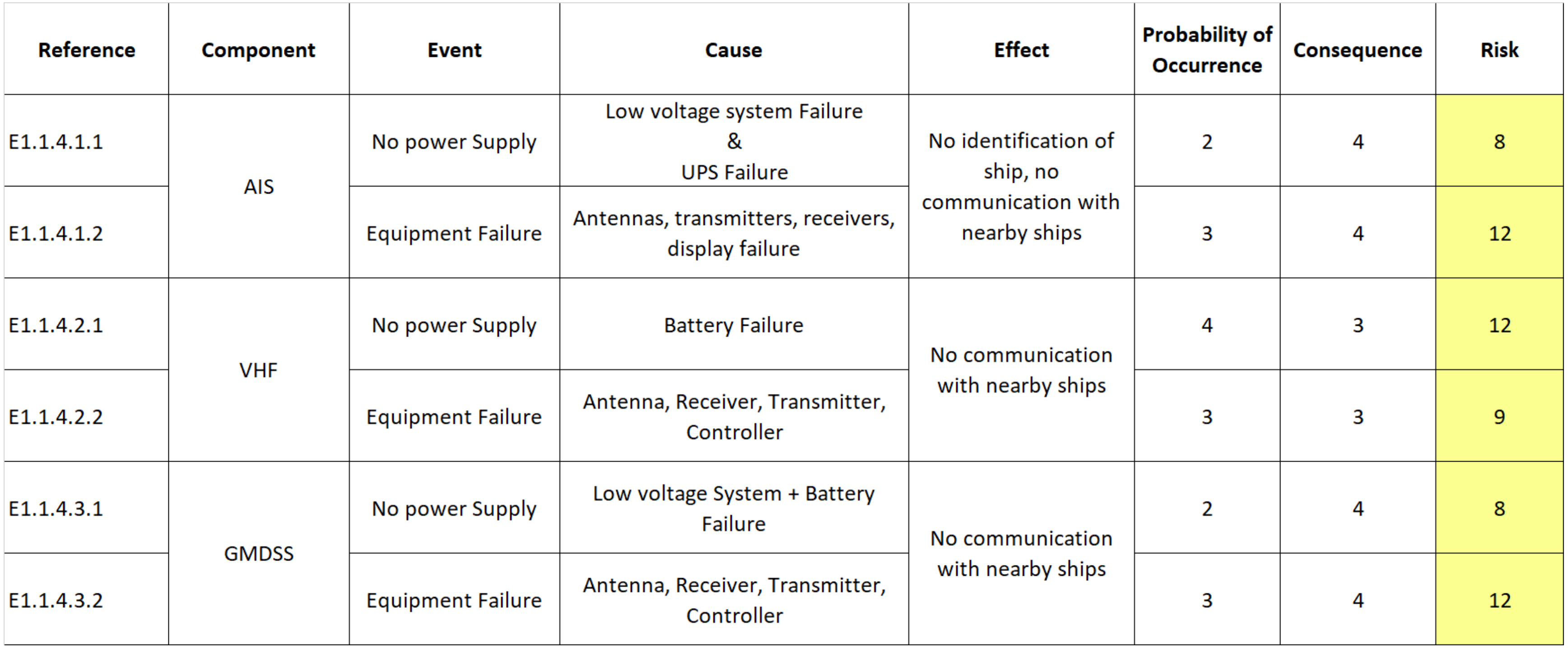
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.1.2.1.1	Radar/ARPA	No power Supply	Low voltage system Failure & UPS Failure	No detection of nearby vessels and calculation of distance	2	4	8
E1.1.1.2.1.2		Equipment Failure	Antenna, Receiver, Display, Extractor, Control Panel		3	4	12
E1.1.1.2.2.1.1	LiDAR	No power Supply	Low voltage system Failure & UPS Failure	No visual mapping of surroundings	2	3	6
E1.1.1.2.2.1.2		Equipment Failure	Laser Transmitter, Receiver, Processor, Display		3	3	9



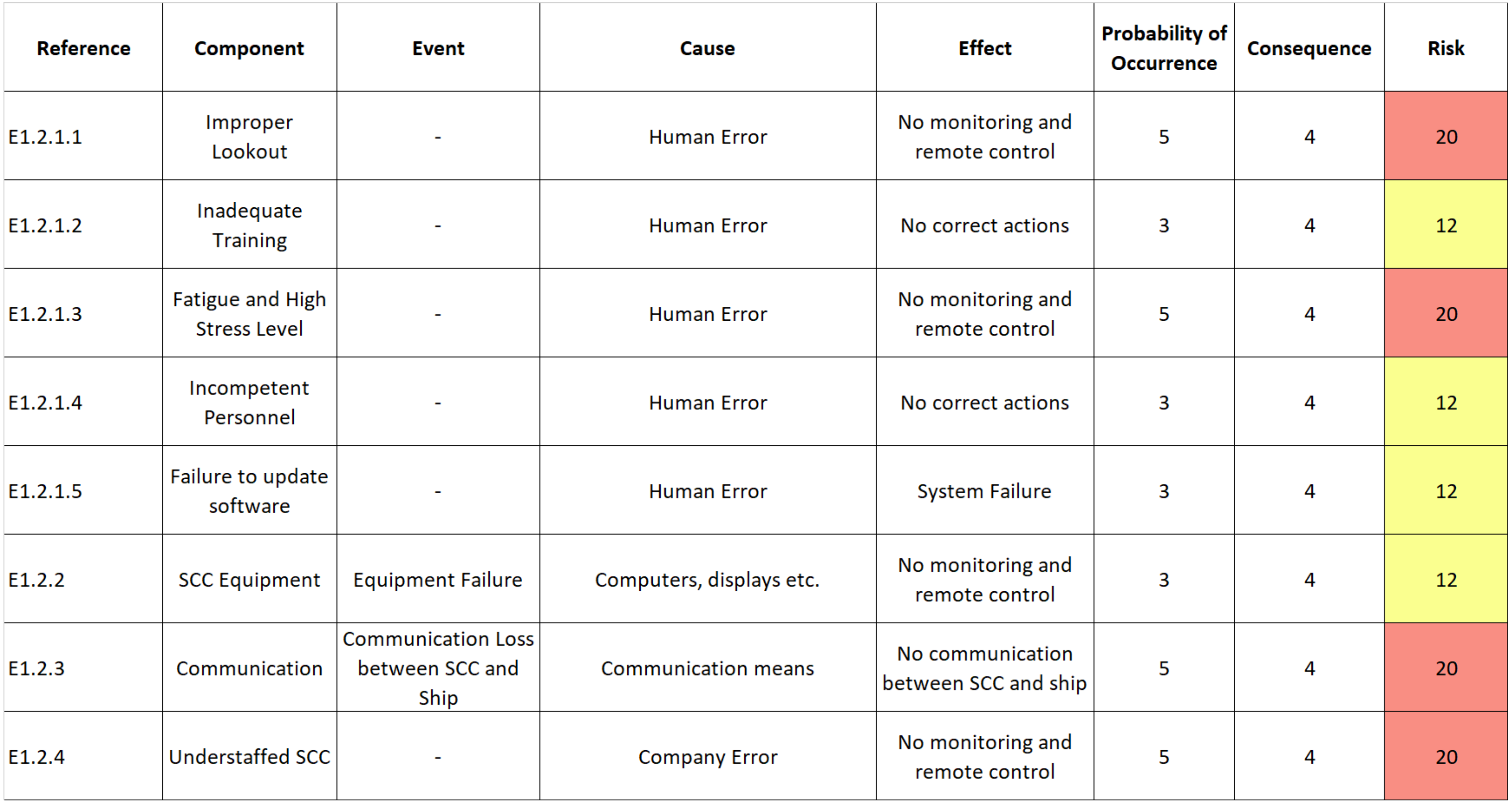
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.1.2.2.2.1.1	HD Cameras	No power Supply	Low voltage system Failure & UPS Failure	No visual mapping of surroundings	2	3	6
E1.1.1.2.2.2.1.2		Equipment Failure	Camera, Processor		3	3	9
E1.1.1.2.2.2.1.3		Out of date Software	Not updated by the SCC		3	3	9
E1.1.1.2.2.2.2.1	IR Cameras	No power Supply	Low voltage system Failure & UPS Failure	No visual mapping of surroundings	2	1	2
E1.1.1.2.2.2.2.2		Equipment Failure	Camera, Processor		3	1	3
E1.1.1.2.2.2.2.3		Out of date Software	Not updated by the SCC		3	1	3

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.2.1	GPC	No power Supply	Low voltage system Failure & UPS Failure	No decision about correct collision avoidance plan	2	4	8
E1.1.2.2		Equipment Failure	Hard disk, overheating, Motherboard		3	4	12
E1.1.2.3		Out of date Software	Not updated by the SCC		3	4	12

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.3.1.1-4	Generator	Failure to operate	Various Reasons	No propulsion action for collision avoidance	5	4	20
E1.1.3.2.1-2	Switchboard	Failure to operate	Various Reasons		3	4	12
E1.1.3.3.1-2	Propulsion Transformer	Failure to operate	Various Reasons		3	4	12
E1.1.3.4.1-2	Frequency Converter	Failure to operate	Various Reasons		3	4	12
E1.1.3.5.1-2	Azipod	Failure to operate	Various Reasons		3	4	12



Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.1.4.1.1	AIS	No power Supply	Low voltage system Failure & UPS Failure	No identification of ship, no communication with nearby ships	2	4	8
E1.1.4.1.2		Equipment Failure	Antennas, transmitters, receivers, display failure		3	4	12
E1.1.4.2.1	VHF	No power Supply	Battery Failure	No communication with nearby ships	4	3	12
E1.1.4.2.2		Equipment Failure	Antenna, Receiver, Transmitter, Controller		3	3	9
E1.1.4.3.1	GMDSS	No power Supply	Low voltage System + Battery Failure	No communication with nearby ships	2	4	8
E1.1.4.3.2		Equipment Failure	Antenna, Receiver, Transmitter, Controller		3	4	12



Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E1.2.1.1	Improper Lookout	-	Human Error	No monitoring and remote control	5	4	20
E1.2.1.2	Inadequate Training	-	Human Error	No correct actions	3	4	12
E1.2.1.3	Fatigue and High Stress Level	-	Human Error	No monitoring and remote control	5	4	20
E1.2.1.4	Incompetent Personnel	-	Human Error	No correct actions	3	4	12
E1.2.1.5	Failure to update software	-	Human Error	System Failure	3	4	12
E1.2.2	SCC Equipment	Equipment Failure	Computers, displays etc.	No monitoring and remote control	3	4	12
E1.2.3	Communication	Communication Loss between SCC and Ship	Communication means	No communication between SCC and ship	5	4	20
E1.2.4	Understaffed SCC	-	Company Error	No monitoring and remote control	5	4	20

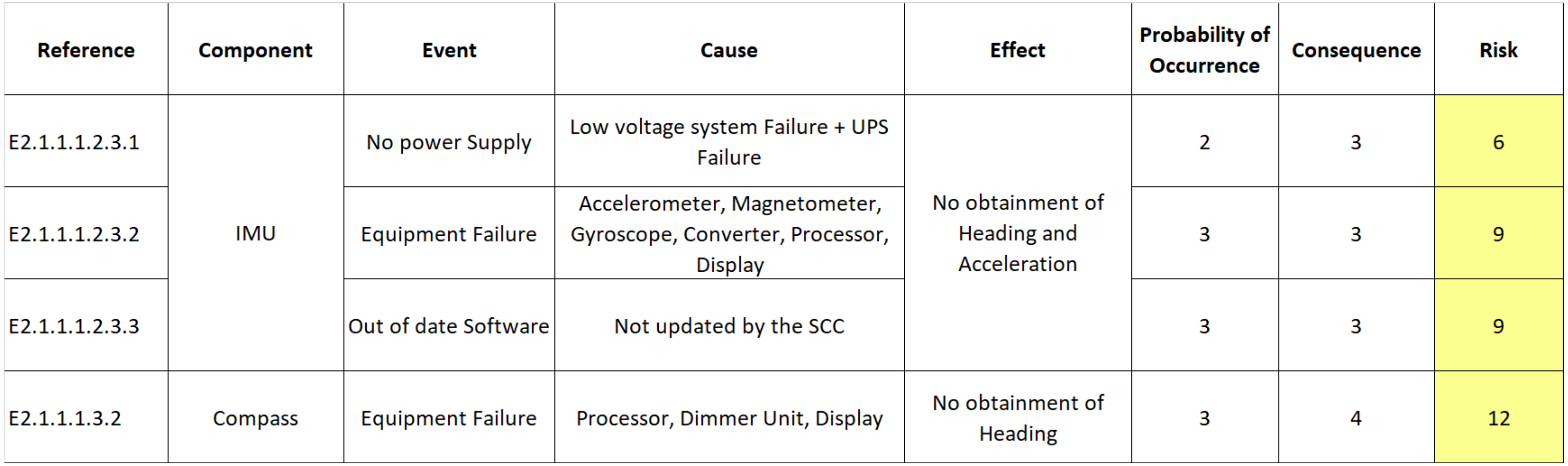
APPENDIX 1B. HARSH WEATHER SCENARIO

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.1.1.1.1.1	ECDIS	No Power Supply	Low voltage system Failure + UPS Failure	No obtainment of Depth Clearance, Location and Heading	2	4	8
E2.1.1.1.1.1.2		Equipment Failure	Processors, Control Units, Displays		3	4	12
E2.1.1.1.1.1.3		Out of date Software	Not updated by the SCC		3	4	12
E2.1.1.1.1.1.4		Vessels without AIS aren't Displayed	Vessels with AIS turned off, or vessels less than 300 gt and naval ships		5	4	20

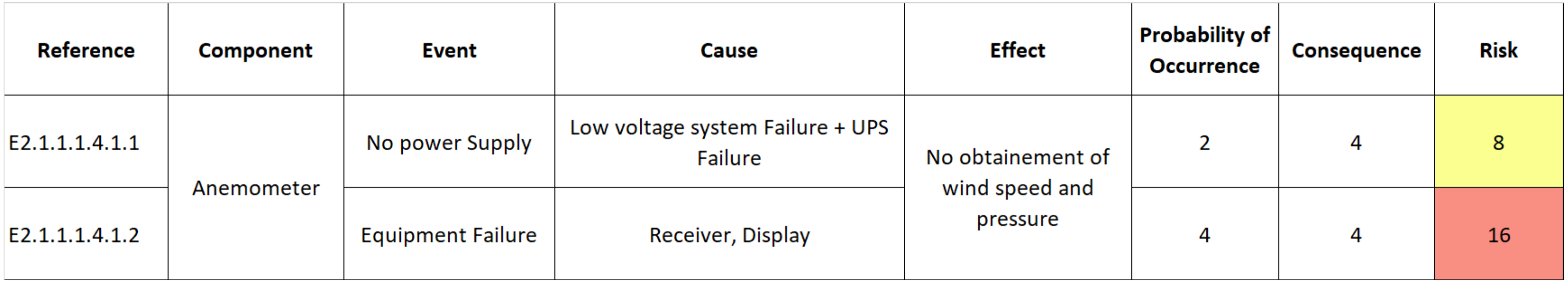
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.1.1.1.2.1	Echo Sounder	No power Supply	Low voltage system Failure + UPS Failure	No obtainment of Depth Clearance	2	3	6
E2.1.1.1.1.2.2		Equipment Failure	Transducer, Processor, Display		3	3	9
E2.1.1.1.1.2.3		Out of date Software	Not updated by the SCC		3	3	9

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.1.1.1.3.1	GNSS	No No power Supply	Low voltage system Failure + UPS Failure	No obtainment of Depth Clearance, Location, Speed and Heading	2	4	8
E2.1.1.1.1.3.2		Equipment Failure	Antennas, amplifiers, converters, Processors, Displays		3	4	12
E2.1.1.1.1.3.3		Out of date Software	Not updated by the SCC		3	4	12
E2.1.1.1.1.3.4		No Signal	Military Exercises		4	4	16

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.1.1.2.2.1	Speed Log	No power Supply	Low voltage system Failure + UPS Failure	No obtainment of Speed	2	2	4
E2.1.1.1.2.2.2		Equipment Failure	Transducer, Processor, Display		3	2	6
E2.1.1.1.2.2.3		Out of date Software	Not updated by the SCC		3	2	6



Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.1.1.2.3.1	IMU	No power Supply	Low voltage system Failure + UPS Failure	No obtainment of Heading and Acceleration	2	3	6
E2.1.1.1.2.3.2		Equipment Failure	Accelerometer, Magnetometer, Gyroscope, Converter, Processor, Display		3	3	9
E2.1.1.1.2.3.3		Out of date Software	Not updated by the SCC		3	3	9
E2.1.1.1.3.2	Compass	Equipment Failure	Processor, Dimmer Unit, Display	No obtainment of Heading	3	4	12



Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.1.1.4.1.1	Anemometer	No power Supply	Low voltage system Failure + UPS Failure	No obtainement of wind speed and pressure	2	4	8
E2.1.1.1.4.1.2		Equipment Failure	Receiver, Display		4	4	16

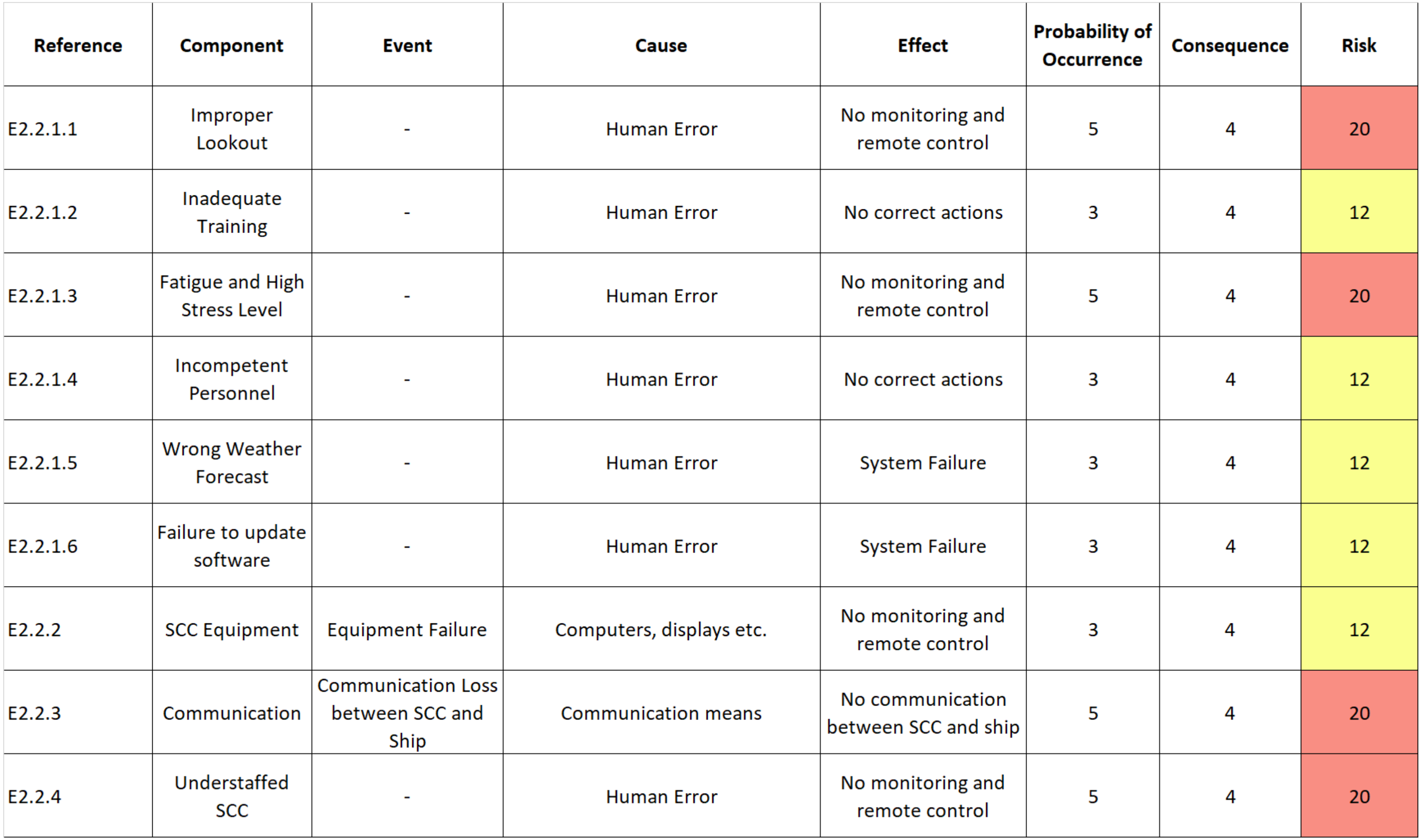
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.1.2.1.1	Radar/ARPA	No power Supply	Low voltage system Failure + UPS Failure	No detection of nearby vessels and calculation of distance	2	4	8
E2.1.1.2.1.2		Equipment Failure	Antenna, Receiver, Display, Extractor, Control Panel		3	4	12
E2.1.1.2.2.1.1	LiDAR	No power Supply	Low voltage system Failure + UPS Failure	No visual mapping of surroundings	2	3	6
E2.1.1.2.2.1.2		Equipment Failure	Laser Transmitter, Receiver, Processor, Display		4	3	12

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.1.2.2.2.1.1	HD Cameras	No power Supply	Low voltage system Failure + UPS Failure	No visual mapping of surroundings	2	3	6
E2.1.1.2.2.2.1.2		Equipment Failure	Camera, Processor		4	3	12
E2.1.1.2.2.2.1.3		Out of date Software	Not updated by the SCC		3	3	9
E2.1.1.2.2.2.2.1	IR Cameras	No power Supply	Low voltage system Failure + UPS Failure	No visual mapping of surroundings	2	1	2
E2.1.1.2.2.2.2.2		Equipment Failure	Camera, Processor		4	1	4
E2.1.1.2.2.2.2.3		Out of date Software	Not updated by the SCC		3	1	3

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.2.1	GPC	No power Supply	Low voltage system Failure + UPS Failure	No decision about correct collision avoidance plan	2	4	8
E2.1.2.2		Equipment Failure	Hard disk, overheating, Motherboard		3	4	12
E2.1.2.3		Out of date Software	Not updated by the SCC		3	4	12

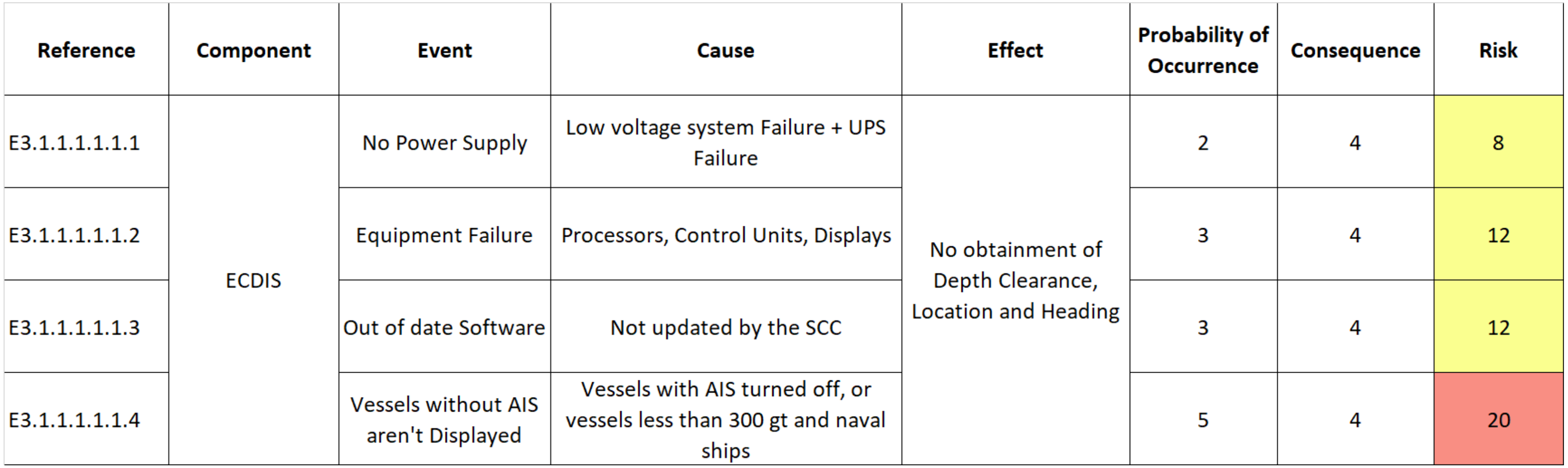
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.3.1.1-4	Generator	Failure to operate	Various Reasons	No propulsion action for collision avoidance	5	4	20
E2.1.3.2.1-2	Switchboard	Failure to operate	Various Reasons		3	4	12
E2.1.3.3.1-2	Propulsion Transformer	Failure to operate	Various Reasons		3	4	12
E2.1.3.4.1-2	Frequency Converter	Failure to operate	Various Reasons		3	4	12
E2.1.3.5.1-2	Azipod	Failure to operate	Various Reasons		4	4	16

