UNIVERSITY of STRATHCLYDE
MARITIME SAFETY
RESEARCH CENTRE
DEPARTMENT OF NAVAL ARCHITECTURE, OCEAN & MARINE ENGINEERING

University of
Strathclyde
Engineering

A NOVEL SAFETY ANALYSIS METHOD FOR MARINE CYBER-PHYSICAL SYSTEMS

By

Victor Bolbot

A thesis presented in fulfilment of the requirements for the degree of

Doctor of Philosophy

To Department of Naval Architecture, Ocean & Marine Engineering

University of Strathclyde

Glasgow, United Kingdom

2020

This page has been intentionally left blank

DECLARATION OF AUTHENTICITY AND AUTHOR'S RIGHTS

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination, which has led to the award of a degree.

To cite this work, please use the following reference:

Bolbot Victor, 2020, A Novel Safety Analysis Method for Marine Cyber-Physical Systems, PhD thesis, University of Strathclyde, Glasgow

Signed: Victor Bolbot Date:

Review committee:

Dr Byongug Jeong

Prof Ingrid Bouwer Utne

This page has been intentionally left blank

Out of complexity, find simplicity!

Albert Einstein (1879-1955)

This page has been intentionally left blank

DEDICATION

Dedicated to those, who love me and whose love and support brought me here.

This page has been intentionally left blank

ABSTRACT

Cyber-Physical Systems (CPSs) represent a systems category expected to enhance the safety and improve the efficiency of maritime operations. However, new challenges due to the CPSs complexity are also anticipated leading to an unpredictable system behaviour, thus jeopardising safety.

This thesis aims at developing a novel safety analysis method and system for enhancing the safety of the marine CPSs considering both their design and operation. Based on a comprehensive literature review, the safety-related properties for CPSs are identified. Then, the different hazard identification methods are analysed on their effectiveness to identify scenarios linked to the CPSs safety related properties. As the existing literature demonstrates, the existing hazard identification methods such as Fault Tree Analysis (FTA), Failure Modes and Effects Analysis and System-Theoretic Process Analysis (STPA) applications to the CPSs have been criticised for not capturing either the software-intensive character of CPSs or not allowing for quantitative safety analysis.

To address these limitations, a novel Combinatorial Approach for Safety Analysis (CASA) is developed by integrating STPA, Events Sequence Identification (ESI) method and FTA. The method initiates with STPA, then employs ESI using input from STPA to identify the different scenarios and develops a Fault Tree based on ESI results. This Fault Tree is populated with STPA results, further refined, and enriched with the FTA results. The final Fault Tree can be used for estimation of the top-event failure rate and frequency, importance measures estimation and uncertainty analysis.

The novel method is applied for estimating the failure rate and importance measures estimation of two types of marine CPSs: exhaust gas open-loop scrubber system and a reference cruise ship Diesel-Electric Propulsion (DEP). Failure rate for 12 DEP system alternatives blackout is also estimated. The derived results for the scrubber system and DEP system demonstrate that the developed Fault Tree is much richer than for the previous studies. Moreover, it is demonstrated that the increase of the DEP system reliability/availability does not always result in DEP system blackout frequency reduction, as other system parameters have significant influence on blackout.

Based on the CASA method results for the DEP reference system, a novel automated blackout monitoring concept for the DEP system is proposed. This concept is used to estimate the blackout probability variation in time in a virtual environment for the reference DEP system by integrating a number of measured system parameters, historical data and the CASA developed Fault Tree by providing a functional alarm to the crew and allowing better system monitoring and control.

The novel CASA method is expected to support the system safety analysis and enhancement during the system design, whilst the proposed blackout monitoring concept is expected to enhance the safety of the DEP system operations.

Keywords: Cyber-Physical Systems, Safety analysis, Diesel-Electric Propulsion system, Exhaust gas open loop scrubber system, Blackout, Cruise ships, Blackout monitoring system.

This page has been intentionally left blank

ACKNOWLEDGEMENTS

Our life is nothing more than a journey and my PhD studies has been just one of the most fascinating phases in this journey. During my PhD studies, my knowledge and skills have been elevated to a new level, whilst it was a period of severe transformations in my worldview and my character. During my stay at Glasgow, I managed to obtain more friends than I had ever before, to gain new experience and to travel to many new places. It has been a journey with its deep highs and lows at the same time, and I feel very grateful to God and to the people who supported me through all this time.

First, I would like to express my gratitude to my supervisor Dr Gerasimos Theotokatos for the continuous support during my PhD studies and related research, for his patience, motivation, and immense knowledge. His guidance and example were of crucial importance for the success of the whole PhD progress.

I feel also thankful to Dr Evangelos Boulougouris and Prof Dracos Vassalos for offering me the opportunity to undertake the PhD at Maritime Safety Research Centre, one of the leading places in the area of safety of marine systems and operation.

Extraordinary thanks go to DNV GL and Royal Caribbean Cruise Lines for establishing the Maritime Safety Research Centre, especially to DNV GL for offering the funding for the PhD position related to research on Cyber-Physical Systems safety and offering ideas for research. Particularly I would like to thank Dr George Psarros, Dr Ing Rainer Hamann and Dr Ole Christian Astrup for their continuous interactions and constructive comments about my PhD thesis.

Special thanks and appreciation must go to my family such as my father Alexei, my mother Elena, and my sister Sofiya. Words cannot express how grateful I am to my parents for all of the sacrifices that you have made on my behalf! Your prayer for me was what sustained me so far!

Additionally, I would like to take the opportunity to thank researchers/colleagues from Maritime Safety Research Centre. I would like to thank Dr Stuart Williams for his support with accident data acquisition for the PhD thesis and those colleagues who have supported me through the everyday struggle of my research work: Athanasios Niotis, Dr George Atzampos, Alexandros Komianos, Fotios Stefanidis, Christos Gkerekos, Dr Romanas Puisa, Sokratis Stoumpos, Dr Alexandros Priftis and Dr Luminita Bujorianu.

My sincere gratefulness also goes to all the administrative personnel of the department of NAOME for assisting me with the day-to-day details of my work at the University of Strathclyde.

Last, but not least I would like to thank my friends from Glasgow City Free Church and Glasgow Navigators who supported me during my spiritual struggles.

This page has been intentionally left blank

RESEARCH OUTPUT

The research output in terms of conference papers and journal publications from the present PhD research is demonstrated graphically in Figure 1.

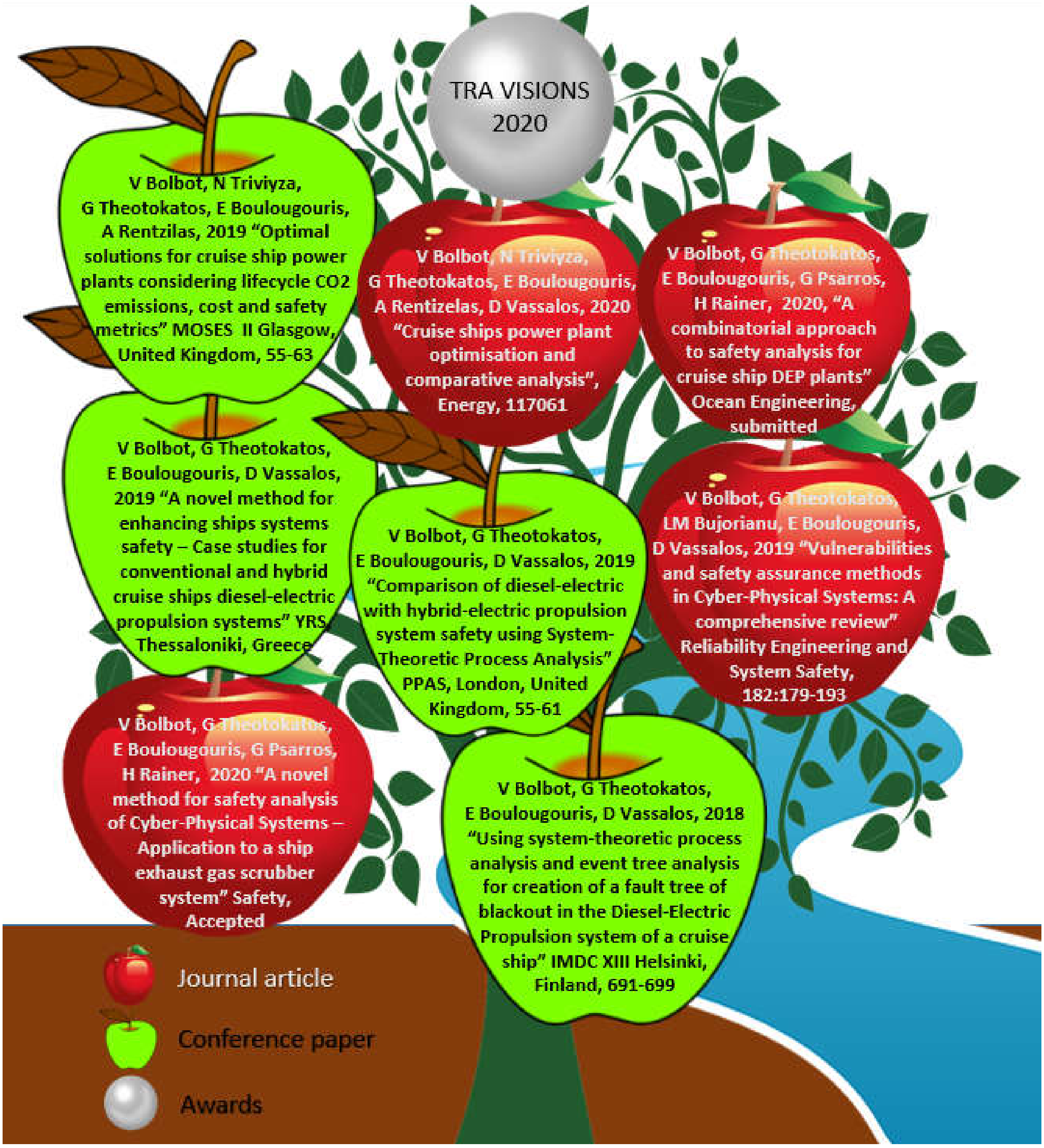

TRA VISIONS 2020
V Bolbot, N Triviyza, G Theotokatos, E Boulougouris, A Rentzilas, 2019 "Optimal solutions for cruise ship power plants considering lifecycle CO2 emissions, cost and safety metrics" MOSES II Glasgow, United Kingdom, 55-63
V Bolbot, N Triviyza, G Theotokatos, E Boulougouris, A Rentizelas, D Vassalos, 2020 "Cruise ships power plant optimisation and comparative analysis", Energy, 117061
V Bolbot, G Theotokatos, E Boulougouris, G Psarros, H Rainer, 2020, "A combinatorial approach to safety analysis for cruise ship DEP plants" Ocean Engineering, submitted
V Bolbot, G Theotokatos, E Boulougouris, D Vassalos, 2019 "A novel method for enhancing ships systems safety – Case studies for conventional and hybrid cruise ships diesel-electric propulsion systems" YRS Thessaloniki, Greece
V Bolbot, G Theotokatos, E Boulougouris, D Vassalos, 2019 "Comparison of diesel-electric with hybrid-electric propulsion system safety using System-Theoretic Process Analysis" PPAS, London, United Kingdom, 55-61
V Bolbot, G Theotokatos, LM Bujorianu, E Boulougouris, D Vassalos, 2019 "Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review" Reliability Engineering and System Safety, 182:179-193
V Bolbot, G Theotokatos, E Boulougouris, G Psarros, H Rainer, 2020 "A novel method for safety analysis of Cyber-Physical Systems – Application to a ship exhaust gas scrubber system" Safety, Accepted
V Bolbot, G Theotokatos, E Boulougouris, D Vassalos, 2018 "Using system-theoretic process analysis and event tree analysis for creation of a fault tree of blackout in the Diesel-Electric Propulsion system of a cruise ship" IMDC XIII Helsinki, Finland, 691-699
Journal article
Conference paper
Awards

Figure 1 Research output

This page has been intentionally left blank

CONTENTS

This page has been intentionally left blank

FIGURES LIST

This page has been intentionally left blank

TABLES LIST

ABBREVIATIONS AND NOMENCLATURE LIST

Table 1 Abbreviations list

Abbreviation	**Definition**
AADL	Architecture Analysis and Description Language
ACPSs	Autonomous CPSs (for CPSs please see below)
AVR	Automatic Voltage Regulator
BBN	Bayesian Belief Network
BDMP	Boolean Driven Markov Processes
BMS	Battery Management System
BSI	British Standards Institution
BT	Bow Thruster
CA	Criticality Analysis
CASA	Combinatory Approach to Safety Analysis
CHAZOP	Control HAZOP (for HAZOP please see below)
CLIA	Cruise Lines International Association
CPSoSs	Cyber-Physical Systems of Systems
CPSs	Cyber-Physical Systems
DEP	Diesel-Electric Propulsion
DFG	Dual Fuel Generator
DG or D/G	Diesel Generator
DGT	Diesel Generator Type
ER	Engine Room
ERT	Emission reduction technology
ESI	Event Sequence Identification
ETA	Event Tree Analysis
FHA	Functional Hazard Analysis
FI	Fault Injection
FLSA	Failure Logic and Safety Analysis
FMEA	Failure Modes and Effects Analysis
FOB	Frequency of blackout
FRAM	Functional Resonance Accident Model
FSAP/ NuSMV	Formal Safety Analysis Platform – New Symbolic Model Verifier
FT	Fault Tree

FTA	Fault Tree Analysis
FT	Fault Tree
G	General
H	Harbour
HAZID	HAZard IDentification
HAZOP	Hazard and Operability studies
HFMEA	Healthcare FMEA
HFO	Heavy Fuel Oil
HI	Health Index
HiP-HOPS	Hierarchically Performed Hazard Origin & Propagation Studies
HT	High Temperature
IAS	Integrated Automation System
ICSs	Industrial automation and Control Systems
IPS	Integrated Propulsion System
ISO	International Organization for Standardisation
IMO	International Maritime Organisation
LN	Lognormal
LNG	Liquefied Natural Gas
LOPA	Layer Protection Analysis
LSHFO	Low Sulphur Heavy Fuel Oil
LT	Low Temperature
M	Manoeuvring
MCR	Maximum Continuous Rating
MDO	Marine Diesel Oil
ME	Main Engine
OM	Operating Mode
OP	Operating Profile
P&I	Protection & Indemnity
PDF	Probability Density Function
PHA	Preliminary Hazard Analysis
PM	Propulsion Motor
PMS	Power Management System
PoB	Probability of Blackout
PoDGloss	Probability of DG set loss

QA	Quantitative Analysis
S	Sailing
SASWG	Safety of Autonomous Systems Working Group
SCR	Selective Catalytic Reduction
SOLAS	Safety Of Life At Sea
STPA	System-Theoretic Process Analysis
SW	Switchboard
SWIFT	Structured What-If
TC	Turbocharger
TR	Triangular
TRL	Technology Readiness Level
UCAs	Unsafe Control Actions
UML	Unified Modelling Language
UN	Uniform
UNP	Unit Nominal Power

Table 2 Nomenclature list

Greek symbols	
Symbol	**Explanation**
β_i	Weibull shape factor [-]
$\lambda_{i,A}$	Aggregated failure rate for component estimated using sensor measurements and reliability data
λ^B	Blackout failure rate [h^{-1}]
λ_i	Failure rate for component [h^{-1}]
λ^{TE}	The overall top event failure rate [h^{-1}]
$\overline{\lambda_t}$	Mean failure rate for component as per uncertainty analysis [h^{-1}]
$\overline{\lambda_i^t}$	Mean value of λ estimated from simulations [event/hours] or [event/years]
λ_i^{upper}	The upper limit of the failure rate [h^{-1}]
λ_i^{lower}	The lower limit of the failure rate [h^{-1}]
$\lambda_{\mathrm{i,m}}$	Failure rate for component estimated using sensor measurements [h^{-1}]
μ_i	Repair rate for component [h^{-1}]
σ	Standard deviation [h^{-1}]
English symbols	

Symbol	Explanation
E_j	Basic event in Fault Tree
EF_i	Error factor [-]
Err	Achieved accuracy [-]
Err_{acc}	Target accuracy [-]
F_i	Feature [variable units]
F_i^{norm}	Normal feature value [variable units]
F_i^{deg}	Feature degradation slope [variable units/h]
f	Frequency of the top event [events per year]
f_p	Frequency of the top event in specific system configuration [events per year]
HI_i	Health index for component i
I_j^B	Birnbaum's importance measure [-]
I_j^{Bt}	An averaged over time I_i^Bmetric [-]
I_j^{FV}	Fussell-Vesely importance measure [-]
I_i^{FVt}	An averaged over time I_i^{FV} metric [-]
MCR	Maximum Continuous Rating power [kW]
n_s	Number of simulations [-]
n_t	Number of criticality assessments implemented [-]
OM	Time system is working in specific operating mode [%]
OP	Operational parameters [depending on parameter]
OP_p	Time system is working in a specific configuration [%]
OT	Operational time [h]
$p_{i,A}$	Aggregated probability [-]
$p_{i,j}^{OC}$	Probability of failure for operating component [-]
$p_{i,j}^{SS}$	Probability of failure of safety system [-]
$p_{i,j}^{SSS}$	Probability of specific system states [-]
PFD_i	The probability of failure on demand [-]
p_p	Probability of top event in specific system configuration [-]
p^{TE}	Probability of top event [-]
r_{xy}	Pearson correlation coefficient [-]

r	Number of identical components
t	Time [h]
t_i^m	Time of last maintenance [h]
T_i	Inspection or maintenance interval [h]
w	Weight depicting which information is selected. w=1, sensors are used to estimate failure rate, w=0 failure rate from database is used.
$z_{a/2}$	is critical value of a normal distribution with zero mean value, standard deviation equal to one for (1-a) confidence interval [-]
Subscripts	
Symbol	**Explanation**
cr	Importance measure estimation number in dynamic simulation
i	Component
j	Basic event in Fault Tree
p	Specific system configuration
q	Number of specific system configuration
t	Simulation number in uncertainty analysis
OM	Operating mode

This page has been intentionally left blank

TERMINOLOGY

The different terms along with their definition are provided in Table 3.

Table 3 PhD used terms with their definitions and sources.

Term	Definition
Accident	'An unintended event involving fatality, injury, ship loss or damage, other property loss or damage, or environmental damage' (International Maritime Organisation (IMO), (2018)
Accident model	'The theory of accident causation used to analyse or design a system'(Thomas, 2013)
Accident scenario	'A sequence of events from the initiating event to one of the final stages' (IMO, 2018)
Consequence	'Outcome of an accident'(IMO, 2018)
Criticality analysis	'A procedure by which each potential failure mode is ranked according to the combined influence of severity and probability of occurrence' (US Department of Defence, 1980)
Frequency	'The number of occurrences per unit time (e.g. per year)' (IMO, 2018)
Hazard	'A potential to threaten human life, health, property or the environment' or equivalently 'the system states or the set of conditions that together with a worst-case set of environmental conditions will lead to an accident' (Leveson and Thomas, 2018)
Hazards identification analysis	'Structured process for identifying fault conditions that lead to hazards reducing the chance of missing hazardous events'(Glossop *et al.*, 2000)
Hazardous scenario	An accidental scenario which terminates at hazard (not accident or consequence)
Importance measure	Metric for assessing the contribution of a component, basic event or cut set to risk analysis result (Gomez, 1996)
Probability	'The relative frequency that an event will occur, as expressed by the ratio of the number of occurrences to the total number of possible occurrences'(IMO, 2018)
Risk	'The answer to three questions 1) What can happen (Accident scenarios), 2) How likely is it, and 3) What are the consequences?'(Kaplan and Garrick, 1981)
Risk analysis	'The process to comprehend the nature of risk and to determine the level of risk' (International Standardisation Organisation, (2018))
Risk assessment	'Overall process of risk identification, risk analysis and risk evaluation' (ISO, 2018)
Risk identification	Process of finding, recognising and describing risks (ISO, 2018)
Risk metric	'A quantitative expression that can be used to answer an aspect of the three questions of risk.' (Johansen and Rausand, 2014b)
Safety	'Freedom from unacceptable risk' (ISO, 2010)
Safety analysis	Equivalent to risk analysis (ISO, 2010)
Safety assessment	Equivalent to risk assessment (ISO, 2010)
Scenario	See above accident scenario

This page has been intentionally left blank

1 INTRODUCTION

1.1 Chapter outline

In this chapter, the PhD background and motivation are provided. Based on the PhD background and motivation, the selected scope, the aim, objectives and research methodology are presented. These sections then are followed by the thesis outline and the chapter summary.

1.2 Background

The continuous research and innovative projects developments have resulted in new types of systems implementing functionalities unforeseen in the past, thus requiring the development of new methods to ensure their safety (Leveson, 2011a). One category of such systems is the *Cyber-Physical Systems* (Leveson, 2011a, Sinha, 2014).

The term *Cyber-Physical Systems* (CPSs) was first introduced through a series of discussions between the members of academic staff at Berkeley University in 2006 (Gunes *et al.*, 2014). The CPSs can be defined as 'systems which collect the information from the physical environment using sensors and communication channels, analyse it using controllers and affect the physical environment and relevant processes through actuators to achieve specific goal during their operation' as show in Figure 2 (Gunes *et al.*, 2014). Compared with the mechatronic systems of the past, the CPSs consist of integrated components/subsystems and can be also interconnected with other CPSs (Hehenberger *et al.*, 2016).