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.1.4.1.1	AIS	No power Supply	Low voltage system Failure + UPS Failure	No identification of ship, no communication with nearby ships	2	4	8
E2.1.4.1.2		Equipment Failure	Antennas, transmitters, receivers, display failure		3	4	12
E2.1.4.2.1	VHF	No power Supply	Battery Failure	No communication with nearby ships	4	3	12
E2.1.4.2.2		Equipment Failure	Antenna, Receiver, Transmitter, Controller		3	3	9
E2.1.4.3.1	GMDSS	No power Supply	Low voltage System + Battery Failure	No communication with nearby ships	2	4	8
E2.1.4.3.2		Equipment Failure	Antenna, Receiver, Transmitter, Controller		3	4	12

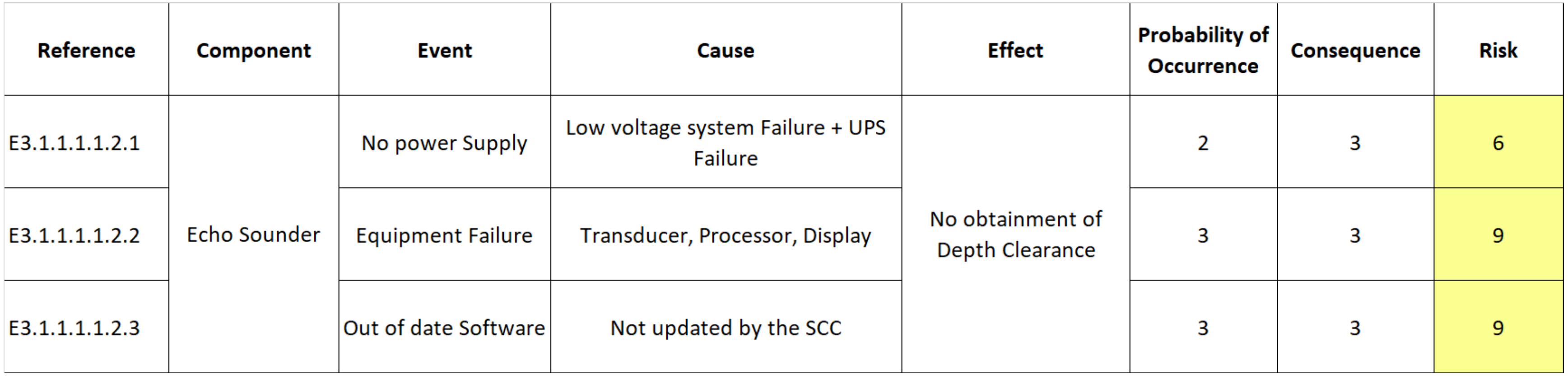


Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E2.2.1.1	Improper Lookout	-	Human Error	No monitoring and remote control	5	4	20
E2.2.1.2	Inadequate Training	-	Human Error	No correct actions	3	4	12
E2.2.1.3	Fatigue and High Stress Level	-	Human Error	No monitoring and remote control	5	4	20
E2.2.1.4	Incompetent Personnel	-	Human Error	No correct actions	3	4	12
E2.2.1.5	Wrong Weather Forecast	-	Human Error	System Failure	3	4	12
E2.2.1.6	Failure to update software	-	Human Error	System Failure	3	4	12
E2.2.2	SCC Equipment	Equipment Failure	Computers, displays etc.	No monitoring and remote control	3	4	12
E2.2.3	Communication	Communication Loss between SCC and Ship	Communication means	No communication between SCC and ship	5	4	20
E2.2.4	Understaffed SCC	-	Human Error	No monitoring and remote control	5	4	20

APPENDIX 1C. NIGHT AND GOOD WETAHER SCENARIO



Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.1.1.1.1.1	ECDIS	No Power Supply	Low voltage system Failure + UPS Failure	No obtainment of Depth Clearance, Location and Heading	2	4	8
E3.1.1.1.1.1.2		Equipment Failure	Processors, Control Units, Displays		3	4	12
E3.1.1.1.1.1.3		Out of date Software	Not updated by the SCC		3	4	12
E3.1.1.1.1.1.4		Vessels without AIS aren't Displayed	Vessels with AIS turned off, or vessels less than 300 gt and naval ships		5	4	20



Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.1.1.1.2.1	Echo Sounder	No power Supply	Low voltage system Failure + UPS Failure	No obtainment of Depth Clearance	2	3	6
E3.1.1.1.1.2.2		Equipment Failure	Transducer, Processor, Display		3	3	9
E3.1.1.1.1.2.3		Out of date Software	Not updated by the SCC		3	3	9

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.1.1.1.3.1	GNSS	No power Supply	Low voltage system Failure + UPS Failure	No obtainment of Depth Clearance, Location, Speed and Heading	2	4	8
E3.1.1.1.1.3.2		Equipment Failure	Antennas, amplifiers, converters, Processors, Displays		3	4	12
E3.1.1.1.1.3.3		Out of date Software	Not updated by the SCC		3	4	12
E3.1.1.1.1.3.4		No Signal	Military Exercises		4	4	16

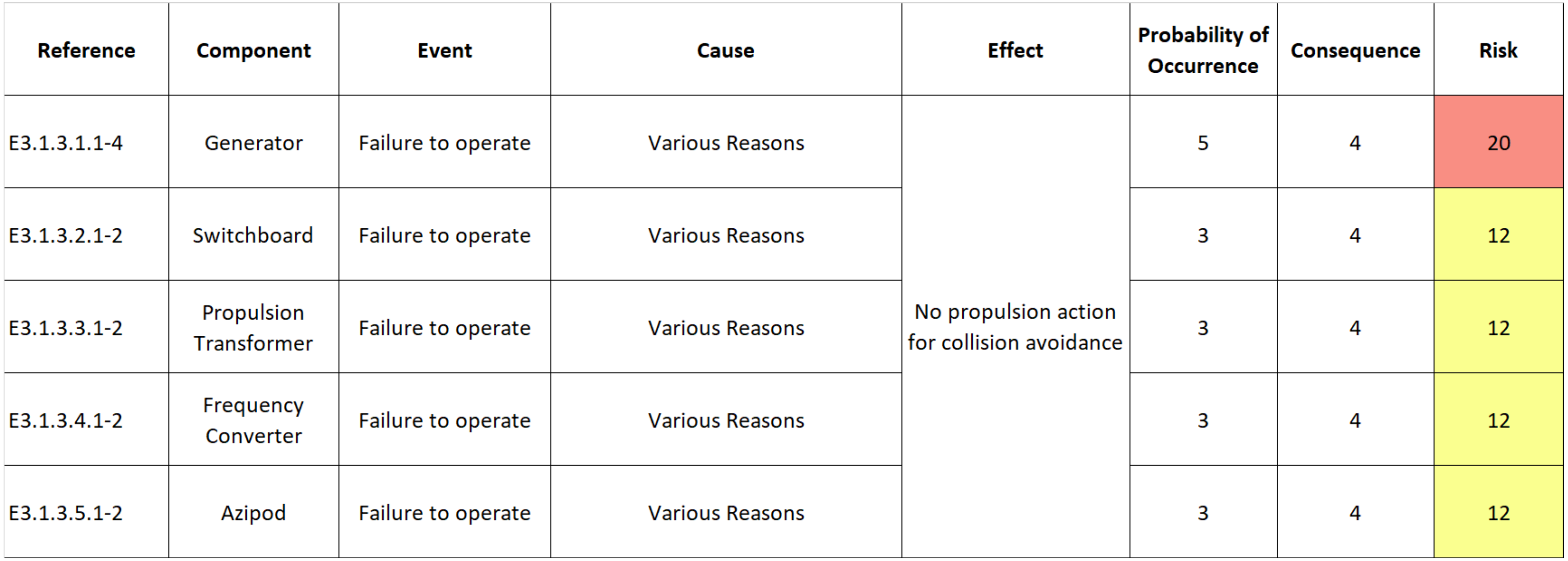
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.1.1.2.2.1	Speed Log	No power Supply	Low voltage system Failure + UPS Failure	No obtainment of Speed	2	2	4
E3.1.1.1.2.2.2		Equipment Failure	Transducer, Processor, Display		3	2	6
E3.1.1.1.2.2.3		Out of date Software	Not updated by the SCC		3	2	6

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.1.1.2.3.1	IMU	No power Supply	Low voltage system Failure + UPS Failure	No obtainment of Heading and Acceleration	2	3	6
E3.1.1.1.2.3.2		Equipment Failure	Accelerometer, Magnetometer, Gyroscope, Converter, Processor, Display		3	3	9
E3.1.1.1.2.3.3		Out of date Software	Not updated by the SCC		3	3	9
E3.1.1.1.3.2	Compass	Equipment Failure	Processor, Dimmer Unit, Display	No obtainment of Heading	3	4	12

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.1.2.1.1	Radar/ARPA	No power Supply	Low voltage system Failure + UPS Failure	No detection of nearby vessels and calculation of distance	2	4	8
E3.1.1.2.1.2		Equipment Failure	Antenna, Receiver, Display, Extractor, Control Panel		3	4	12
E3.1.1.2.2.1.1	LiDAR	No power Supply	Low voltage system Failure + UPS Failure	No visual mapping of surroundings	2	3	6
E3.1.1.2.2.1.2		Equipment Failure	Laser Transmitter, Receiver, Processor, Display		3	3	9

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.1.2.2.2.1.1	HD Cameras	No power Supply	Low voltage system Failure + UPS Failure	No visual mapping of surroundings	5	3	15
E3.1.1.2.2.2.1.2		Equipment Failure	Camera, Processor		5	3	15
E1.1.1.2.2.2.1.3		Out of date Software	Not updated by the SCC		5	3	15
E3.1.1.2.2.2.2.1	IR Cameras	No power Supply	Low voltage system Failure + UPS Failure	No visual mapping of surroundings	2	4	8
E3.1.1.2.2.2.2.2		Equipment Failure	Camera, Processor		3	4	12
E1.1.1.2.2.2.2.3		Out of date Software	Not updated by the SCC		3	4	12

Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.2.1	GPC	No power Supply	Low voltage system Failure + UPS Failure	No decision about correct collision avoidance plan	2	4	8
E3.1.2.2		Equipment Failure	Hard disk, overheating, Motherboard		3	4	12
E3.1.2.3		Out of date Software	Not updated by the SCC		3	4	12



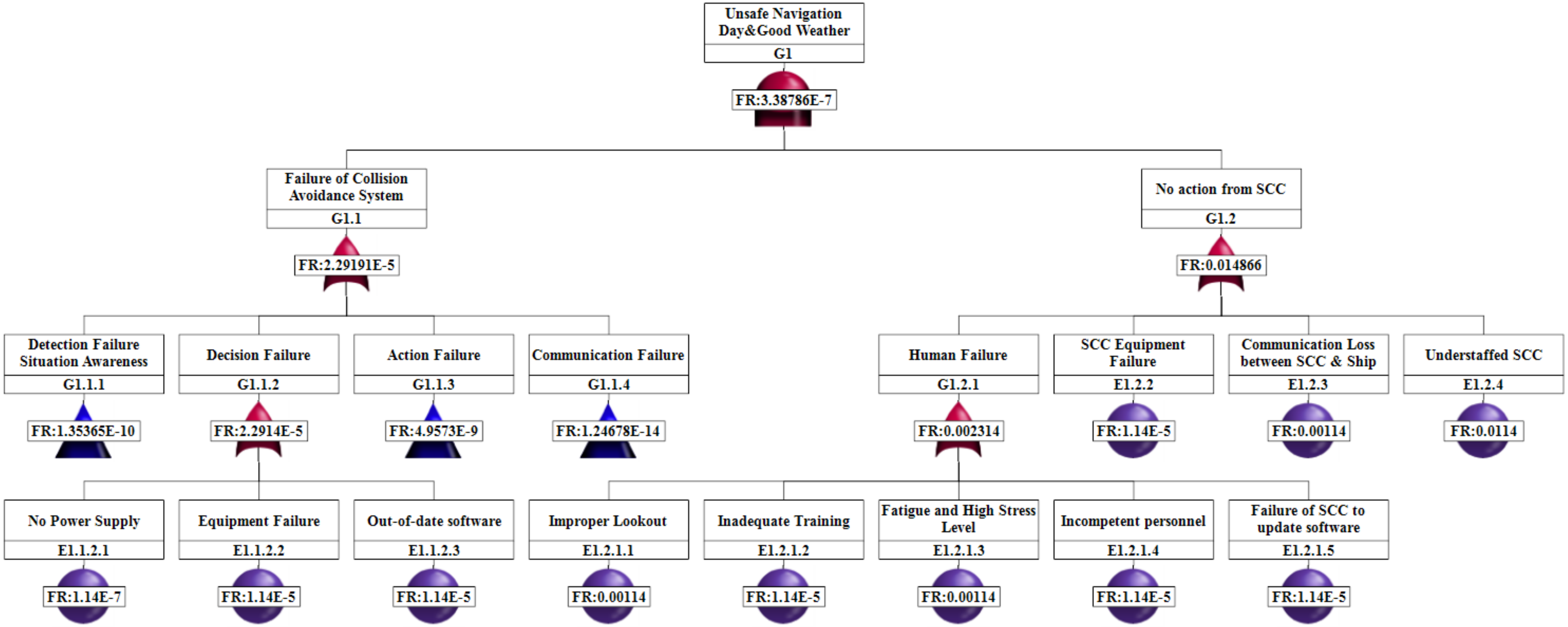
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.3.1.1-4	Generator	Failure to operate	Various Reasons	No propulsion action for collision avoidance	5	4	20
E3.1.3.2.1-2	Switchboard	Failure to operate	Various Reasons		3	4	12
E3.1.3.3.1-2	Propulsion Transformer	Failure to operate	Various Reasons		3	4	12
E3.1.3.4.1-2	Frequency Converter	Failure to operate	Various Reasons		3	4	12
E3.1.3.5.1-2	Azipod	Failure to operate	Various Reasons		3	4	12

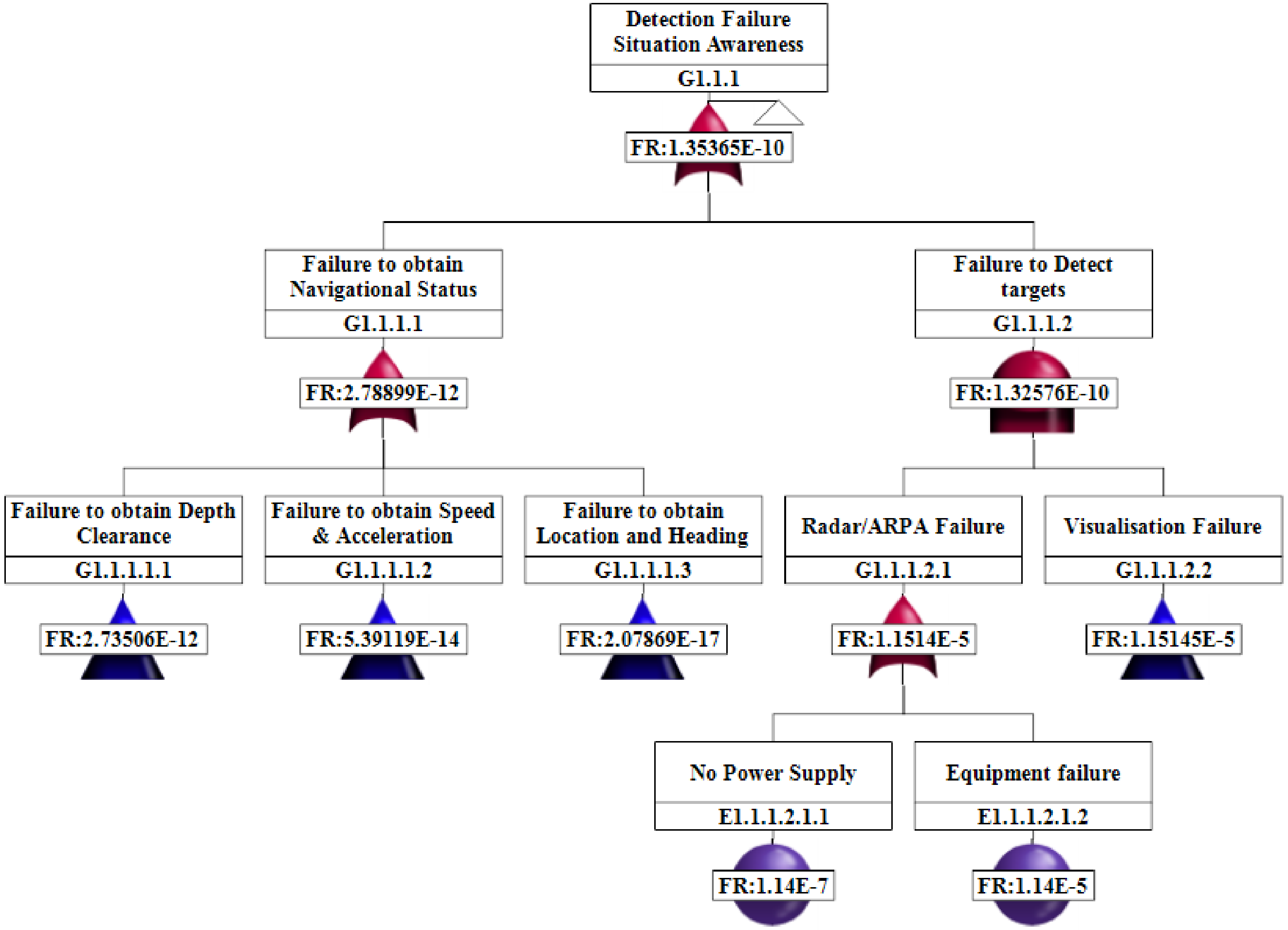
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.1.4.1.1	AIS	No power Supply	Low voltage system Failure + UPS Failure	No identification of ship, no communication with nearby ships	2	4	8
E3.1.4.1.2		Equipment Failure	Antennas, transmitters, receivers, display failure		3	4	12
E3.1.4.2.1	VHF	No power Supply	Battery Failure	No communication with nearby ships	4	3	12
E3.1.4.2.2		Equipment Failure	Antenna, Receiver, Transmitter, Controller		3	3	9
E3.1.4.3.1	GMDSS	No power Supply	Low voltage System + Battery Failure	No communication with nearby ships	2	4	8
E3.1.4.3.2		Equipment Failure	Antenna, Receiver, Transmitter, Controller		3	4	12

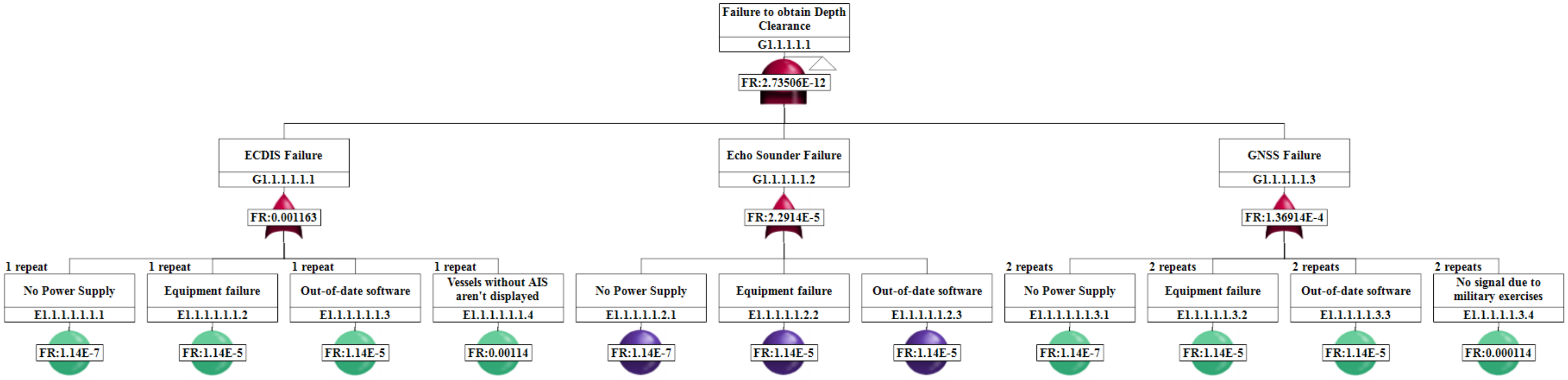
Reference	Component	Event	Cause	Effect	Probability of Occurrence	Consequence	Risk
E3.2.1.1	Improper Lookout	-	Human Error	No monitoring and remote control	5	4	20
E3.2.1.2	Inadequate Training	-	Human Error	No correct actions	3	4	12
E3.2.1.3	Fatigue and High Stress Level	-	Human Error	No monitoring and remote control	5	4	20
E3.2.1.4	Incompetent Personnel	-	Human Error	No correct actions	3	4	12
E3.2.1.5	Failure to update software	-	Human Error	System Failure	3	4	12
E3.2.2	SCC Equipment	Equipment Failure	Computers, displays etc.	No monitoring and remote control	3	4	12
E3.2.3	Communication	Communication Loss between SCC and Ship	Communication means	No communication between SCC and ship	5	4	20
E3.2.4	Understaffed SCC	-	Company Error	No monitoring and remote control	5	4	20

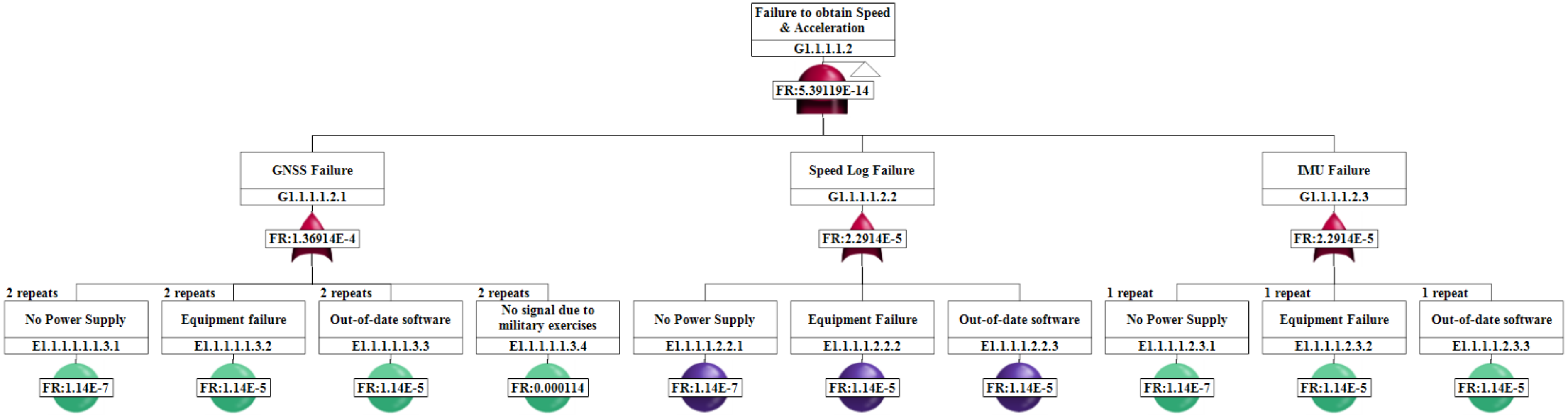
APPENDIX 2. FAULT TREE DIAGRAMS

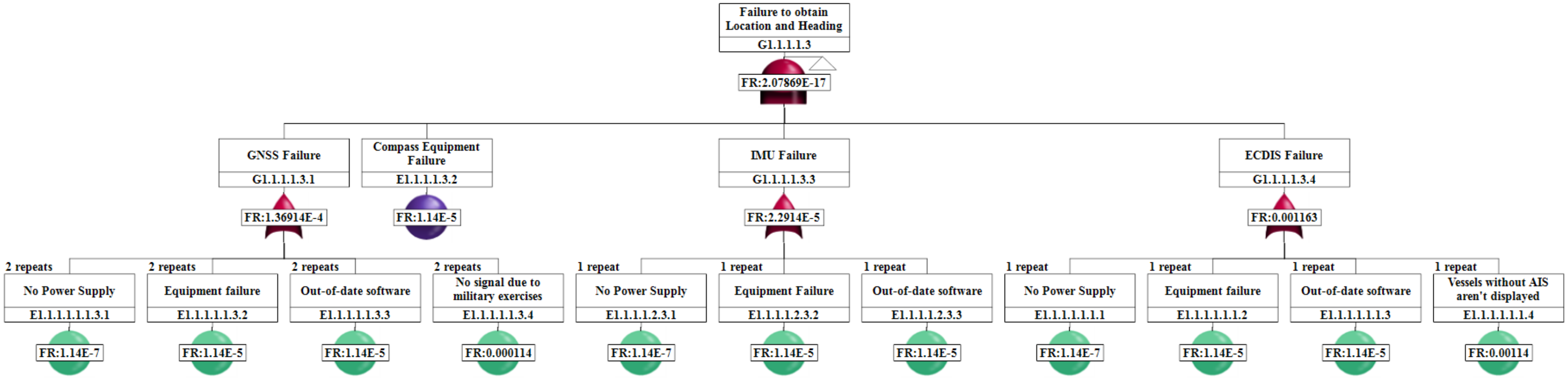
APPENDIX 2A. DAY AND GOOD WEATHER SCENARIO – DYNAMIC LoA