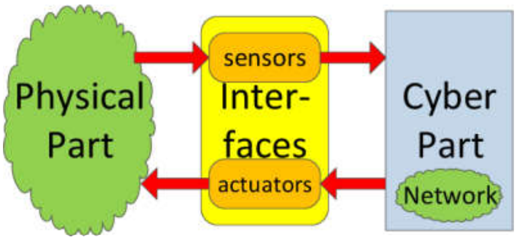


Figure 2 The structure of CPS (Steffen, 2017)

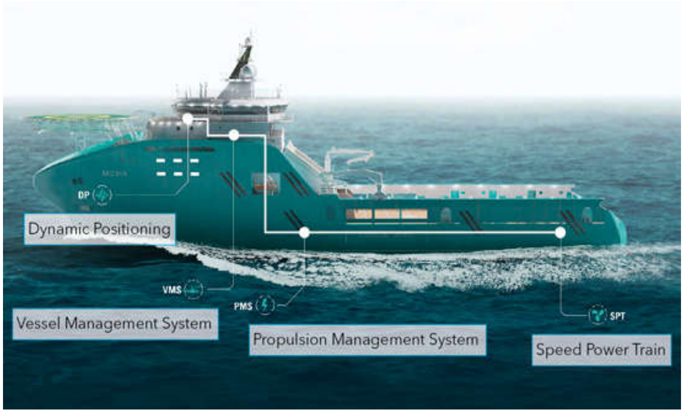


Figure 3 The CPSs of the ship (DNV GL, 2015).

The CPSs have been used and advanced in a number of application areas including automotive systems, avionics systems, defence systems, manufacturing systems, process control systems, traffic control systems, robots, smart medical devices, smart home applications and marine systems (Möller, 2016, Gunes *et al.*, 2014, Engell *et al.*, 2015, Hehenberger *et al.*, 2016). The list of the CPSs across the ship systems includes the Power Management System (PMS), the Diesel-electric Propulsion (DEP) system, the Safety Monitoring and Control System, the Dynamic Positioning System, and the Heat Ventilation Air Conditioning systems (DNV GL, 2015) (Figure 3). The list of the CPSs will be expanded further in autonomous ships, while the existing CPSs are being constantly evolving, obtaining new features and functions. The CPSs could be classified into three large categories (Figure 4), although there may be overlaps between these categories:

- Autonomous CPSs (ACPSs), which include the industrial and advanced robots and autonomous navigation systems (Guiochet *et al.*, 2017).
- Networked CPSs or Cyber-Physical Systems of Systems (CPSoSs), which are large, distributed systems, for example, the smart grids and the railway systems (Engell *et al.*, 2015).
- Industrial automation and Control Systems (ICSs), which are used to control the physical processes in the oil and gas industry, nuclear industry, etc. (Flaus, 2019, Kriaa *et al.*, 2015).

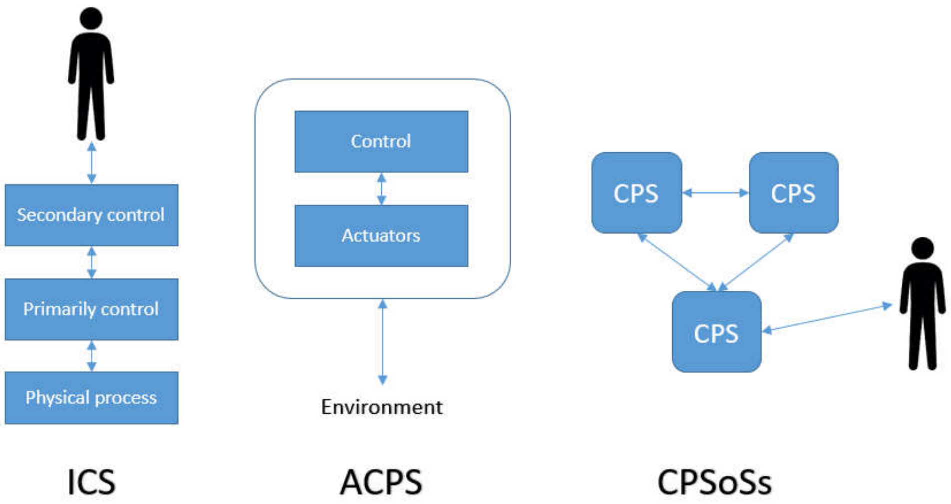


Figure 4 Types of CPSs.

1.3 Motivation

Safety is a key requirement for the CPSs, where *safety* can be comprehended as 'the freedom from those conditions that can cause death, injury, occupational illness and damage or loss of equipment or property' (US Department of Defence, 2012) or as 'the freedom from unacceptable risk of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to the property or to the environment' (ISO, 2010).

In this respect, it can be a special challenge to design safe CPSs as they belong to the category of *complex systems* (Sinha, 2014, Gunes *et al.*, 2014), where *complexity* expresses the increased unpredictability of the system behaviour, which may jeopardize its safe and reliable operation (Sinha, 2014, Johansen and Rausand, 2014a). The CPSs complexity leads to new unknown failure mechanisms, new unknown functional and structural dependencies, new hazards and risks (Zio, 2016b). The unpredictability in CPSs coexists with tight interactions between their components, especially between the cyber and the physical parts, allowing little "slack" or deviation in their functions/response (Qureshi, 2007, Sierla *et al.*, 2013, Bagade *et al.*, 2017). The combination of tight interactions with complexity is the perfect recipe for accidents, as small deviations, due to a component degradation or unpredicted environmental disturbances can lead to a new emergent behaviour (Perrow, 1999). In this respect, complexity negatively affects CPSs, rendering them *vulnerable*, where vulnerability is a 'weakness of a product or a system that may lead to the destruction if exposed to a threat' (Zio, 2016a).

Renown accidents in CPSs include the Ariane 5, the Mars Polar Lander (Leveson, 2004, Leveson, 2011a) and the Boeing 737-8 (MAX) accident (Komite Nasional Keselamatan Transportasi, 2019). During the landing of the Mars Polar Lander additional unexpected noise was generated. The system interpreted this as the fact that the landing had occurred and gave the order to shut down the descent engines causing the spacecraft to crash into the Mars surface. Similarly, in the Ariane 5 accident, the inertial reference software of the Ariane 5 was the same as for the Ariane 4, but the followed trajectory had been changed. This small difference led to the loss of the spacecraft. In case of the Boeing 737-8 (MAX) accident that occurred in Indonesia, a wrong sensor measurement in the manoeuvring characteristics augmentation system in combination with other factors lead to the loss of 189 passengers and crew (Komite Nasional Keselamatan Transportasi, 2019). These accidents and many others have led to a conclusion that the safety in general, and especially, for the CPSs must be viewed as an *emergent property* (Leveson, 2011a, Thompson *et al.*, 2015) and has to be addressed at the system level (Asare *et al.*, 2013, Reimann *et al.*, 2017).

The maritime safety has achieved significant improvement within the last century, with the annual loss rate declining from 3% to 0.25% in the beginning of the 21st century (Kristiansen, 2013). However, this number is several of orders of magnitude higher than similar numbers in aviation (IATA (International Air Transport Association), 2018, Eloranta and Whitehead, 2016). As the majority of accidents in the maritime industry have been attributed to the human factor (80%) (Hetherington *et al.*, 2006, Eloranta and Whitehead, 2016), it is expected that increased automation will drive to a better safety level (Kretschmann *et al.*, 2012, Eloranta and Whitehead, 2016) and cost-effectiveness (Jokioinen *et al.*, 2016). However, considering all the issues discussed above, it can be a special challenge to design safe CPSs. Furthermore, accidents in modern complex systems including CPSs may have more severe consequences in terms of financial loss, human losses and environmental damage compared to systems used in past (Leveson, 2011a). In addition, the present public's tolerance to accidents today is much lower, especially when it comes to autonomous systems, thus increasing the pressure on the involved authorities as well as the CPSs designers and operators (Leveson, 2011a). All this renders requisite further advancement and enhancement of CPSs safety assurance methods and techniques ensuring their cost-efficient design and operation.

At the same time, the ship propulsion and electric power generating functions of modern cruise ships are realised using the DEP system (Geertsma *et al.*, 2017). The loss of the electric power (blackout) on a cruise ship during the sailing or manoeuvring modes may result into a number of accidents such as collision, contact and grounding, which, in turn, may cause considerable human losses of passenger and crew (Nilsen *et al.*, 2005). As the cruise ship industry has been rapidly developing, with both the vessels size and number constantly growing (Cruise Lines International Association (CLIA), 2016), ensuring the passengers, crew and ship safety is a paramount necessity. Despite the redundancy incorporated in each DEP system design, a number of blackout incidences were reported for cruise ships with DEP or ships with similar power plants (Hossain *et al.*, 2013, MAIB, 2011, Rokseth *et al.*, 2017). The recent total blackout incident on-board a cruise ship (Ullah *et al.*, 2019), where all the generator sets in both engine rooms shut down due to a low lubrication oil alarm, provides a representative example of the potential safety, financial and social implications associated with blackout events. In this respect, it is important to minimise the blackout probability of the cruise ships power plant designs as well as to ascertain that adequate power will be available when required (DNV GL, 2016).

Another critical parameter is the significant cognitive load imposed by the ship systems on the cruise ships crew and operators. As referred previously, the DEP system belongs to the category of complex and cyber-physical systems (DNV GL, 2015) consisting from a significant number of heterogeneous components, interacting with each other in multiple ways. Such complexity leads to significant amount of alarms that the crew has to deal constantly (Stefani, 2013) and impeding the distinction of one critical alarm from the another. This type of cognitive operator overload has been identified as one of the contributory factors to Three Mile Island nuclear reactor accident (Malone *et al.*, 1980). In the recent blackout case on a cruise ship, whilst it still unclear why the crew accepted and cleared low lubrication oil alarms, this in combination with heavy roll and pitch led to loss of 3 Diesel Generators (DGs) out of 4 (AIBN (Accident Investigation Board Norway), 2019). Therefore, there is a need to support the human operator in decision-making during critical operations.

1.4 The PhD scope

1.4.1 Investigated methods

As CPSs can be viewed as complex systems, with respect to safety, it is important to push the available system information as far as possible from the area of unknown unknowns to the area of known knowns as shown in Figure 5 (Hafver *et al.*, 2017). Consequently, the safety of a CPS can be ensured if its behaviour is handled and well understood during its development. The more it is known about interactions and how to control them effectively, the more it is possible to intervene into the design and develop a safer system.

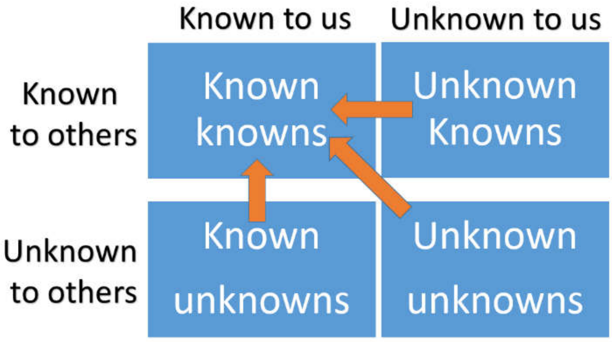


Figure 5 The problem of complexity handling. Adapted from (Luft and Ingham, 1961).

Although all the safety related activities are important, the hazard identification and risk analysis can be viewed as having higher importance for the safe system design. Hazard identification allow the identification of scenarios, which if not dealt properly will lead to an accident (Park *et al.*, 2018). Hazard identification and analysis is undertaken at an earlier stage and is used to derive the system requirements, guiding the system design and verification process (Leveson, 2011a). In addition, it is widely acknowledged that the earlier potential issues are identified, the lower will be the cost to fix them (INCOSE, 2015). Risk analysis is also widely used for verification and approval process as in automotive industry; however, it is heavily dependent on the hazard identification and analysis methods, as it is an important part of risk identification. Omitting a specific scenario can be more dangerous than improper ranking (Kaplan and Garrick, 1981).

For this reason, the discussion and developments in this thesis will focus on the hazard identification and analysis methods, excluding methods used for human reliability analysis, as it is out of the scope of the present research. Whilst the thesis will also discuss some issues related to cybersecurity issues, the detailed analysis and enhancement of systems resilience/safety against cyberattacks is out of the scope of the present research. Methods addressing the autonomous functions of CPSs will be also partly addressed, but the primary scope will be on internal system properties rather than interactions with surrounding environment.

1.4.2 The investigated systems

As referred in the introduction, CPSs represent a class of systems advancing in a number of application areas including the maritime industry (DNV GL, 2015). At the same time the ship propulsion and electric power generating functions of modern cruise ships are realised using the DEP system, which implements a function critical for the ship safety (Nilsen *et al.*, 2005). A blackout on a cruise ship may lead to significant safety and financial consequences. Therefore, the discussion and developments in this thesis will concentrate on the DEP system and blackout, with focus on the left side of the Bow Tie, without estimating the potential blackout consequences. The analysis will also not consider blackout due to human errors, flooding and cyberattacks. Fire will be considered on a very high level.

In addition to that, the open loop exhaust gases scrubber systems use has become popular due to recent regulatory restrictions on SOx emissions from ships (Panasiuk and Turkina, 2015). Open loop exhaust gas scrubber can be considered as a simple example of a CPS system, which is used for reducing the SOx emissions from ships engines. Its failure can lead to noncompliance with SOx emissions regulations which in turn may lead to SOx emissions deteriorating the air quality in the local area with negative effects on humans health (International Agency for Research on Cancer, 2012) and the environment as SOx emissions contribute to acid rains (United States Environmental Protection Agency, 2019). In addition, noncompliance with the SOx emissions regulations can result in significant financial sanctions against the ship owner/operator. Therefore, this system is worth of attention and its analyses can support the discussion and developments with respect to the DEP system.

The new developments in the safety area include the use of sensors measurements for better safety management (Knegtering and Pasman, 2013) based on Industry 4 revolution advancements. This include development of systems which integrate safety models with condition based monitoring data and existing monitoring systems(Aizpurua *et al.*, 2017a). It is expected that such systems will reduce the operator cognitive load (Papadopoulos and McDermid, 2001). At the same time DEP system proper management is important. Therefore, the discussion in this thesis will focus on developments in that directions in connection to the DEP system.

The investigation will focus on the systems, excluding the system interactions with humans, human operators and management systems.

1.4.3 The targeted audience

This PhD thesis will address issues of interest for the following public categories:

- Researchers conducting research in safety of CPSs.
- Safety engineers applying the hazard identification and risk analysis methods.
- Marine system designers and specifically the DEP and scrubber system designers.
- Classification society’s experts focusing on the above system and methods.
- DEPs and scrubber systems operators.

1.5 Aim, objectives and research methodology

The aim of this research thus is to enhance the safety of marine Cyber-Physical Systems by developing a novel safety analysis method and safety monitoring system. The specific objectives, related to the above-mentioned aim, are provided below. The research methodology and the objectives in connection with different Chapters are graphically depicted in the flowchart of Figure 6.

The set objectives are the following:

1. To investigate and critically review the challenges with related to the CPSs safety and how the hazard identification methods address them. (Addressed in Chapters 2 and 3).
2. To propose and develop a novel safety analysis method by addressing gaps in existing methods. (Addressed in Chapter 4).
3. To demonstrate the effectiveness of the developed novel safety analysis method by applying it to modern marine CPSs (DEP system, open loop scrubber). (Addressed in Chapters 5, 6 and 7).
4. To develop an automated blackout monitoring system supporting decision-making during a marine CPS operation based on the new method results and recent CPSs developments with application to the DEP system. (Addressed in Chapter 8).
5. To summarise the main findings, conclusions and contribution of this research and to propose new directions for further research. (Addressed in Chapters 9-10).

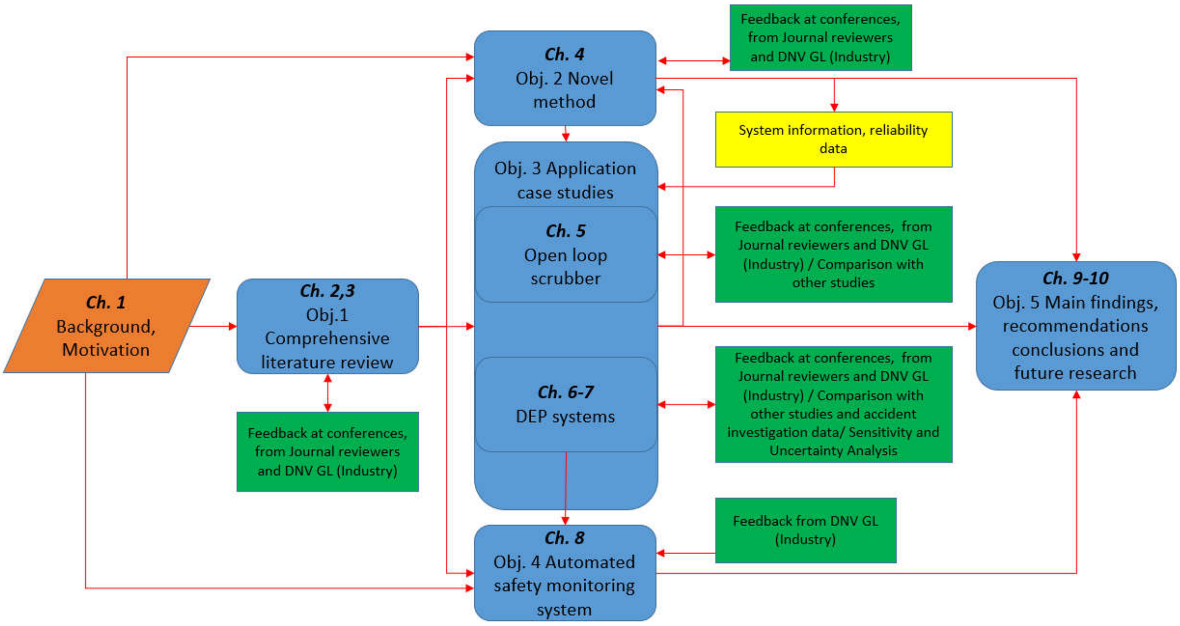

Ch. 1
Background, Motivation
Ch. 2,3
Obj.1 Comprehensive literature review
Feedback at conferences, from Journal reviewers and DNV GL (Industry)
Ch. 4
Obj. 2 Novel method
Feedback at conferences, from Journal reviewers and DNV GL (Industry)
System information, reliability data
Obj. 3 Application case studies
Ch. 5
Open loop scrubber
Feedback at conferences, from Journal reviewers and DNV GL (Industry) / Comparison with other studies
Ch. 6-7
DEP systems
Feedback at conferences, from Journal reviewers and DNV GL (Industry) / Comparison with other studies and accident investigation data/ Sensitivity and Uncertainty Analysis
Ch. 8
Obj. 4 Automated safety monitoring system
Feedback from DNV GL (Industry)
Ch. 9-10
Obj. 5 Main findings, recommendations conclusions and future research

Figure 6 Research methodology flowchart.

For the objective 1, the results are realised by conducting an extensive and systematic literature review on the CPS safety related properties and advantages/disadvantages of existing hazard identification and analysis methods on Google Scholar, Science Direct and Scopus using relevant keywords. The quality of the literature review results in ensured by reviewed by the experts in the area of CPSs safety during the journal review process and by safety experts at DNV GL and relevant feedback is provided and incorporated (Figure 6). These results and insights are used to develop the novel method in the objective 2.

For the objective 2, the novel method rationale, steps, used equations, method assumptions and consistency are ensured by the feedback provided during the relevant conferences, through article review process and by safety experts at DNV GL. The novel method is used then for the safety analysis of the relevant systems.

For the objective 3, the relevant input is gathered from a number of available sources, including manufacturer drawings, available publications, reliability databases based on the method needs. The results of the novel safety analysis method are reviewed by the partners at DNV GL and by the relevant journal/conference reviewers. In addition to that, the quality of results for the reference DEP system is enhanced by implementing sensitivity analysis with respect to some model parameters, applying uncertainty analysis and comparing results with relevant accident investigation data. The results of the objective 3 are used to enhance the novel method, to identify its advantages/disadvantages and derive safety recommendations for the investigated systems.

For the objective 4, the quality is ensured by receiving the relevant feedback from the safety experts at DNV GL. However, the results of this analysis were heavily based on the quality of results for objectives 2 and 3, so the quality was ensured before that.

For the objective 5, the quality is ensured through feedback provided by examining committee.

1.6 Thesis structure and overview

The thesis structure with respect to aim and objectives was provided in Figure 6. In this section, the contents of each Chapter are elaborated in more detail.

This thesis commences with the background, the motivation and generic aim and objectives of the conducted research in the Introduction (Chapter 1).

In Chapter 2, a general review of challenges and the CPSs safety related properties is provided. Subsequently, the focus of this chapter shifts to the review of hazard identification and analysis methods, where the different methods are compared and analysed for their suitability to the CPSs.

The literature review becomes more focused in Chapter 3, where literature related to the STPA, DEP propulsion systems and intelligent safety monitoring systems are further analysed and compared. Based on the results of this analysis, the literature review gaps and proposal for PhD research are provided.

In Chapter 4, the proposed novel safety analysis method is described and elaborated. This method steps are explained in detail and the assumptions required for the application of the method are also provided.

In Chapter 5, the investigated open loop scrubber system with relevant input is provided. Then the results of applying the novel method to the specific system are provided.

In Chapter 6, the reference and alternative DEP systems main parameters, functions and assumptions with respect to their operation are provided. Subsequently, the analysis input is also delineated.

In Chapter 7, the results of applying the CASA method to a number of DEP systems are provided and discussed.

In Chapter 8, the new safety monitoring system concept related to the operation of the DEP system is demonstrated. The method followed to simulate the DEP and estimate the safety metrics time variations as well as the method application are provided. In addition, the main functionalities of the novel concept are demonstrated through the presented application study.

In Chapter 9, the novelty, method advantages, main contributions and limitations of the present research are provided.

In Chapter 10, the main conclusions and findings of this research are summarised. Finally, suggestions for future research and reflection on research objectives are provided.

1.7 Chapter summary

The maritime industry has been developing rapidly employing new systems and technologies. In specific, Cyber-Physical Systems have been introduced to implement safety critical ship functions; therefore, ensuring their safe design and operation is of a paramount necessity. This thesis focuses on the hazard analysis methods, DEP and scrubber system and development of novel monitoring systems by targeting both industry and academia readers. The aim of this thesis is to enhance the safety analysis methods and suggest new systems for safety monitoring in CPSs. To ensure the results quality feedback from industry and academia, comparison with available studies and accident statistics are used.

2 BACKGROUND LITERATURE REVIEW

2.1 Chapter outline

The purpose of this chapter is to provide the necessary theoretical background required to justify the novelty and the rationale of the developed method. For this purpose, some safety-related properties of the CPSs are first identified based on the available literature. Then, the hazard identification and analysis methods are critically reviewed for comparing their effectiveness in identifying hazardous scenarios in the CPSs based on the relevant CPSs properties and previous research studies conclusions. Finally, the chapter findings are summarised.

2.2 CPSs safety related properties

A CPS, as can be inferred from the term, consists of two parts, the physical and the cyber. The cyber part represents the associated controller, whilst the physical part represents the controlled physical process and the components required to control the process. Both the physical and the cyber parts implement some assigned *functions* by transforming input into specific output (Buede and Miller, 2016). These functions are supported by *components,* which carry out some smaller functions at a lower level. To achieve a desired high-level function, these components are connected into an *architecture* (Buede and Miller, 2016). Compared to the typical systems though, CPSs react to the physical processes, thus it is important to understand their *response;* or in other words to understand the type and implemented sequence of functions and the reactions of the system to the environmental stimuli resulting into system transfer from a specific state to another (Banerjee *et al.*, 2012, Bujorianu and Piterman, 2015). Last, the overall system performance is affected by the management procedures and the associated *socio-technical* system (Leveson, 2012). These are provided schematically in Figure 7.

The *internal complexity* of systems can be classified as *structural, dynamic* and *organisational* according to pertinent literature in the context of the system design and development (Sinha, 2014, Zio, 2016a). Structural complexity is a characteristic of the systems that consist of a large components number and have unpredictable interactions among their components (Zio, 2016a, Sinha, 2014). Dynamic complexity exists when the comprehension of the system behaviour and system dynamics in time, including interactions with environment, is impeded (Sinha, 2014). *Organisational* complexity refers to the organisation of the group responsible for the design and the operation of the complex system (Sinha, 2014). Other CPSs safety related sources of complexity have been provided in Table 4. They are provided and are elaborated in the following paragraphs.

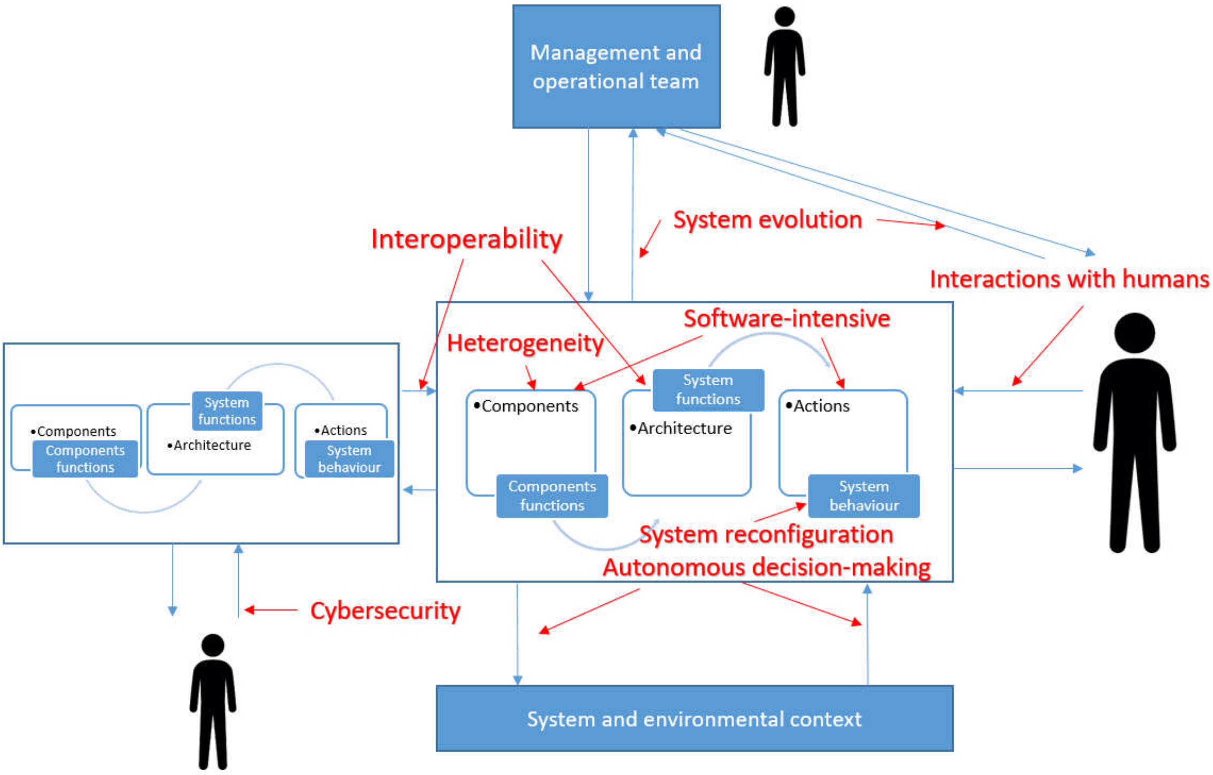


Figure 7 Description of logical elements of CPSs.

Table 4 Sources of complexity in CPSs.

Complexity dimension	Source	ACPSs	CPSoSs	ICSs
Structural (Sinha, 2014)	Heterogeneity (Rajhans *et al.*, 2014, Petnga and Austin, 2013, Marwedel and Engel, 2016)		√	√
	Interoperability (Gunes *et al.*, 2014, Möller, 2016)		√	√
	Connectivity (Marwedel and Engel, 2016, Wolf and Serpanos, 2018, Delange *et al.*, 2009, Schmittner *et al.*, 2015)	√	√	√
	Software-intensiveness (Bures *et al.*, 2015, Safety of Autonomous Systems Working Group (SASWG), 2020)	√	√	√
	Humans in the loop (Leveson, 2011a, Engell *et al.*, 2015, Reimann *et al.*, 2017)	√	√	√
Dynamic (Sinha, 2014)	Evolution in time (Engell *et al.*, 2015)	√	√	√
	Dynamic reconfiguration (Gunes *et al.*, 2014)		√	√
	Autonomous decision making (Murashov *et al.*, 2016)	√		
Organisational (Sinha, 2014)	The complexity of design and operation team	√	√	√

The complexity in CPSs can be attributed to the fact, that many CPSs are *heterogeneous* systems consisting of a considerable number of different components, such as mechanical, electrical, control and networking, which cooperate for an achievement of the desired system goal (Rajhans *et al.*, 2014, Petnga and Austin, 2013, Marwedel and Engel, 2016). The heterogeneity contributes to complexity, as it impedes an understanding of the system interactions, especially between the cyber and physical part, leading to subsequent unpredicted interactions (Sampigethaya and Poovendran, 2013, Liu *et al.*, 2017). The CPS design requires the involvement of engineers from different disciplines, which also contributes to *organisational* complexity.

The *interoperability* can be described as the ability of systems/components to work together for the achievement of the common goal in a System of Systems (SoS)/System (Gunes *et al.*, 2014, Möller, 2016). The interoperability in the CPSs can be viewed at a component level, as a result of interconnecting mechatronic systems and at a system level as a result of interconnecting a number of CPSs (Hehenberger *et al.*, 2016). Although this adds new functionalities to the systems, it enhances the complexity of CPSs due to the fact that the networking elements of CPSs obtain data from other CPSs or mechatronic systems, thus increasing the number and types of interactions (Johansen and Rausand, 2014a, Placke *et al.*, 2015, Reimann *et al.*, 2017, Kim and Kumar, 2012). Delays in delivery of information and loss of information from one computing element to other can lead to the realisation of significant hazards (Wolf and Serpanos, 2018, Kim and Kumar, 2012). Hidden defects of a component may expose the interconnected systems to cascading failures (Zio, 2016a, Jaskolka and Villasenor, 2017). In this respect, it is important to ensure that CPSs and their components are safely integrated (Lee *et al.*, 2012).

The interoperability of the systems very often comes along with their *interconnection*, but this leads to problems related to *cybersecurity* (Marwedel and Engel, 2016, Wolf and Serpanos, 2018, Delange *et al.*, 2009, Schmittner *et al.*, 2015). The relationship between safety and security in CPSs can be characterised as a relationship of conditional dependence, as cyberattacks can exploit deficiencies in the defence systems, protocols or human recklessness and directly affect the integrity or availability of the data and control systems (Wolf and Serpanos, 2018, Kriaa *et al.*, 2015). An example of compromising the system safety because of a breach of the cybersecurity was the case of the Stuxnet worm, which successfully destroyed the centrifuges pumps at Iranian nuclear facilities, impeding the process of uranium enrichment (Axelrod, 2013). Another example was a targeted attack on a steel mill in Germany, where attackers managed to destroy a blast furnace (Federal Office for Information Security, 2014).

CPSs are *software-intensive* systems, as the algorithms, software and hardware is a primary entity of the CPSs cyber part (Bures *et al.*, 2015, Safety of Autonomous Systems Working Group (SASWG), 2020). However, errors in algorithms, software and hardware are of a great concern for the designer (Lee *et al.*, 2012). As the functionalities of the CPSs increase, the number of interactions and potential errors in software also increases and the more likely a software error may lead to an undesired behaviour (Wolf and Serpanos, 2018). An accident can be also caused by a fully functional software, due to improper handling of the system requirements (Thomas, 2013). An outcome of a statistical study on medical safety-critical CPSs showed that about 33.7% of recalls of medical CPSs during 1999-2006 occurred due to a problem with the software (Bliznakov *et al.*, 2007). It was also observed that this trend was increasing reaching almost 50% between 2004 and 2005 (Bliznakov *et al.*, 2007). Another noticeable example of accidents caused by the software flaws is an accident with a radiation therapy machine Therac-25, which led six patients to death due to the radiation overexposure (Baier and Katoen, 2008).

Many of the CPSs involve *humans* in charge of the decision-making at a high level of control (Leveson, 2011a, Engell *et al.*, 2015, Reimann *et al.*, 2017). Inadequate communication between people and machines, due to the lack of proper situational awareness can lead to an accident (Leveson, 2011a, Allen *et al.*, 2018). The problem can also come from overreliance on the technology, as was revealed from the crash of Turkish Airlines flight in 2009 (Kevin Anthony and Masooda, 2014) and during the collision of a Tesla Model car in 2016 (National Transportation Safety Board (NTSB), 2017). Other problems include the loss of the short-term and long-term situational awareness due to the lack of system understanding and the deterioration of the skills required in critical situations (Stefani, 2013). The human factors can be seen as an additional component to CPSs adding interactions and non-linearity.

Several classes of CPSs are planned to operate for a very long period and during their operation, it may be required to add new functionalities or to improve their performance. Some CPSs also follow an evolutionary design process with new updated versions being launched constantly to the market. Practically it means that some of the CPSs components and functionalities can be changed (Engell *et al.*, 2015). In addition, the system components health deteriorates over time. Yet, it may lead to hazardous situations, as an improper software or hardware update or component degradation, through tight interactions may lead to an inappropriate behaviour of these systems. A typical example of such an accident was the Ariane 5 crash, where the inertial reference software that was installed on Ariane 4 was also installed on Ariane 5, but as the trajectory of Ariane 5 was changed it led to new inappropriate interactions (Leveson, 2011a).

Dynamic reconfiguration and *adaptability* can be defined as 'the capability of a system to change its state by adjusting its own configuration in response to different circumstances in the environment' (Gunes *et al.*, 2014). The dynamic reconfiguration and adaptability can be also expressed in terms of fault tolerance (Engell *et al.*, 2015, Yang *et al.*, 2010). This ability of CPSs is, to a great extent, supported by intelligent prognosis and diagnosis techniques and allows CPSs to fail safely, avoiding accidents (Engell *et al.*, 2015, Guillén *et al.*, 2016). Such initiatives exist in a number of application areas (Xu and Xu, 2017). Therefore, it is required to ensure that these reconfiguration functions, diagnostics and prognostics work properly taking into account the complexities of the physical processes and the system evolution in time (Lee *et al.*, 2012, SafeCOP, 2016, Goebel *et al.*, 2017, Reimann *et al.*, 2017).

Autonomous decision-making is robotic systems or autonomous CPSs property and can be defined as an ability to undertake decisions and to perform simple and complex tasks by considering the changes in the environment without human intervention (Murashov *et al.*, 2016). It is absolutely necessary to ensure that the autonomous CPSs can make decisions not leading to accidents (Reimann *et al.*, 2017). Such was the cause of an accident with an industrial robot that resulted in the death of a worker (Guiochet *et al.*, 2017). In addition, as the autonomous decision-making CPSs may rely on artificial intelligence and machine learning algorithms, their behaviour can be quite unpredictable, like in the case of the human-like robot Sophia, which "promised" to destroy humanity (Sputnik, 2016). This is attributed to the fact that these algorithms verification using available methods is quite challenging (Ghosh *et al.*, 2016, Huang *et al.*, 2017, Van Wesel and Goodloe, 2017).

Concluding the section, the CPSs can be viewed as complex systems. As it was demonstrated in the preceding paragraphs, the CPSs complexity leads to unpredicted interactions in CPSs and can be attributed to:

- Heterogeneity
- Interoperability
- Interconnectivity
- Software-intensiveness
- Interactions with humans
- Evolution in time
- Dynamic reconfiguration
- Autonomous decision making
- The complexity of design and operation team

The next section discusses the available hazard identification and analysis methods tackling the problem of complexity in the CPSs. The discussion will exclude the interactions with humans and organisational complexity, as it is out of the scope (Section 1.4.2).

2.3 Hazard identification and analysis methods limitations

Hazard identification and analysis is the process of defining all possible scenarios, which can lead to an accident. Hazard identification is a process dependent on the understanding of the safety engineer on how the accident can occur or, as otherwise stated, based on the accident models (Thomas, 2013, Johansen and Rausand, 2014a, Qureshi, 2007). A sequential accident model describes an accident as a chain of discrete events that occur in a particular order (Qureshi, 2007). The epidemiological accident models including the Swiss Cheese Model, view an accident as a result of a combination of inadvertent latent and manifest factors, addressing in this way the multi-point failures (Qureshi, 2007). The thinking according to epidemiological accident models has set the background for development of hazard analysis techniques as the Event Tree Analysis (ETA), the Failure Mode and Effect Analysis (FMEA) and the Fault Tree Analysis (FTA) (Qureshi, 2007). Systemic accident models describe the accident as an outcome of dysfunctional interactions between the system components (Qureshi, 2007, Johansen and Rausand, 2014a). Based on the systemic accident models, methods including the System-Theoretic Process Analysis (STPA) and the Functional Resonance Accident Model (FRAM) have been emerged. Failure Logic Synthesis and Analysis (FLSA) methods are mainly based on the idea of compositionality or that the system behaviour can be captured through a localised form of an FMEA. Fault Injection (FI) is a dependability technique, in which the system behaviour is analysed under the presence of faults and can be applied to a system abstraction, detailed system model or built system. Some of the fault injection methods, using model abstractions can be used for development of Fault Trees and consequent risk analysis.

A short description of the most commonly used methods according to literature such as in (IMO, 2018) is provided in the subsequent paragraphs. As there are at least 800 techniques, methods, databases or models for safety assessment (Everdij and Blom, 2016) and it would be impossible to provide an overwhelming picture for all the methods, the focus will be on few methods. An overview of the investigated methods effectiveness is provided in the form of a heat map in Table 5. The methods are assessed using qualitative ranking for their effectiveness in capturing specific CPSs complexity sources based on information in the identified and cited publications.

Table 5 Heat map on hazard identification methods for CPSs.

	PHA	SWIFT	FMEA	HAZOP	FTA	ETA	FHA	STPA	FRAM	FLSA	FI
Heterogeneity (Missing interactions between heterogeneous components)	+	+	++	++	++	++	++	++	++	++	++
Interoperability (Common cause failures/ dependencies between components/architecture)	+	+	++	+	++	++	++	+	+++	+++	++
Connectivity (Cyber-security threats)	+	+	++	+	+	+	+	++	++	++	++
Software-intensive (Control failures)	+	+	++	++	+	+	++	+++	+	++	++
Evolution in time (Model-based approach) (Socio-technical system/alterations in time)	+	+	+	+	+	+	+	+	+	+++	+++
Dynamic reconfiguration (Multipoint failures/Temporal relationships)	+	+	+	+	++	+++	+	+	++	+	+++
Autonomous decision-making (Environmental context)	+	+	+	+	+	+	+	++	+	+	++

High effectiveness: The method naturally leads to identification of related scenarios	+++	Moderate effectiveness: The method leads to identification/capturing of some related scenarios	++	Low effectiveness: The method leads to identification of limited number of related scenarios	+

Preliminary Hazard Analysis (PHA) also often called as HAZard IDentification (HAZID) (Rausand, 2013) is a simple method for identification of hazard and hazardous events, with wide application in maritime industry. It requires a team of experts and through brainstorming process generates an output of analysis, which is a list of hazards, their causes and potential control measures. Structured What-If (SWIFT) belongs to more advanced methods used for hazard identification and is suggested as a simpler alternative to HAZOP (ISO, 2009). In SWIFT, the facilitator and team members use standard 'what-if' type phrases to assess how a deviation in system behaviour will affect the overall system performance. Advantages include the applicability of these methods (PHA, SWIFT) with limited system information, early at the design stage and will little cost (ISO, 2009, Khan and Abbasi, 1998, Raspotnig and Opdahl, 2013). On the other hand, SWIFT is implemented rather on qualitative level and not on quantitative. PHA and SWIFT have been classified as methods with low creativity and they are not considered so systematic (Khan and Abbasi, 1998, Raspotnig and Opdahl, 2013), which has a direct impact on completeness of identified scenarios. For this reason these methods are suggested to be applied at initial system design phases as supplementary to more detailed methods (Raspotnig and Opdahl, 2013, ISO, 2009). In relation to autonomous CPSs, the PHA and SWIFT require appropriate modification to be able to identify more efficiently scenarios (Dogramadzi *et al.*, 2014). Hence, these methods effectiveness for tackling CPSs has been ranked as low.

Failure Modes and Effects Analysis (FMEA) is among the oldest methods used for safety assessment (BSI, 2006). FMEA is bottom-up or inductive hazard identification and analysis method. The method identifies the system components, the effects that components failure may have on the system, the potential causes for the system components failure and the proposed safeguards against their failures. FMEA is used for system design and manufacturing processes analysis. FMEA can be enhanced with ranking named Criticality Analysis (CA) to identify the most safety-critical scenarios. For its implementation, FMEA usually require system detailed information and is labour intensive (BSI, 2006, Thomas, 2013). Whilst FMEA is among the oldest methods used for safety assessment (BSI, 2006), it is not structured (Peeters *et al.*, 2018) but can be assisted by failure mode checklists (Raspotnig and Opdahl, 2013); therefore, FMEA can be efficient for hazard identification in heterogeneous systems. However, it captures the architecture only implicitly, which has an impact on identification of scenarios related to dependencies between components. Furthermore, FMEA was proved to support analyst to identify less interactions and software related failure modes than STPA (Sulaman *et al.*, 2017), which implies that FMEA is less efficient in addressing the software failures and raises concerns about addressing the common cause failures. It is widely acknowledged that FMEA is not supportive for tackling multi-point failure modes (Glossop *et al.*, 2000) and less suitable for describing complex logic (Khan and Abbasi, 1998). Modified FMEA versions were used for cybersecurity vulnerability assessment in systems (Schmittner *et al.*, 2015). However, FMEA tables number can be huge, which implies difficulty in handling the results of analysis and updating them (Thomas, 2013). Traditional methods including FMEA have been criticised for identifying failure related to autonomous functions implemented in robots and advanced CPSs (Dogramadzi *et al.*, 2014, Guiochet, 2016).

HAZard and OPerability studies (HAZOP) is a general method for identification of system deviations from the expected performance that lead to hazards (ISO, 2009). In this respect, HAZOP is more general than FMEA, although share similarities with this method. A major difference of HAZOP from FMEA is that it starts with the outcome, which is undesired deviation and proceeds to the identification of their causes. HAZOP is conducted by a group of experts, using a set of guidewords. Control HaZOP is a specific type of HAZOP, which is applied to safety critical instruments and control systems. As referred previously, HAZOP is among the most rigour methods for the hazard identification, as it is supported by a number of guide words (Raspotnig and Opdahl, 2013). Thus, properly selected guidewords can support the identification of heterogeneous failure modes. However, similarly with FMEA in HAZOP, multiple point deviations are not properly addressed (Glossop *et al.*, 2000). Furthermore, no specific guidance is given for the assessing how the deviations will impact the system. As a result capturing the event sequences and dynamic reconfiguration can be a specific challenge in HAZOP. Considering software, HAZOP has been criticised for ambiguity, incompleteness, nonsensicality and redundancy (Hulin and Tschachtli, 2011). A modified HAZOP has been applied for cybersecurity risk assessment purposes (Winther *et al.*, 2001). Similar with PHA enhancement is required for HAZOP when applied to ACPSs (Guiochet, 2016).