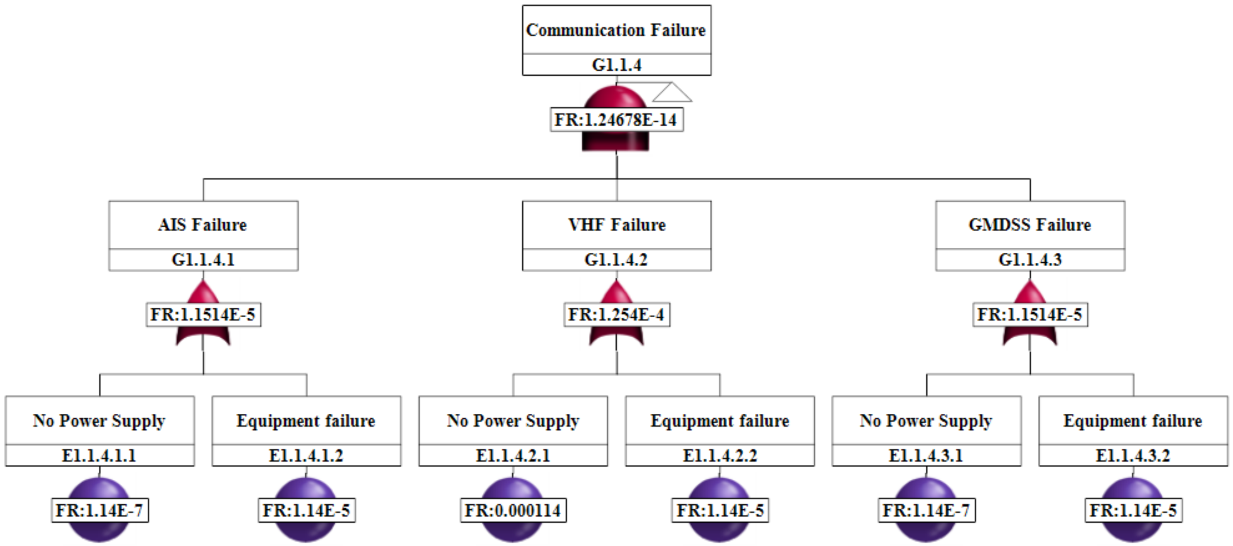


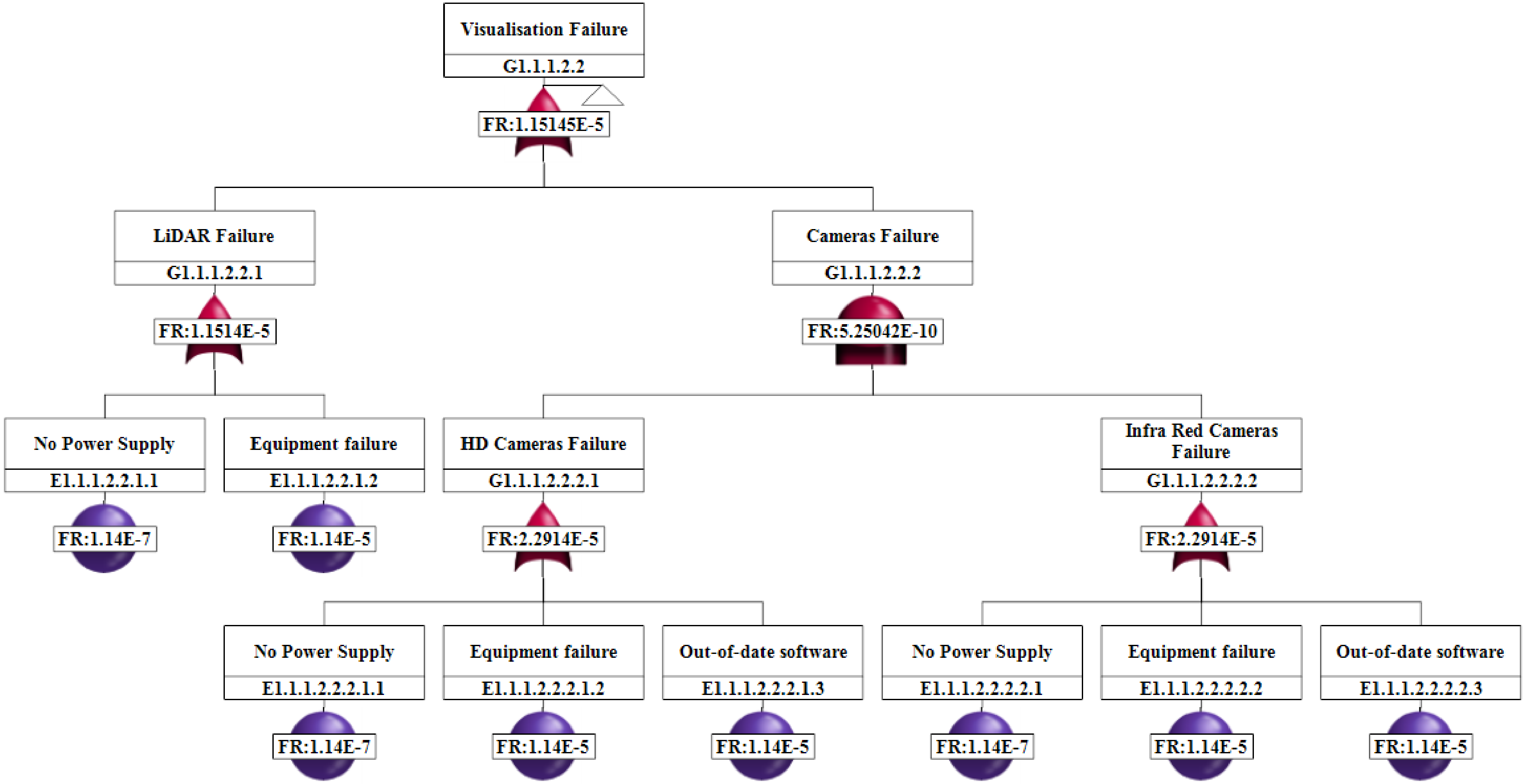

Detection Failure Situation Awareness
G1.1.1
FR:1.35365E-10
Failure to obtain Navigational Status
G1.1.1.1
FR:2.78899E-12
Failure to Detect targets
G1.1.1.2
FR:1.32576E-10
Failure to obtain Depth Clearance
G1.1.1.1.1
FR:2.73506E-12
Failure to obtain Speed & Acceleration
G1.1.1.1.2
FR:5.39119E-14
Failure to obtain Location and Heading
G1.1.1.1.3
FR:2.07869E-17
Radar/ARPA Failure
G1.1.1.2.1
FR:1.1514E-5
Visualisation Failure
G1.1.1.2.2
FR:1.15145E-5
No Power Supply
E1.1.1.2.1.1
FR:1.14E-7
Equipment failure
E1.1.1.2.1.2
FR:1.14E-5

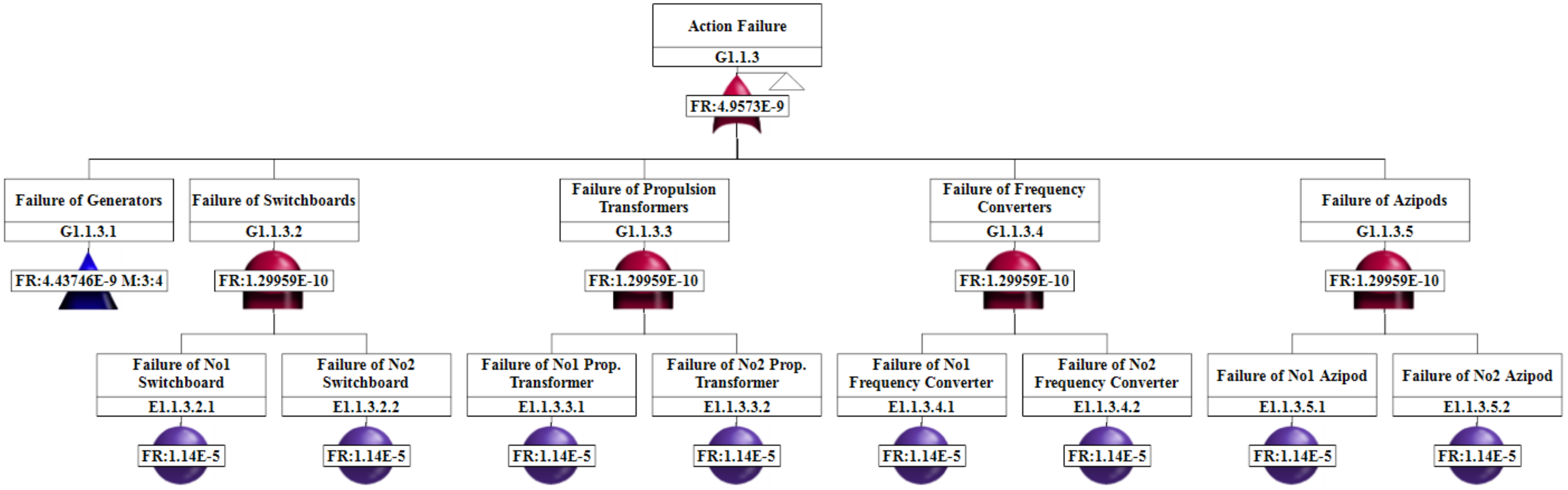

Failure to obtain Depth Clearance
G1.1.1.1.1
FR:2.73506E-12
ECDIS Failure
G1.1.1.1.1.1
FR:0.001163
Echo Sounder Failure
G1.1.1.1.1.2
FR:2.2914E-5
GNSS Failure
G1.1.1.1.1.3
FR:1.36914E-4
1 repeat
No Power Supply
E1.1.1.1.1.1.1
FR:1.14E-7
1 repeat
Equipment failure
E1.1.1.1.1.1.2
FR:1.14E-5
1 repeat
Out-of-date software
E1.1.1.1.1.1.3
FR:1.14E-5
1 repeat
Vessels without AIS aren't displayed
E1.1.1.1.1.1.4
FR:0.00114
No Power Supply
E1.1.1.1.1.2.1
FR:1.14E-7
Equipment failure
E1.1.1.1.1.2.2
FR:1.14E-5
Out-of-date software
E1.1.1.1.1.2.3
FR:1.14E-5
2 repeats
No Power Supply
E1.1.1.1.1.3.1
FR:1.14E-7
2 repeats
Equipment failure
E1.1.1.1.1.3.2
FR:1.14E-5
2 repeats
Out-of-date software
E1.1.1.1.1.3.3
FR:1.14E-5
2 repeats
No signal due to military exercises
E1.1.1.1.1.3.4
FR:0.000114

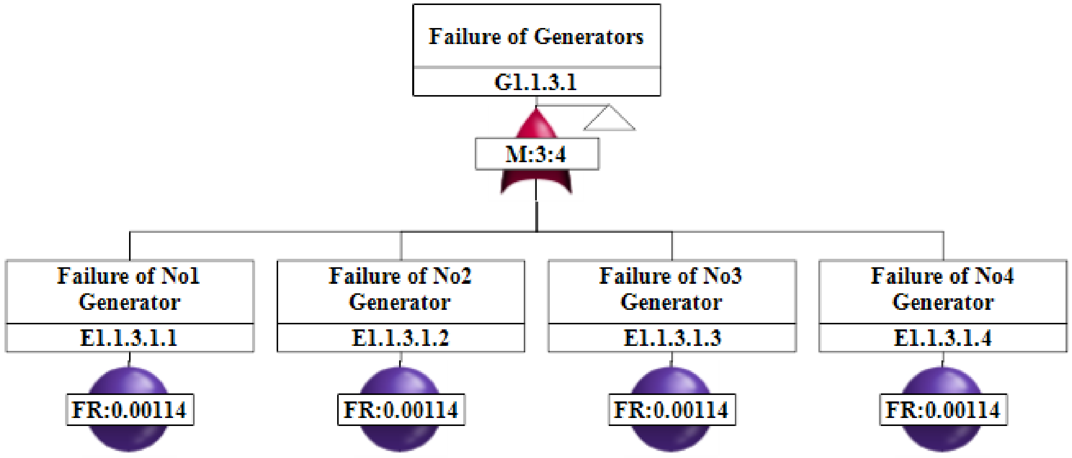

Failure to obtain Speed & Acceleration
G1.1.1.1.2
FR:5.39119E-14
GNSS Failure
G1.1.1.1.2.1
FR:1.36914E-4
Speed Log Failure
G1.1.1.1.2.2
FR:2.2914E-5
IMU Failure
G1.1.1.1.2.3
FR:2.2914E-5
2 repeats
No Power Supply
E1.1.1.1.1.3.1
FR:1.14E-7
2 repeats
Equipment failure
E1.1.1.1.1.3.2
FR:1.14E-5
2 repeats
Out-of-date software
E1.1.1.1.1.3.3
FR:1.14E-5
2 repeats
No signal due to military exercises
E1.1.1.1.1.3.4
FR:0.000114
No Power Supply
E1.1.1.1.2.2.1
FR:1.14E-7
Equipment Failure
E1.1.1.1.2.2.2
FR:1.14E-5
Out-of-date software
E1.1.1.1.2.2.3
FR:1.14E-5
1 repeat
No Power Supply
E1.1.1.1.2.3.1
FR:1.14E-7
1 repeat
Equipment Failure
E1.1.1.1.2.3.2
FR:1.14E-5
1 repeat
Out-of-date software
E1.1.1.1.2.3.3
FR:1.14E-5


Failure to obtain Location and Heading
G1.1.1.1.3
FR:2.07869E-17
GNSS Failure
G1.1.1.1.3.1
FR:1.36914E-4
Compass Equipment Failure
E1.1.1.1.3.2
FR:1.14E-5
IMU Failure
G1.1.1.1.3.3
FR:2.2914E-5
ECDIS Failure
G1.1.1.1.3.4
FR:0.001163
2 repeats
No Power Supply
E1.1.1.1.1.1.3.1
FR:1.14E-7
2 repeats
Equipment failure
E1.1.1.1.1.1.3.2
FR:1.14E-5
2 repeats
Out-of-date software
E1.1.1.1.1.1.3.3
FR:1.14E-5
2 repeats
No signal due to military exercises
E1.1.1.1.1.1.3.4
FR:0.000114
1 repeat
No Power Supply
E1.1.1.1.2.3.1
FR:1.14E-7
1 repeat
Equipment Failure
E1.1.1.1.2.3.2
FR:1.14E-5
1 repeat
Out-of-date software
E1.1.1.1.2.3.3
FR:1.14E-5
1 repeat
No Power Supply
E1.1.1.1.1.1.1
FR:1.14E-7
1 repeat
Equipment failure
E1.1.1.1.1.1.2
FR:1.14E-5
1 repeat
Out-of-date software
E1.1.1.1.1.1.3
FR:1.14E-5
1 repeat
Vessels without AIS aren't displayed
E1.1.1.1.1.1.4
FR:0.00114

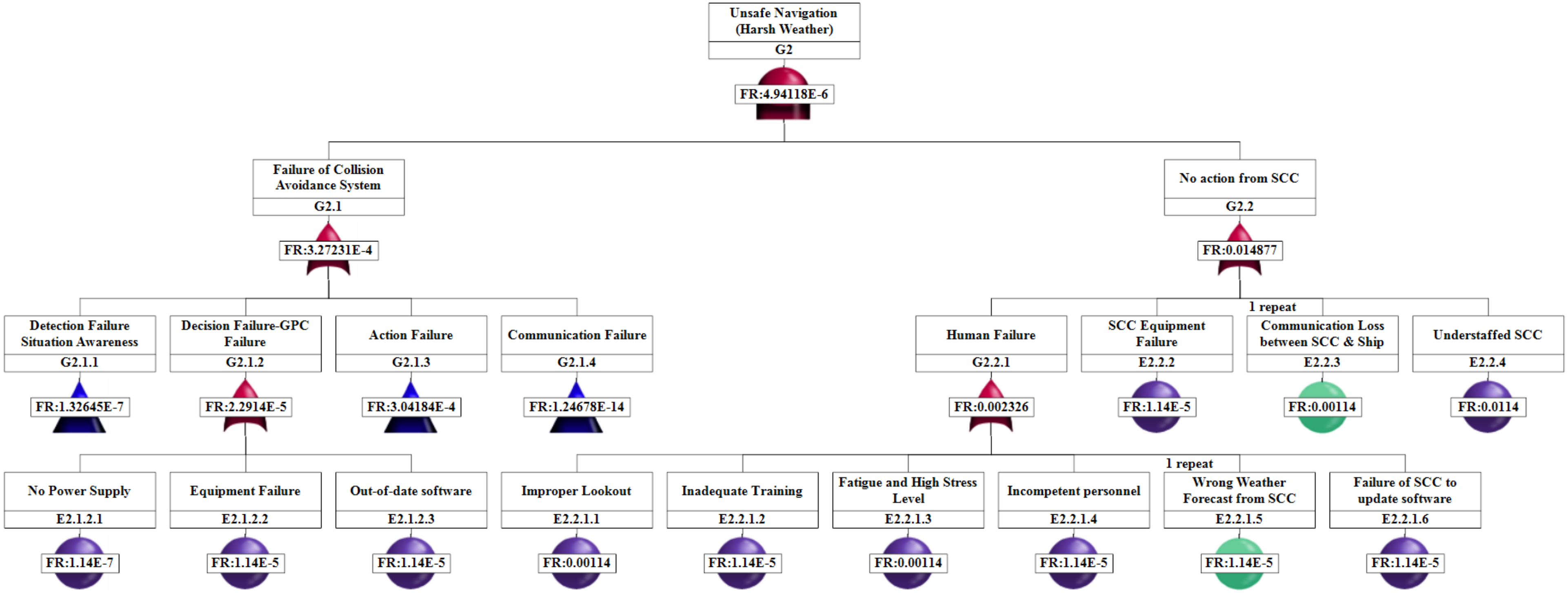

Communication Failure
G1.1.4
FR:1.24678E-14
AIS Failure
G1.1.4.1
FR:1.1514E-5
VHF Failure
G1.1.4.2
FR:1.254E-4
GMDSS Failure
G1.1.4.3
FR:1.1514E-5
No Power Supply
E1.1.4.1.1
FR:1.14E-7
Equipment failure
E1.1.4.1.2
FR:1.14E-5
No Power Supply
E1.1.4.2.1
FR:0.000114
Equipment failure
E1.1.4.2.2
FR:1.14E-5
No Power Supply
E1.1.4.3.1
FR:1.14E-7
Equipment failure
E1.1.4.3.2
FR:1.14E-5

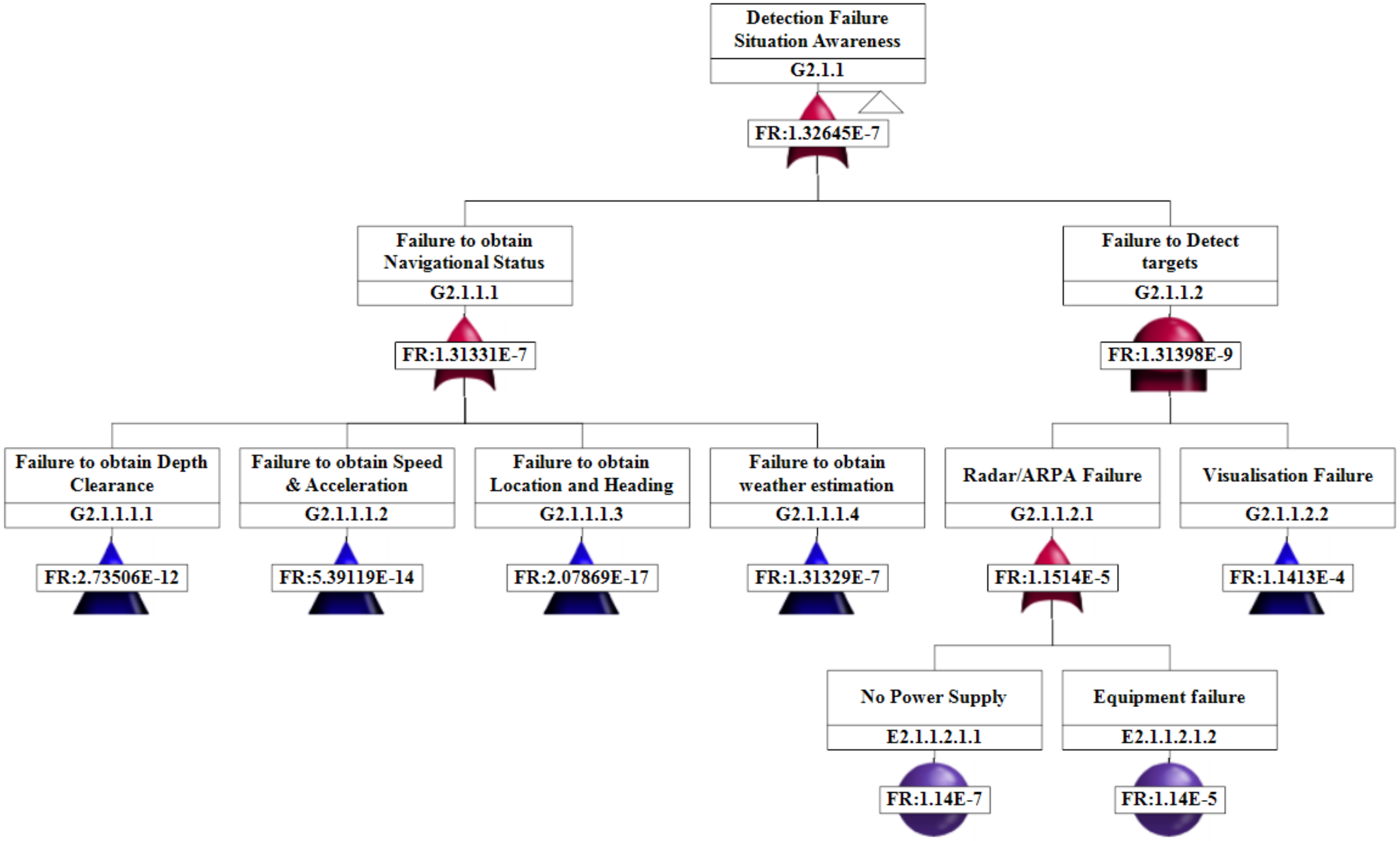

Visualisation Failure
G1.1.1.2.2
FR:1.15145E-5
LiDAR Failure
G1.1.1.2.2.1
FR:1.1514E-5
Cameras Failure
G1.1.1.2.2.2
FR:5.25042E-10
No Power Supply
E1.1.1.2.2.1.1
FR:1.14E-7
Equipment failure
E1.1.1.2.2.1.2
FR:1.14E-5
HD Cameras Failure
G1.1.1.2.2.2.1
FR:2.2914E-5
Infra Red Cameras Failure
G1.1.1.2.2.2.2
FR:2.2914E-5
No Power Supply
E1.1.1.2.2.2.1.1
FR:1.14E-7
Equipment failure
E1.1.1.2.2.2.1.2
FR:1.14E-5
Out-of-date software
E1.1.1.2.2.2.1.3
FR:1.14E-5
No Power Supply
E1.1.1.2.2.2.2.1
FR:1.14E-7
Equipment failure
E1.1.1.2.2.2.2.2
FR:1.14E-5
Out-of-date software
E1.1.1.2.2.2.2.3
FR:1.14E-5

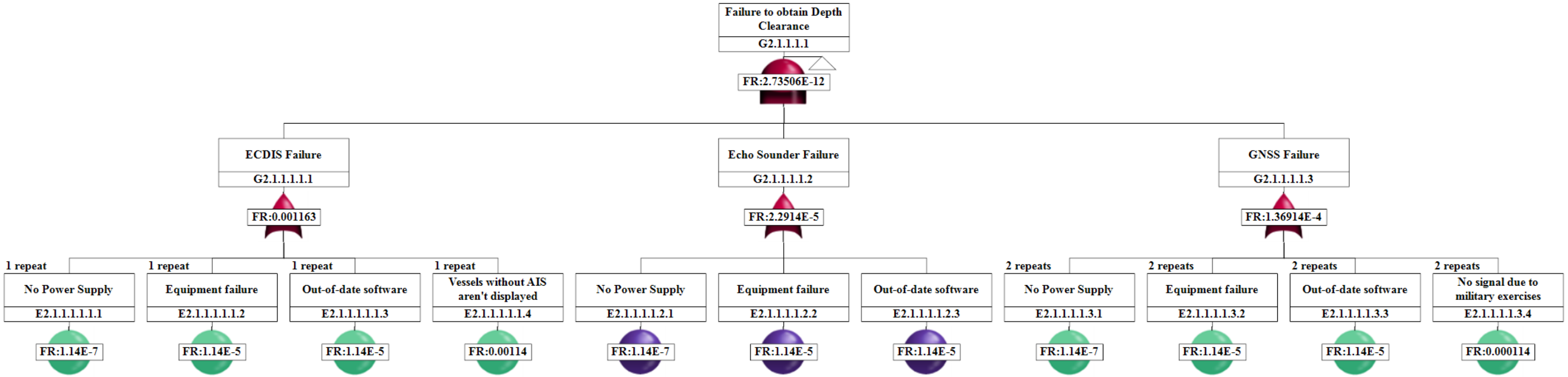

Action Failure
G1.1.3
FR:4.9573E-9
Failure of Generators
G1.1.3.1
FR:4.43746E-9 M:3:4
Failure of Switchboards
G1.1.3.2
FR:1.29959E-10
Failure of Propulsion Transformers
G1.1.3.3
FR:1.29959E-10
Failure of Frequency Converters
G1.1.3.4
FR:1.29959E-10
Failure of Azipods
G1.1.3.5
FR:1.29959E-10
Failure of No1 Switchboard
E1.1.3.2.1
FR:1.14E-5
Failure of No2 Switchboard
E1.1.3.2.2
FR:1.14E-5
Failure of No1 Prop. Transformer
E1.1.3.3.1
FR:1.14E-5
Failure of No2 Prop. Transformer
E1.1.3.3.2
FR:1.14E-5
Failure of No1 Frequency Converter
E1.1.3.4.1
FR:1.14E-5
Failure of No2 Frequency Converter
E1.1.3.4.2
FR:1.14E-5
Failure of No1 Azipod
E1.1.3.5.1
FR:1.14E-5
Failure of No2 Azipod
E1.1.3.5.2
FR:1.14E-5