Fault Tree Analysis (FTA) is a top-down graphical hazard and safety analysis method (ISO, 2009). It initiates with an undesired event in system and deductively proceeds to identification of its causes. It represents the occurrence of a failure using a logical tree and describes all the conditions necessary for its occurrence. FTA can be used both qualitatively and quantitatively during design and operation (Kabir *et al.*, 2016). FTA has strong semantics for capturing the heterogeneous character of CPSs (Khan and Abbasi, 1998), however it does not provide any specific guidance for identification of heterogeneous failures using failures as in FMEA. Whilst FTA can be used to capture dependencies between functions and components failures (Thomas, 2013, Raspotnig and Opdahl, 2013), still some refinement can be required to incorporate common cause failures (Khan and Abbasi, 1998). FTA is not designed to capture the software failures in an explicit manner, which reduces its effectiveness in capturing the software and cybersecurity related failures (Dawson *et al.*, 2015). FTA can be used to derive failure paths or logical sequences, addressing in this way issues related to multipoint failures (Glossop *et al.*, 2000, Khan and Abbasi, 1998) by using some generic questions (Raspotnig and Opdahl, 2013), but the end criteria in FTA is not defined (Peeters *et al.*, 2018, Thomas, 2013). The FTA also struggles to capture some system temporal behaviour properties (Kabir *et al.*, 2016).

Event Tree Analysis (ETA) is a method used for identification of event sequences leading to specific accident scenarios (ISO, 2009). ETA is based on PHA and HAZOP results to identify specific initiating events and their propagation into accidents. Together with FTA, ETA can be used for estimation of risk in Bow Tie analysis. ETA has also strong semantics allowing inclusion of heterogeneous failures. Specific issues may arise due to the incorporation of the common cause failures, which require careful consideration (ISO, 2009). As it incorporates explicitly the events sequences, it is an appropriate method for capturing the dynamic reconfiguration in CPSs. However, ETA considers only one failure mode per event (ISO, 2009), so it can be inappropriate for identification of intricate software failure modes and consequently cybersecurity related hazards. Furthermore, ETA is usually dependent on other hazard identification techniques as PHA (ISO, 2009), so Event Trees completeness will depend on the completeness of the employed techniques.

Functional Hazard Analysis (FHA) method is used in aviation industry and military industry of the United States of America (Joshi *et al.*, 2006). The process is based on the identification of the system functions, their inputs and outputs and their failure modes (Scharl *et al.*, 2014). The failure modes with their causes are used for developing the relevant safety measures. FHA has been described as a structured approach for hazard identification and analysis (Raspotnig and Opdahl, 2013). It is similar in effectiveness to FMEA for addressing heterogeneity, but it incorporates more effectively the dependencies between the components and functions (Joshi *et al.*, 2006). Software failures can be also incorporated in this manner. However, a smaller number of scenarios were identified compared with STPA, when implemented to the same system. (Fleming, 2015). Sequential dependencies are not incorporated, whilst the technique does not seem to be addressing the issue of environmental context, which both are important in ACPSs.

In System-Theoretic Process Analysis (STPA), the system is represented by a control structure and the hazardous conditions are generated by the lack, the presence or the improper timing of the control actions (Leveson, 2011a). After the identification of the Unsafe Control Actions (UCAs), the safety engineer duty is to identify the underlying factors causing the occurrence of the unsafe control actions. The identified hazards, unsafe control actions and causal factors are used to develop safety related requirements. The STPA, as a top-down method, can be used to define more accurately the scope and the target of the hazard analysis. Moreover, it is capable of identifying the potential hazardous control actions by capturing the system context and in this way addressing sufficiently the software-intensive character of CPSs as well as identifying additional scenarios not captured by FMEA (Thomas, 2013, Sulaman *et al.*, 2017, Rokseth *et al.*, 2017). A number of studies applied to systems with control elements confirmed that some scenarios identified using STPA related to control functions where not tackled by using FMEA (Rokseth *et al.*, 2017, Sulaman *et al.*, 2017), PHA at initial design phases (Fleming, 2015), FTA (Ishimatsu *et al.*, 2010) or even HAZOP (Teikari *et al.*, 2014). In a controlled test study among master and bachelor students, results indicated that the STPA assisted in the identification of more software safety requirements than FMEA and FTA (Abdulkhaleq and Wagner, 2015). STPA can be also used in conjunction with other methods for cyber-security safety assessment (Young and Leveson, 2014). However, this method considers the system behaviour phenomena in a static way. It may provide information on specific hazardous control actions at different snapshots of the system life, but it cannot describe how these hazardous control actions will propagate into an accident, incidents or hazards (Abdulkhaleq and Wagner, 2013). Furthermore, the method was proved weaker in finding the single cause failures, albeit it has the potential for their identification (Sulaman *et al.*, 2017). Moreover, STPA is applied at a functional level, not considering the actual system architecture (Rokseth *et al.*, 2017). STPA was also criticised for applications in SoS, as it does not support identification of the environmental context variables (Baumgart *et al.*, 2018), which affects its applicability to ACPSs.

Functional Resonance Accident Model (FRAM) is a systemic approach for hazard analysis, according to which, accidents occur due to concurrent deviations from the standard performance of the system components (Qureshi, 2007, Yang *et al.*, 2017). In FRAM, the potential variabilities in system functions are identified and their impact on the overall system behaviour is assessed. In this way, FRAM emphasises the interactions between the subsystems and components (Tian *et al.*, 2016). FRAM has extensively applied in aviation systems (Tian *et al.*, 2016). It guides the identification of potential interactions between components (Tian *et al.*, 2016), although it may require to be complemented by an FMEA checklist to capture the heterogeneous failures of the system. Its efficiency in identifying hazards due to software failures is under question (Thomas, 2013). FRAM was applied for cyberattacks impact assessment, but it mostly focuses on socio-technical rather technical systems (Tian *et al.*, 2016, Patriarca *et al.*, 2017). Some dynamic features seems to be captured by the method (Hollnagel, 2012).

Failure Logic and Safety Analysis (FLSA) methods are based on system models extended with fault models capturing the components malfunctions (Joshi *et al.*, 2006, Lisagor *et al.*, 2006, Adler *et al.*, 2010, Kong *et al.*, 2017). Two elements are essential for the analysis, the system architecture and the component failures (Sharvia *et al.*, 2016). The fault model represents the failure and fault modes of the each component, as well as how they can be triggered and how they are propagated to the other components (Adler *et al.*, 2010, Li and Li, 2014, Joshi *et al.*, 2006). FLSA methods can be used to derive automatically Fault Trees and FMEA tables using appropriate algorithms. Examples of FLSA methods include HiP-HOPS, Design Structure Matrices, Architecture Analysis and Design Language (AADL) methods. FLSA methods add rigour to the analysis as it is a Model-Based Safety Assessment (MBSA) approach (Papadopoulos *et al.*, 2016). In FLSA methods, dependencies between components are explicitly captured in model and are used as input in analysis (Joshi *et al.*, 2006). Still the consideration of potential software failure mode can be enigmatic, as this approach is dependent on a localised FMEA form; thus, it inherits all its limitations. When updated with appropriate semantics, FLSA methods can be used for cybersecurity assessment (Delange *et al.*, 2009). However, FLSA methods do not effectively represent the system behaviour, as it does not consider system functions in time (Sharvia *et al.*, 2016). So, it seems not to be applicable for identification of scenarios in ACPSs.

Fault Injection is a dependability technique, in which the system behaviour is observed under the presence of faults to guarantee that the system behaviour will be sound despite the presence of malfunctions in the system (Gamble *et al.*, 2014, Elks, 2012, Adler *et al.*, 2010). A number of fault injection methods was based on the system abstraction including the COMPASS toolset, the AADL based methods and the Alta Rica language. Fault injections methods can be also used for development of Fault Trees and FMEA tables. Fault injection to detailed models and systems, as well as testing applied to the models of the systems or real systems is more suitable for addressing the system heterogeneity and components dependency (Wolf and Serpanos, 2018). The system behaviour and reconfiguration functions can be assessed with the assistance of fault injection methods (Sharvia *et al.*, 2016), but it is under question if all the multipoint failures can be addressed due to state-explosion problem. Several other limitations exist in using these methods as well, like dependence on localised form of FMEA method or FMEA, issues with completeness and hardship to represent results in easy and comprehensive way (Sharvia *et al.*, 2016). As an MBSA approach, still it can be very convenient for controlling the system modifications and safety assessment updates.

It is deduced from the preceding analysis that none of the methods is the best for identifying all the scenarios in the CPSs. These methods are either incapable or do not provide effective guidance on tackling specific safety related CPSs properties. The preceding analysis results are summarised as follows.

- PHA and SWIFT have applicability at initial design stages and may struggle with identifying complex accident scenarios.
- FMEA can be viewed useful in capturing some of the safety properties but may be inappropriate for incorporating multipoint failures and software failures.
- Being a rigour method, HAZOP still may not support analyst identifying multipoint failures and software related failures.
- FTA can be used to identify and model multipoint failures but does not support so effectively interaction and software failures identification.
- ETA can be used to identify failure sequences but may be not suitable for identifying complex accident scenarios.
- FHA can be useful for identifying dependencies among components and system functions but does not consider the sequential effects.
- STPA is capturing complex software interactions in system but is disconnected from the system architecture.
- FRAM is focusing on component interactions but has been applied more to socio-technical than technical systems.
- FLSA methods are suitable for capturing the components interactions and system modifications fast hazard identification and analysis. Still they seem to be incapable of confronting complex temporal relationships.
- Fault injection methods can be useful for representing interactions in system, but not for multiple failure modes.

Considering the STPA effectiveness in identifying scenarios compared with other methods, especially with respect to interactions and software functions in systems, which are very important in CPSs, it has been decided to focus more on this method and associated research studies in the next chapter. FLSA seem to be also good methods, but developments in this direction would require significant resources. FI methods are applicable at a later design stage, therefore, their use would not support the generation of safety requirements.

2.4 Chapter summary

In this chapter, the main CPSs complexity sources were identified and then hazard identification methods were assessed for their effectiveness in identifying the scenarios connected to these CPSs complexity sources based on available research studies. The results of this analysis suggested that none of the main hazard and widely used identification methods is supportive enough for identifying all the accident scenarios attributed to different sources of complexity in CPSs. As demonstrated though from the previous studies analysis, the STPA supports better the analyst for identifying scenarios compared with other methods, especially for interactions and software related functions in CPSs.

This page has been intentionally left blank

3 RELATED WORK REVIEW

3.1 Chapter outline

The literature review become more focused in this Chapter. First, the System-Theoretic Process Analysis (STPA) related research is further elaborated and critically reviewed. Subsequently, a literature review results on to the ship power plants reliability, availability, and safety assessment and on related automated safety monitoring systems studies are provided. Based on the findings, the research gaps with respect to the STPA method, the investigated power plant and safety monitoring systems are identified. The selected research gaps also provided.

3.2 STPA-based research studies

In this section, a number of previously published studies that were dedicated to improving or supplement the STPA are critically reviewed. As the present thesis focuses on CPSs technical related properties, the STPA studies focusing on socio-technical aspects were excluded from this review. The related research studies are split into the following categories:

- Enhanced STPA approaches, either implemented in semi-automatic way or facilitating STPA application and improving its quality.
- Automated STPA approaches, where at least one of the STPA steps is implemented fully automatically based on a formal system model representation.
- Group of research studies, where STPA was combined with other hazard identification and analysis methods.
- In other research studies where STPA was integrated with design methods and modelling techniques.

The new methods have been assessed based on the previously identified CPSs safety-related criteria (Chapter 2) and based on the available information presented in the published studies. Additionally to these criteria, three utility criteria have been added to the assessment retrieved from (Dawson *et al.*, 2015) and (Papadopoulos and McDermid, 2001) (a) the risk estimation criteria, depicting the ability of the method to allow for the comparison of two similar systems safety based on the safety metrics; (b) ranking criteria, according to which, it is investigated whether the different failure modes are ranked and prioritised in employed approach or importance measures are estimated; (c) suitability of the approach for automated safety monitoring of a system function. The additional criteria are added to depict new developments in STPA with respect to its use and suitability for safety analysis. The results of this review are provided in Table 6, whilst they are further elaborated in the subsequent sections.

Table 6 Gap analysis of existing research studies on STPA method.

	Research studies	Enhanced STPA approaches								Automated approaches			Combined with other safety methods					Integrated with design methods					
Criteria		Initial STPA	Thomas (2013)	Abdulkhaleq and Wagner (2013)	Asare *et al.* (2013)	Zhong *et al.* (2015)	Procter and Hatcliff (2014)	Gurgel *et al.* (2015)	Chen *et al.* (2018)	Wang *et al.* (2016)	Liu *et al.* (2016)	Zhu *et al.* (2018)	Faiella *et al.* (2018)	Wheeler *et al.* (2016), Clark *et al.* (2018)	Combination with cybersecurity methods	(Zhang *et al.*, 2019)	Utne *et al.* (2020)	Dokas *et al.* (2013)	(Dakwat and Villani, 2018)	(Han *et al.*, 2019)	(Abdulkhaleq *et al.*, 2015)	(Becker, 2018)	(Alemzadeh, 2016) (Rokseth *et al.*, 2018)
Efficiency criteria	Heterogeneity (Missing interactions between heterogeneous components)	++	+++	++	++	++	+++	+++	++	++	++	++	++	++	++	++	++	++	++	++	++	++	++
	Interoperability (Common cause failures/ dependencies between components/architecture)	+	+	+	+	+	++	+	+	+	+	++	+	++	++	++	++	+	+	+	+	++	++
	Connectivity (Cyber-security threats)	++	++	++	++	++	++	++	++	++	++	++	++	++	+++	++	++	++	++	++	++	++	++
	Software-intensive (Control failures)	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++
	Evolution in time (Model-based approach/alterations in time)	+	++	+	+	++	++	++	+	++	++	++	+	+	+	++	+	+	++	+	++	++	+
	Dynamic reconfiguration (Multipoint failures/Temporal relationships)	+	+	+	+	++	+	+	+	+	++	+	+	++	+	+++	+	+	+	+	+	+	+
	Autonomous decision-making (Environmental context)	+	+	+	+	+	+	+	++	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Utility criteria	Risk metrics criteria estimation	+	+	+	+	+	+	+	+	+	+	+	+	++	+	+++	++	+	+	+	+	+	+
	Scenarios ranking	+	+	+	+	+	+	+	+	+	+	+	+	++	+	+	++	+	+	+	+	+	+
	Automated safety monitoring system	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	++	+	+	+	+	+

High effectiveness: The method naturally leads to identification of related scenarios / risk metrics estimation / ranking based on importance criteria / development of model fit for automated safety monitoring including sensors measurements	+++	Moderate effectiveness: The method leads to identification/capturing of some related scenarios / approximate risk metrics estimation / qualitative ranking / development of model fit for some scenarios automated safety monitoring with indication of how to integrate with sensors	++	Low effectiveness: The method leads to identification of limited number of related scenarios /no risk metrics estimation / no ranking / model not fit for automated safety monitoring or no integration with sensor measurements	+

3.2.1 Enhanced STPA approaches

Thomas (2013) formalised the STPA application to enhance Unsafe Control Actions (UCAs) identification. In this approach, the control actions are assessed for their relation to safety based on the system context, expressed using context tables. Based on the context tables, the hazards, source controllers, set of control actions, process variables and potential values for each variable are expressed using formal language. This is required for the first step of STPA. With the support of some rules, this approach allowed facilitation of UCAs identification. The new approach was applied to nuclear power plant system. Whilst the context tables can give a broader system context, in which the UCAs can be generated, add rigour, and facilitate the analysis, these ignore the actual sequence of UCAs, which will be undertaken in the system. The automation is also not complete, which impedes the analysis efficiency and completeness. Importance analysis and risk assessment were also out of scope of this work. The analysis is implemented on functional level disconnected from actual system architecture and consider the dependency between components only implicitly. As all the other method presented in this (3.2.1) and next section (3.2.2), this method does not aim to support development of automated safety monitoring system.

Abdulkhaleq and Wagner (2013) proposed the use of STPA along with finite state machines to connect the control actions, hazards and controller states. In the suggested method, the process model of each controller is used to model the dynamic behaviour and safety constraints of system and to analyse whether control actions lead to hazards. The approach was applied to car anti-locking system. Whilst finite state machines similarly with context tables can give a broader system context, in which the UCAs can be generated, and the finite state machines can be used to comprehend the system dynamics better, there is very little automation in the presented approach. The idea seems to require further development to demonstrate its applicability to more complex systems and its use in connection with criticality and risk analysis.

Similarly, Asare *et al.* (2013) suggested a formal framework for the initial STPA steps to ensure completeness in the hazard identification process by representing the system using finite-automata. The approach was demonstrated on aerospace transport vehicle. However, the approach still required significant input from analyst who would have to define, which event sequences are hazardous and which not and offered very little automation. No ranking accompanied the study.

Zhong *et al.* (2015) have used the Unified Modelling Language (UML) to support STPA steps. The UML views were used to establish the object, functional and dynamic system model and each of the views was used to support the hazard analysis. The applicability of this approach was demonstrated on train door controller example. As previous study, there was no follow up application to complex system and no ranking. The use of UML notations was considered the events sequence only for better system representation and not for hazard analysis purposes.

Procter and Hatcliff (2014) combined STPA with system modelling in the Architecture Analysis and Description Language (AADL) to assist the STPA, FMEA and FTA and their results reporting. The interaction between the STPA and between failures denoted in AADL model assisted the STPA implementation. This approach was applied to a medical patient-controlled analgesia pump. Whilst this methodology is in direction to bridging the gap between system models and STPA, it remained at concept level and requires reinforcement and improvement. This also offers a platform for identifying adequately the physical failures in the system. All the other STPA limitations have not been addressed too.

Gurgel *et al.* (2015) proposed the use of rules which can be used to derived hazardous combinations of context and control actions based on the analysis results for speeding up the STPA. This is a modest concept idea and allows automation of some activities. Still, it was applied to train controller, which is rather a simple system. The other STPA limitations hence have not been addressed.

Chen *et al.* (2018) suggested a formal approach for identifying process variables required for STPA. According to that, the process variables can be identified by observing monitored variables, controlled variables, input, and output variables of controller. The approach was applied to automatic train door controller. This approach seems to be enhancing the STPA, focusing on ACPSs, but not addressing the other limitations of the method.

3.2.2 Automated approaches to STPA

Wang *et al.* (2016) proposed a model-based approach for STPA. According to that, a coloured Petri net model was used to represent the socio-technical control structure. Whilst STPA guiding failure modes were used to identify the UCAs, causal factors for UCAs were identified via state space reachability graphs base on the Petri net model of control structure. The approach was applied to Chinese Train Control System. However, the UCAs were identified manually, and only their causes and sequence could be retrieved in an automated way.

In order to capture the temporal relationships between the inadequate control actions, which may also have an impact on system hazards, Liu *et al.* (2016) combined the STPA with control action temporal logic to identify the combination of control actions that can lead to hazards. According to this approach, network control action relation model for system components is developed, depicting the system behaviour. Then appropriate search algorithms are used to identify the UCAs. In this study some combinations of UCAs at different times leading to hazards were identified in an automated way but, there was no further consideration on how to apply them for quantitative safety assessment or analysis. In the research studies of Wang *et al.* (2016) and Liu *et al.* (2016), there has been no consideration of how to analyse further the physical failures and to incorporate the actual system architecture as their approaches has been applied to a sociotechnical system.

Zhu *et al.* (2018) were also motivated to use model-based approach for representing and analysing the vehicle control systems in line with STPA. The system was represented using Control Logical Petri Nets, whilst four types of dysfunctional interactions, leading to conflicts were identified using reachable tree. Whilst this approach is automated, it does not consider the temporal relationship between the control actions and focuses only on conflicting control actions, so cannot be considered as complete. Although, it is applied to a technical system, it does not consider the actual architecture and physical failure modes as well.

3.2.3 STPA combined with other safety methods

Faiella *et al.* (2018) combined STPA, Healthcare FMEA and Systematic Human Error Reduction and Prediction Analysis for investigating the safety assessment of a socio-technical healthcare system. However, they used STPA as supplementary to Health FMEA and Systematic Human Error Reduction and Prediction Analysis. Again, the method has its applicability to socio-technical systems.

Wheeler *et al.* (2016) used STPA results to update an FTA of a nuclear reactor and combined it with cyber-attack graphs to capture more accurately the impact of potential cyber-attacks. Similarly Clark *et al.* (2018) used STPA to update their FTA results for nuclear power plant subsystem in combination with ETA for determination of consequences. This approach is better aligned with the needs of safety analysis for technical systems with a potential to be applied for scenarios ranking and risk estimation, although their application was not demonstrated. It still can be criticised for the use of FTA, as the FTA consider only implicitly the events sequence that would occur in the system. It is under question whether the method considered appropriate refinement for the common cause failures after updating the Fault Tree as well.

In another developed method (Sabaliauskaite *et al.*, 2018) STPA was integrated with a six-step model and attack tree analysis to align safety assessment with cyber-security assessment. Similarly, Triginer *et al.* (2020) suggested the parallel use of ISO 26262 (ISO, 2011), STPA and STPA-sec (Young and Leveson, 2014) for deriving safety and security requirements. Glomsrud and Xie (2019) suggested the combination of STPA and attack trees for identification of cyber-attacks induced accident scenarios. All these approaches contribute to tackling the problem of cybersecurity of the CPSs but do not address the rest.

Zhang *et al.* (2019) integrated STPA with availability assessment based on stochastic petri nets, which is a method widely used for safety analysis. Such analysis supported the estimation of frequency of specific accident scenarios identified by STPA. In this way some sequential failures can be addressed capturing the dynamic CPSs nature. However, such an approach did not allow an implementation of ranking due to significant computational cost for simulations. Hence, it would be challenging to use such a model for automated safety monitoring. It would be interesting to see application of this approach to a more complex systems and accident scenarios. A significant advantage of stochastic petri nets is that is a model-based approach, which supports the repeatability of analysis.

Utne *et al.* (2020) suggested using the STPA results to generate Bayesian Belief Network (BBN). The new method was applied for a navigation and collision avoidance system of an unmanned autonomous ship. The advantage of this approach is that the STPA results after small refinement can be integrated in BBN structure. In this way a top node of the BBN can provide a functional alert for an ACPS. BBN can be updated easily to Dynamic BBN and the risk estimation can be updated based on new information. Thanks to incorporation of STPA results the method also considers explicitly the potential software failures. The method could potentially to be integrated with cybersecurity risk assessment methods. However, due to simplicity of application case study, it was not clear how the sequential dynamics could be incorporated in such approach. It would be expected that some information with respect to the functionality of mitigation/preventative barriers on between UCAs, hazards and accidents sequence is provided. No practical demonstration of estimating the risk or importance measures was provided as analysis has been implemented on a qualitative level. It is not a model-based approach as well, which impedes updating the results of the safety analysis, in case new functions/systems are added.

3.2.4 STPA combined with other methods

Dokas *et al.* (2013) extended the STPA with an additional step aiming at identifying early warning signals for causal factors. The approach was applied to drinking water treatment system. Whilst this approach is useful for developing an alarm monitoring system for a CPS, it does not allow risks metrics estimation and importance measures estimation. The different parameters of safety monitoring system are selected independently from each other. No other accident scenarios have been considered as no other hazardous methods have been employed.

Dakwat and Villani (2018) combined STPA and UPAAL model checking in parallel for the purposes of safety assessment and system safe design. The approach was applied to an anthropomorphic robot used in aviation for training purposes. The STPA results were used to propose system modifications, whilst the UPAAL model checking to verify safety and other properties. This approach add rigour to the hazard analysis results incorporation but has no direct impact on the STPA results themselves. Still the interconnection with models supports the implementation of necessary updates in system after a system modification.

Han *et al.* (2019) used STAMP framework to complement train control system verification. In this study, STPA was used to understand and model the system for hazard analysis. Then the safety verification problem was decomposed to into safety verification of smaller control loops. In this case, as above, the verification process had little impact on the STPA results but instead supported the verification of system requirements.

Abdulkhaleq *et al.* (2015) suggested the use of STPA along with model checking and testing for verification of software safety requirements. The approach was demonstrated on software code of an adaptive cruise control system, demonstrating that the safety related requirements are satisfied. This approach is software oriented and supports the identification of software bugs. It can also support a safe system software update. Still it does not support identification of further scenarios, risk metrics and ranking.

Becker (2018) suggested integrating STPA with standard system engineering methods. According to this approach, STPA and safety-driven system design modification are implemented one after another, as the design proceeds from coarser to more detailed design. Functional and building blocks diagrams were used for that, with application to ventilator system. Such approach allows to increase the rigour in analysis through greater interconnection between system architecture and STPA results, as they are constantly reviewed. Still, it has only indirect impact on quality of hazard analysis results.

Alemzadeh (2016) implemented hazard identification using STPA and then the identified faults were injected to the robotic surgical platform either to software or hardware part of the real system during runtime using GNU Project Debugger for Linux. Such approach allows impact assessment of different faults in the system by considering all the potential interactions and reconfiguration functions. Still it can be applied only at later stages of system design and cannot be used to address multi-point failures. Similarly, (Rokseth *et al.*, 2018) suggested using STPA to derive testing requirements in addition to functional and FMEA derived requirements. The method allowed to identify new safety-based testing scenarios for ship power management system. This approach can be useful for verification and validation of system design as well. However, this approach was not tested on a real or virtual system and it would be interesting to see its application.

3.3 Research on reliability, availability, and safety of ships power plants

According to the existing regulatory framework, a modified version of the FMEA method is required for the availability assessment of the cruise ships propulsion and other systems after flooding and fire to ensure the vessel safe return to port after an accident (Safe Return to Port regulations) (DNV GL, 2016). Furthermore, a functional FMEA is implemented for vessels with dynamic positioning capabilities to ensure that no single failure will lead to loss of power required for critical systems operations (Rokseth *et al.*, 2017). In addition, several recent studies focused on the reliability and availability assessment of the ships DEP plants. The assessment of the implemented studies with respect to their effectiveness on capturing the safety assessment method requirements for CPSs is provided in Table 7.

Chang *et al.* (2008) employed Reliability Block Diagrams to estimate and compare the availability of various power plant alternatives for an Liquefied Natural Gas carrier using the OREDA database data (OREDA, 2002). According to the results of this analysis, the dual fuel electric propulsion system exhibits the lowest availability, followed by dual fuel mechanical propulsion and single fuel diesel-mechanical propulsion. In addition, a high-level FMEA was implemented for the dual-fuel propulsion systems. However, the control failures and availability of the investigated propulsion plants control systems were not considered.

Vedachalam and Ramadass (2017) compared the reliability of different Dynamic Positioning systems, also addressing the reliability of ships DEP systems. These systems were analysed using the FTA method and the overall reliability of the systems was estimated considering the reliability of their components. The results demonstrated that significant improvement in the overall system reliability could be achieved by increasing the redundancy in the power plant. Still, the control and software functions of the DEP, such as the failure to reduce the propulsion power or unavailability of heavy load reducing functions, were not considered. These functions have significant influence on the blackout susceptibility.

Dubey *et al.* (2015) compared the reliability of a planar and a three-dimensional ship power networks using a combination of FTA and Markov models. According to the conclusions of their study, the calculated system reliability differences were insignificant. Yet, this study primarily focused on the power network components used for electric power distribution; in specific, the circuit breakers, the buses and the converters, whilst not considering the reliability of the generator sets or the control systems and the impact of these components reliability on the overall system safety.

Santoso *et al.* (2015) also compared the reliability of different DEP plants topologies in terms of their ability to respond to the system demands, reporting small differences in the reliability of the investigated alternatives. Moreover, they applied a qualitative functional Failure Modes and Effects Analysis (FMEA) for investigating the interactions between the different sections of the DEP plant. This study also did not incorporate the reliability of generators or control systems.

Rokseth *et al.* (2017) and (Rokseth *et al.*, 2018) applied the STPA to a generic DEP plant by focusing on the identification of factors that can lead to blackouts. With the assistance of STPA, they identified new causes and scenarios leading to a blackout. This analysis results also demonstrated that the STPA captures more effectively the software-intensive character of the DEP plant than the dynamic-positioning FMEA, although these two approaches seem to be complimentary according to their study. However, prioritisation or ranking of the identified hazardous scenarios was not considered.

Menis *et al.* (2012) proposed the simultaneous application of the FTA and the FMEA for a cruise ship DEP hazard analysis to define the hazardous scenarios. In their presented study a physical breakdown of the system was implemented, which supported the FTA. A modified version of FMEA was used for the identification of hazards as well. Still, this study has been applied on a high-level and qualitatively without estimating any safety metrics.

Jeong *et al.* (2018) compared the conventional, the diesel-electric and the hybrid propulsion systems for a roll-on/roll-off ferry by converting risk into cost. The safety analysis was conducted using FMEA estimating some risk priority numbers. It was concluded that the hybrid propulsion cost is less than the diesel-electric system cost, whereas the DEP plant cost is lower than the conventional mechanical propulsion system cost. Still, the considered failures in the FMEA are high-level failures. The contribution of different control failures has not been evaluated, whilst the influence of different failures on the blackout probability has not been assessed.

As it was reported in (Roskilly, 2016), the calculation of availability and reliability of a containership power plant with and without power shedding functions was realised by using the Fault Tree derived from the HiP-HOPS method (Papadopoulos and McDermid, 1999). The results indicated that the two systems have almost identical reliability and availability. However, the frequency (or probability) of safety-related events including blackout estimation was roughly approximated and reasoned (Roskilly, 2016). It is expected though that the safety of the system with power reduction functions would be improved. This indicated that the followed method was not adequate to capture the safety enhancement due to the alternative systems design.

Aziz *et al.* (2019) developed a Fault Tree of the power trip loss based on accident investigation data for an ice class bulk carrier. In the developed Fault Tree, they have incorporated some control failures and electrical failures. Yet, the developed Fault Tree did not incorporate sequential dependencies. The control failures also lacked specificity. Since, it is based on accident investigation data, the developed Fault Tree incorporates only the scenarios that had occurred. New hazardous scenarios, which can be anticipated and had not occurred, were not incorporated.

Table 7 Evaluation of research studies and methods employed for ship power systems hazard and safety analysis.

Study / Method	Efficiency criteria							Utility criteria			Comment
	Heterogeneity	Interoperability	Connectivity	Software-intensive	Evolution in time	Dynamic reconfiguration	Autonomous decision-making	Risk criteria estimation	Scenarios ranking criteria	Automated safety monitoring system	
DNV GL (2016) / FMEA	++	++	+	+	+	+	+	+	+	++	To assess the availability of systems after flooding / fire No safety metrics are estimated
Chang *et al.* (2008) / FTA and FMEA	++	++	+	+	+	++	+	++	++	++	Applied on a very high level / Applied to LNG carrier / FTA used for availability comparison, FMEA on qualitative level
Vedachalam and Ramadass (2017)/FTA	++	++	+	+	+	++	+	++	++	++	FTA of dynamic positioning system / Applied to offshore support vessel / Reliability metrics estimated
Dubey *et al.* (2015) and Santoso *et al.* (2015)	++	++	+	+	+	+	+	++	++	++	Main engine and generator not included in analysis / Applied to military ship / Reliability and availability metrics estimated
Rokseth *et al.* (2017) and Rokseth *et al.* (2018)/ STPA	++	+	++	+++	+	+	++	+	+	+	Applied to a generic Power Management System / Qualitative study
Menis *et al.* (2012) / FTA and FMEA	++	++	+	+	+	+	+	+	+	++	Applied to cruise ship propulsion system but only qualitatively
Jeong *et al.* (2018) / FMEA	++	++	+	+	+	+	+	+++	+	++	Implemented using high level FMEA / Applied to a Ferry
Roskilly (2016) / Hip-HOPS	++	+++	+	+	+++	+	+	+++	+++	++	Reliability metrics estimation / Applied to a containership
Aziz et al. (2019) / Fault Tree	++	+	+	++	+	+	+	++	+++	++	Developed based on accident investigation data / Generic power system

High effectiveness: The method/study naturally leads to identification of related scenarios / risk metrics estimation / ranking based on importance criteria / development of model fit for automated safety monitoring including sensors measurements	+++	Moderate effectiveness: The method/study leads to identification/capturing of some related scenarios / approximate risk metrics estimation / qualitative ranking / development of model fit for some scenarios automated safety monitoring with indication of how to integrate with sensors	++	Low effectiveness: The method/study leads to identification of limited number of related scenarios / no risk metrics estimation / no ranking / model not fit for automated safety monitoring or no integration with sensor measurements	+

3.4 Automated safety monitoring systems

The accidents in complex systems occur due to a combination of factors (Knegtering and Pasman, 2013) as complex systems and specifically the CPSs have the ability to reconfigure in response to faults in the system components. This increases the complexity of the CPSs operations, and the cognitive load imposed on the human operator. This challenge can be tackled by alternative design and operational solutions integrating existing sensor measurements and alarms with safety models and automatically analysing the monitored data. The idea of using sensor measurements for enhancing the safety during operations was introduced during 1980s (Papadopoulos and McDermid, 2001), e.g. used in condition monitoring systems (Hafver *et al.*, 2017). Since then, the available research studies number is huge; herein the focus is on the most recent ones, discussing the integration of sensor measurements with available safety models, and related to the cruise ships power plants. These studies are critically reviewed based on the criteria proposed by (Papadopoulos and McDermid, 2001) and some additional criteria in Table 8.

Xing *et al.* (2019) integrated condition monitoring data and inspection data for assessing the risk of a nuclear power plant system. A Hidden Markov Gaussian Mixture Model was developed for modelling the health state of bearings. Bayesian networks were employed for combining the data from inspection results and sensor measurements. Then, the estimated reliability metrics were used to assess the risk in Event Tree. Such an approach allowed more accurate system health estimation compared to approaches based on the traditional Event Trees. Whilst this approach allowed for the estimation of a functional alarm in the investigated system, still the estimation of criticality/importance metrics for different components has not been demonstrated.

Hu *et al.* (2010) used a Hazard and Operability study results to develop a Dynamic Bayesian network for a gas turbine compressor system. In a follow-up study (Hu *et al.*, 2011), the previously developed dynamic Bayesian network was applied to the gas turbine compressor together with an integer algorithm for the purposes of risk assessment. In both studies, the HAZOP method was used for the safety assessment and the development of the Dynamic Bayesian network structure. Historical data was further used for the training of the Dynamic Bayesian network and the concept validation. The developed system could estimate the probability of different failures as well as recommending the safety-related rectification actions. Still, the system did not consider the impact of inspection intervals and maintenance activities. In addition, it has not been integrated with sensor measurements.

Aizpurua *et al.* (2017a) and Aizpurua *et al.* (2017b) integrated the prognostics estimations for a power distribution system with Boolean Driven Markov Processes (BDMP) (Bouissou and Bon, 2003) and Stochastic Activity Networks. In this approaches, the main idea was to calculate the probability of failure based on the Remaining Useful Life estimation carried out by employing prognostics, whilst the Stochastic Activity Networks were used to model the system and derive the relevant Boolean Driven

Markov Processes. The degradation of transformers was modelled using semi-empirical equations, which incorporates some sensors measurements. The advantage of this approach is that it does not require the use of experimental or actual data, whilst the developed safety model considers the different potential system configurations. Yet, it was applied at a conceptual level and it has not been demonstrated how this model could be integrated with the existing alarm and monitoring systems. The selected time scale for the modelling of components also did not allow for the timely alarms' detection.

Gomes *et al.* (2013) combined FTA with a prognostic based Remaining Useful Life estimation for an aircraft control system. In this approach, a degradation index was estimated for two valves of the investigated system based on system pressure measurements. The Remaining Useful Life of each component and the whole system was predicted based on a Fault Tree. Although this study is interesting, it has been applied to a relatively simple system, therefore its results are not directly transferrable to other application studies. As the safety model employed was also relatively simple, there was no functional alarm available. In addition, ranking was not been implemented.

Kim *et al.* (2015) combined the ETA with condition monitoring data for a nuclear reactor safety system. The value and uncertainty of initial crack were estimated based on some historical data and measured parameters. The investigated safety systems reliability was estimated based on their thermal loading and temperature. This information was used to dynamically update the Event Tree probabilities. The developed model allowed for the estimation of the risk metric during the actual system operation. Yet, this study focused on a subsystem of the whole power plant, so the developed method could provide alarm only for one system function. Diagnosis or prognosis techniques have not been incorporated. The developed model was not employed in conjunction with the measured maintenance and inspection data.

A number of initiatives were undertaken by the industry for the development of condition-based monitoring systems (Lipsith, 2019, ABB, 2011b, ABB, 2012, ABB, 2010, ABB, 2011a). Yet, these initiatives focused on the different components of the DEP system, rather than the whole system. Therefore, the developed condition-based monitoring systems do not provide the support to the human operator that is required as the sensors measurements are disconnected from safety models.

The preceding studies review reveals that rather simple safety models combined with sensor measurements. Xing *et al.* (2019) did not use any complex safety model for bearings, Hu *et al.* (2010) used HAZOP, which does not consider multiple point failures. Aizpurua *et al.* (2017a) and Aizpurua *et al.* (2017b) used safety models depicting temporal dependencies, which did not consider safety failures in the investigated system. Gomes *et al.* (2013) used FTA based model for a simple system. Kim *et al.* (2015) used ETA. It must be also noted that all these studies were applied to systems different than the ships DEP plants.

Table 8 Analysis of research studies on automated safety monitoring.

		Academia					Industry	
		Xing *et al.* (2019) / BBN	Hu *et al.* (2010) and Hu *et al.* (2011) / HAZOP and BBN	(Aizpurua *et al.*, 2017a) / BDMP	Gomes *et al.* (2013) / FTA	Kim *et al.* (2015) / ETA	Industry / No safety models	Proposed in this PhD / CASA based
Optimisation of status monitoring and alarm	Filtering of false and unimportant alarms	++	++	++	+	+	+++	+
	Organisation of alarms to reflect priority or causal relationships	+	++	++	+	+	+	++
	Provision of high level functional alarms	+++	+++	+++	++	++	+	+++
On-line fault diagnosis and prognosis	Early detection of escalating disturbances and prediction of failures	+++	+++	++	++	+	+++	+
	Isolation of root failures from observed anomalous symptoms	+++	+++	+	++	+	+++	+
Failure control and correction	Assessment, and provision to the operator, of the effects of failure	+++	+++	+++	++	++	+	+++
	Guidance on corrective measures that remove or minimize the effects of failure	++	+++	+++	++	++	++	+++
Inspection and maintenance data incorporation		+++	+	+	+	+	+	+++
Relevance to the DEP blackout		+	+	++	+	+	+++	+++

Addressed	+++	Moderately addressed	++	Slightly or not addressed	+

3.5 Identification of research and development directions

Based on the analysis in the preceding sections, a number research gaps and suggestions for further research were identified. They are elaborated in the next paragraphs using bullet points.

With respect to the hazard identification methods:

1. Improvement of the available hazard identification methods and usage of advanced hazard identification techniques to ensure the completeness of the identified accident scenarios should be pursued.
2. The processes for implementation of hazard analysis could be enhanced through additional automation or combination of methods to reduce the dependency on the expert's skills or supported by simulation techniques and modelling.
3. Detailed model simulations could potentially substitute the hazard identification techniques in CPSs and can be used to derive the STPA, HAZOP results and Fault Trees. Systemic methods like STPA could be potentially automated in a similar manner with FLSA.
4. The hazard identification techniques could be extended with appropriate checklists for hazard identification in CPSoSs.
5. FLSA methods could be also extended to consider the cyberattacks induced failures and their application can be investigated on more complex systems like CPSoSs, with an adapted formalism and analysis algorithms.
6. Applicability of machine learning algorithms for hazard identification in the above cases could be also explored.

With respect to the STPA method (hazard identification method as well):

7. Development of logical/dynamic models allowing elicitation of UCAs and causal factors in automatic way in CPSs could be investigated.
8. Integration of STPA with several other hazard identification and analysis techniques to ensure the completeness of identified scenarios could be pursued.
9. Adoption of STPA results for implementation of safety analysis in a technical system could be explored.
10. New guidelines for enhancement of STPA with respect to identification of UCAs and causal factor could be investigated with focus on autonomous CPSs.
11. Better incorporation of temporal aspect in STPA or support of STPA with other methods to incorporate that could be considered.

With respect to the DEP system safety assessment:

12. Application of novel safety analysis methods to DEP plant.

13. Estimation of more representative safety metrics for the ship DEP plant in addition to reliability and availability such as probability of blackout, duration of blackout, risk of blackout, probability, and duration of power reduction, etc.
14. Comparison of alternative propulsion systems on cruise ships in terms of their safety metrics other than reliability or/and availability.
15. Use of novel safety analysis method in combination with modelling techniques for ensuring the safety of DEP system.

With respect to the DEP system operation:

16. Integration of safety models with sensor measurements and alarm monitoring system on the ship.
17. Integration of condition-based maintenance results with the safety models for supporting safer ship operation.

3.6 The selection of the investigated research gaps

In this PhD thesis, the following research gaps from the one presented in Section 3.5 are selected to be covered:

3.6.1 Research gaps 1, 4, 8, 9 and 11

As it is important to ensure the completeness of identified scenarios and their analysis (1.4.1), so that all possible scenarios are properly addressed, the focus will be on enhancement of hazard identification methods, in specific STPA, with application to technical system.

The STPA method has been considered as useful method for identifying new interactions between the control and physical parts addressing in this way the software-effective character of CPSs. Furthermore, the STPA has the potential to identify ways in which a successful cyberattack can become harmful to a CPS. Therefore, it would be beneficial for a new method to incorporate STPA. Still, it would be required to enhance STPA and to add to the method quantitative step to allow for proper decision-making process.

On the other hand, FTA can be effective method for capturing the dependencies between components and analysing the physical failures. Potentially, FTA could be substituted using other methods, however, FTA is rather simple to be applied. The ETA strength is on identifying the event sequences of the investigated system. In addition, the ETA exhibits strength in identifying the event sequences of the investigated system and identifying multi-point failures (ISO, 2009). This is important in CPSs, as CPSs can reconfigure responding to specific fault or control commands. Potentially, Event Sequence Diagrams as reported in (Ramos *et al.*, 2020) could be used, but ETA based method was selected herein, due its formalism simplicity.

Consequently, by combining these three hazard identification and safety analysis methods to develop a novel method, it is expected that the rigour of the analysis will be improved through increasing the number of identified complex scenarios, capturing the dependencies between different component failures, more effectively capturing the software related failures and identifying the temporal relationship between different events, as the methods offer different perspectives of the system. The combined novel method (Combinatory Approach to Safety Analysis (CASA)) still is required to manage and capture the problem of evolution in time, as it will not be model based. However, the developed problem-solving algorithm can give insights on how to automate or semi-automate the method. In addition, the novel method will not be capable of identifying the different scenarios arising in complex environment related to autonomous CPSs, and potential scenarios related to cyberattacks, but this can be left as suggestion for future research, since it is out of the scope (Chapter 1.4.1).

3.6.2 Research gaps 12-14

The previous research studies on ships DEP system focused on these systems reliability and availability assessment. Although, these metrics are valuable for the systems safety comparison, they are not representative metrics for the system safety. Experience has shown that reliability can be improved without influencing the system safety Leveson (2011a). Therefore, there is a need to estimate metrics, which more effectively characterise the safety of ships DEP systems using novel methods.

Examples of such metrics are the probability or the frequency of blackout, which is a safety related event. For this purpose, the CASA method is developed to estimate this metric. Other methods potentially could be integrated with the CASA method, to estimate other system safety metrics, such as the blackout risk or the blackout duration; however this was excluded from the scope of the present study (Chapter 1.4.2).