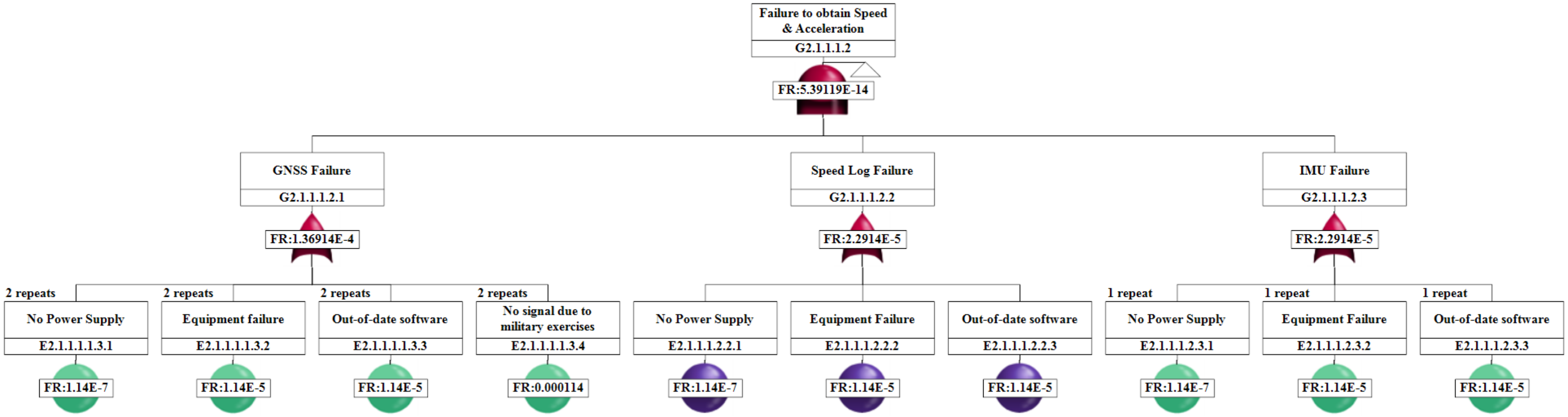

Failure of Generators
G1.1.3.1
M:3:4
Failure of No1 Generator
E1.1.3.1.1
FR:0.00114
Failure of No2 Generator
E1.1.3.1.2
FR:0.00114
Failure of No3 Generator
E1.1.3.1.3
FR:0.00114
Failure of No4 Generator
E1.1.3.1.4
FR:0.00114

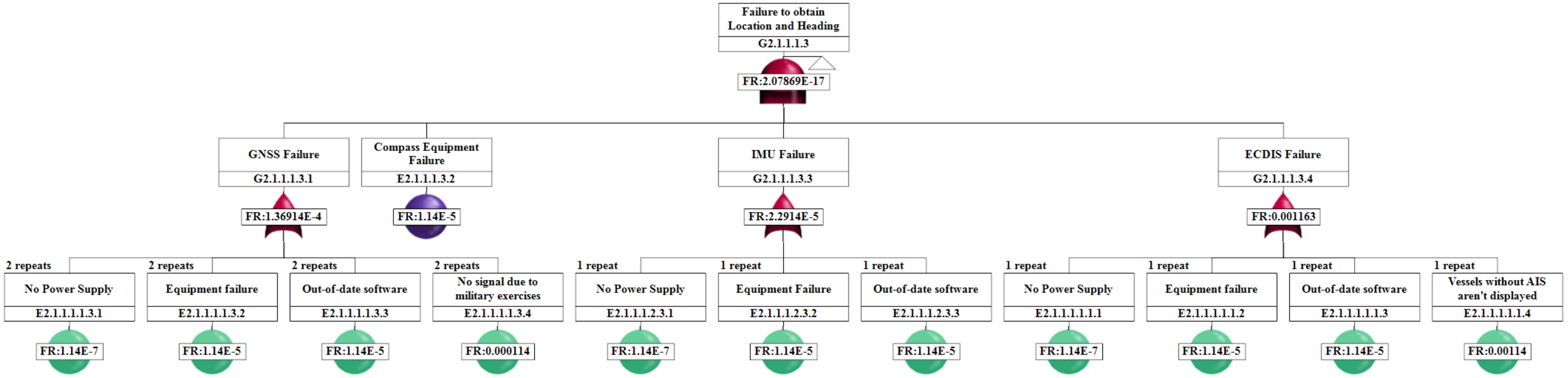
APPENDIX 2B. HARSH WEATHER SCENARIO – DYNAMIC LoA

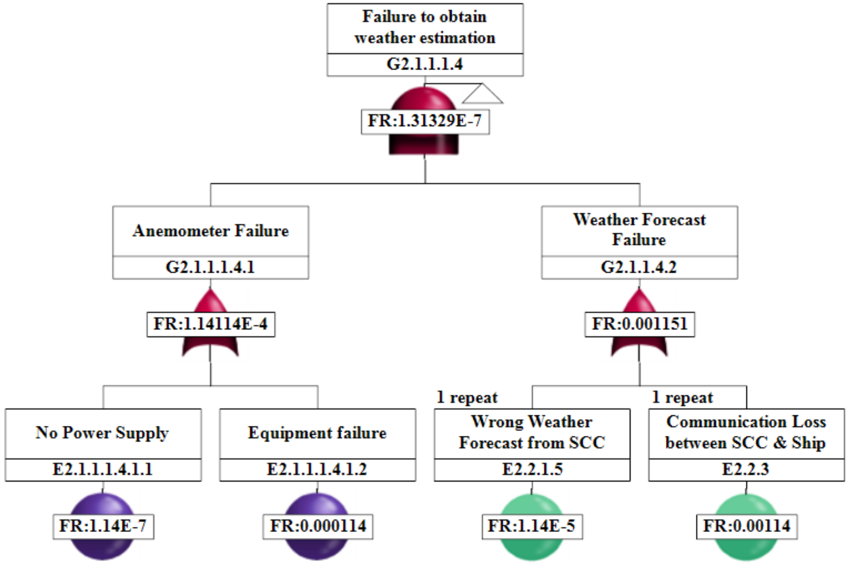


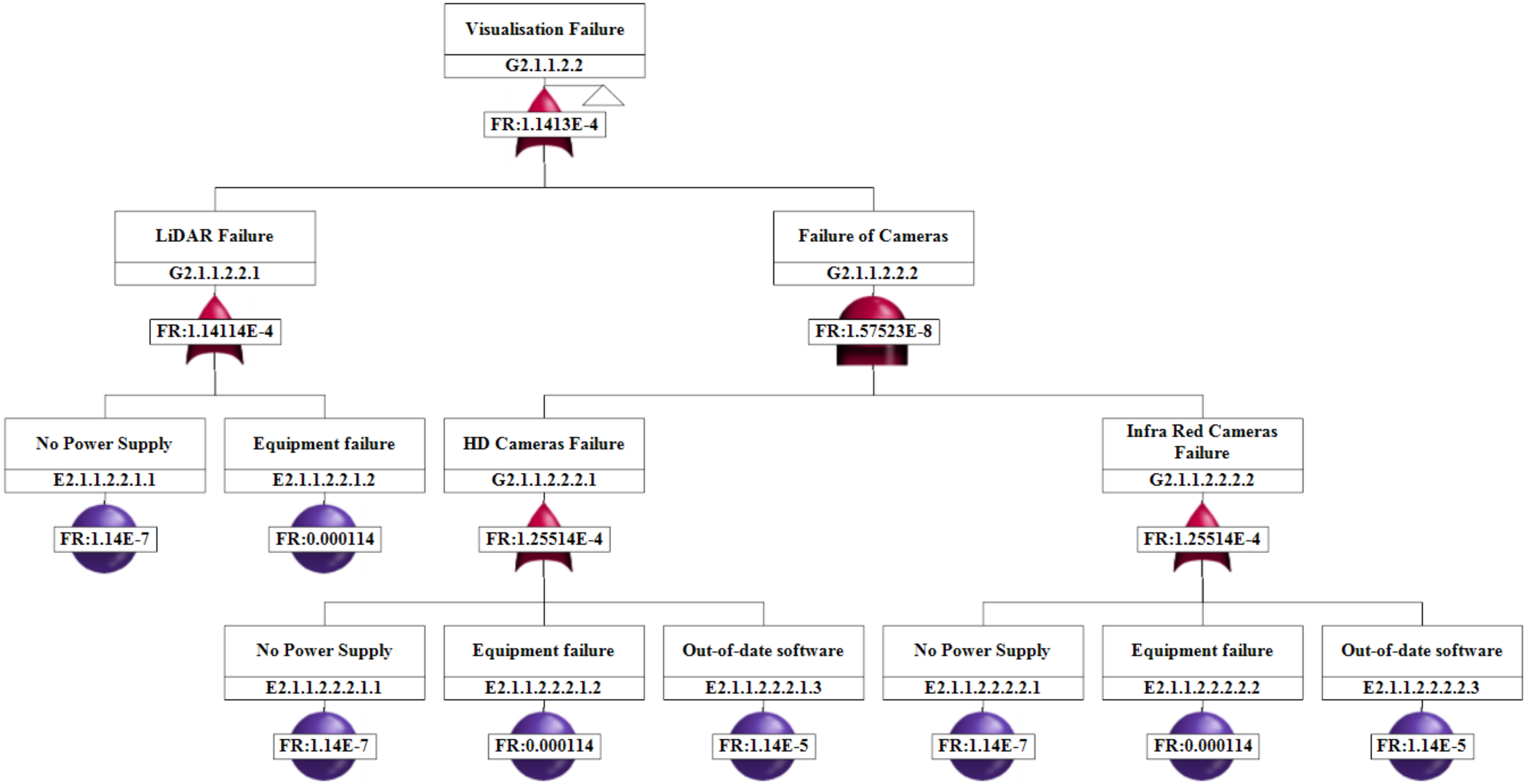

Detection Failure Situation Awareness
G2.1.1
FR:1.32645E-7
Failure to obtain Navigational Status
G2.1.1.1
FR:1.31331E-7
Failure to Detect targets
G2.1.1.2
FR:1.31398E-9
Failure to obtain Depth Clearance
G2.1.1.1.1
FR:2.73506E-12
Failure to obtain Speed & Acceleration
G2.1.1.1.2
FR:5.39119E-14
Failure to obtain Location and Heading
G2.1.1.1.3
FR:2.07869E-17
Failure to obtain weather estimation
G2.1.1.1.4
FR:1.31329E-7
Radar/ARPA Failure
G2.1.1.2.1
FR:1.1514E-5
Visualisation Failure
G2.1.1.2.2
FR:1.1413E-4
No Power Supply
E2.1.1.2.1.1
FR:1.14E-7
Equipment failure
E2.1.1.2.1.2
FR:1.14E-5

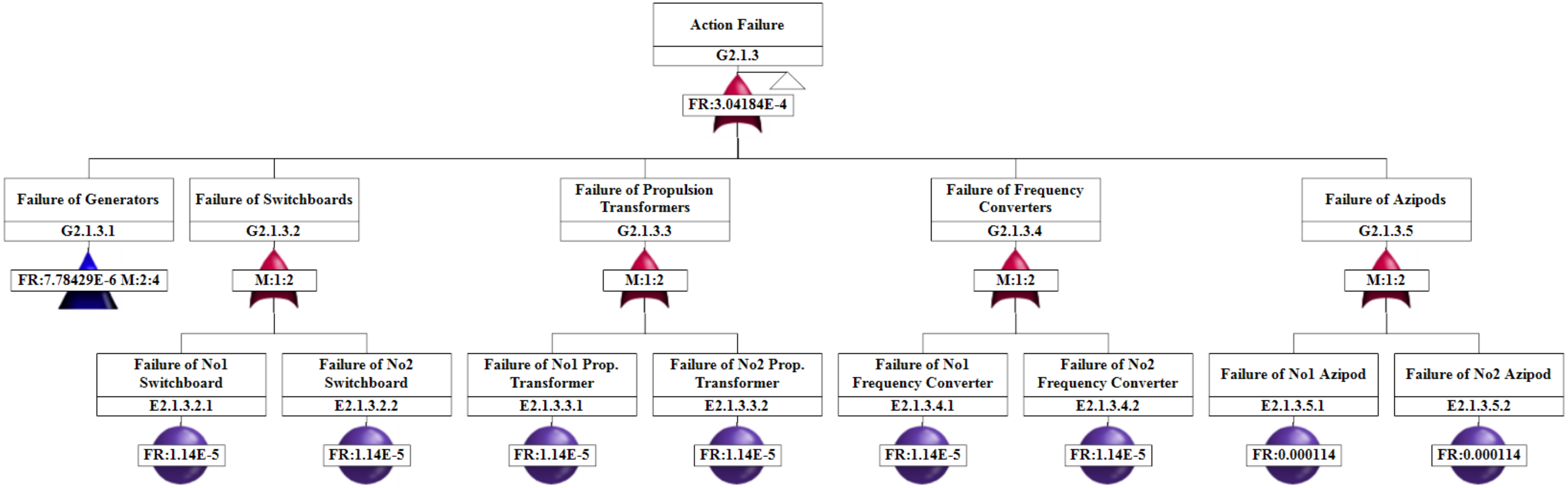

Failure to obtain Depth Clearance
G2.1.1.1.1
FR:2.73506E-12
ECDIS Failure
G2.1.1.1.1.1
FR:0.001163
Echo Sounder Failure
G2.1.1.1.1.2
FR:2.2914E-5
GNSS Failure
G2.1.1.1.1.3
FR:1.36914E-4
1 repeat
No Power Supply
E2.1.1.1.1.1.1
FR:1.14E-7
1 repeat
Equipment failure
E2.1.1.1.1.1.2
FR:1.14E-5
1 repeat
Out-of-date software
E2.1.1.1.1.1.3
FR:1.14E-5
1 repeat
Vessels without AIS aren't displayed
E2.1.1.1.1.1.4
FR:0.00114
No Power Supply
E2.1.1.1.1.2.1
FR:1.14E-7
Equipment failure
E2.1.1.1.1.2.2
FR:1.14E-5
Out-of-date software
E2.1.1.1.1.2.3
FR:1.14E-5
2 repeats
No Power Supply
E2.1.1.1.1.3.1
FR:1.14E-7
2 repeats
Equipment failure
E2.1.1.1.1.3.2
FR:1.14E-5
2 repeats
Out-of-date software
E2.1.1.1.1.3.3
FR:1.14E-5
2 repeats
No signal due to military exercises
E2.1.1.1.1.3.4
FR:0.000114

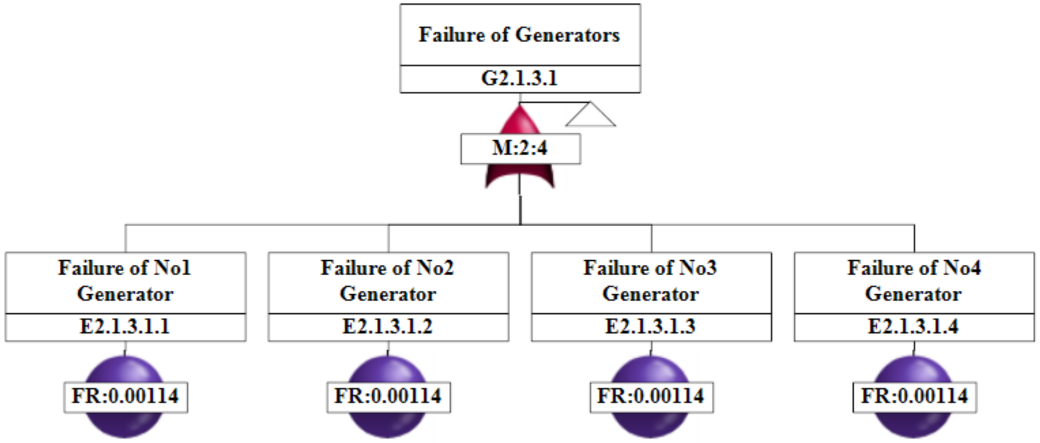

Failure to obtain Speed & Acceleration
G2.1.1.1.2
FR:5.39119E-14
GNSS Failure
G2.1.1.1.2.1
FR:1.36914E-4
Speed Log Failure
G2.1.1.1.2.2
FR:2.2914E-5
IMU Failure
G2.1.1.1.2.3
FR:2.2914E-5
2 repeats
No Power Supply
E2.1.1.1.1.3.1
FR:1.14E-7
2 repeats
Equipment failure
E2.1.1.1.1.3.2
FR:1.14E-5
2 repeats
Out-of-date software
E2.1.1.1.1.3.3
FR:1.14E-5
2 repeats
No signal due to military exercises
E2.1.1.1.1.3.4
FR:0.000114
No Power Supply
E2.1.1.1.2.2.1
FR:1.14E-7
Equipment Failure
E2.1.1.1.2.2.2
FR:1.14E-5
Out-of-date software
E2.1.1.1.2.2.3
FR:1.14E-5
1 repeat
No Power Supply
E2.1.1.1.2.3.1
FR:1.14E-7
1 repeat
Equipment Failure
E2.1.1.1.2.3.2
FR:1.14E-5
1 repeat
Out-of-date software
E2.1.1.1.2.3.3
FR:1.14E-5

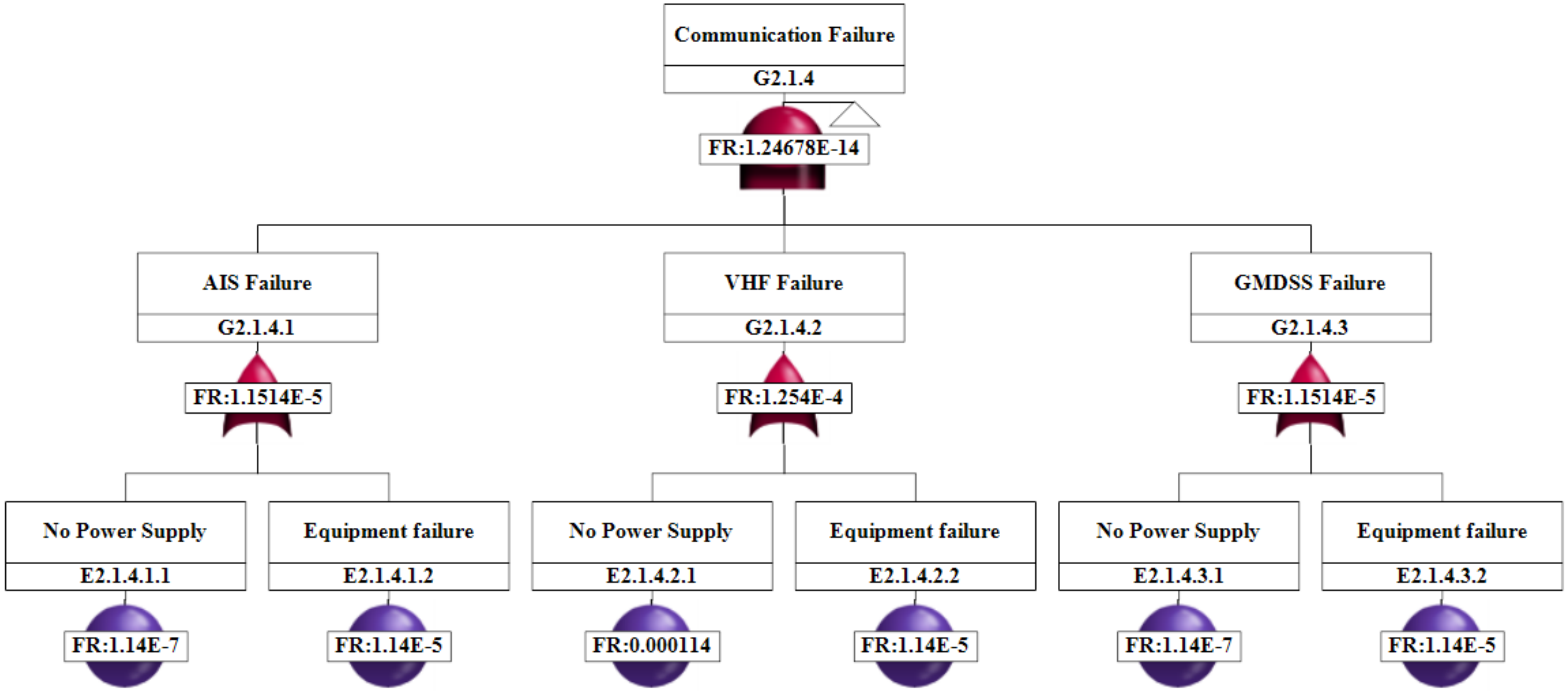

Failure to obtain Location and Heading
G2.1.1.1.3
FR:2.07869E-17
GNSS Failure
G2.1.1.1.3.1
FR:1.36914E-4
Compass Equipment Failure
E2.1.1.1.3.2
FR:1.14E-5
IMU Failure
G2.1.1.1.3.3
FR:2.2914E-5
ECDIS Failure
G2.1.1.1.3.4
FR:0.001163
2 repeats
No Power Supply
E2.1.1.1.1.3.1
FR:1.14E-7
2 repeats
Equipment failure
E2.1.1.1.1.3.2
FR:1.14E-5
2 repeats
Out-of-date software
E2.1.1.1.1.3.3
FR:1.14E-5
2 repeats
No signal due to military exercises
E2.1.1.1.1.3.4
FR:0.000114
1 repeat
No Power Supply
E2.1.1.1.2.3.1
FR:1.14E-7
1 repeat
Equipment Failure
E2.1.1.1.2.3.2
FR:1.14E-5
1 repeat
Out-of-date software
E2.1.1.1.2.3.3
FR:1.14E-5
1 repeat
No Power Supply
E2.1.1.1.1.1.1
FR:1.14E-7
1 repeat
Equipment failure
E2.1.1.1.1.1.2
FR:1.14E-5
1 repeat
Out-of-date software
E2.1.1.1.1.1.3
FR:1.14E-5
1 repeat
Vessels without AIS aren't displayed
E2.1.1.1.1.1.4
FR:0.00114


Failure to obtain weather estimation
G2.1.1.1.4
FR:1.31329E-7
Anemometer Failure
G2.1.1.1.4.1
FR:1.14114E-4
Weather Forecast Failure
G2.1.1.4.2
FR:0.001151
No Power Supply
E2.1.1.1.4.1.1
FR:1.14E-7
Equipment failure
E2.1.1.1.4.1.2
FR:0.000114
1 repeat
Wrong Weather Forecast from SCC
E2.2.1.5
FR:1.14E-5
1 repeat
Communication Loss between SCC & Ship
E2.2.3
FR:0.00114


Visualisation Failure
G2.1.1.2.2
FR:1.1413E-4
LiDAR Failure
G2.1.1.2.2.1
FR:1.14114E-4
Failure of Cameras
G2.1.1.2.2.2
FR:1.57523E-8
No Power Supply
E2.1.1.2.2.1.1
FR:1.14E-7
Equipment failure
E2.1.1.2.2.1.2
FR:0.000114
HD Cameras Failure
G2.1.1.2.2.2.1
FR:1.25514E-4
Infra Red Cameras Failure
G2.1.1.2.2.2.2
FR:1.25514E-4
No Power Supply
E2.1.1.2.2.2.1.1
FR:1.14E-7
Equipment failure
E2.1.1.2.2.2.1.2
FR:0.000114
Out-of-date software
E2.1.1.2.2.2.1.3
FR:1.14E-5
No Power Supply
E2.1.1.2.2.2.2.1
FR:1.14E-7
Equipment failure
E2.1.1.2.2.2.2.2
FR:0.000114
Out-of-date software
E2.1.1.2.2.2.2.3
FR:1.14E-5

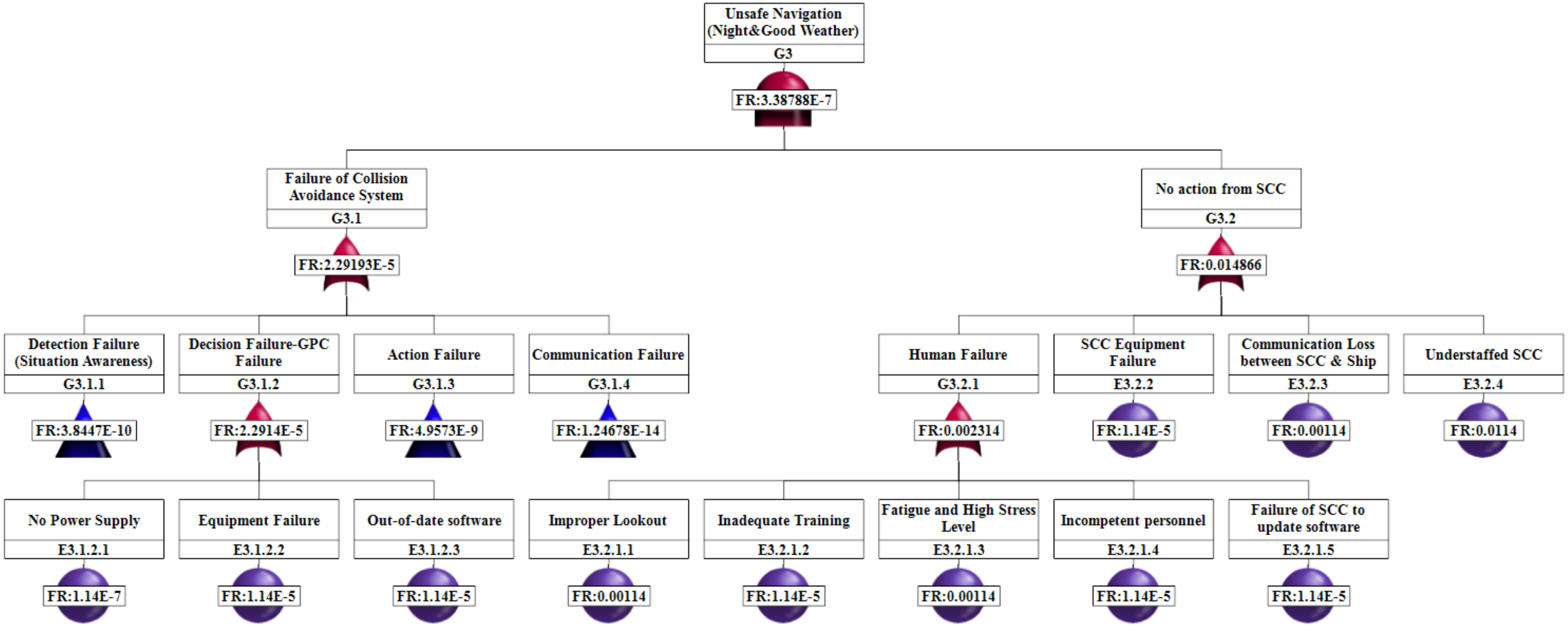

Action Failure
G2.1.3
FR:3.04184E-4
Failure of Generators
G2.1.3.1
FR:7.78429E-6 M:2:4
Failure of Switchboards
G2.1.3.2
M:1:2
Failure of Propulsion Transformers
G2.1.3.3
M:1:2
Failure of Frequency Converters
G2.1.3.4
M:1:2
Failure of Azipods
G2.1.3.5
M:1:2
Failure of No1 Switchboard
E2.1.3.2.1
FR:1.14E-5
Failure of No2 Switchboard
E2.1.3.2.2
FR:1.14E-5
Failure of No1 Prop. Transformer
E2.1.3.3.1
FR:1.14E-5
Failure of No2 Prop. Transformer
E2.1.3.3.2
FR:1.14E-5
Failure of No1 Frequency Converter
E2.1.3.4.1
FR:1.14E-5
Failure of No2 Frequency Converter
E2.1.3.4.2
FR:1.14E-5
Failure of No1 Azipod
E2.1.3.5.1
FR:0.000114
Failure of No2 Azipod
E2.1.3.5.2
FR:0.000114

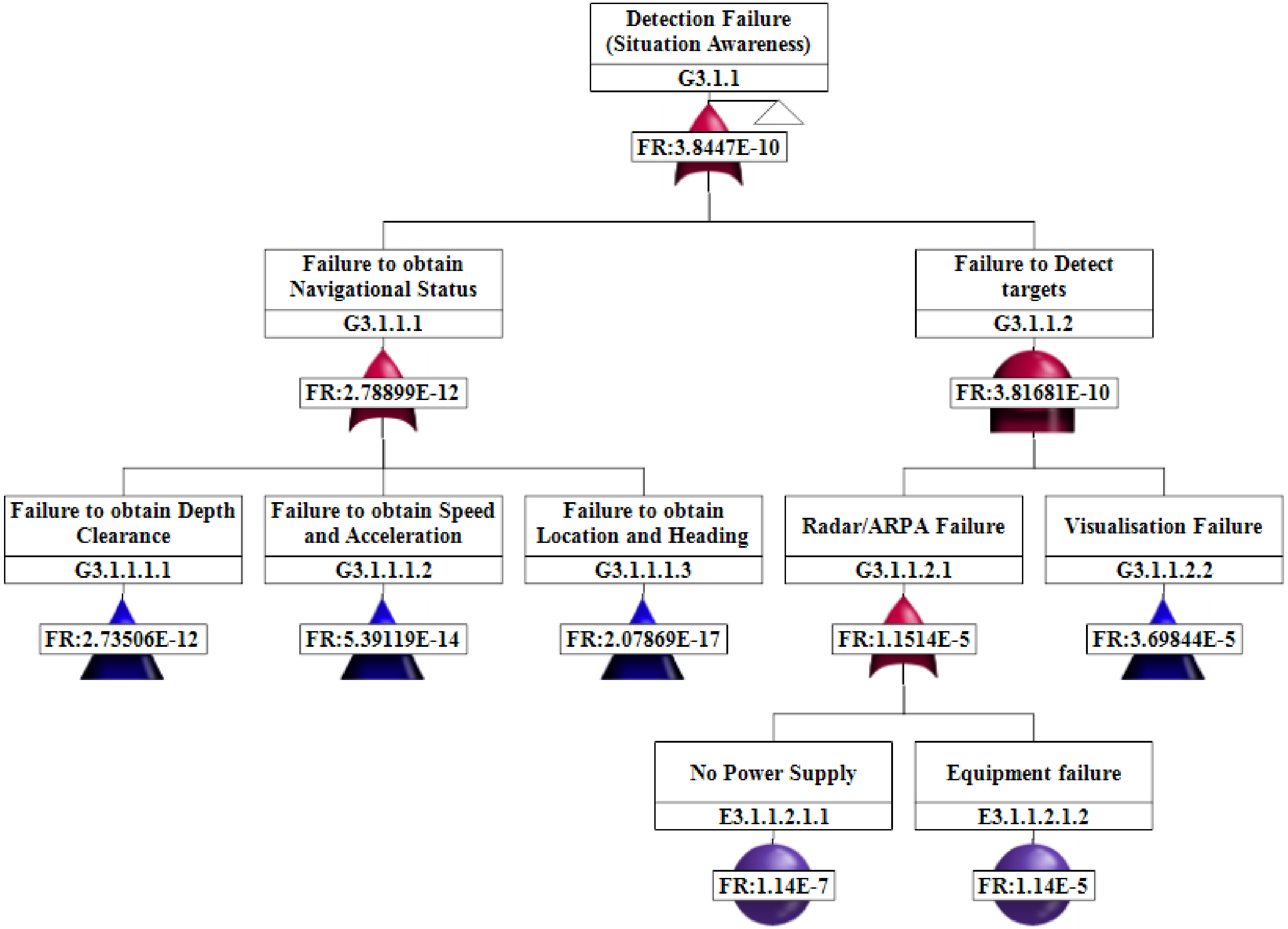

Failure of Generators
G2.1.3.1
M:2:4
Failure of No1 Generator
E2.1.3.1.1
FR:0.00114
Failure of No2 Generator
E2.1.3.1.2
FR:0.00114
Failure of No3 Generator
E2.1.3.1.3
FR:0.00114
Failure of No4 Generator
E2.1.3.1.4
FR:0.00114

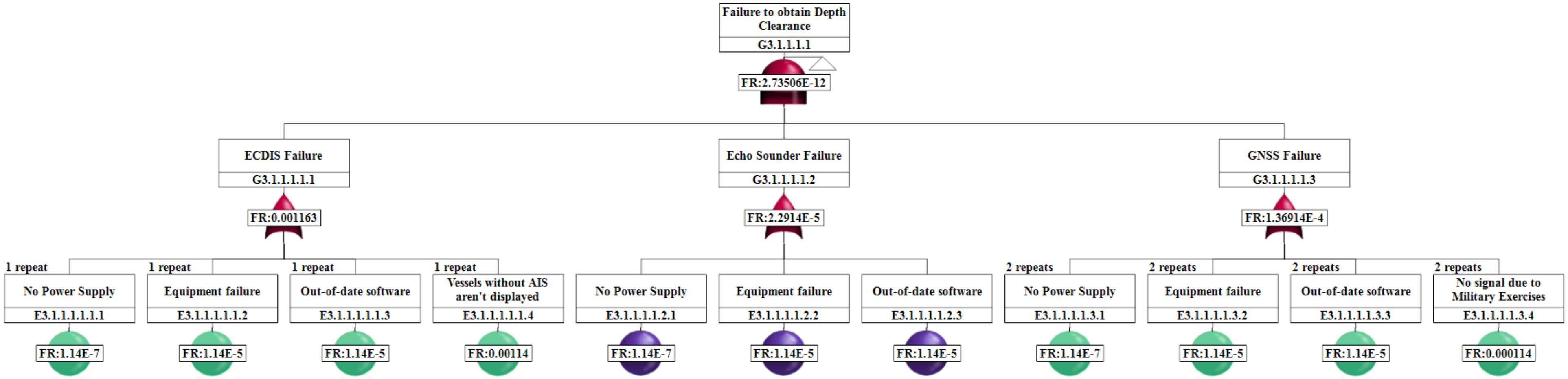


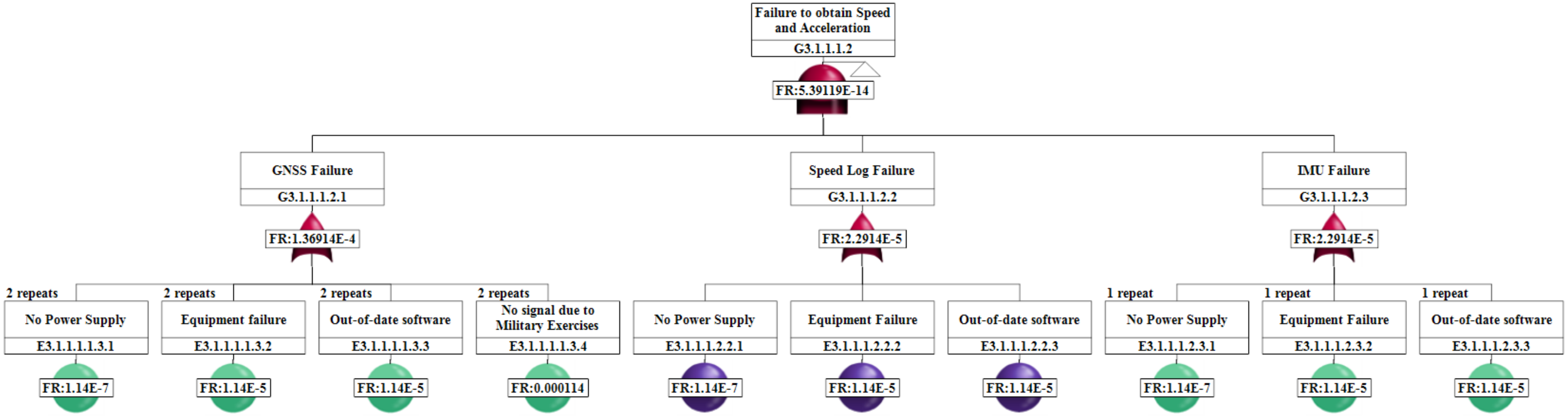
Communication Failure
G2.1.4
FR:1.24678E-14
AIS Failure
G2.1.4.1
FR:1.1514E-5
VHF Failure
G2.1.4.2
FR:1.254E-4
GMDSS Failure
G2.1.4.3
FR:1.1514E-5
No Power Supply
E2.1.4.1.1
FR:1.14E-7
Equipment failure
E2.1.4.1.2
FR:1.14E-5
No Power Supply
E2.1.4.2.1
FR:0.000114
Equipment failure
E2.1.4.2.2
FR:1.14E-5
No Power Supply
E2.1.4.3.1
FR:1.14E-7
Equipment failure
E2.1.4.3.2
FR:1.14E-5

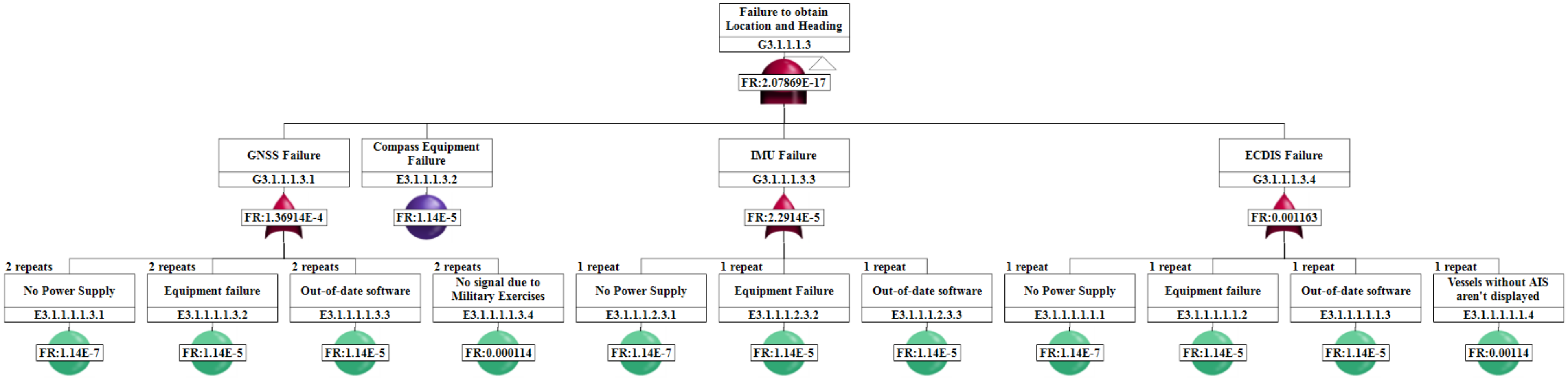
APPENDIX 2C. NIGHT AND GOOD WEATHER SCENARIO – DYNAMIC LoA

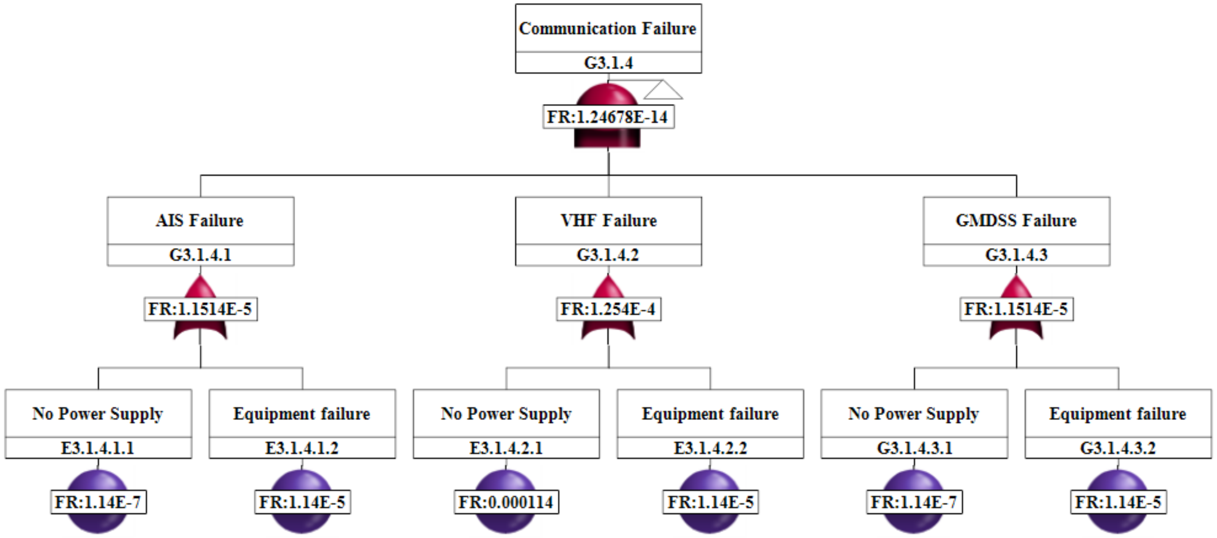


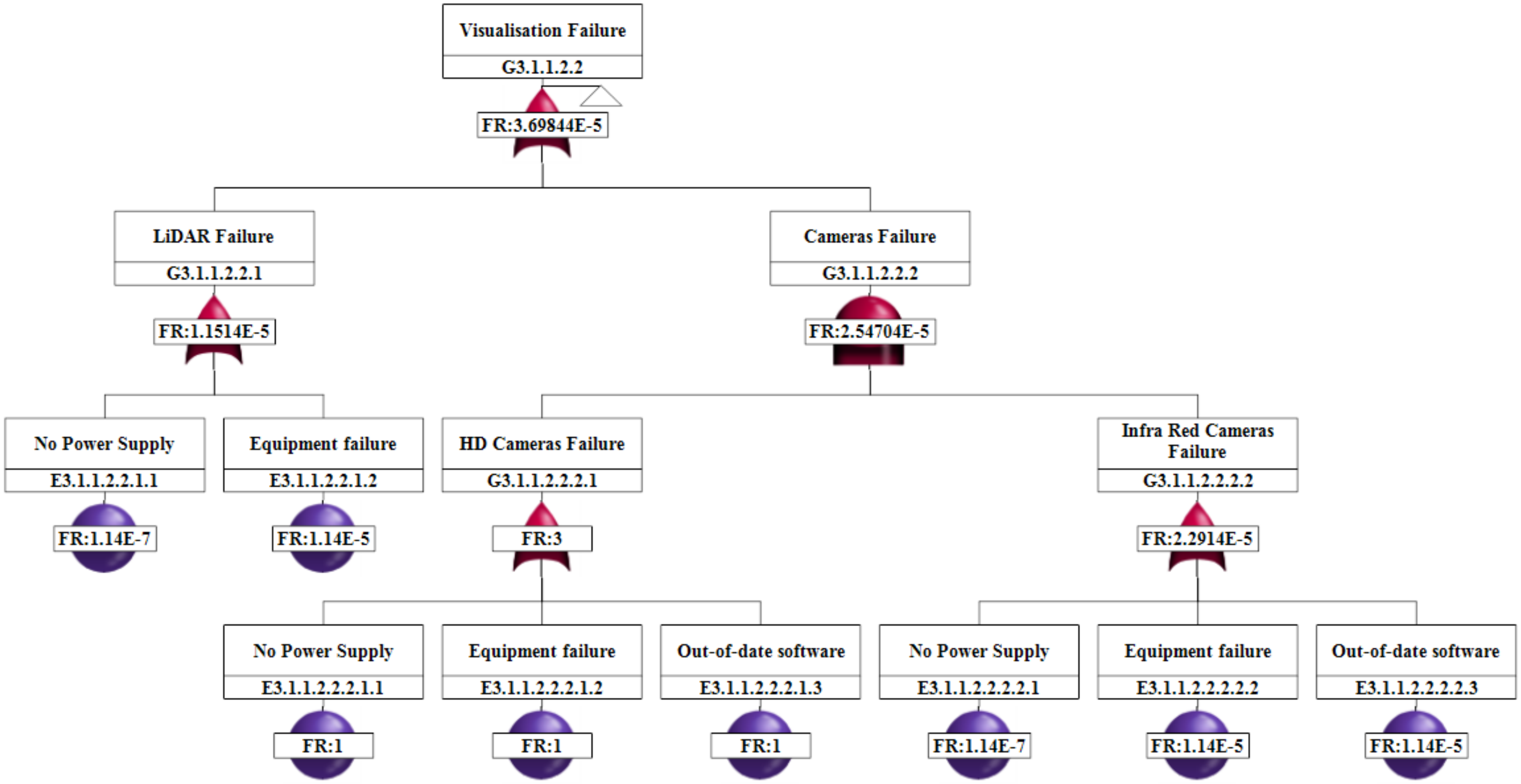

Detection Failure (Situation Awareness)
G3.1.1
FR:3.8447E-10
Failure to obtain Navigational Status
G3.1.1.1
FR:2.78899E-12
Failure to Detect targets
G3.1.1.2
FR:3.81681E-10
Failure to obtain Depth Clearance
G3.1.1.1.1
FR:2.73506E-12
Failure to obtain Speed and Acceleration
G3.1.1.1.2
FR:5.39119E-14
Failure to obtain Location and Heading
G3.1.1.1.3
FR:2.07869E-17
Radar/ARPA Failure
G3.1.1.2.1
FR:1.1514E-5
Visualisation Failure
G3.1.1.2.2
FR:3.69844E-5
No Power Supply
E3.1.1.2.1.1
FR:1.14E-7
Equipment failure
E3.1.1.2.1.2
FR:1.14E-5

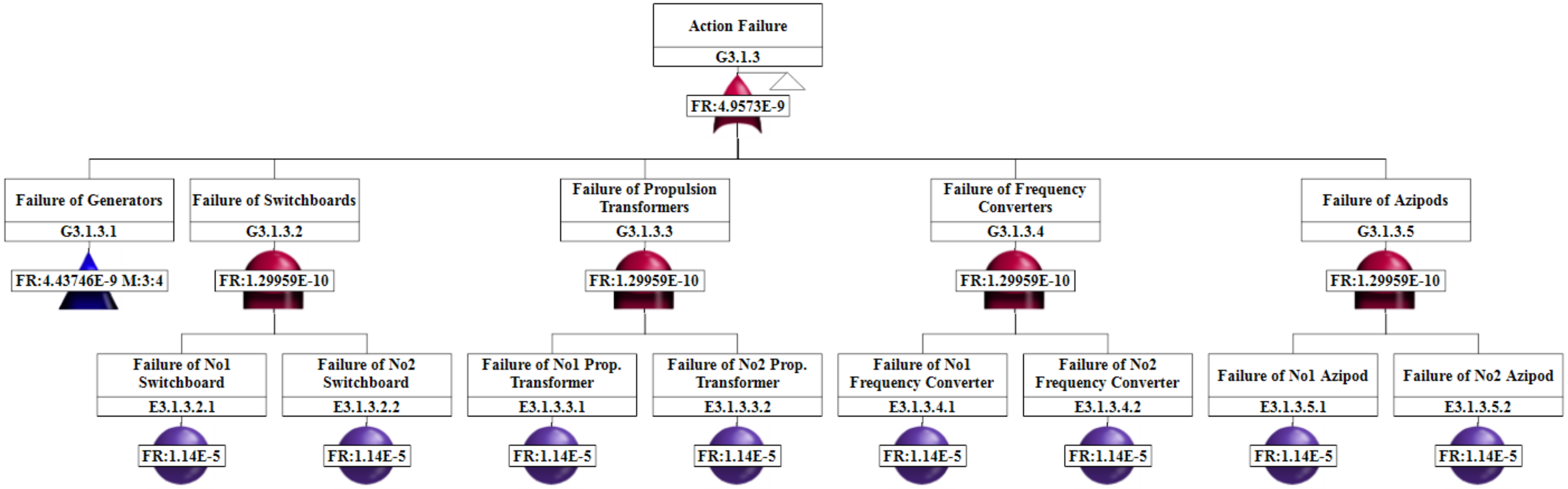

Failure to obtain Depth Clearance
G3.1.1.1.1
FR:2.73506E-12
ECDIS Failure
G3.1.1.1.1.1
FR:0.001163
Echo Sounder Failure
G3.1.1.1.1.2
FR:2.2914E-5
GNSS Failure
G3.1.1.1.1.3
FR:1.36914E-4
1 repeat
No Power Supply
E3.1.1.1.1.1.1
FR:1.14E-7
1 repeat
Equipment failure
E3.1.1.1.1.1.2
FR:1.14E-5
1 repeat
Out-of-date software
E3.1.1.1.1.1.3
FR:1.14E-5
1 repeat
Vessels without AIS aren't displayed
E3.1.1.1.1.1.4
FR:0.00114
No Power Supply
E3.1.1.1.1.2.1
FR:1.14E-7
Equipment failure
E3.1.1.1.1.2.2
FR:1.14E-5
Out-of-date software
E3.1.1.1.1.2.3
FR:1.14E-5
2 repeats
No Power Supply
E3.1.1.1.1.3.1
FR:1.14E-7
2 repeats
Equipment failure
E3.1.1.1.1.3.2
FR:1.14E-5
2 repeats
Out-of-date software
E3.1.1.1.1.3.3
FR:1.14E-5
2 repeats
No signal due to Military Exercises
E3.1.1.1.1.3.4
FR:0.000114