3.6.3 Research gap 16

The focus also will be on integration of safety models with sensor measurements and alarm monitoring system on the cruise ship, as potential innovative solution can be developed there. In addition, considering the significant cognitive load of the operator/crew considering the modern marine CPSs, it can be very important to support him/her by using appropriate automated safety monitoring systems. Such a system must incorporate several system parameters and estimate the probability of system failure. Therefore, it could be investigated how the CASA results could be used to develop such an automated safety monitoring system and how different system parameters could be incorporated in that.

3.6.4 Excluded research gaps rationale

Whilst the primary reason for focusing on the above research gaps and excluding others is the limited PhD duration, additional reasons are provided below:

- Research gaps 2 and 7: The development of automated hazard identification tool would demand significant effort in investigation of potential tools, algorithms for analysis, graphical user interface development. It would be prudent first to enhance the existing methods and to understand the algorithm for problem solving before developing the tool.

- Research gap 3 and 15: The development of detailed model would require its verification and validation using empirical data, resulting in substantial cost in terms of time. In addition, such an approach, would be applicable at later stages of design, making the derivation of safety requirements challenging at initial design stages. As it was referred in 1.4.1, it is important to ensure safe and cost-efficient design process and safety must drive the design as early as possible.
- Research gap 5: The cybersecurity is considered to be out of the scope of this research (Chapter 1.4.1).
- Research gap 6: The use of artificial intelligence would require significant amount of data for training, which is rather difficult to obtain. It would also require significant resources to review and filter the data.
- Research gap 13: The estimation of risk is excluded as the focus is on the left-side of the Bow Tie (Chapter 1.4.2). Other metrics estimation is excluded due to time limitations.
- Research gap 17: The procurement of reliable data for condition-based monitoring systems development is rather challenging. It would require significant resources for its analysis as well.

3.7 Conclusions

Based on the preceding discussion, this thesis will develop a novel method for safety analysis based on STPA method. This method will be also used to estimate new safety metrics for cruise ships propulsion systems. Last, but not least this thesis will demonstrate a new automated safety monitoring system for enhancing the safety of cruise ship operations.

3.8 Chapter summary

STPA is a method effectively capturing the interactions between software and physical parts in the CPSs. The existing body of research focused on how to enhance the method by enriching the different steps, combining STPA with other methods or automating the method. Several research studies focused on safety and reliability analysis of DEP system and on development of automated safety monitoring systems. There still a significant number of research gaps with respect to the STPA method and the DEP system safety assessment. By combining STPA with other methods such as ETA and FTA and properly integrating the results it is expected that some of STPA limitations will be overcome. This integration of methods to develop a novel method can be considered as the main novel contribution of the present thesis. Other novel contributions of this thesis that can be considered are the application of the novel method to cruise ship DEP system and initial development of automated safety monitoring system for cruise ship blackout.

This page has been intentionally left blank

4 NOVEL METHOD DESCRIPTION

4.1 Chapter outline

In this Chapter, the novel method steps are elaborated in detail. It is explained why the selected methods have been combined in specific sequence. Each method steps and how the results are integrated together are also discussed. Then, after the final Fault Tree development, it is explained how a quantitative analysis can be implemented using the generated Fault Tree.

4.2 Rationale behind the method steps

As it was discussed in Chapter 3, the hazard identification methods are not adequate for identifying properly the scenarios in CPSs, as specific scenarios can be omitted during hazard identification and analysis process. Thus, it is suggested to combine different hazard identification and analysis techniques, in specific STPA, FTA and ETA, to form a novel Combinatory Approach to Safety Analysis (CASA), which can provide a more comprehensive understanding of a system scenarios. The rationale for selection and the expected advantages was provided in Section 3.6.1, but elaborated more below to give the rationale for the sequence of applied methods.

STPA is a top-down (deductive) approach effective in capturing the overall system context. It starts with an undesired event for the system and descends deductively to the lower levels for identifying the local interactions leading to the top event. In addition, the STPA results can support the identification of failures in safety barriers represented by UCAs. STPA does not require a detailed system description and can be implemented on a functional level during the initial stages of system design (Fleming, 2015). Thus, it is proposed to start the hazard identification of a system using the STPA. Event Sequence Identification (ESI) based on ETA is an inductive method, which can be used for identifying the sequence of events leading to the unsafe condition or a hazard starting from an undesired event or hazard in the system. In this way, the event sequence, system response and multipoint failures leading to an accident can be identified. FTA can be used to provide deductively more detailed causation to physical failures identified by the STPA. Consequently, by combining STPA, ESI and FTA a more comprehensive picture for an undesired event in a CPS can be attained.

In addition, the results of these methods should be presented in a neat and unified format suitable for the implementation of the quantitative system safety analysis. This leads to the consideration that results from different ESI “Event Trees” must be combined. The use of a Fault Tree is proposed herein for the unification of the analysis results, although the use of other methods such as Bayesian Networks is not excluded. Then, the results of the FTA can be allocated to the previously developed Fault Tree and the Fault Tree is further refined.

The preceding considerations lead to the development of the following steps, which are also described in Figure 8 and in Table 9. The first four steps are similar to the ones of the classical STPA approach.

In subsequence, the ESI "Event Trees" are developed by analysing the system and using input from the STPA application. The sixth step is based on the developed ESI "Event Trees" and synthesises them into one Fault Tree. In the seventh step, the generated Fault Tree is populated with the results from the STPA. In the eight step Fault Tree is further refined to address inconsistencies due to the integration of STPA and ESI results. The ninth step expands on some physical failures by expanding some failures indicated by STPA (nodes of step 8 Fault Tree). The last step includes the quantitative safety analysis that needs to be implemented for the system failure occurrence estimation. The CASA results are used to derive the safety recommendations for the system safety enhancement. The method steps have to be applied in specified sequence, otherwise the results will differentiate from CASA results. These steps are presented in more details in following sections, whilst the followed steps for the investigated case studies are provided in Chapter 5 and 7, where a set of the derived results is also provided and discussed.

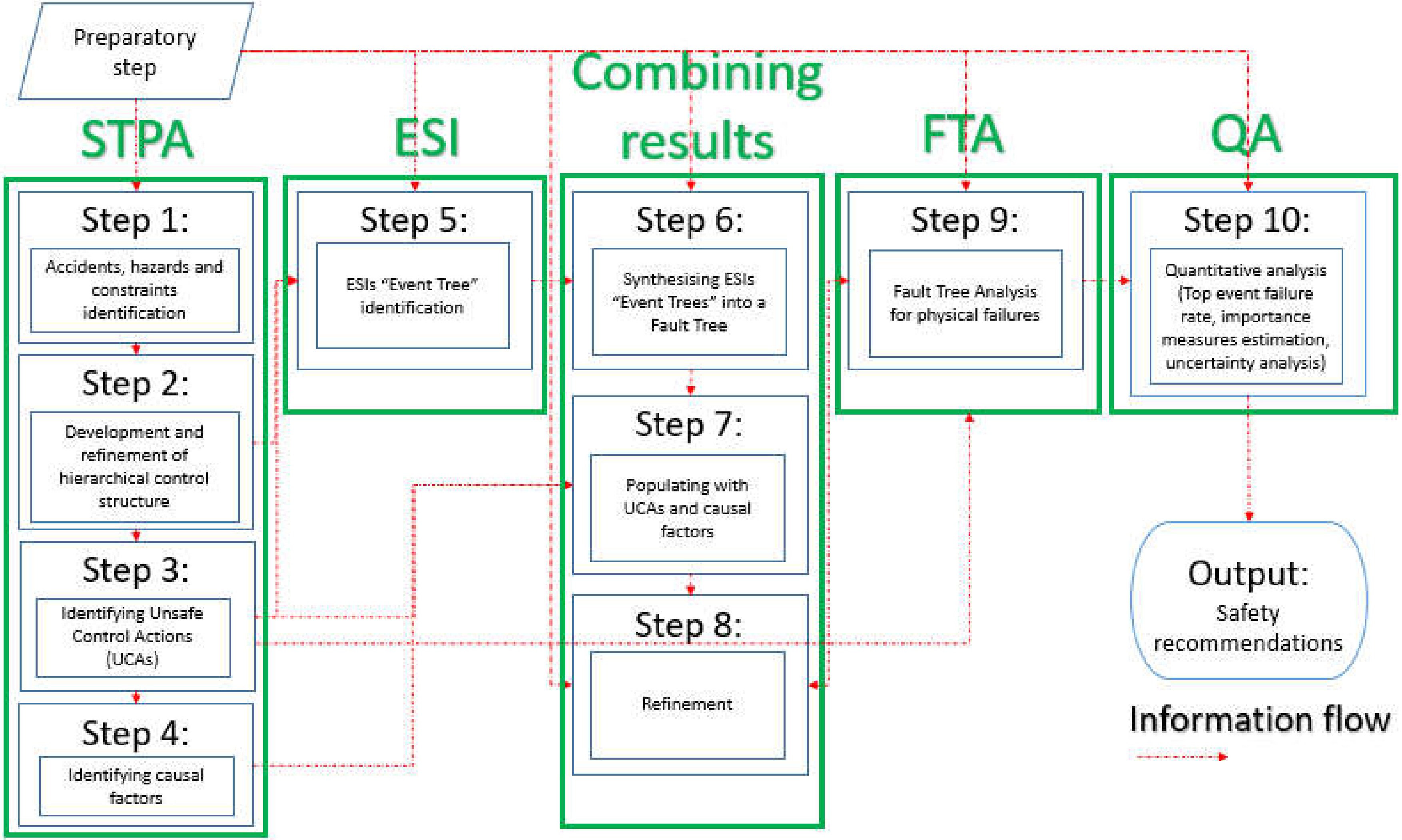

Preparatory step
STPA
ESI
Combining results
FTA
QA
Step 1:
Accidents, hazards and constraints identification
Step 2:
Development and refinement of hierarchical control structure
Step 3:
Identifying Unsafe Control Actions (UCAs)
Step 4:
Identifying causal factors
Step 5:
ESIs "Event Tree" identification
Step 6:
Synthesising ESIs "Event Trees" into a Fault Tree
Step 7:
Populating with UCAs and causal factors
Step 8:
Refinement
Step 9:
Fault Tree Analysis for physical failures
Step 10:
Quantitative analysis (Top event failure rate, importance measures estimation, uncertainty analysis)
Output:
Safety recommendations
Information flow

Figure 8 The proposed method workflow and input-output relations.

Table 9 The proposed method steps overview.

Steps		Step description	Employed technique	Justification	Required resources	Output	Output to steps
Initiation	Step 0: Preparation	Accumulating system data: accidents investigations reports, previous hazards analyses, components failure rates, system simulations, etc.	Publications and accident investigation reports analysis	Good understanding of system problems required for analysis	Access to data	Good understanding of the system	All other steps
STPA	Step 1: Defining the scope of analysis	Identification/selection of accident, system hazards, sub hazards and safety constraints for the system	Hazard review / Brainstorming	Setting the boundaries of analysis	Good understanding of the system, potentially team of experts	List of accidents, hazards and safety constraints, hierarchical control structure	Step 2, 3, 5
	Step 2: Hierarchical control structure	Development of the system control structure	Following the STPA guidelines	Developing system model for the STPA	Access to the manuals and the drawings	Hierarchical control structure	Step 3, 4
	Step 3: UCAs identification	UCAs are identified	Following the STPA guidelines	To identify control failures	List of the control actions and the context variables	List of UCAs in tabular format	Steps 4, 5 and 9
	Step 4: Causal factors analysis	For each of the UCAs causal factors are identified	Using a developed checklist	Identification of the causal factors for the UCAs	List of the UCAs, control structure, checklist	List of the causal factors for the UCAs	Step 7
ESI	Step 5: Developing event sequences	ESI using hazards/ sub hazards as Initiating Events following logic similar to Event Tree Analysis	ESI	Connecting UCAs, sub hazards and hazards	List of the hazards, safety constraints and UCAs	ESI results for each of the hazards	Step 6
Integration of STPA and ESI results	Step 6: Synthesis of ESI results	Unification of the ESI results	Applying a number of logic rules	To connect different ESI results	ESI results from the previous step	Combined Fault Tree	Step 7
	Step 7: Populating the Fault Tree	Enriching the Fault Tree with results of the STPA	Manually	Connecting the UCAs, hazards and accidents	Results of STPA and initial Fault Tree	More detailed Fault Tree	Step 8
	Step 8: Refinement	Refinement of already developed Fault Tree	Applying a number of logic rules	Correcting inconsistencies	Fault Tree from the previous step	Refined Fault Tree	Step 9
FTA	Step 9: Fault Tree Analysis	Fault Tree Analysis	Fault Tree Analysis	Analysis of the physical failures	Access to the manuals and the drawings	Final Fault Tree	Step 10
QA	Step 10: Quantitative analysis	Estimation of the frequency of the top event, ranking, etc.	Fault Tree and equations calculations	Critical components identification and performance prediction	Failure rates, operational data, inspection and maintenance intervals	Safety recommendations	Risk estimation

4.3 Preparatory step (Step 0)

This step involves the activities required to gather the information about the system and system hazards. This includes, if available, the system simulations using detailed models depicting the system behaviour and responses, previous hazard identification analyses, the study of the system operation and maintenance manuals, development and analysis of system experts' questionnaires and the analysis of previous accident investigation reports, as well as, getting access to the failure rates databases for the system components.

4.4 STPA (Steps 1-4)

The aim of the first step is to accurately define the targets of the whole analysis. The process starts with the accidents identification for the investigated system. Based on the identified accidents, the relevant hazards in subsequence can be identified. In the STPA framework hazards are understood as 'the system states or the set of conditions that together with a worst-case set of environmental conditions will lead to an accident' (Leveson and Thomas, 2018). The hazard identification can be implemented either with the assistance of a hazard review by individual or team or experts team brainstorming. According to the STPA, only the hazards related to the accident under consideration are taken into account, which can be further broken down in sub hazards (Leveson and Thomas, 2018). Based on the hazards and the sub hazards, the existing safety constraints and requirements that must be implemented in the system design are identified. The list of existing control measures can be used to augment the ESI implementation as explained in the next step.

Step 2 focuses on the development of the investigated system control structure, which is one of the differentiating points of the STPA analysis compared with the other methods (Leveson and Thomas, 2018). As shown in Figure 9, the process commences with a high-level system abstraction and proceeds to a more detailed level. The initial control structure consists of the high-level controller, the human operator and the controlled process with its basic control, feedback, and communication links. A more detailed description incorporates the controllers' hierarchies. The final refined control structure includes the information on responsibilities of each controller, the process model with the process variables and their ranges, the control actions, the actuators behaviour, the information provided by sensors and the interactions between the controllers. The development of a hierarchical control structure is influenced by the system identified accidents and hazards. This analysis output is expected to be in the form shown in the right hand side of Figure 9.

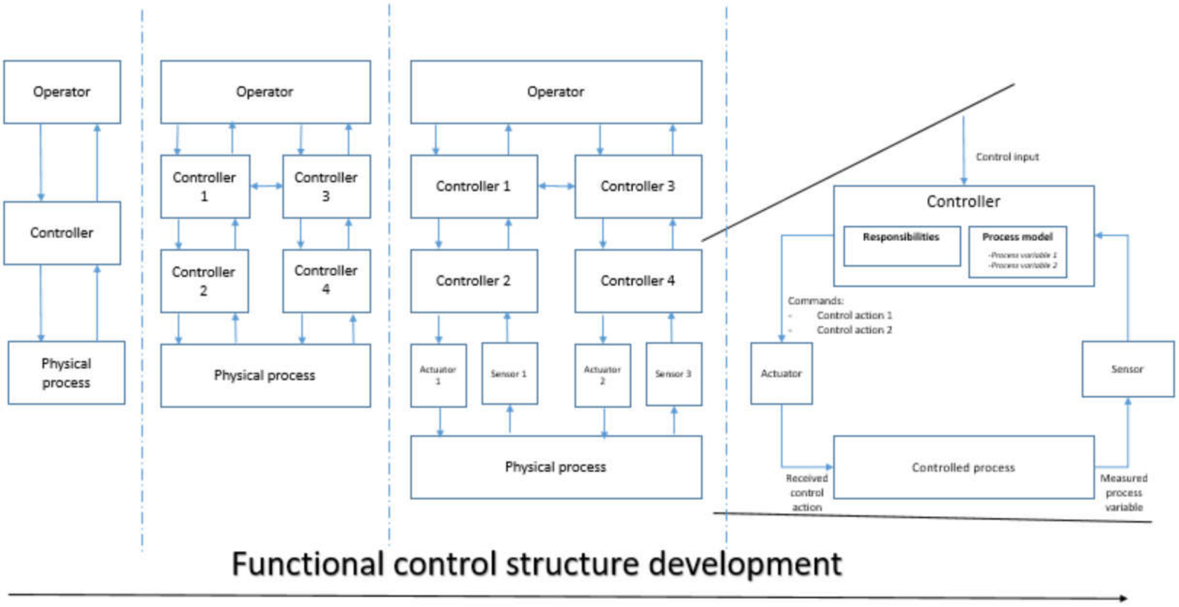


Figure 9 Flowchart demonstrating the steps for developing a control structure.

The previous steps are the STPA initial steps. The actual hazard identification process starts in step 3 as shown in Figure 8, having as an objective to identify the UCAs that lead to hazards. The possible UCAs are categorised as follows (Leveson and Thomas, 2018):

- Not providing the control action that leads to a hazard (Type 1).
- Providing a control action that leads to a hazard (Type 2).
- A control action is untimely provided (too late, too early, or out of sequence) (Type 3).
- A control action duration is not adequate (stopped too soon or applied for too long) (Type 4).

According to the STPA, there is also the following type of UCAs: when a safe control action is provided but not followed. This is considered equivalent to the Type 1 UCAs (Leveson and Thomas, 2018). This type of failure mode is analysed during the identification of causal factors in the next paragraph.

For each control action, the potential process variables values are considered, and it is investigated whether the control action will lead to a hazard/sub hazard or not. Similarly, with the system hazard identification, safety constraints can be derived from the UCAs, aiding the identification of appropriate hazard control measures.

The fourth step includes the causal factors identification and forms an essential step for the STPA (Figure 8) as the causal factors explain why an UCA can occur. In this study, the process was augmented by the usage of a modified tree structure proposed in Blandine (2013), which was enhanced by a list of causal factors from (Becker and Van Eikema Hommes, 2014), and it is shown in Figure 10. This allows the easy transition from the STPA results into a Fault Tree structure, as in this way the causal factors can be connected to the UCAs by using the OR gate of a Fault Tree. The UCAs are considered undeveloped events and their causal factors are connected to these UCAs using OR gates. Practically, this step is very similar to the checklist procedures. The list of typical generic causal factors is given in Appendix H. Such a provision of this checklist is beneficial, as it supports the repeatability and objectiveness of the STPA results. In this thesis, the term "scenario" is not used according to STPA framework; instead, scenario is considered in a much wider context, as a generic hazardous or accident scenario.

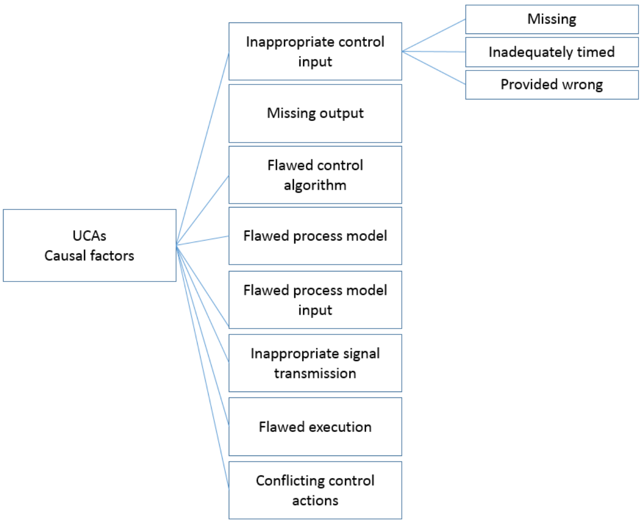


Figure 10 Causal factors categories.

4.5 ESI (Step 5)

The Events Sequence Identification (ESI) commences after the STPA results have been derived (Figure 8). The methodology employed in the ESI is very similar to Event Tree Analysis (ETA) (ISO, 2009) and all the tools relevant to ETA are also used herein to ensure the identified scenarios completeness and to capture potential sequences of events in the investigated system. Each sub hazard/hazard is used as an initiating event and the propagation of sub hazards/hazard into a hazard or an accident is investigated by considering (a) the protective barriers designed to mitigate the sub hazards/hazards consequences, (b) the relevant system states and, (c) the identified UCAs from previous step. The "Event Trees" is considered fully developed when all the outcomes end at either the safe condition, another sub hazard/hazard, or the investigated hazard/accident. It was assumed that the events duration has no effect on the identified event sequences, but it affects the probability of each selected branch and consequently the specific states calculation (described in Chapter 4.8).

Despite the similarities between the ESI and the ETA, the following differences exist (justifying the method name): (a) the ESI analysis is completely internal to the system compared to the ETA, which can be external to the investigated system; (b) the ESI does not incorporate the calculation of the protective barriers failure probability and it is implemented only qualitatively; (c) the ESI outcome is not necessary an accident but can be a hazard at the system level (the ESI corresponds to the left side of the classical Bow Tie, in comparison to the ETA that corresponds to the bow tie right side); (d) as a consequence to the previous point, no estimation of risk is provided by the ESI; (e) the ESI along with STPA results are used to develop a Fault Tree as described in the next section. It must be noted that the introduction of the ESI term was followed for distinguishing between the two methods (ESI and ETA).