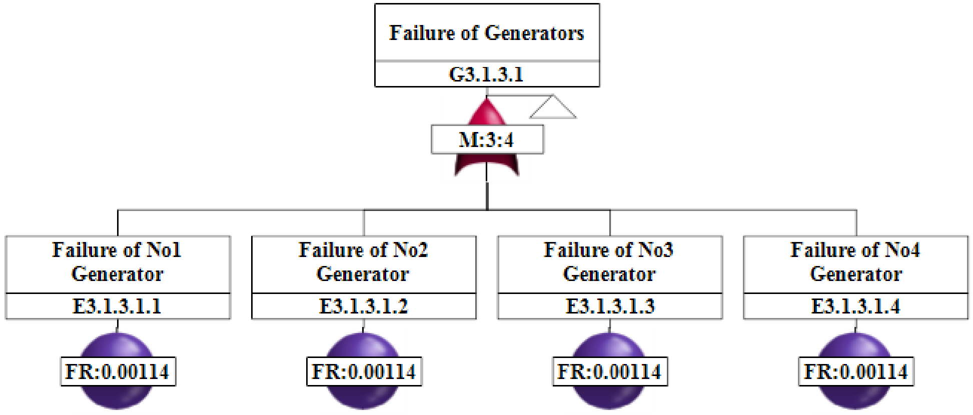

Failure to obtain Speed and Acceleration
G3.1.1.1.2
FR:5.39119E-14
GNSS Failure
G3.1.1.1.2.1
FR:1.36914E-4
Speed Log Failure
G3.1.1.1.2.2
FR:2.2914E-5
IMU Failure
G3.1.1.1.2.3
FR:2.2914E-5
2 repeats
No Power Supply
E3.1.1.1.1.3.1
FR:1.14E-7
2 repeats
Equipment failure
E3.1.1.1.1.3.2
FR:1.14E-5
2 repeats
Out-of-date software
E3.1.1.1.1.3.3
FR:1.14E-5
2 repeats
No signal due to Military Exercises
E3.1.1.1.1.3.4
FR:0.000114
No Power Supply
E3.1.1.1.2.2.1
FR:1.14E-7
Equipment Failure
E3.1.1.1.2.2.2
FR:1.14E-5
Out-of-date software
E3.1.1.1.2.2.3
FR:1.14E-5
1 repeat
No Power Supply
E3.1.1.1.2.3.1
FR:1.14E-7
1 repeat
Equipment Failure
E3.1.1.1.2.3.2
FR:1.14E-5
1 repeat
Out-of-date software
E3.1.1.1.2.3.3
FR:1.14E-5


Failure to obtain Location and Heading
G3.1.1.1.3
FR:2.07869E-17
GNSS Failure
G3.1.1.1.3.1
FR:1.36914E-4
Compass Equipment Failure
E3.1.1.1.3.2
FR:1.14E-5
IMU Failure
G3.1.1.1.3.3
FR:2.2914E-5
ECDIS Failure
G3.1.1.1.3.4
FR:0.001163
2 repeats
No Power Supply
E3.1.1.1.1.3.1
FR:1.14E-7
2 repeats
Equipment failure
E3.1.1.1.1.3.2
FR:1.14E-5
2 repeats
Out-of-date software
E3.1.1.1.1.3.3
FR:1.14E-5
2 repeats
No signal due to Military Exercises
E3.1.1.1.1.3.4
FR:0.000114
1 repeat
No Power Supply
E3.1.1.1.2.3.1
FR:1.14E-7
1 repeat
Equipment Failure
E3.1.1.1.2.3.2
FR:1.14E-5
1 repeat
Out-of-date software
E3.1.1.1.2.3.3
FR:1.14E-5
1 repeat
No Power Supply
E3.1.1.1.1.1.1
FR:1.14E-7
1 repeat
Equipment failure
E3.1.1.1.1.1.2
FR:1.14E-5
1 repeat
Out-of-date software
E3.1.1.1.1.1.3
FR:1.14E-5
1 repeat
Vessels without AIS aren't displayed
E3.1.1.1.1.1.4
FR:0.00114

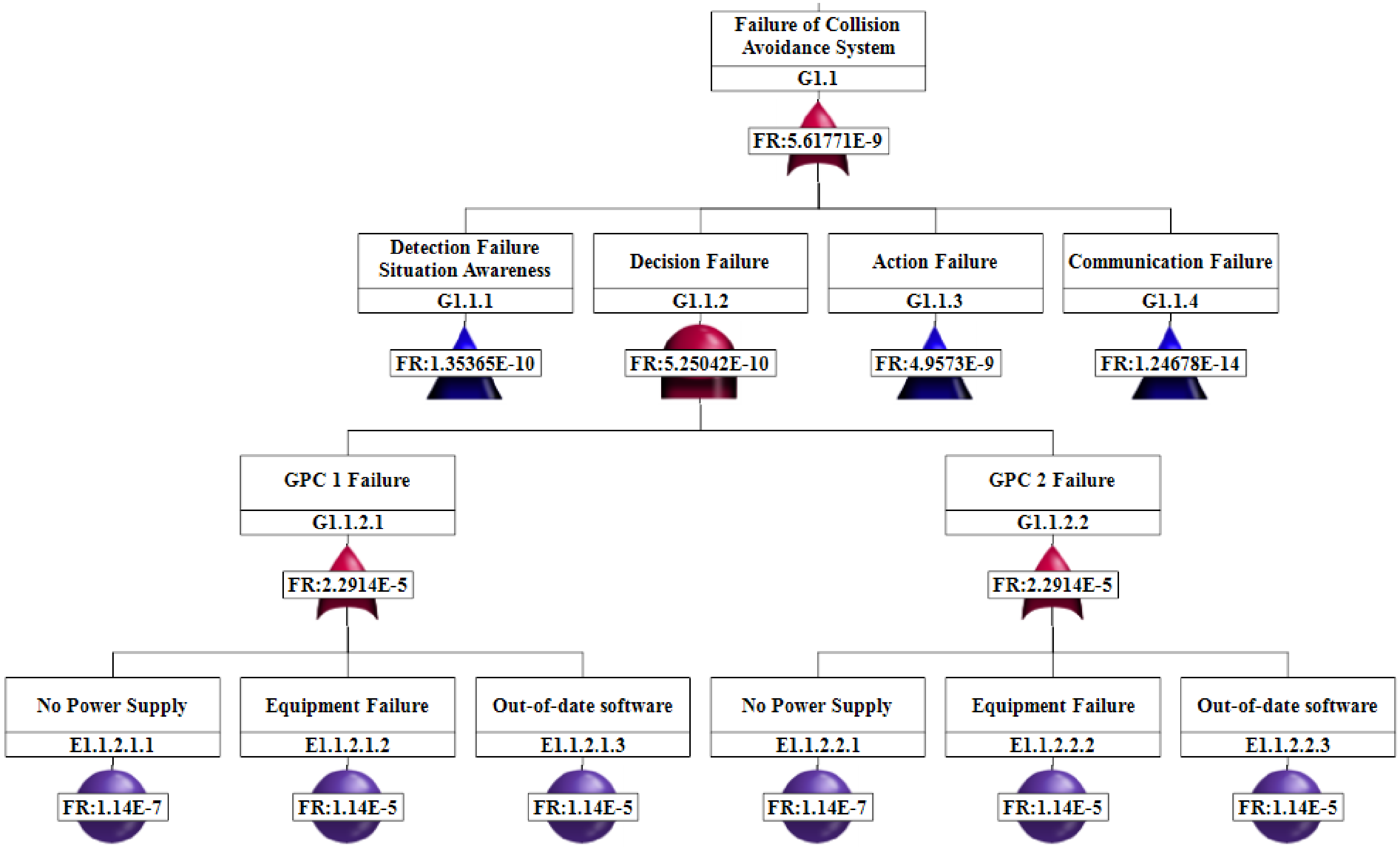

Communication Failure
G3.1.4
FR:1.24678E-14
AIS Failure
G3.1.4.1
FR:1.1514E-5
VHF Failure
G3.1.4.2
FR:1.254E-4
GMDSS Failure
G3.1.4.3
FR:1.1514E-5
No Power Supply
E3.1.4.1.1
FR:1.14E-7
Equipment failure
E3.1.4.1.2
FR:1.14E-5
No Power Supply
E3.1.4.2.1
FR:0.000114
Equipment failure
E3.1.4.2.2
FR:1.14E-5
No Power Supply
G3.1.4.3.1
FR:1.14E-7
Equipment failure
G3.1.4.3.2
FR:1.14E-5


Visualisation Failure
G3.1.1.2.2
FR:3.69844E-5
LiDAR Failure
G3.1.1.2.2.1
FR:1.1514E-5
Cameras Failure
G3.1.1.2.2.2
FR:2.54704E-5
No Power Supply
E3.1.1.2.2.1.1
FR:1.14E-7
Equipment failure
E3.1.1.2.2.1.2
FR:1.14E-5
HD Cameras Failure
G3.1.1.2.2.2.1
FR:3
Infra Red Cameras Failure
G3.1.1.2.2.2.2
FR:2.2914E-5
No Power Supply
E3.1.1.2.2.2.1.1
FR:1
Equipment failure
E3.1.1.2.2.2.1.2
FR:1
Out-of-date software
E3.1.1.2.2.2.1.3
FR:1
No Power Supply
E3.1.1.2.2.2.2.1
FR:1.14E-7
Equipment failure
E3.1.1.2.2.2.2.2
FR:1.14E-5
Out-of-date software
E3.1.1.2.2.2.2.3
FR:1.14E-5

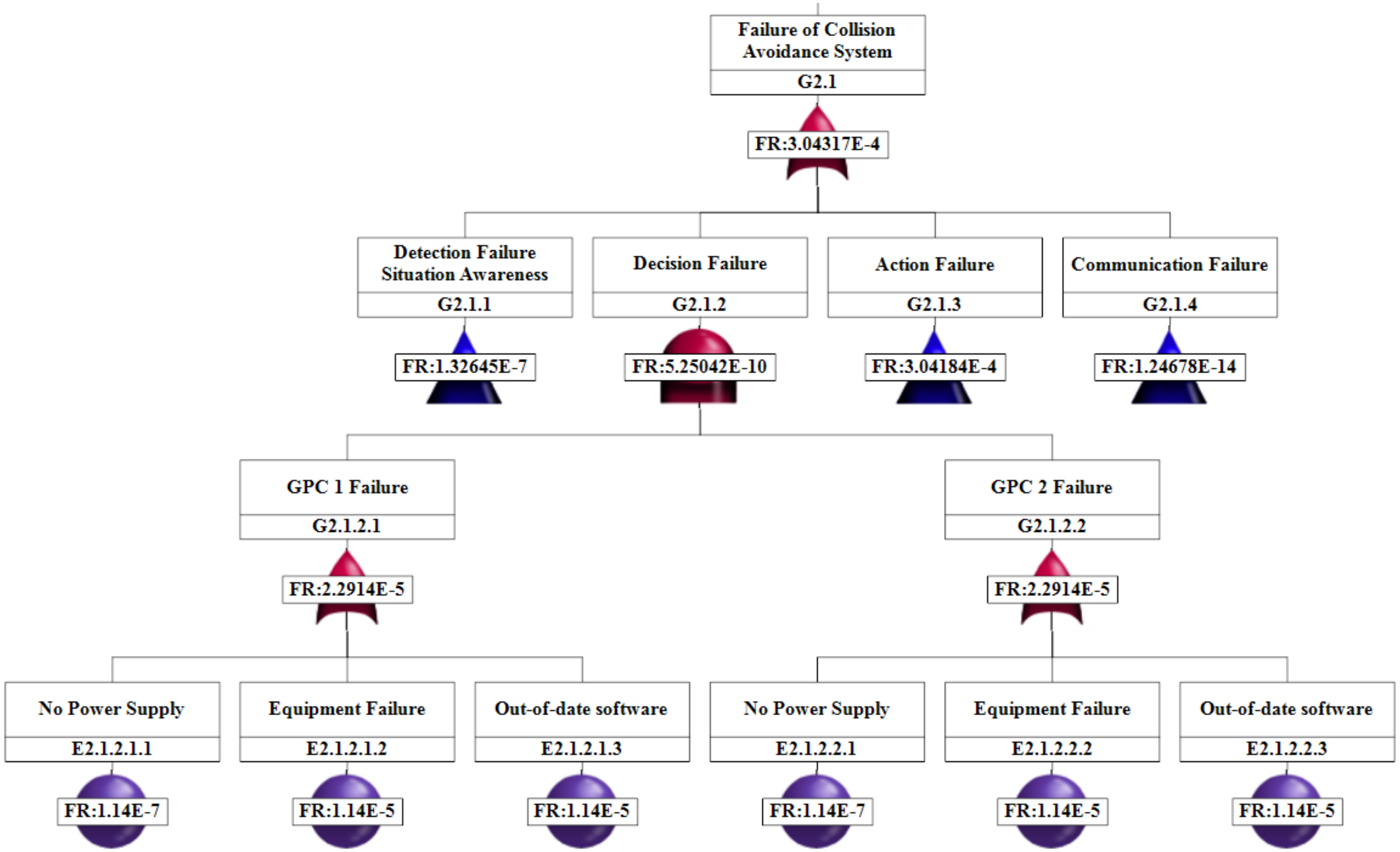

Action Failure
G3.1.3
FR:4.9573E-9
Failure of Generators
G3.1.3.1
FR:4.43746E-9 M:3:4
Failure of Switchboards
G3.1.3.2
FR:1.29959E-10
Failure of Propulsion Transformers
G3.1.3.3
FR:1.29959E-10
Failure of Frequency Converters
G3.1.3.4
FR:1.29959E-10
Failure of Azipods
G3.1.3.5
FR:1.29959E-10
Failure of No1 Switchboard
E3.1.3.2.1
FR:1.14E-5
Failure of No2 Switchboard
E3.1.3.2.2
FR:1.14E-5
Failure of No1 Prop. Transformer
E3.1.3.3.1
FR:1.14E-5
Failure of No2 Prop. Transformer
E3.1.3.3.2
FR:1.14E-5
Failure of No1 Frequency Converter
E3.1.3.4.1
FR:1.14E-5
Failure of No2 Frequency Converter
E3.1.3.4.2
FR:1.14E-5
Failure of No1 Azipod
E3.1.3.5.1
FR:1.14E-5
Failure of No2 Azipod
E3.1.3.5.2
FR:1.14E-5


Failure of Generators
G3.1.3.1
M:3:4
Failure of No1 Generator
E3.1.3.1.1
FR:0.00114
Failure of No2 Generator
E3.1.3.1.2
FR:0.00114
Failure of No3 Generator
E3.1.3.1.3
FR:0.00114
Failure of No4 Generator
E3.1.3.1.4
FR:0.00114

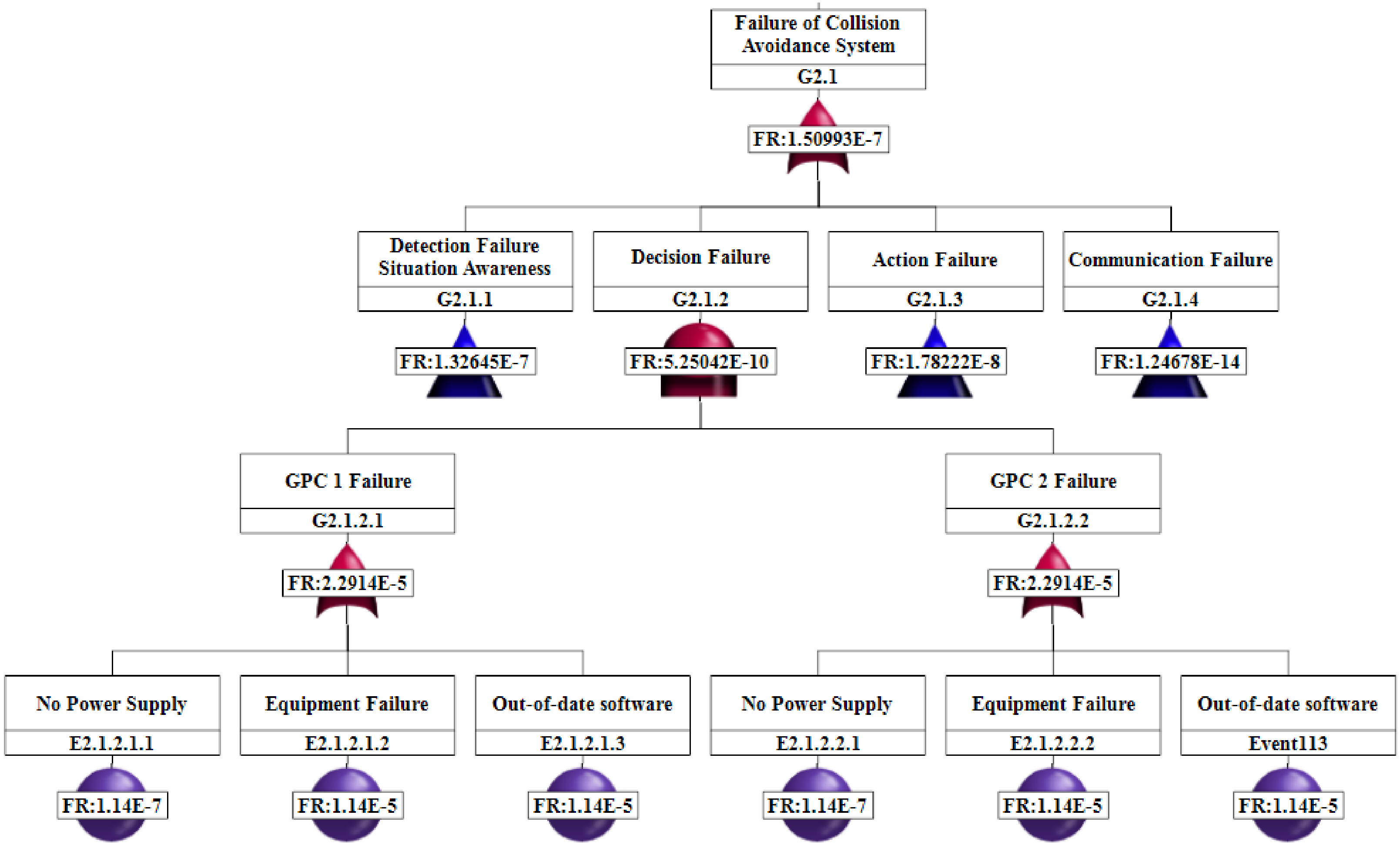
APPENDIX 2D. DAY SCENARIO – FULLY AUTONOMOUS (MODIFIED)



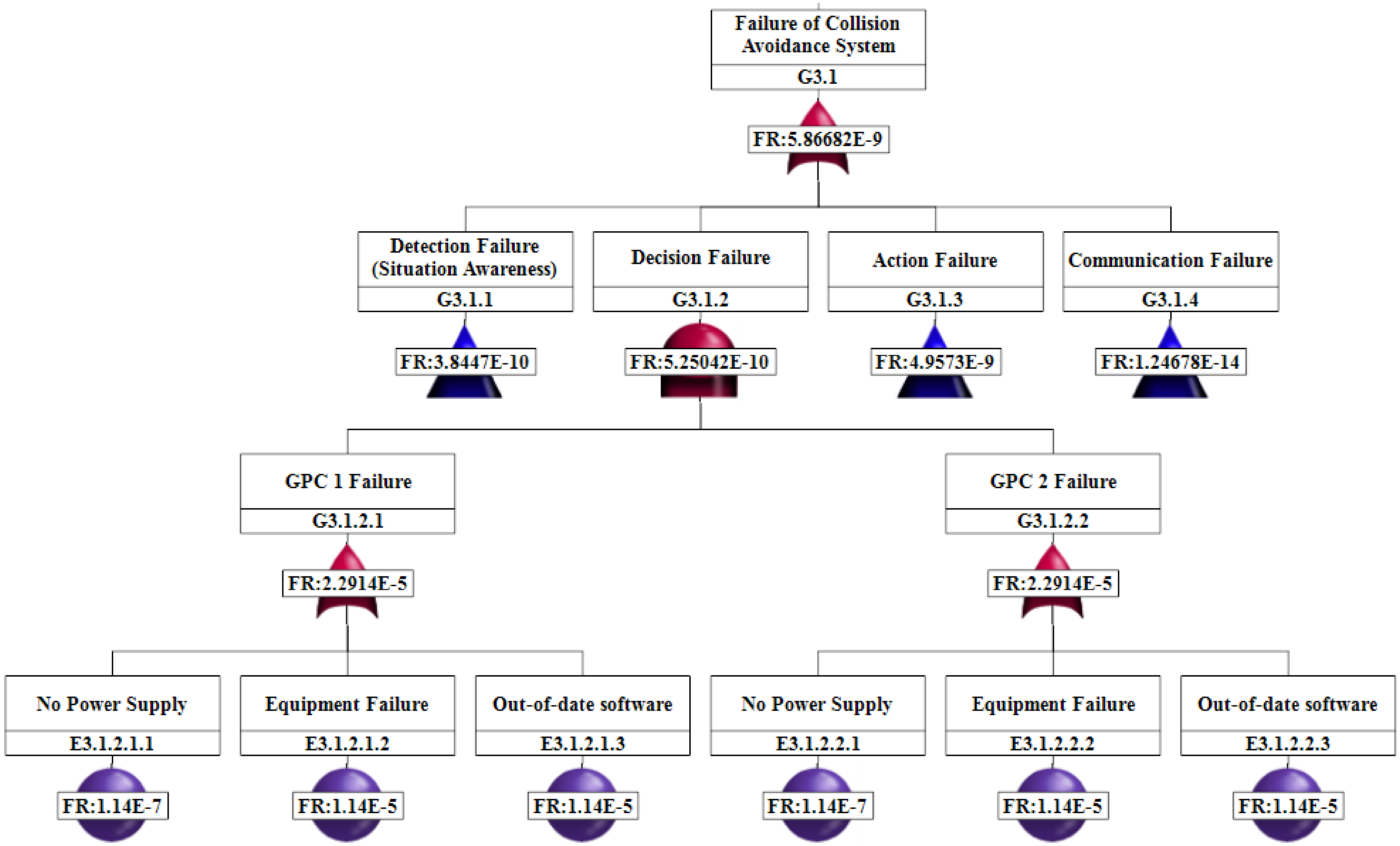
APPENDIX 2E. HARSH WEATHER SCENARIO – FULLY AUTONOMOUS (MODIFIED)



APPENDIX 2F. HARSH WEATHER SCENARIO – FULLY AUTONOMOUS (MODIFIED&ASSUMPTION)

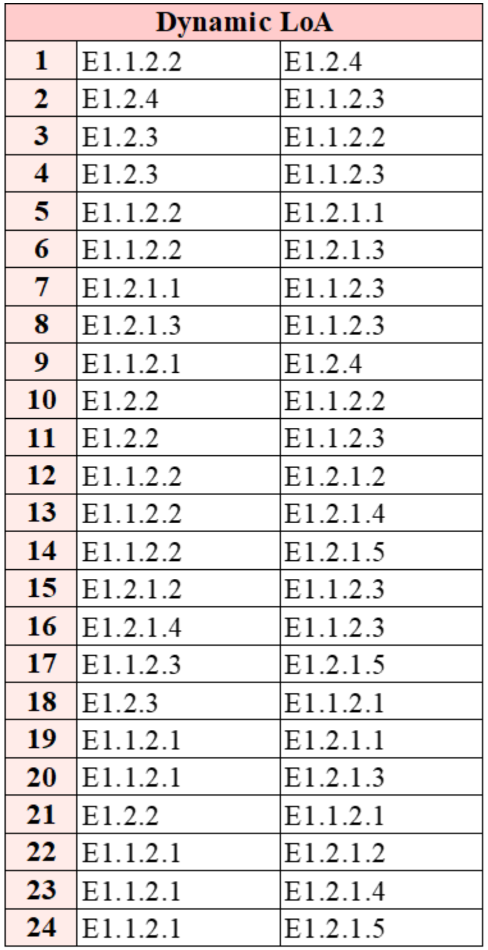


APPENDIX 2G. NIGHT SCENARIO – FULLY AUTONOMOUS (MODIFIED)

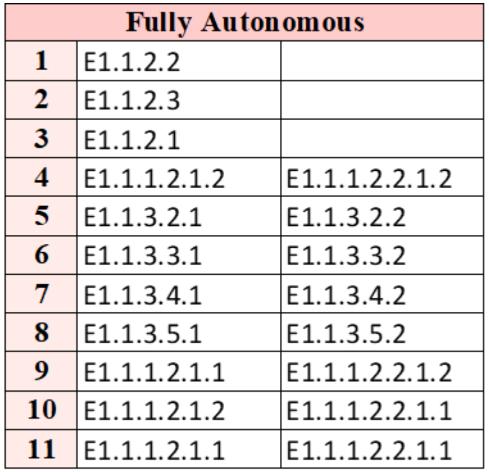


APPENDIX 3. FAULT TREE RESULTS – CUT SETS

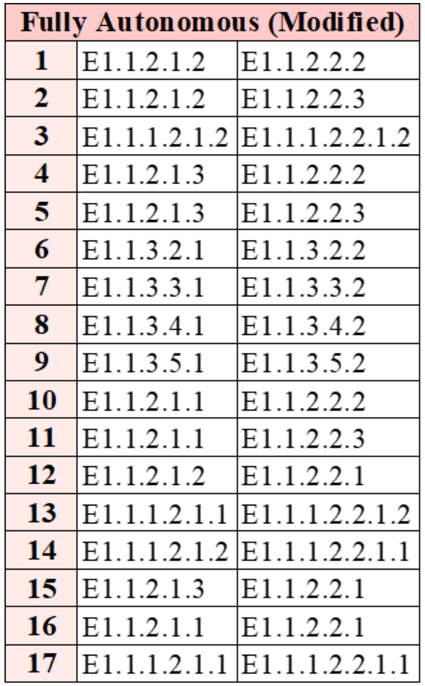
APPENDIX 3A. DAY AND GOOD WEATHER SCENARIO



Dynamic LoA		
1	E1.1.2.2	E1.2.4
2	E1.2.4	E1.1.2.3
3	E1.2.3	E1.1.2.2
4	E1.2.3	E1.1.2.3
5	E1.1.2.2	E1.2.1.1
6	E1.1.2.2	E1.2.1.3
7	E1.2.1.1	E1.1.2.3
8	E1.2.1.3	E1.1.2.3
9	E1.1.2.1	E1.2.4
10	E1.2.2	E1.1.2.2
11	E1.2.2	E1.1.2.3
12	E1.1.2.2	E1.2.1.2
13	E1.1.2.2	E1.2.1.4
14	E1.1.2.2	E1.2.1.5
15	E1.2.1.2	E1.1.2.3
16	E1.2.1.4	E1.1.2.3
17	E1.1.2.3	E1.2.1.5
18	E1.2.3	E1.1.2.1
19	E1.1.2.1	E1.2.1.1
20	E1.1.2.1	E1.2.1.3
21	E1.2.2	E1.1.2.1
22	E1.1.2.1	E1.2.1.2
23	E1.1.2.1	E1.2.1.4
24	E1.1.2.1	E1.2.1.5



Fully Autonomous		
1	E1.1.2.2	
2	E1.1.2.3	
3	E1.1.2.1	
4	E1.1.1.2.1.2	E1.1.1.2.2.1.2
5	E1.1.3.2.1	E1.1.3.2.2
6	E1.1.3.3.1	E1.1.3.3.2
7	E1.1.3.4.1	E1.1.3.4.2
8	E1.1.3.5.1	E1.1.3.5.2
9	E1.1.1.2.1.1	E1.1.1.2.2.1.2
10	E1.1.1.2.1.2	E1.1.1.2.2.1.1
11	E1.1.1.2.1.1	E1.1.1.2.2.1.1



Fully Autonomous (Modified)		
1	E1.1.2.1.2	E1.1.2.2.2
2	E1.1.2.1.2	E1.1.2.2.3
3	E1.1.1.2.1.2	E1.1.1.2.2.1.2
4	E1.1.2.1.3	E1.1.2.2.2
5	E1.1.2.1.3	E1.1.2.2.3
6	E1.1.3.2.1	E1.1.3.2.2
7	E1.1.3.3.1	E1.1.3.3.2
8	E1.1.3.4.1	E1.1.3.4.2
9	E1.1.3.5.1	E1.1.3.5.2
10	E1.1.2.1.1	E1.1.2.2.2
11	E1.1.2.1.1	E1.1.2.2.3
12	E1.1.2.1.2	E1.1.2.2.1
13	E1.1.1.2.1.1	E1.1.1.2.2.1.2
14	E1.1.1.2.1.2	E1.1.1.2.2.1.1
15	E1.1.2.1.3	E1.1.2.2.1
16	E1.1.2.1.1	E1.1.2.2.1
17	E1.1.1.2.1.1	E1.1.1.2.2.1.1

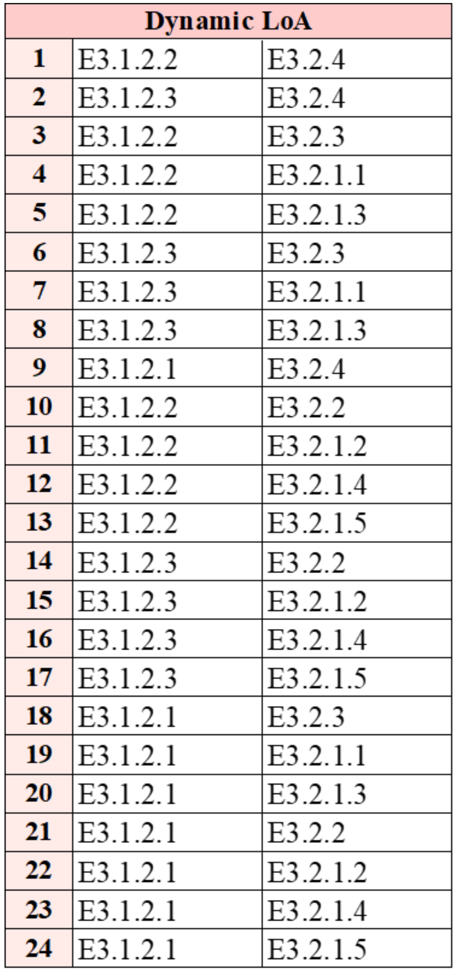
APPENDIX 3B. HARSH WEATHER SCENARIO

Dynamic LoA								
1	E2.2.4	E2.1.3.5.1	**35**	E2.2.1.3	E2.1.3.4.2	**69**	E2.2.1.2	E2.1.3.4.2
2	E2.2.4	E2.1.3.5.2	**36**	E2.2.3	E2.1.3.2.1	**70**	E2.2.1.4	E2.1.3.2.1
3	E2.2.1.1	E2.1.3.5.1	**37**	E2.2.3	E2.1.3.2.2	**71**	E2.2.1.4	E2.1.3.2.2
4	E2.2.1.1	E2.1.3.5.2	**38**	E2.2.3	E2.1.3.3.1	**72**	E2.2.1.4	E2.1.3.3.1
5	E2.2.1.3	E2.1.3.5.1	**39**	E2.2.3	E2.1.3.3.2	**73**	E2.2.1.4	E2.1.3.3.2
6	E2.2.1.3	E2.1.3.5.2	**40**	E2.2.3	E2.1.3.4.1	**74**	E2.2.1.4	E2.1.3.4.1
7	E2.1.1.1.4.1.2	E2.2.3	**41**	E2.2.3	E2.1.3.4.2	**75**	E2.2.1.4	E2.1.3.4.2
8	E2.2.3	E2.1.3.5.1	**42**	E2.2.1.2	E2.1.3.5.1	**76**	E2.2.2	E2.1.3.2.1
9	E2.2.3	E2.1.3.5.2	**43**	E2.2.1.2	E2.1.3.5.2	**77**	E2.2.2	E2.1.3.2.2
10	E2.1.2.2	E2.2.4	**44**	E2.2.1.4	E2.1.3.5.1	**78**	E2.2.2	E2.1.3.3.1
11	E2.1.2.3	E2.2.4	**45**	E2.2.1.4	E2.1.3.5.2	**79**	E2.2.2	E2.1.3.3.2
12	E2.2.4	E2.1.3.2.1	**46**	E2.2.2	E2.1.3.5.1	**80**	E2.2.2	E2.1.3.4.1
13	E2.2.4	E2.1.3.2.2	**47**	E2.2.2	E2.1.3.5.2	**81**	E2.2.2	E2.1.3.4.2
14	E2.2.4	E2.1.3.3.1	**48**	E2.1.1.1.4.1.2	E2.2.1.5	**82**	E2.1.3.2.1	E2.2.1.6
15	E2.2.4	E2.1.3.3.2	**49**	E2.1.3.5.1	E2.2.1.6	**83**	E2.1.3.2.1	E2.2.1.5
16	E2.2.4	E2.1.3.4.1	**50**	E2.1.3.5.1	E2.2.1.5	**84**	E2.1.3.2.2	E2.2.1.6
17	E2.2.4	E2.1.3.4.2	**51**	E2.1.3.5.2	E2.2.1.6	**85**	E2.1.3.2.2	E2.2.1.5
18	E2.1.2.2	E2.2.1.1	**52**	E2.1.3.5.2	E2.2.1.5	**86**	E2.1.3.3.1	E2.2.1.6
19	E2.1.2.2	E2.2.1.3	**53**	E2.1.2.1	E2.2.4	**87**	E2.1.3.3.1	E2.2.1.5
20	E2.1.2.2	E2.2.3	**54**	E2.1.2.2	E2.2.1.2	**88**	E2.1.3.3.2	E2.2.1.6
21	E2.1.2.3	E2.2.1.1	**55**	E2.1.2.2	E2.2.1.4	**89**	E2.1.3.3.2	E2.2.1.5
22	E2.1.2.3	E2.2.1.3	**56**	E2.1.2.2	E2.2.2	**90**	E2.1.3.4.1	E2.2.1.6
23	E2.1.2.3	E2.2.3	**57**	E2.1.2.2	E2.2.1.6	**91**	E2.1.3.4.1	E2.2.1.5
24	E2.2.1.1	E2.1.3.2.1	**58**	E2.1.2.2	E2.2.1.5	**92**	E2.1.3.4.2	E2.2.1.6
25	E2.2.1.1	E2.1.3.2.2	**59**	E2.1.2.3	E2.2.1.2	**93**	E2.1.3.4.2	E2.2.1.5
26	E2.2.1.1	E2.1.3.3.1	**60**	E2.1.2.3	E2.2.1.4	**94**	E2.1.2.1	E2.2.1.1
27	E2.2.1.1	E2.1.3.3.2	**61**	E2.1.2.3	E2.2.2	**95**	E2.1.2.1	E2.2.1.3
28	E2.2.1.1	E2.1.3.4.1	**62**	E2.1.2.3	E2.2.1.6	**96**	E2.1.2.1	E2.2.3
29	E2.2.1.1	E2.1.3.4.2	**63**	E2.1.2.3	E2.2.1.5	**97**	E2.1.1.1.4.1.1	E2.2.3
30	E2.2.1.3	E2.1.3.2.1	**64**	E2.2.1.2	E2.1.3.2.1	**98**	E2.1.2.1	E2.2.1.2
31	E2.2.1.3	E2.1.3.2.2	**65**	E2.2.1.2	E2.1.3.2.2	**99**	E2.1.2.1	E2.2.1.4
32	E2.2.1.3	E2.1.3.3.1	**66**	E2.2.1.2	E2.1.3.3.1	**100**	E2.1.2.1	E2.2.2
33	E2.2.1.3	E2.1.3.3.2	**67**	E2.2.1.2	E2.1.3.3.2	**101**	E2.1.2.1	E2.2.1.6
34	E2.2.1.3	E2.1.3.4.1	**68**	E2.2.1.2	E2.1.3.4.1	**102**	E2.1.2.1	E2.2.1.5

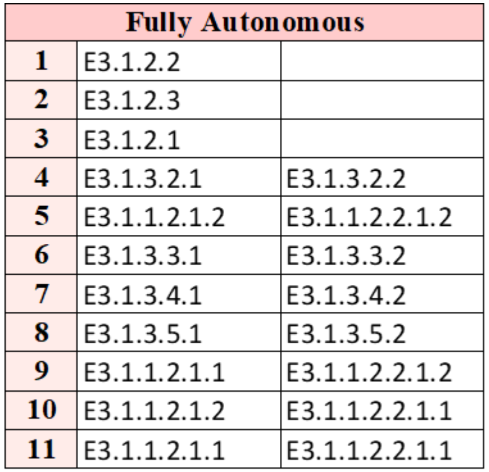
Fully Autonomous		
1	E2.1.3.5.1	
2	E2.1.3.5.2	
3	E2.1.2.2	
4	E2.1.2.3	
5	E2.1.3.2.1	
6	E2.1.3.2.2	
7	E2.1.3.3.1	
8	E2.1.3.3.2	
9	E2.1.3.4.1	
10	E2.1.3.4.2	
11	E2.1.2.1	
12	E2.1.3.1.1	E2.1.3.1.2
13	E2.1.3.1.1	E2.1.3.1.3
14	E2.1.3.1.1	E2.1.3.1.4
15	E2.1.3.1.2	E2.1.3.1.3
16	E2.1.3.1.2	E2.1.3.1.4
17	E2.1.3.1.3	E2.1.3.1.4
18	E2.1.1.1.4.1.2	E2.2.3
19	E2.1.1.2.1.2	E2.1.1.2.2.1.2
20	E2.1.1.1.4.1.2	E2.2.1.5
21	E2.1.1.1.4.1.1	E2.2.3
22	E2.1.1.2.1.1	E2.1.1.2.2.1.2
23	E2.1.1.2.1.2	E2.1.1.2.2.1.1
24	E2.1.1.1.4.1.1	E2.2.1.5
25	E2.1.1.2.1.1	E2.1.1.2.2.1.1

Fully Autonomous (Modified)		
1	E2.1.3.5.1	
2	E2.1.3.5.2	
3	E2.1.3.2.1	
4	E2.1.3.2.2	
5	E2.1.3.3.1	
6	E2.1.3.3.2	
7	E2.1.3.4.1	
8	E2.1.3.4.2	
9	E2.1.3.1.1	E2.1.3.1.2
10	E2.1.3.1.1	E2.1.3.1.3
11	E2.1.3.1.1	E2.1.3.1.4
12	E2.1.3.1.2	E2.1.3.1.3
13	E2.1.3.1.2	E2.1.3.1.4
14	E2.1.3.1.3	E2.1.3.1.4
15	E2.1.1.1.4.1.2	E2.2.3
16	E2.1.1.2.1.2	E2.1.1.2.2.1.2
17	E2.1.1.1.4.1.2	E2.2.1.5
18	E2.1.2.1.2	E2.1.2.2.2
19	E2.1.2.1.2	E2.1.2.2.3
20	E2.1.2.1.3	E2.1.2.2.2
21	E2.1.2.1.3	E2.1.2.2.3
22	E2.1.1.1.4.1.1	E2.2.3
23	E2.1.1.2.1.1	E2.1.1.2.2.1.2
24	E2.1.1.2.1.2	E2.1.1.2.2.1.1
25	E2.1.2.1.1	E2.1.2.2.2
26	E2.1.2.1.1	E2.1.2.2.3
27	E2.1.2.1.2	E2.1.2.2.1
28	E2.1.2.1.3	E2.1.2.2.1
29	E2.1.1.1.4.1.1	E2.2.1.5
30	E2.1.1.2.1.1	E2.1.1.2.2.1.1
31	E2.1.2.1.1	E2.1.2.2.1

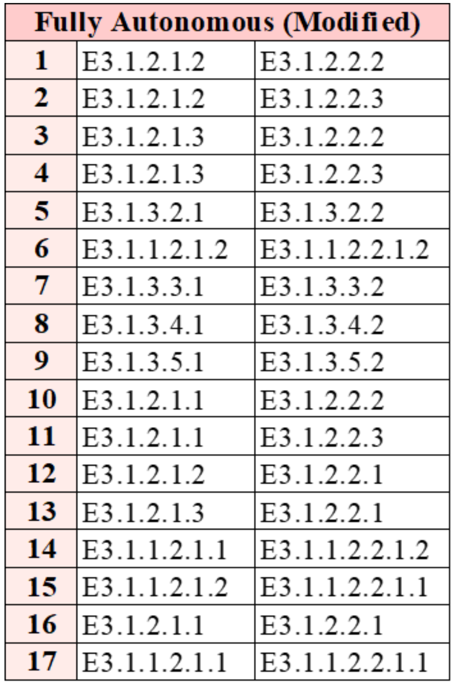
APPENDIX 3C. NIGHT AND GOOD WEATHER SCENARIO



Dynamic LoA		
1	E3.1.2.2	E3.2.4
2	E3.1.2.3	E3.2.4
3	E3.1.2.2	E3.2.3
4	E3.1.2.2	E3.2.1.1
5	E3.1.2.2	E3.2.1.3
6	E3.1.2.3	E3.2.3
7	E3.1.2.3	E3.2.1.1
8	E3.1.2.3	E3.2.1.3
9	E3.1.2.1	E3.2.4
10	E3.1.2.2	E3.2.2
11	E3.1.2.2	E3.2.1.2
12	E3.1.2.2	E3.2.1.4
13	E3.1.2.2	E3.2.1.5
14	E3.1.2.3	E3.2.2
15	E3.1.2.3	E3.2.1.2
16	E3.1.2.3	E3.2.1.4
17	E3.1.2.3	E3.2.1.5
18	E3.1.2.1	E3.2.3
19	E3.1.2.1	E3.2.1.1
20	E3.1.2.1	E3.2.1.3
21	E3.1.2.1	E3.2.2
22	E3.1.2.1	E3.2.1.2
23	E3.1.2.1	E3.2.1.4
24	E3.1.2.1	E3.2.1.5



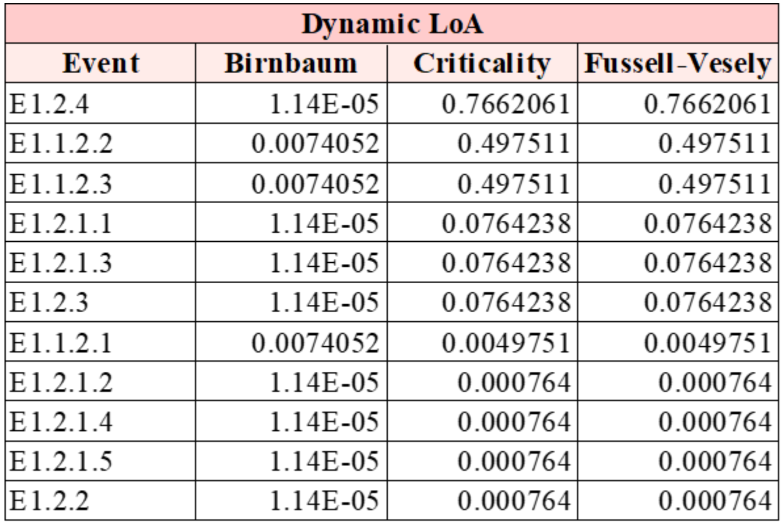
Fully Autonomous		
1	E3.1.2.2	
2	E3.1.2.3	
3	E3.1.2.1	
4	E3.1.3.2.1	E3.1.3.2.2
5	E3.1.1.2.1.2	E3.1.1.2.2.1.2
6	E3.1.3.3.1	E3.1.3.3.2
7	E3.1.3.4.1	E3.1.3.4.2
8	E3.1.3.5.1	E3.1.3.5.2
9	E3.1.1.2.1.1	E3.1.1.2.2.1.2
10	E3.1.1.2.1.2	E3.1.1.2.2.1.1
11	E3.1.1.2.1.1	E3.1.1.2.2.1.1



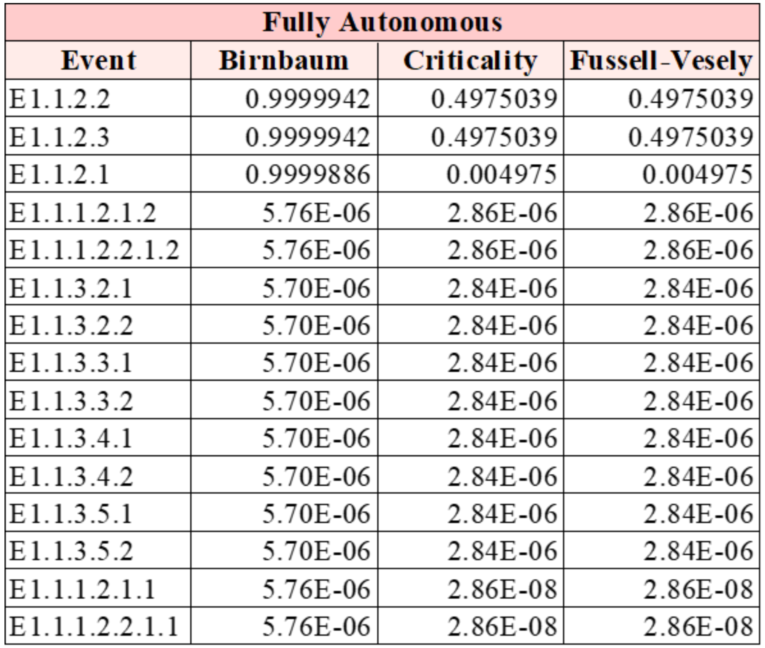
Fully Autonomous (Modified)		
1	E3.1.2.1.2	E3.1.2.2.2
2	E3.1.2.1.2	E3.1.2.2.3
3	E3.1.2.1.3	E3.1.2.2.2
4	E3.1.2.1.3	E3.1.2.2.3
5	E3.1.3.2.1	E3.1.3.2.2
6	E3.1.1.2.1.2	E3.1.1.2.2.1.2
7	E3.1.3.3.1	E3.1.3.3.2
8	E3.1.3.4.1	E3.1.3.4.2
9	E3.1.3.5.1	E3.1.3.5.2
10	E3.1.2.1.1	E3.1.2.2.2
11	E3.1.2.1.1	E3.1.2.2.3
12	E3.1.2.1.2	E3.1.2.2.1
13	E3.1.2.1.3	E3.1.2.2.1
14	E3.1.1.2.1.1	E3.1.1.2.2.1.2
15	E3.1.1.2.1.2	E3.1.1.2.2.1.1
16	E3.1.2.1.1	E3.1.2.2.1
17	E3.1.1.2.1.1	E3.1.1.2.2.1.1

APPENDIX 4. FAULT TREE RESULTS – IMPORTANCE MEASURES

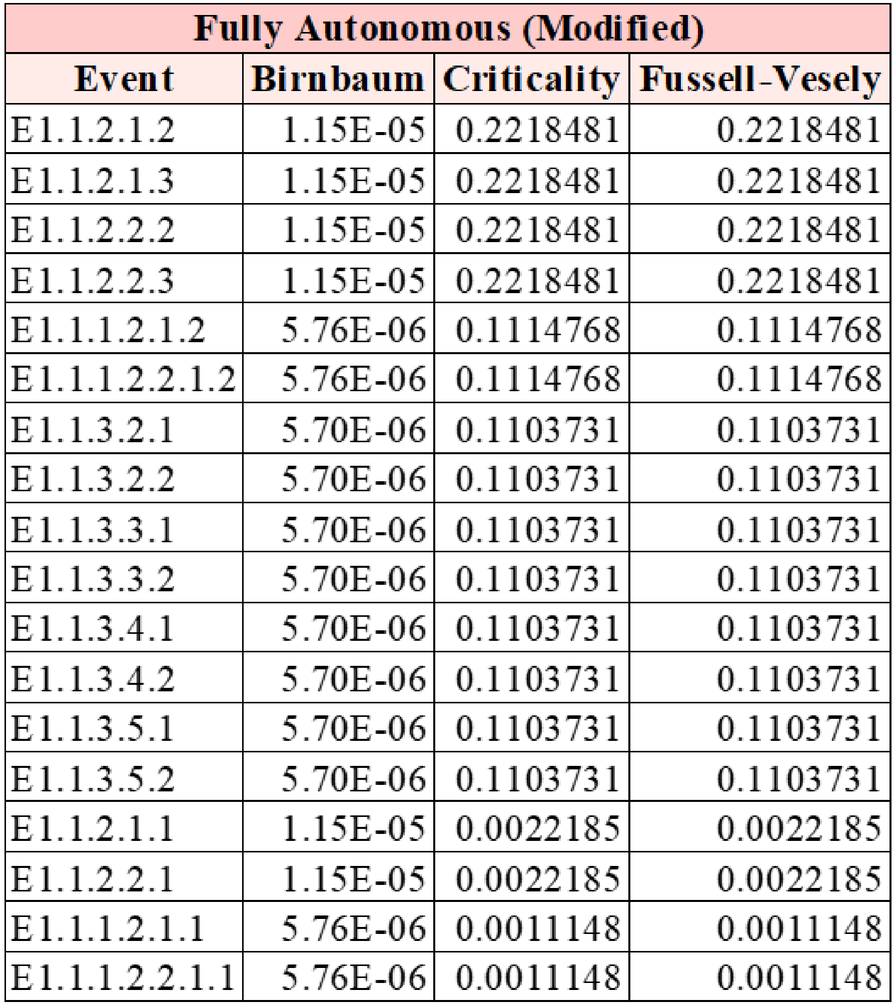
APPENDIX 4A. DAY AND GOOD WEATHER SCENARIO



Dynamic LoA			
Event	Birnbaum	Criticality	Fussell-Vesely
E1.2.4	1.14E-05	0.7662061	0.7662061
E1.1.2.2	0.0074052	0.497511	0.497511
E1.1.2.3	0.0074052	0.497511	0.497511
E1.2.1.1	1.14E-05	0.0764238	0.0764238
E1.2.1.3	1.14E-05	0.0764238	0.0764238
E1.2.3	1.14E-05	0.0764238	0.0764238
E1.1.2.1	0.0074052	0.0049751	0.0049751
E1.2.1.2	1.14E-05	0.000764	0.000764
E1.2.1.4	1.14E-05	0.000764	0.000764
E1.2.1.5	1.14E-05	0.000764	0.000764
E1.2.2	1.14E-05	0.000764	0.000764