4.6 STPA and ESI results integration (Steps 6-8)

Since not all sub hazards/hazards lead directly to the system hazard/accident and some interactions exist between the various sub hazards/hazards, the developed "Event Trees" are restructured in the sixth step of the proposed method (Figure 8), so that the investigated sub hazards/hazards propagation is identified. Subsequently, the ESIs are transformed into a Fault Tree by connecting the events in a hazardous sequence using AND gates as shown in Figure 11. The different scenarios resulting in the same hazard/accident are connected using the OR gates (Figure 11). The paths from a sub hazard/hazard to another sub hazard/hazard are connected using OR gates (Figure 11). As a result, a preliminary Fault Tree is developed, which is enriched and refined in the next steps of the proposed method. This is an important difference between the proposed approach for employing the ETs to develop a FT and the typical approach according to which, FTA is used to model the causes identified in ETA. In this way, accident becomes a top event in the Fault Tree, which is rather uncommon. However, accidents/hazards were used as the Fault Tree top events or nodes in BBN in the pertinent literature, as reported in (Utne *et al.*, 2020, Hamann *et al.*, 2013). ISO 31010 allows using a broader outcome of a specific failure as top event (ISO, 2009).

In the seventh step (Figure 8), the preliminary Fault Tree is enriched by using the derived STPA results. This is implemented in two sub steps. First, the UCAs are related to the branches in the ESI "Event Trees" (and consequently, the events of the preliminary Fault Tree). These UCAs are connected to the event in a Fault Tree using an OR gate. During the second sub step for each UCA, the causal factors are developed under the UCAs with an OR gate. An example for the implementation of this step is shown in Figure 12.

The Fault Tree development is not accomplished by populating the Fault Tree with the UCAs and the causal factors as inconsistencies may arise since the results from the two different methods are merged into one structure. Therefore, the developed Fault Tree further refinement takes place in Step 8 (Figure 8). This step also considers the system architecture and the common causal factors. The conditions and applied refinements are described in Table 10. An applied refinement example is provided in Figure 13, where UCA 1 is split into the UCA 1 representing its causal factors and the system state (in which UCA 1 occurs); UCA2 is split into UCA 2 representing its causal factors and the system fault (with which it occurs), whereas the common causal factor for UCA 3 and UCA 4 is 'upgraded' to a higher level in Fault Tree. The refinement is required to ensure that the OR and AND gates calculation involve non repeated and independent events.

A refinement for causal factors is also required. Initially, the causal factors for each of the UCAs are considered independent and thus connected with the OR gate. Quite often though, UCAs are sharing common causal factors; the one causal factor will cause several UCAs to occur. For instance, failure of PMS hardware will lead to failure of multiple functions. This creates a problem, as in a single path from hazard or UCA, less UCAs working as barriers will be operational. The path in Fault Tree is represented using AND and OR gate. If the connecting gate is OR then the event propagates vertically, if the connected gate is AND then the event propagates horizontally. For each of the causal factor, it is checked, whether it is repeated on a path. For the events connected with OR gate on the path, the check is implemented toward down for basic events, as long as they are connected with OR gate. If events are connected with AND gate, the going down procedure stops, and these events are neglected. If the basic events are the same, then they are promoted to the same level with the OR gate and connected using OR gate. In a similar, but a bit more complicated way, for the events connected with AND gate on the path, the check is implemented for basic events, starting from the top event at the level of AND gate, as long as they are connected with OR gate. If they relate to AND gate the going down procedure stops. If a common causal factor is found, then the two or more events connected with AND gate and with common causal factor are demoted to a lower level higher than initial AND gate and connected to this common factor using OR gate. Then the new structure is connected to initial AND gate using OR gate. The previous refinement is shown in Figure 13.

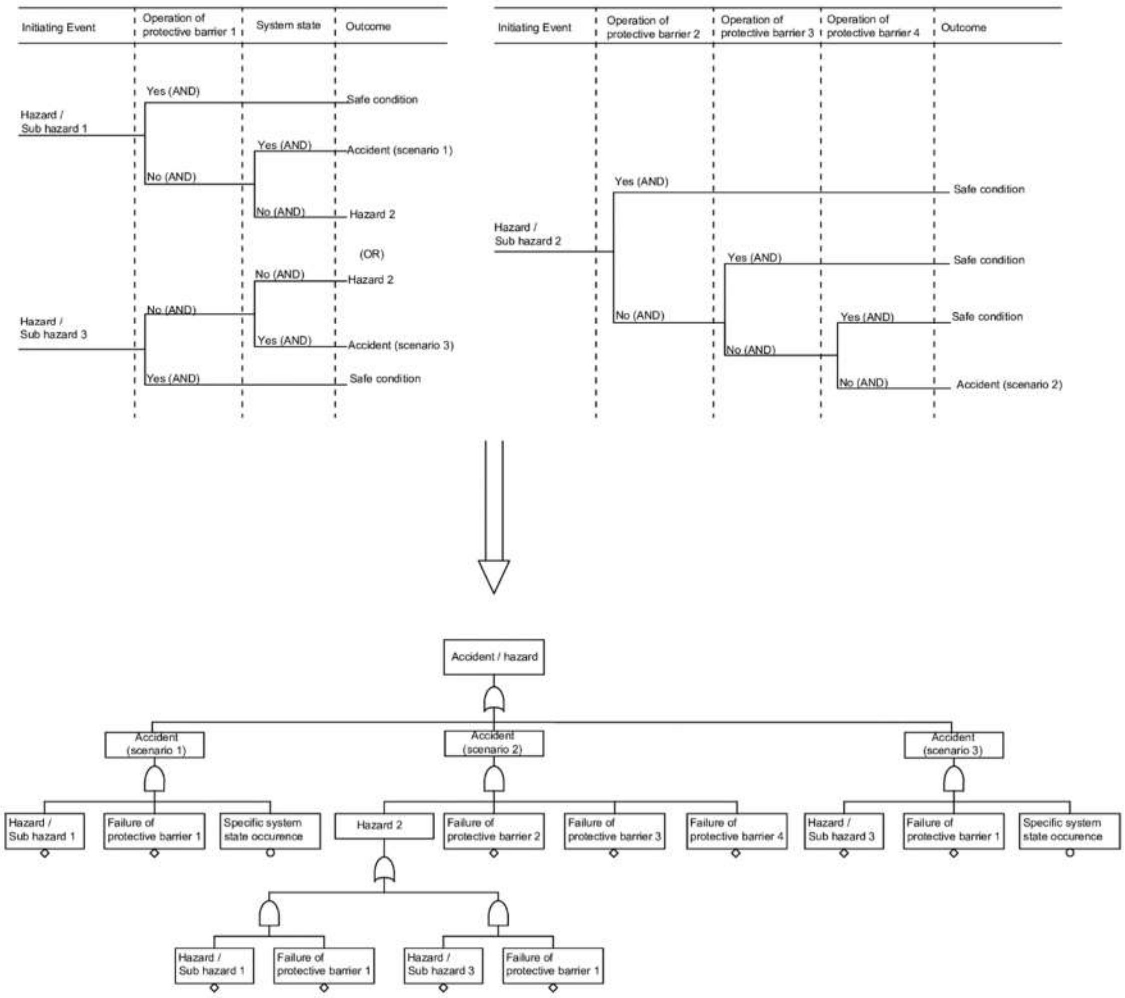


Figure 11 “Event Trees” transformation into Fault Tree

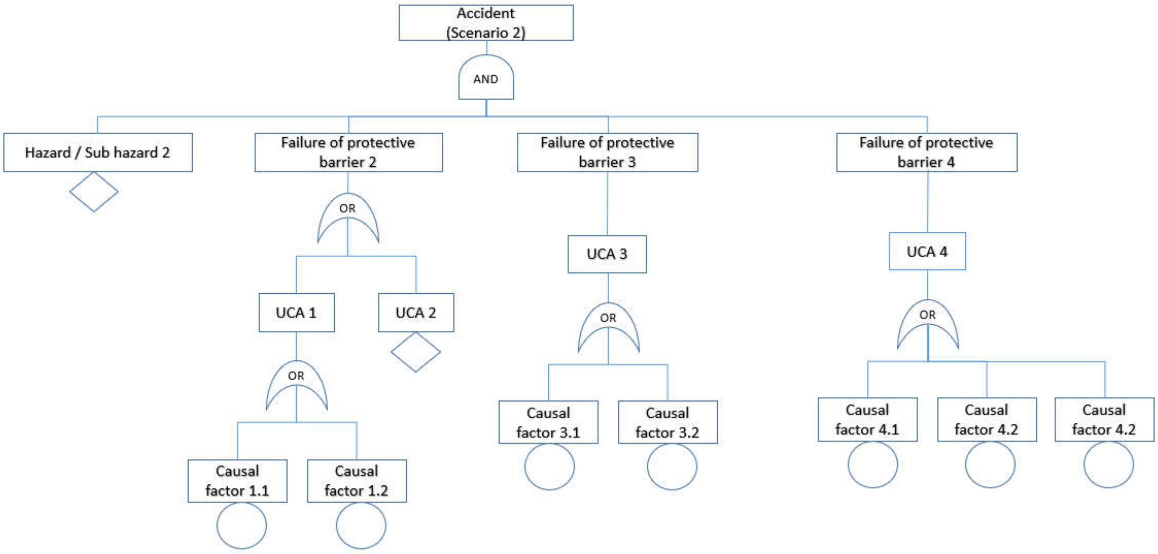


Figure 12 Fault Tree populated with UCAs and causal factors.

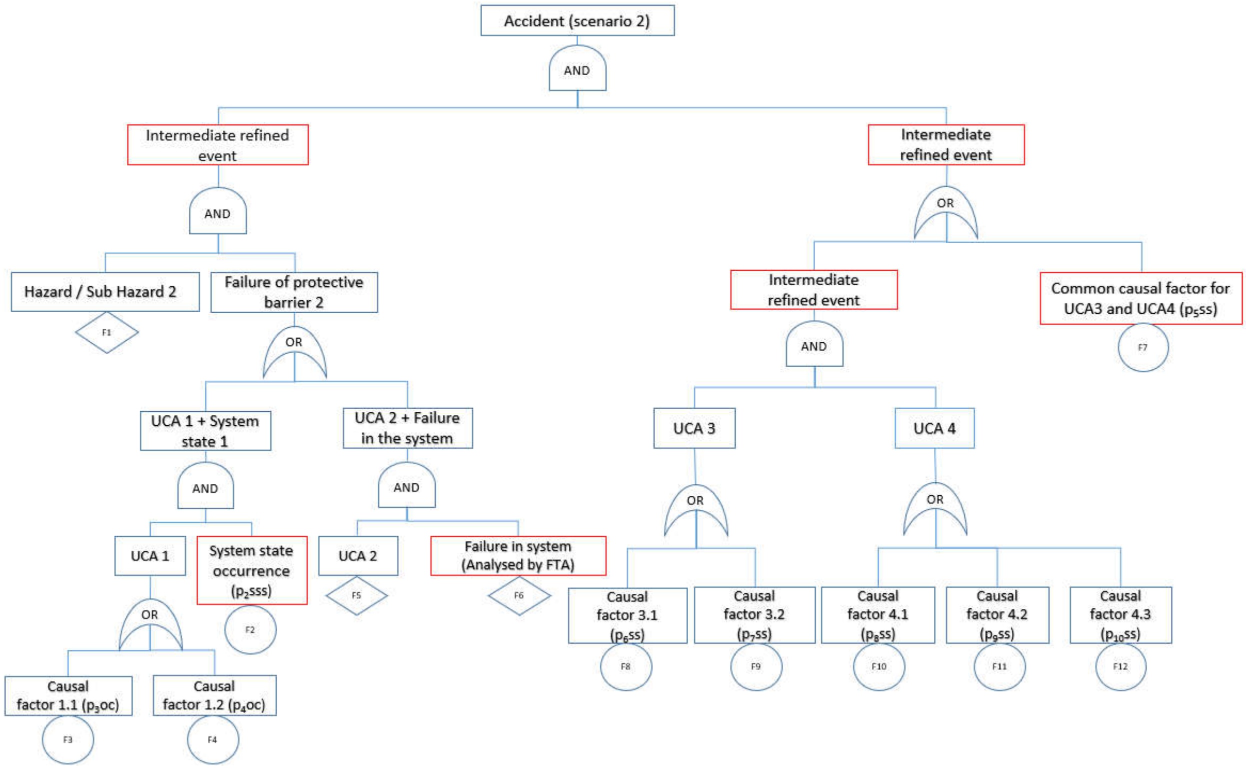

Accident (scenario 2)
AND
Intermediate refined event
Intermediate refined event
AND
OR
Hazard / Sub Hazard 2
Failure of protective barrier 2
Intermediate refined event
Common causal factor for UCA3 and UCA4 ($p_5$ss)
F1
OR
AND
F7
UCA 1 + System state 1
UCA 2 + Failure in the system
UCA 3
UCA 4
AND
AND
OR
OR
UCA 1
System state occurrence ($p_2$sss)
UCA 2
Failure in system (Analysed by FTA)
F5
F6
F2
OR
Causal factor 3.1 ($p_6$ss)
Causal factor 3.2 ($p_7$ss)
Causal factor 4.1 ($p_8$ss)
Causal factor 4.2 ($p_9$ss)
Causal factor 4.3 (p_{10}ss)
F8
F9
F10
F11
F12
Causal factor 1.1 ($p_3$oc)
Causal factor 1.2 ($p_4$oc)
F3
F4

Figure 13 Refined Fault Tree example.

Table 10 The conditions for refinement and refinement actions.

Rule number	Condition	Refinement action
1	An UCA is hazardous in a specific context and this is not captured by the ESI "Event Tree"	An UCA is split into control action and the context variable, representing context connected using AND gate
2	An UCA is a causal factor of another UCA	Grouping is applied, the UCA is connected to the other one using OR gate
3	UCAs have identical causal factors and are located in the same position of the ESI "Event Tree"/Fault Tree	Merging of these UCAs is applied
4	A common causal factor for the UCAs at different points of "Event Tree"/Fault Tree	Causal factors are promoted to a higher level of the Fault Tree
5	A contradiction in a sequence of events occurs	Elimination of the contradictory events
6	An UCA is caused by a complex physical failure, which is refined by a Fault Tree	Subcases are defined for each physical failure
7	Common cause failures leading to complex physical failure	Subcase is defined for the common cause failure in Fault Tree

4.7 FTA (Step 9)

According to the STPA, some of the hazardous situations are related to a combination of a control action and a system state, which in turn is caused by a physical failure. For the cases where this system state is attributed to a number of a subsystem physical components failures, a FTA is employed to identify these components failures, thus allowing for this state quantification taking place in the tenth step of the proposed method (Figure 8). The top event in the FTA is taken as the system state from the relevant UCA (a high level physical failure) and the causes are identified by (a) breaking down the subsystem into components, (b) assessing which component failure will lead to the top event of the local FTA and, (c) considering the functional dependencies between the identified components. The identification of components failures leading to the top failure can be supported by considering the conditions under which the safety functions in specific components are activated. This step requires much more detailed information about the investigated subsystem and its components dependencies, as well as the subsystem components specific failures. The different components failures are connected using OR gates. If the same components are connected in parallel, their failures are connected to other failures using AND gates. If some of the components have identical standby components, then these components failures are connected using OR gates, but special treatment is provided for estimating its probability of failure as described in next section. The developed Fault Tree in this step is connected to the previous steps Fault Tree (as shown in Figure 13), resulting in a more detailed Fault Tree, linked to the investigated system components failures, which can be used for the purposes of the Quantitative Analysis (QA) described in the next section.

4.8 Quantitative Analysis (Step 10)

The purpose of the QA is to support the decision-making process and the safer systems design (Bjerga *et al.*, 2016, Goerlandt *et al.*, 2016). The approach followed in this study is probabilistic based and the QA output includes the calculation of top event failure rate (λ^{TE}) based on the top event failure rate in a specific operating mode (λ_p). This differentiates the present study from previous studies, which employed the system reliability or/and the system availability as metrics for the presented quantitative analyses. However, the top event frequency is considered to be a more representative metric, as it corresponds to the investigated event and therefore, historical data for its frequency can be retrieved through available accidents data. The top event frequency is a risk metric (Johansen and Rausand, 2014b) and therefore it is considered as a metric that represents the system safety. In this respect, computationally expensive calculation of the top event frequency (for example by employing Markov chains) can be avoided.

In addition, this step includes a importance measures estimation and a supplementary uncertainty analysis to identify the critical failures and the uncertainty in estimated top event frequency estimation, as they are required for system safety enhancement.

The following assumptions were made for the QA purposes:

- The basic events in the Fault Tree can be grouped to three categories: (a) the operating system components failures (p_i^{oc}); (b) the safety systems failures (p_i^{ss}) (it must be noted that the safety systems function is to control and handle the operating system components failures) and; (c) specific system states, for example overloading of the generation sets (p_i^{sss}).
- The considered safety systems components failure rates follow an Exponential failure probability distribution.
- The operating system components failure rates follow either an Exponential or a Weibull failure probability distribution. The Weibull failure probability distribution has been employed in the case of components for which preventive maintenance practices are followed.
- The operating system components follow the Weibull failure probability distribution, whilst the standby components follow the Exponential failure probability distribution.
- When the Weibull probability distributions is used, the respective component employed failure rate is averaged considering the corresponding failure rates for the interval periods between maintenance/inspection activities.
- A correction can be applied to components failures rates initially estimated using Exponential distribution, to use them as components with Weibull probability distribution using correction ratio provided in Table 4 (Denson *et al.*, 1994).

- The inspection of the system components is performed according to the manufacturers' guidelines and can effectively detect the system components condition including their failures and degradation level.

- The implemented maintenance practice for the systems components is according to the manufacturers' guidelines and restores the system components to the best possible condition (repairing their detected faults and mitigating their degradation). The maintenance intervals of the system components are timely as proposed by the respective manufacturers.

- The probability of failure in one system configuration (or operating mode) is independent from probability of failure in other system configurations (or operating modes).
- The duration of testing and duration of repairs of faults detected during testing have negligible impact on the availability of the standby components or the components implementing safety functions.
- The top event probability deferential can be adequately approximated by employing the respective difference considering a relatively small-time interval, which was taken as 1 h.

4.8.1 Top event frequency estimation

The frequency of the top event (f) is calculated according to the following equation by considering the frequency of the top event (f_p) in each system configuration (operating mode) and the respective operating time percentage in each configuration (OP_p):

$$f = \sum_{p=1}^{q} OP_p \, f_p \tag{1}$$

where p denotes the system configuration.

The OP_p values in each specific configuration are estimated by using the investigated ship operating profile. For calculating the f_p, the specific operational time (OT) is considered along with the undesired event failure rate in the specific system configuration *(λ_{p})* (Schüller *et al.*, 1997):

$$f_p = \lambda_p OT \tag{2}$$

The λ_p is estimated using the approximation based on the failure rate definition (Schüller *et al.*, 1997):

$$\lambda_p = \frac{P[failure\ occurs\ between\ t\ and\ t\ +\ dt|no\ prior\ failure]}{dt} = \frac{dP_p}{dt} \approx \frac{\Delta P_p}{\Delta t}, \Delta t = 1hour \tag{3}$$

The overall top event failure rate (λ^{TE}) can be estimated according to the following equation based on the λ_p and the respective operating time percentage in each configuration (OP_p):

$$\lambda^{TE} = \sum_{p=1}^{q} OP_p \lambda_p \tag{4}$$

For estimating the top event probability in a specific system configuration (P_p), the derived Fault Tree (from Step 9) was employed. For each distinct configuration, the active branches of the finalised Fault Tree are identified (whereas a number of branches are deactivated or not considered based on the components and subsystems that do not operate or contribute in the operation of the investigated system). In subsequence, the P_p is calculated by considering the respective Fault Tree (an example is shown in Figure 13) by applying the specific calculation rules for the Fault Tree gates.

The following equation is employed to calculate the probability outcome of an OR gate with z input events (E_z) (Verma et al., 2010):

$$P = 1 - P[\overline{E_1} \cap \overline{E_2} \cap \overline{E_3} \cap \ldots \cap \overline{E_z}] =$$

$$= \sum_{k=1}^{n} P(E_k) - \sum_{k<l} P(E_k \cap E_l) + \cdots + (-1)^{z-1} P(E_1 \cap E_2 \cap E_3 \cap \ldots \cap E_z) \tag{5}$$

The following equation is employed to calculate the probability outcome of an AND gate with z input events (E_z) (Verma *et al.*, 2010):

$$P = P(E_1)P(E_2) \ldots P(E_z) \tag{6}$$

The equations used for the calculation of the basic events probability $P(E_j)$ (for the basic event E_j of the Fault Tree), which were derived considering the event type and the assumptions presented previously, are provided in Table 11. The required input parameters include the number of the redundant components, the components maintenance and testing intervals (T_i), the maintenance repair rates (μ_i), the components failure rates (λ_i), the beta factor of the Weibull distribution (β_i) and the probability of failure on demand for the software components (PFD_i).

Table 11 Equations employed for estimation of probability of basic event E_j (based on (Schüller *et al.*, 1997) and (Verma *et al.*, 2010)).