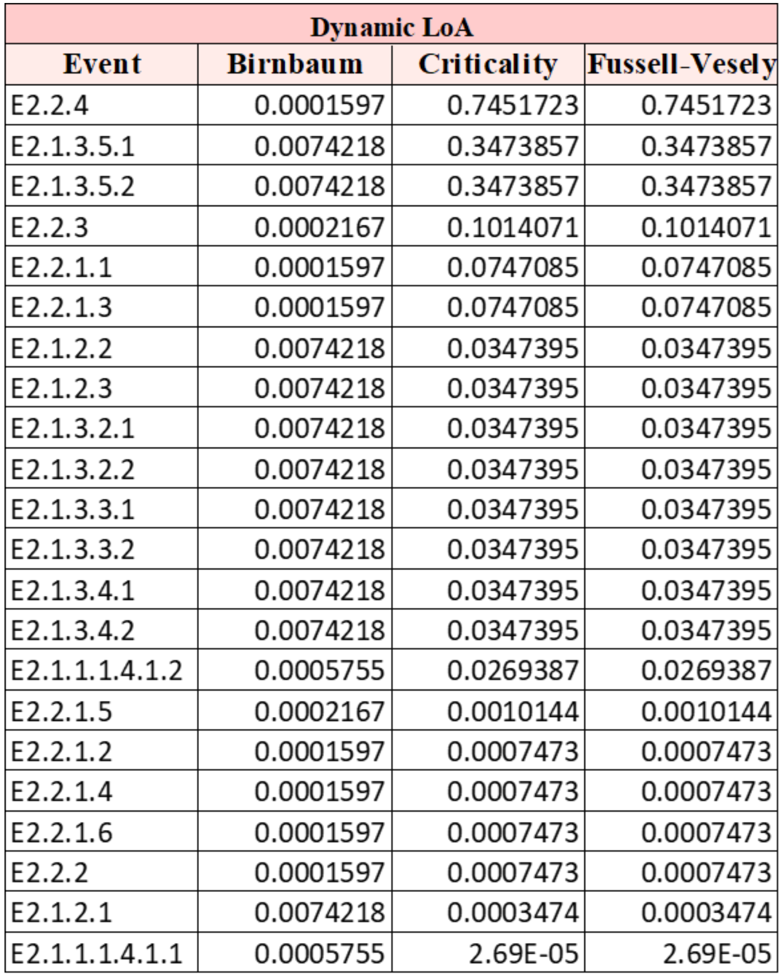


Fully Autonomous			
Event	Birnbaum	Criticality	Fussell-Vesely
E1.1.2.2	0.9999942	0.4975039	0.4975039
E1.1.2.3	0.9999942	0.4975039	0.4975039
E1.1.2.1	0.9999886	0.004975	0.004975
E1.1.1.2.1.2	5.76E-06	2.86E-06	2.86E-06
E1.1.1.2.2.1.2	5.76E-06	2.86E-06	2.86E-06
E1.1.3.2.1	5.70E-06	2.84E-06	2.84E-06
E1.1.3.2.2	5.70E-06	2.84E-06	2.84E-06
E1.1.3.3.1	5.70E-06	2.84E-06	2.84E-06
E1.1.3.3.2	5.70E-06	2.84E-06	2.84E-06
E1.1.3.4.1	5.70E-06	2.84E-06	2.84E-06
E1.1.3.4.2	5.70E-06	2.84E-06	2.84E-06
E1.1.3.5.1	5.70E-06	2.84E-06	2.84E-06
E1.1.3.5.2	5.70E-06	2.84E-06	2.84E-06
E1.1.1.2.1.1	5.76E-06	2.86E-08	2.86E-08
E1.1.1.2.2.1.1	5.76E-06	2.86E-08	2.86E-08

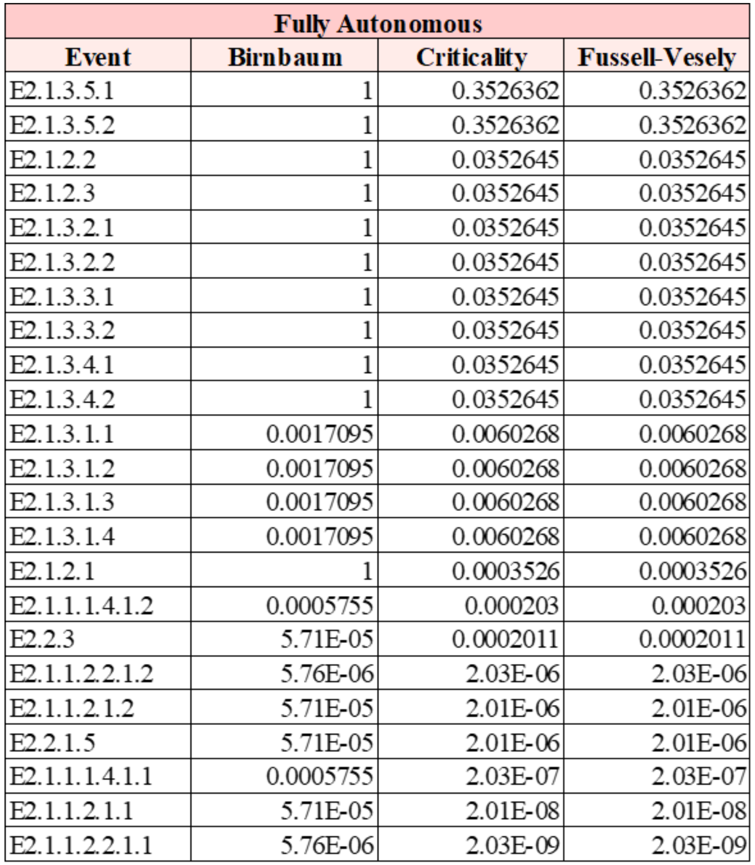


Fully Autonomous (Modified)			
Event	Birnbaum	Criticality	Fussell-Vesely
E1.1.2.1.2	1.15E-05	0.2218481	0.2218481
E1.1.2.1.3	1.15E-05	0.2218481	0.2218481
E1.1.2.2.2	1.15E-05	0.2218481	0.2218481
E1.1.2.2.3	1.15E-05	0.2218481	0.2218481
E1.1.1.2.1.2	5.76E-06	0.1114768	0.1114768
E1.1.1.2.2.1.2	5.76E-06	0.1114768	0.1114768
E1.1.3.2.1	5.70E-06	0.1103731	0.1103731
E1.1.3.2.2	5.70E-06	0.1103731	0.1103731
E1.1.3.3.1	5.70E-06	0.1103731	0.1103731
E1.1.3.3.2	5.70E-06	0.1103731	0.1103731
E1.1.3.4.1	5.70E-06	0.1103731	0.1103731
E1.1.3.4.2	5.70E-06	0.1103731	0.1103731
E1.1.3.5.1	5.70E-06	0.1103731	0.1103731
E1.1.3.5.2	5.70E-06	0.1103731	0.1103731
E1.1.2.1.1	1.15E-05	0.0022185	0.0022185
E1.1.2.2.1	1.15E-05	0.0022185	0.0022185
E1.1.1.2.1.1	5.76E-06	0.0011148	0.0011148
E1.1.1.2.2.1.1	5.76E-06	0.0011148	0.0011148

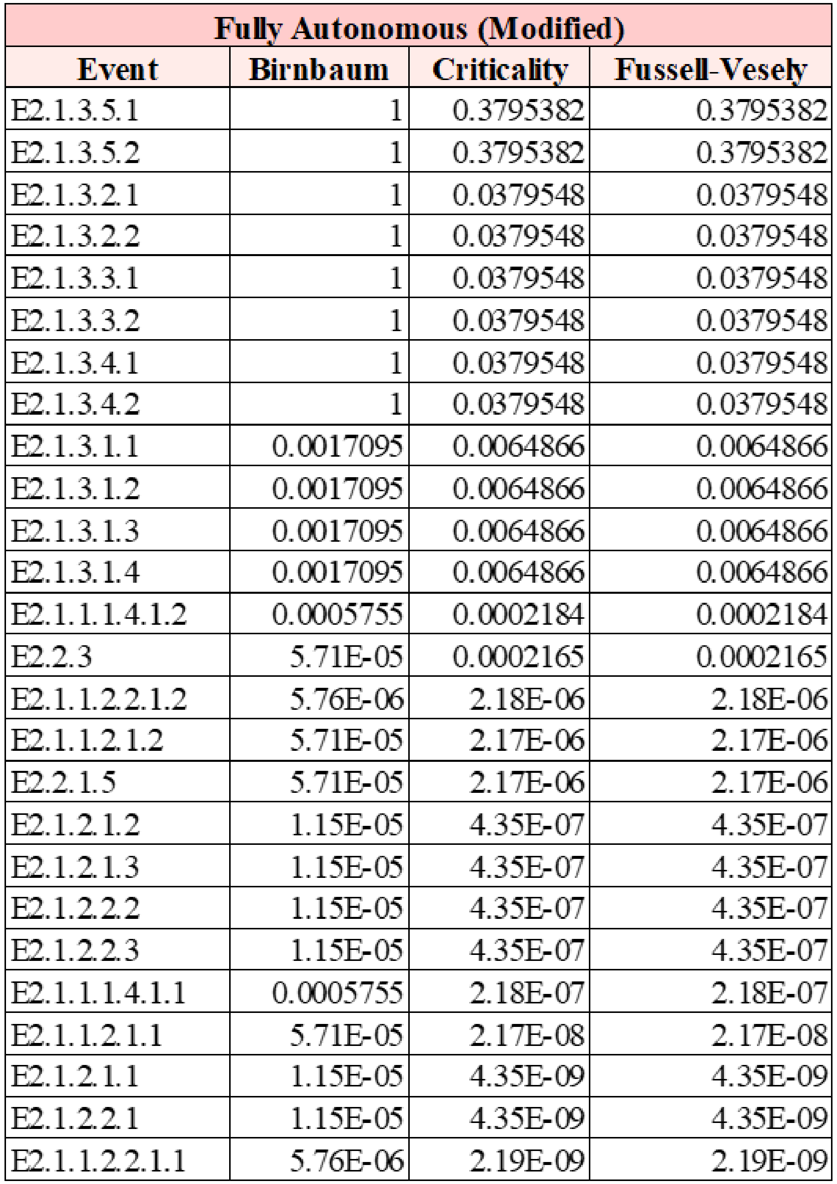
APPENDIX 4B. HARSH WEATHER SCENARIO



Dynamic LoA			
Event	Birnbaum	Criticality	Fussell-Vesely
E2.2.4	0.0001597	0.7451723	0.7451723
E2.1.3.5.1	0.0074218	0.3473857	0.3473857
E2.1.3.5.2	0.0074218	0.3473857	0.3473857
E2.2.3	0.0002167	0.1014071	0.1014071
E2.2.1.1	0.0001597	0.0747085	0.0747085
E2.2.1.3	0.0001597	0.0747085	0.0747085
E2.1.2.2	0.0074218	0.0347395	0.0347395
E2.1.2.3	0.0074218	0.0347395	0.0347395
E2.1.3.2.1	0.0074218	0.0347395	0.0347395
E2.1.3.2.2	0.0074218	0.0347395	0.0347395
E2.1.3.3.1	0.0074218	0.0347395	0.0347395
E2.1.3.3.2	0.0074218	0.0347395	0.0347395
E2.1.3.4.1	0.0074218	0.0347395	0.0347395
E2.1.3.4.2	0.0074218	0.0347395	0.0347395
E2.1.1.1.4.1.2	0.0005755	0.0269387	0.0269387
E2.2.1.5	0.0002167	0.0010144	0.0010144
E2.2.1.2	0.0001597	0.0007473	0.0007473
E2.2.1.4	0.0001597	0.0007473	0.0007473
E2.2.1.6	0.0001597	0.0007473	0.0007473
E2.2.2	0.0001597	0.0007473	0.0007473
E2.1.2.1	0.0074218	0.0003474	0.0003474
E2.1.1.1.4.1.1	0.0005755	2.69E-05	2.69E-05

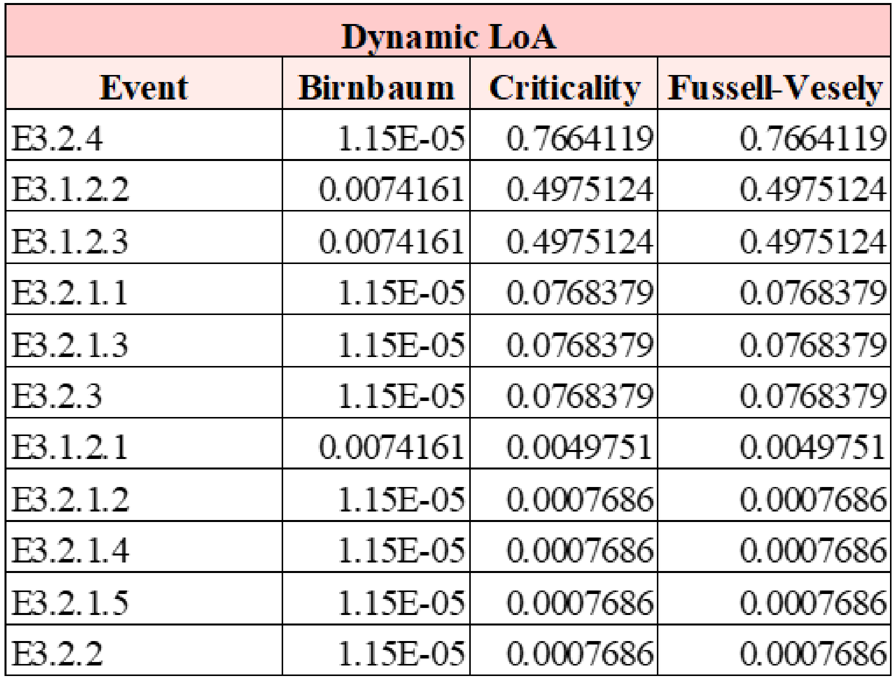


Fully Autonomous			
Event	Birnbaum	Criticality	Fussell-Vesely
E2.1.3.5.1	1	0.3526362	0.3526362
E2.1.3.5.2	1	0.3526362	0.3526362
E2.1.2.2	1	0.0352645	0.0352645
E2.1.2.3	1	0.0352645	0.0352645
E2.1.3.2.1	1	0.0352645	0.0352645
E2.1.3.2.2	1	0.0352645	0.0352645
E2.1.3.3.1	1	0.0352645	0.0352645
E2.1.3.3.2	1	0.0352645	0.0352645
E2.1.3.4.1	1	0.0352645	0.0352645
E2.1.3.4.2	1	0.0352645	0.0352645
E2.1.3.1.1	0.0017095	0.0060268	0.0060268
E2.1.3.1.2	0.0017095	0.0060268	0.0060268
E2.1.3.1.3	0.0017095	0.0060268	0.0060268
E2.1.3.1.4	0.0017095	0.0060268	0.0060268
E2.1.2.1	1	0.0003526	0.0003526
E2.1.1.1.4.1.2	0.0005755	0.000203	0.000203
E2.2.3	5.71E-05	0.0002011	0.0002011
E2.1.1.2.2.1.2	5.76E-06	2.03E-06	2.03E-06
E2.1.1.2.1.2	5.71E-05	2.01E-06	2.01E-06
E2.2.1.5	5.71E-05	2.01E-06	2.01E-06
E2.1.1.1.4.1.1	0.0005755	2.03E-07	2.03E-07
E2.1.1.2.1.1	5.71E-05	2.01E-08	2.01E-08
E2.1.1.2.2.1.1	5.76E-06	2.03E-09	2.03E-09

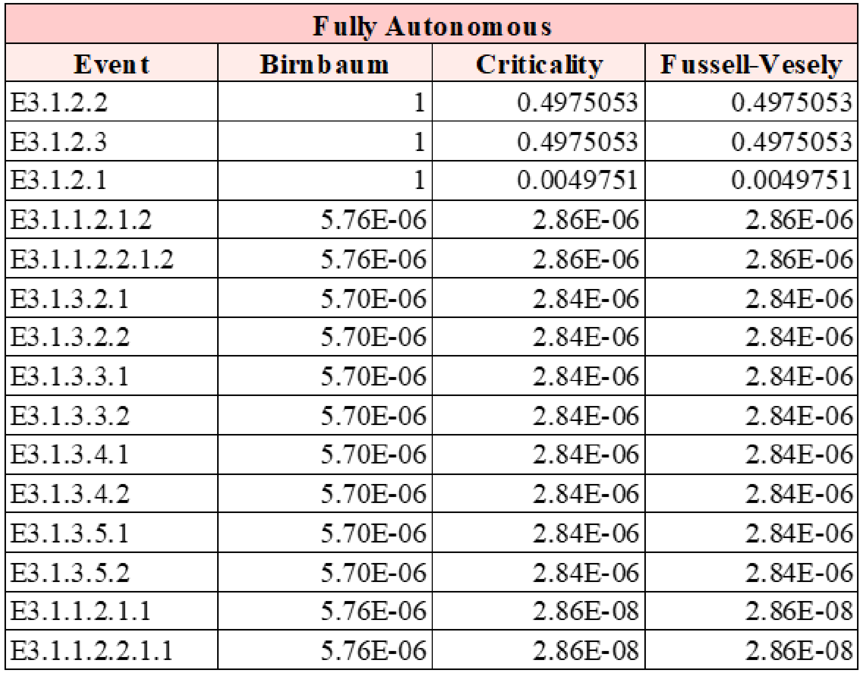


Fully Autonomous (Modified)			
Event	**Birnbaum**	**Criticality**	**Fussell-Vesely**
E2.1.3.5.1	1	0.3795382	0.3795382
E2.1.3.5.2	1	0.3795382	0.3795382
E2.1.3.2.1	1	0.0379548	0.0379548
E2.1.3.2.2	1	0.0379548	0.0379548
E2.1.3.3.1	1	0.0379548	0.0379548
E2.1.3.3.2	1	0.0379548	0.0379548
E2.1.3.4.1	1	0.0379548	0.0379548
E2.1.3.4.2	1	0.0379548	0.0379548
E2.1.3.1.1	0.0017095	0.0064866	0.0064866
E2.1.3.1.2	0.0017095	0.0064866	0.0064866
E2.1.3.1.3	0.0017095	0.0064866	0.0064866
E2.1.3.1.4	0.0017095	0.0064866	0.0064866
E2.1.1.1.4.1.2	0.0005755	0.0002184	0.0002184
E2.2.3	5.71E-05	0.0002165	0.0002165
E2.1.1.2.2.1.2	5.76E-06	2.18E-06	2.18E-06
E2.1.1.2.1.2	5.71E-05	2.17E-06	2.17E-06
E2.2.1.5	5.71E-05	2.17E-06	2.17E-06
E2.1.2.1.2	1.15E-05	4.35E-07	4.35E-07
E2.1.2.1.3	1.15E-05	4.35E-07	4.35E-07
E2.1.2.2.2	1.15E-05	4.35E-07	4.35E-07
E2.1.2.2.3	1.15E-05	4.35E-07	4.35E-07
E2.1.1.1.4.1.1	0.0005755	2.18E-07	2.18E-07
E2.1.1.2.1.1	5.71E-05	2.17E-08	2.17E-08
E2.1.2.1.1	1.15E-05	4.35E-09	4.35E-09
E2.1.2.2.1	1.15E-05	4.35E-09	4.35E-09
E2.1.1.2.2.1.1	5.76E-06	2.19E-09	2.19E-09

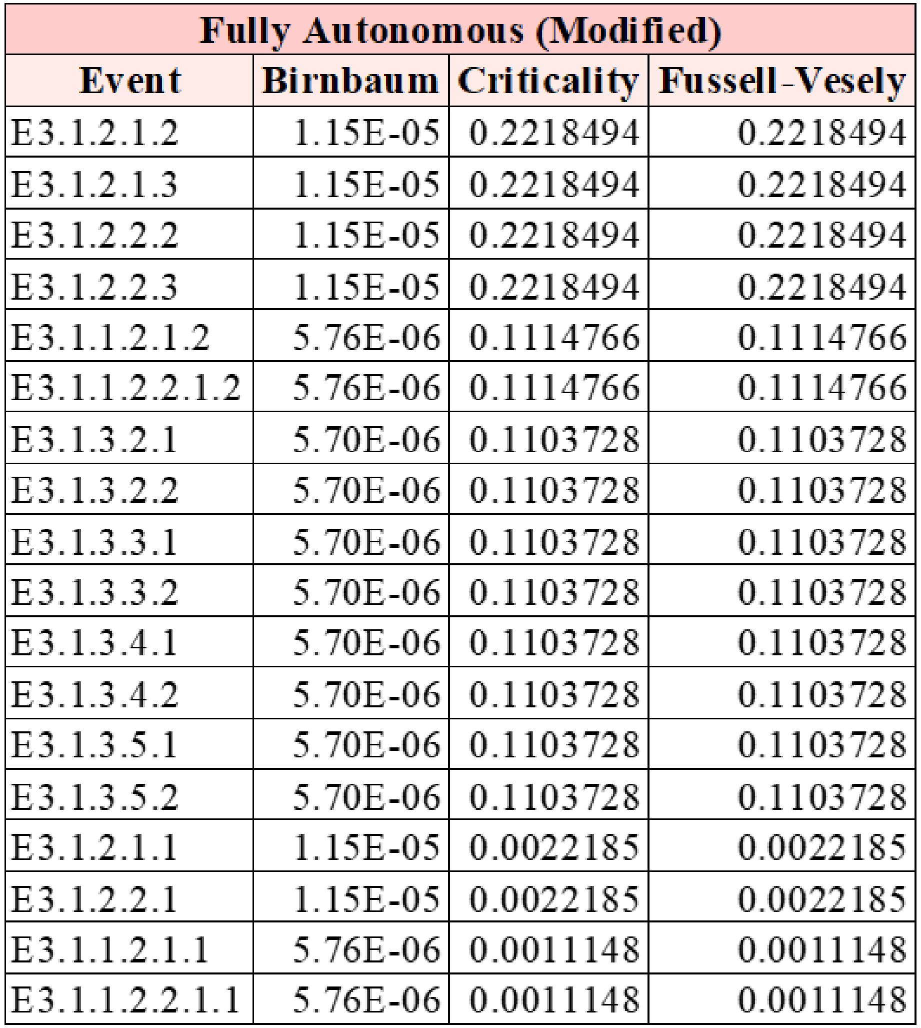
APPENDIX 4C. NIGHT AND GOOD WEATHER SCENARIO



Dynamic LoA			
Event	Birnbaum	Criticality	Fussell-Vesely
E3.2.4	1.15E-05	0.7664119	0.7664119
E3.1.2.2	0.0074161	0.4975124	0.4975124
E3.1.2.3	0.0074161	0.4975124	0.4975124
E3.2.1.1	1.15E-05	0.0768379	0.0768379
E3.2.1.3	1.15E-05	0.0768379	0.0768379
E3.2.3	1.15E-05	0.0768379	0.0768379
E3.1.2.1	0.0074161	0.0049751	0.0049751
E3.2.1.2	1.15E-05	0.0007686	0.0007686
E3.2.1.4	1.15E-05	0.0007686	0.0007686
E3.2.1.5	1.15E-05	0.0007686	0.0007686
E3.2.2	1.15E-05	0.0007686	0.0007686



Fully Autonomous			
Event	Birnbaum	Criticality	Fussell-Vesely
E3.1.2.2	1	0.4975053	0.4975053
E3.1.2.3	1	0.4975053	0.4975053
E3.1.2.1	1	0.0049751	0.0049751
E3.1.1.2.1.2	5.76E-06	2.86E-06	2.86E-06
E3.1.1.2.2.1.2	5.76E-06	2.86E-06	2.86E-06
E3.1.3.2.1	5.70E-06	2.84E-06	2.84E-06
E3.1.3.2.2	5.70E-06	2.84E-06	2.84E-06
E3.1.3.3.1	5.70E-06	2.84E-06	2.84E-06
E3.1.3.3.2	5.70E-06	2.84E-06	2.84E-06
E3.1.3.4.1	5.70E-06	2.84E-06	2.84E-06
E3.1.3.4.2	5.70E-06	2.84E-06	2.84E-06
E3.1.3.5.1	5.70E-06	2.84E-06	2.84E-06
E3.1.3.5.2	5.70E-06	2.84E-06	2.84E-06
E3.1.1.2.1.1	5.76E-06	2.86E-08	2.86E-08
E3.1.1.2.2.1.1	5.76E-06	2.86E-08	2.86E-08



Fully Autonomous (Modified)			
Event	Birnbaum	Criticality	Fussell-Vesely
E3.1.2.1.2	1.15E-05	0.2218494	0.2218494
E3.1.2.1.3	1.15E-05	0.2218494	0.2218494
E3.1.2.2.2	1.15E-05	0.2218494	0.2218494
E3.1.2.2.3	1.15E-05	0.2218494	0.2218494
E3.1.1.2.1.2	5.76E-06	0.1114766	0.1114766
E3.1.1.2.2.1.2	5.76E-06	0.1114766	0.1114766
E3.1.3.2.1	5.70E-06	0.1103728	0.1103728
E3.1.3.2.2	5.70E-06	0.1103728	0.1103728
E3.1.3.3.1	5.70E-06	0.1103728	0.1103728
E3.1.3.3.2	5.70E-06	0.1103728	0.1103728
E3.1.3.4.1	5.70E-06	0.1103728	0.1103728
E3.1.3.4.2	5.70E-06	0.1103728	0.1103728
E3.1.3.5.1	5.70E-06	0.1103728	0.1103728
E3.1.3.5.2	5.70E-06	0.1103728	0.1103728
E3.1.2.1.1	1.15E-05	0.0022185	0.0022185
E3.1.2.2.1	1.15E-05	0.0022185	0.0022185
E3.1.1.2.1.1	5.76E-06	0.0011148	0.0011148
E3.1.1.2.2.1.1	5.76E-06	0.0011148	0.0011148