	System components	**Equation**	**Eq. Number**
Operating components	Software, hardware, communication and sensors failures (Schüller *et al.*, 1997) (conservative assumption for software)	$p_{i,j}^{OC} = \lambda_i t$	(7)
	Other components with preventative maintenance	$p_{i,j}^{OC} = T_i^{\beta_i - 1} \lambda_i^{\beta_j} t$	(8)
	Parts with preventive maintenance where a single component failure out of r identical will lead to event occurence (based on (Schüller *et al.*, 1997))	$p_{i,j}^{OC} = \sum_1^r \binom{r}{1} \left(T_i^{\beta_i - 1} \lambda_i^{\beta_j}\right)^r \left(1 - T_i^{\beta_i - 1} \lambda_i^{\beta_i}\right)^{1-r} t$	(9)
	Parts with preventive maintenance where all the r identical components must fail for event occurrence (based on (Schüller *et al.*, 1997))	$p_{i,j}^{OC} = \left[\left(T_i^{\beta_i - 1} \lambda_i^{\beta_i}\right)^r + r T_i^{\beta_i - 1} \lambda_i^{\beta_i} \left(\frac{\lambda_i}{\lambda_i + \mu_i}\right)^{r-1} + \left(\frac{\lambda_i}{\lambda_i + \mu_i}\right)^r\right] t$	(10)
Safety systems	Tested standby equipment failure on demand (except for software failures) (Schüller *et al.*, 1997)	$p_{i,j}^{SS} = 1 + \frac{\left(e^{-\lambda_i T_i} - 1\right)}{\lambda_i T_i}$	(11)
	For safety system/functions with continuous monitoring failure on demand (Schüller *et al.*, 1997)	$p_{i,j}^{SS} = \frac{\lambda_i}{\lambda_i + \mu_i}\left(1 - e^{-(\lambda_i + \mu_i) T_i}\right)$	(12)
	Safety functions with periodical testing failure on demand (Schüller *et al.*, 1997)	$p_{i,j}^{SS} = 1 + \frac{\left(e^{-\lambda_i T_i} - 1\right)}{\lambda_i T_i}$	(13)
	For software failures in safety functions (Schüller *et al.*, 1997)	$p_{i,j}^{SS} = PFD_i$	(14)
	Unavailability due to periodical maintenance of standby equipment where r standby equipment are involved (based on (Schüller *et al.*, 1997))	$p_{i,j}^{SS} = \left(\frac{1/T_i}{1/T_i + \mu_i}\right)^r$	(15)

Table 12 Correction factor for λ_i ratio as function of β_i (Denson *et al.*, 1994).

β_i	$\lambda_i^{Exponential} / \lambda_i^{Weibull}$
1	1.00
2	1.15
2.5	1.12
3	1.10
4	1.06

4.8.2 Importance measures estimation

The Birnbaum's importance measure (I_j^B) (Verma *et al.*, 2010), which is approximated according to equation (16), is employed for the basic events criticality analysis. This metric can be used to identify the components with a significant impact on the top event failure rate (λ^{TE}), thus requiring an improvement of the respective failure rates/probability for reducing the λ^{TE}. In addition, this metric can be used to identify components having a structural importance or occupying important locations of the Fault Tree for the investigated system (Fricks and Trivedi, 2003) and therefore, it depends on the quality of the developed Fault Tree, which is used for the calculation of the top event failure rate.

$$I_j^B = \frac{\partial p^{TE}(\lambda_i)}{\partial p_j} \cong \frac{\partial \lambda^{TE}(\lambda_i)}{\partial p_j} \partial t \approx \frac{\Delta \lambda^{TE}(\lambda_i)}{\Delta p_j} \Delta t \approx \frac{\lambda^{TE}(\lambda_i) - \lambda^{TE}(\lambda_i = 0)}{p_j} \Delta t \text{ , } \Delta t = 1 \; hour \tag{16}$$

The Fussell-Vesely importance measure (I_j^{FV}), which is approximated according to equation (17), is another metric that is employed in this study for facilitating the system criticality analysis (Fricks and Trivedi, 2003, Gomez, 1996, Verma *et al.*, 2010). Based on this metric, the system components, the failure of which will most probably lead to the undesired event are identified (Chybowski *et al.*, 2014), whereas the data quality used for the QA (step 10) is verified.

$$I_j^{FV} = \frac{\partial p^{TE}(\lambda_i)}{\partial p_j} \frac{p_j}{p^{TE}(p_j)} \cong \frac{\partial \lambda^{TE}(\lambda_i)}{\partial p_j} \frac{p_j}{\lambda^{TE}(p_j)} \approx \frac{\Delta \lambda^{TE}(\lambda_i)}{\Delta p_j} \frac{p_j}{\lambda^{TE}(p_j)} \approx \frac{\lambda^{TE}(p_j) - \lambda^{TE}(p_j = 0)}{\lambda^{TE}(p_j)} \tag{17}$$

4.8.3 Uncertainty analysis

Taking into account that it may be a specific challenge to acquire the accurate failure rate values for all the components and failure modes, an uncertainty analysis can be required for the estimation of the Fault Tree top event (Bjerga *et al.*, 2016). However, this can be considered as a voluntary and not compulsory method step. The uncertainty of the top event is estimated by using Monte Carlo simulations considering the failure rates as random variables with a specific Probability Density Function (PDF) based on λ_i, λ_i^{upper}, λ_i^{lower} values and applying random sampling till a predetermined accuracy and error level (Err_{acc}) is achieved. The flowchart of the Monte Carlo process is shown in Figure 14.

The obtained accuracy and error (Err) is estimated according to the following equation (Oberle, 2015):

$$Err = z_{a/2}\frac{\sigma}{\overline{\lambda^{TE}}\sqrt{n_s}} \tag{18}$$

where $z_{a/2}$ is *the* critical value of a normal distribution with zero mean value and standard deviation equal to one for *(1-a)* confidence interval; σ is standard deviation estimated from simulations; n_s total number of simulations; and $\overline{\lambda^{TE}}$ is the mean value for the failure rate of the top event estimated from simulations.

A Lognormal (LN) distribution is assumed as the basic uncertainty distribution for failure rates, as proposed in previous studies (Schüller *et al.*, 1997, Stamatelatos *et al.*, 2011, Durga Rao *et al.*, 2007, Verma *et al.*, 2010). The Error Factor (EF_i) parameter of the LN distribution is estimated according to eq. (19), whilst the parameters of LN distribution are estimated as in (Schüller *et al.*, 1997). The EF_i is used to depict the uncertainty in the λ_i estimation.

$$EF_i = \frac{\lambda_i^{upper}}{\lambda_i} \tag{19}$$

The contribution of each failure rate uncertainty to the top level failure rate uncertainty is assessed according to eq. (20) using the Pearson correlation coefficient ($r_{\lambda^{TE}\lambda_i}$) (Verma *et al.*, 2010).

$$r_{\lambda^{TE}\lambda_i} = \frac{\sum_{t=1}^{n_s}(\lambda_i^t - \overline{\lambda_i^t})(\lambda_t^{TE} - \overline{\lambda^{TE}})}{\sqrt{\sum_{t=1}^{n_s}(\lambda_i^t - \overline{\lambda_i^t})^2 \sum_{t=1}^{n_s}(\lambda_t^{TE} - \overline{\lambda^{TE}})^2}} \tag{20}$$

where λ_i^t is the failure rate at each estimation for the *i^th^* component; $\overline{\lambda_i^t}$ is the mean value of λ_i according to the derived simulation results; and λ_t^{TE} is the estimated λ^{TE} at the t^{th} simulation. Thus, the $r_{\lambda^{TE}\lambda_i}$ value depends on the λ_i, λ_i^{upper}, λ_i^{lower} values and the selected distribution.

To assess the influence of the distribution on the uncertainty analysis, the uncertainty analysis is repeated for triangular (TR) and uniform (UN) distributions. This is necessary to investigate how the parameters of the distribution affect the uncertainty of λ^{TE}. The parameters of a TR distribution (*a,c,b*) were taken as (λ_i^{lower}, λ_i, λ_i^{upper}), whilst they considered to be (λ_i^{lower}, λ_i^{upper}) for the UN *(a,b).*

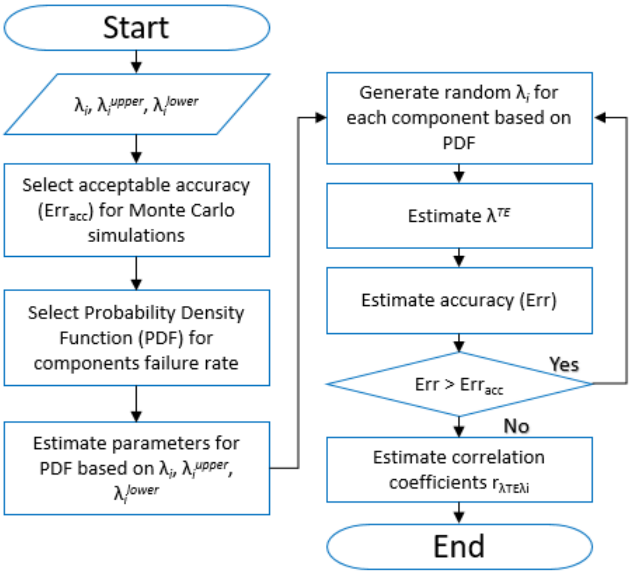

Start
λ$_i$, λ$_i^{upper}$, λ$_i^{lower}$
Select acceptable accuracy (Err$_{acc}$) for Monte Carlo simulations
Select Probability Density Function (PDF) for components failure rate
Estimate parameters for PDF based on λ$_i$, λ$_i^{upper}$, λ$_i^{lower}$
Generate random λ$_i$ for each component based on PDF
Estimate λ^{TE}
Estimate accuracy (Err)
Err > Err$_{acc}$
Yes
No
Estimate correlation coefficients r$_{λTEλi}$
End

Figure 14 Flowchart for Monte Carlo simulations.

4.9 Chapter summary

In this chapter, the rationale behind the proposed method steps was presented. The method starts with STPA, proceeds with "Event Trees" development based on ESI and continues with Fault Tree analysis, integrates the results of different analysis steps at intermediate steps and finishes with quantitative analysis. During the quantitative analysis the failure rate for the top event as well as importance measures are estimated. Provisionally, uncertainty analysis can be implemented. In the next Chapters the different application case studies of the novel method are presented and discussed.

5 APPLICATION CASE STUDY – EXHAUST GAS OPEN LOOP SCRUBBER SYSTEM

5.1 Chapter outline

In this Chapter, the application of the developed novel method on a relatively simple CPS system, in particular for the case of the exhaust gas open loop scrubber system is demonstrated. The system description and the analysis input are provided, whereas the derived results are presented in subsequent section. Based on these results analysis, the method advantages are discussed.

5.2 System description and analysis input

For the application and demonstration of the developed method, a rather simple Industrial automation and Control System (ICS) has been selected, in particular the case of an open loop exhaust gas scrubber system. This can be considered as a simple example of CPS, as it consists of a Programmable Logic Controller, the relevant actuating systems (pumps, scrubber unit, valves, etc.) and the sensors for controlling the exhaust gas treatment process.

The main purpose of the exhaust gas scrubber is to reduce the SOx emissions to air during the ship main engine and auxiliary engines operation running on Heavy Fuel Oil, which has high sulphur content. The exhaust gases exiting the ship main and auxiliary engines are washed by injecting sea water. The sea water has a slightly higher pH (around 8) and it will react with the SOx dissolved in water. The main components of the open loop scrubber system are demonstrated in Figure 15 (Alfa Laval, 2017b).

The main functions of the open loop exhaust gas scrubber system components are provided in Table 13. The exhaust gas scrubber control system can shut-down the scrubber operations by closing the valves and turning off the sea pumps. It also regulates the sea water flow rate and the operating status of the sea water pumps based on the estimation of the ship main and auxiliary engines fuel flow as well as the system pumps health status. The process is supervised by the crew, which can implement switching over to a fuel with a low sulphur content if the SOx emissions exceed the acceptable criteria. As an optional function, the exhaust gas scrubber control system could monitor the health status of the scrubber unit and predict its failures. In such a case, it is assumed that all the scrubber unit failures can be handled by the ship crew by switching over to the low sulphur fuel. For the sake of the case study, it is considered that the scrubber and SOx sensor failure are not continuously monitored by the alarm monitoring system, so the crew is not aware of the specific failures in order to switch off the scrubber system. It is also assumed that the crew can only mitigate the system hazards, but do not introduce the new hazards, so crew cannot inadvertently switch off the exhaust gas scrubber system when the ship engines operate using HFO.

The failure rates used as input for this analysis are provided in Table 14. The inspection and testing intervals for the SOx sensor and the standby pump are considered to be 5,000 hours (Alfa Laval, 2017a) and it is assumed that these components maintenance is in line with the manufactures guidelines (Alfa Laval, 2017a).

The analysis in this study investigated the exhaust gas open loop system shown in Figure 15 considering the following functionalities and alternative configurations: (a) regular testing of the SOx emissions sensor (without continuous monitoring); (b) continuous monitoring of the SOx emissions sensor (the SOx emissions sensor failure/erroneous measurements are immediately identified using advanced diagnostic techniques); (c) when scrubber unit failures (Scrubber body, piping, droplet, venturi, injection nozzles) are monitored using diagnostic/prognostic techniques and immediately diagnosed, and; (d) with two installed SOx emissions sensors.

Table 13 Exhaust gas open loop scrubber system main components and their functions.

Component	Function
Scrubber controller	Control of the sea water flow to the scrubber unit, monitoring of scrubber unit health status (provisional function)
Inlet sea chest valve	Sea water flow control (can be either open or closed)
Outlet sea chest valve	Sea water flow control (can be either open or closed)
Sea Water Pump	Increasing/Decreasing sea water flow
Scrubber Unit (Scrubber body, piping, droplet, venturi, injection nozzles)	Exhaust gases spraying
Sensors (SOx emissions, pressure, pH, conductivity, CO2 emissions)	Measuring operating parameters

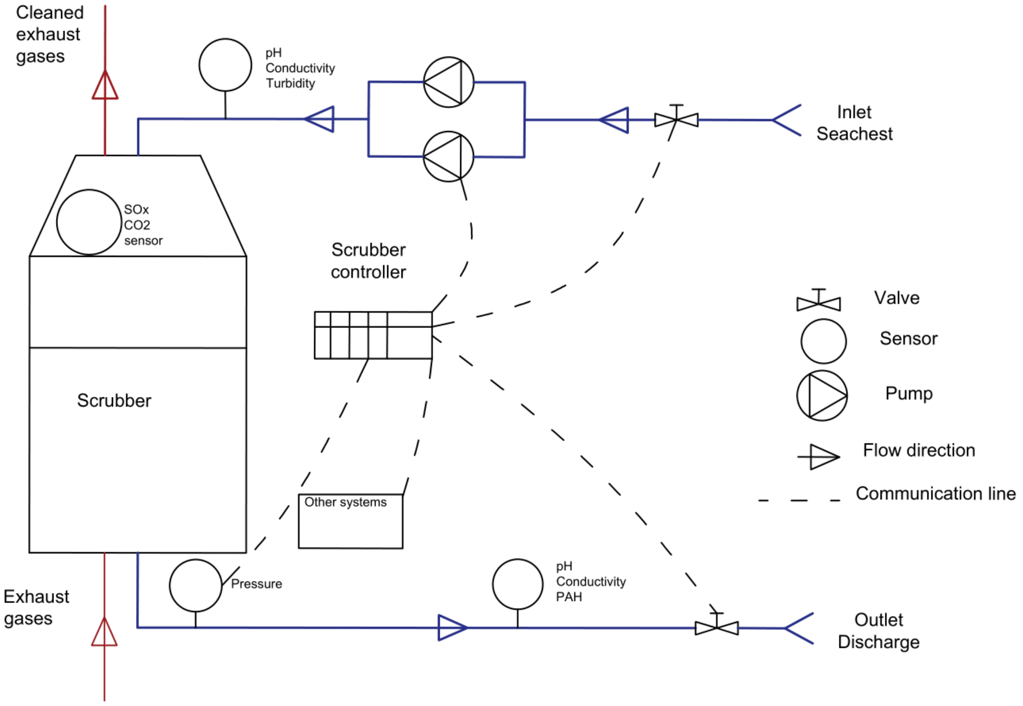


Figure 15 The investigated exhaust gas scrubber system layout (based on (Alfa Laval, 2017b)).

Table 14 Components failure and maintenance rates.

Failure rate description	PFD/failure rate
Commission errors for software functions [h^{-1}] (SINTEF, 2006)	1.00 10^{-5}
Omission errors for software functions (probability of failure on demand (PFD)) (SINTEF, 2006)	5.00 10^{-5}
PID controller failure to react/ overreaction to changes in system configuration due to software errors [h^{-1}] (Aldemir *et al.*, 2007)	1.00 10-6
Controller hardware failure rate [h^{-1}] (SINTEF, 2006)	1.50 10-5
Communication lines failure rate [h^{-1}] (Chai *et al.*, 2016)	2.50 10-8
Fuel sensor failure rate (for engines and auxiliary generating sets) [h^{-1}] (OREDA, 2015)	2.00 10^{-6}
Human error probability of failure on demand (British Standards Institution (BSI), 2004)	1.00 10^{-3}
Pump failure rate [h^{-1}] (OREDA, 2015)	3.02 10^{-5}
Injection nozzles failure rate [h^{-1}] (Andersen, 2015, Pavlidis, 2018)	4.58 10^{-6}
Venturi failure rate [h^{-1}] (Andersen, 2015, Pavlidis, 2018)	1.53 10^{-6}
Droplet separator failure rate [h^{-1}] (Andersen, 2015, Pavlidis, 2018)	1.53 10^{-6}
Body failure rate [h^{-1}] (Andersen, 2015, Pavlidis, 2018)	1.53 10^{-6}
Piping failure rate [h^{-1}] (Andersen, 2015, Pavlidis, 2018)	7.88 10^{-6}
Significant power increase in engine/auxiliary engines load [h^{-1}] Approximation of operating profile, based on cruise ship vessel	1.00 10^{-1}
SO_x sensor failure rate [h^{-1}] (Andersen, 2015, Pavlidis, 2018)	1.76 10^{-6}
Pressure sensors failure rate (OREDA, 2015) [h^{-1}]	2.00 10^{-6}
Sensors maintenance rate – Assumption [h^{-1}] it considered that under continuous monitoring of sensor failures, their correction is implemented almost immediately	1
Inconsistent diagnostic/prognostics model resulting in false negatives (test indicates that no failure is observed in the system whilst it is present) – Assumption (PFD) Rather conservative	0.1
β_i for all components (Exponential distribution is assumed)	0

5.3 Results and discussion

5.3.1 STPA results (CASA Steps 1-4)

A number of accidents and hazardous scenarios that can arise in the investigated exhaust gas scrubber system are provided in Table 15 (results of step 1). The list was identified based on previous research studies(Andersen, 2015, Pavlidis, 2018) as well as reviewed by partners from DNV GL. As it can be observed, even though the system is simple and non-safety-critical, a number of accidents and hazards can occur, which may result in human injury or death, as well as damage to equipment or environment. The analysis in the CASA method subsequent steps will focus on the environmental pollution [A-3] and specifically on [H-5] (Exhaust gas not complying with regulatory requirements.), as this study scope is to demonstrate the functionality of the CASA method. As elaborated in Sections 1 and 3, the proper spraying of exhaust gas is an important scrubber function and its failure may result in environmental pollution and strict financial penalties. The hazard [H-5] is used for the development of the hierarchical control structure (step 2) and the identification of the UCAs (step 3).

The system control structure (results of step 2) is provided in Figure 16. It can be observed that the control loop incorporates two controllers, the scrubber control system, and the human operator. The scrubber controller uses as input the ship engines fuel flow to control the pumps operating status, the sea water flow and the control valves status. The crew can implement the fuel change command and switch off the scrubber, in cases where the measured SOx emissions exceed the regulatory threshold. In cases where a provisional functionality is available in the scrubber controller for monitoring the scrubber body failures based on pressure measurements, then the crew can immediately implement the fuel change to a low Sulphur fuel, when scrubber body failure occurs. Measuring the discharged sea water pH is also an important measure to ensure that the discharged sea water is in compliance with the environmental regulations. But since this measure is not relevant to [H-5], it is not included in the hierarchical control system. The hierarchical control structure is used for the identification of the UCAs (step 3) and their causal factors (step 4).

The list of identified Unsafe Control Actions (UCAs) is provided in Table 16 (results of step 3). In total 10 UCAs were identified for the system hazard [H-5]. The 10th identified UCA is applicable only if a new functionality performing the exhaust gas scrubber unit health diagnosis/prognosis is employed (case c as described in Section 3). The identified UCAs are found to be of Type 1 (not provided), Type 2 (provided) or Type 3 (provided too early/late/out of sequence). This is attributed to the fact that mostly discrete control actions, such as start, open or close are considered. So, Type 4 UCA (stopped too soon/applied for too long) for many of the identified UCAs can be considered as equivalent to Type 1 UCAs; for example, a start pump stopped too soon would be equivalent to not providing a control action (not starting the pump) in its final effect, leading to the specific hazard. Type 4 UCA, instead, is more applicable if the control action exhibits some variation in its effect, as in the case of the PID controllers, where overshoots can occur. However, in this case they are either covered by other UCAs Type or do not lead to the investigated hazard. Based on the UCAs shown in Table 7, their causal factors are identified (step 4). The UCAs are also used to support the "Event Trees" development (step 5) as well as in step 7 to enrich the Fault Tree developed in step 6. The UCAs are also utilised to indicate which physical failures might need further elaboration in step 9.

The causal factors list for the identified UCAs is provided in Table 17 (step 4). In total 26 causal factors are identified. For the majority of the UCAs, software failures are considered as causal factors. In this study, software failure refers to all those conditions, which may lead to the controller inability to implement a specific function due to errors in the software design, integer overflows, software bugs, communication errors in the controller, etc. They are treated as software failure because the available statistical data does not offer their further description. The human error depicts the failure of the human operator to act as a protective barrier. The human error was also treated on a high-level based on the relevant statistical data reported in IEC 61511 (British Standards Institution (BSI), 2004). The identification of human failure causes is out of the scope of this research. The results of this step are used in step 7 to enrich the Fault Tree developed in step 6.

Table 15 Accidents in the scrubber system.

Accident	Open loop scrubber hazard	Risk control measures
[A-1] Human loss or injury	[H-1] Operating personnel touching hot surfaces [H-2] Exhaust gases leakage depriving the engine room from oxygen	Protective surfaces, personnel training, oxygen level monitoring in engine room
[A-2] Damage to ship/ship systems	[H-3] Overpressure in scrubber unit [H-4] Water ingression	Diagnosis of system failures Use of non-return valves
[A-3] Environmental pollution	[H-5] Exhaust gas not complying with regulatory requirements. [H-6] Disposed sea water does not comply with regulations.	SOx sensor Sea water analysers

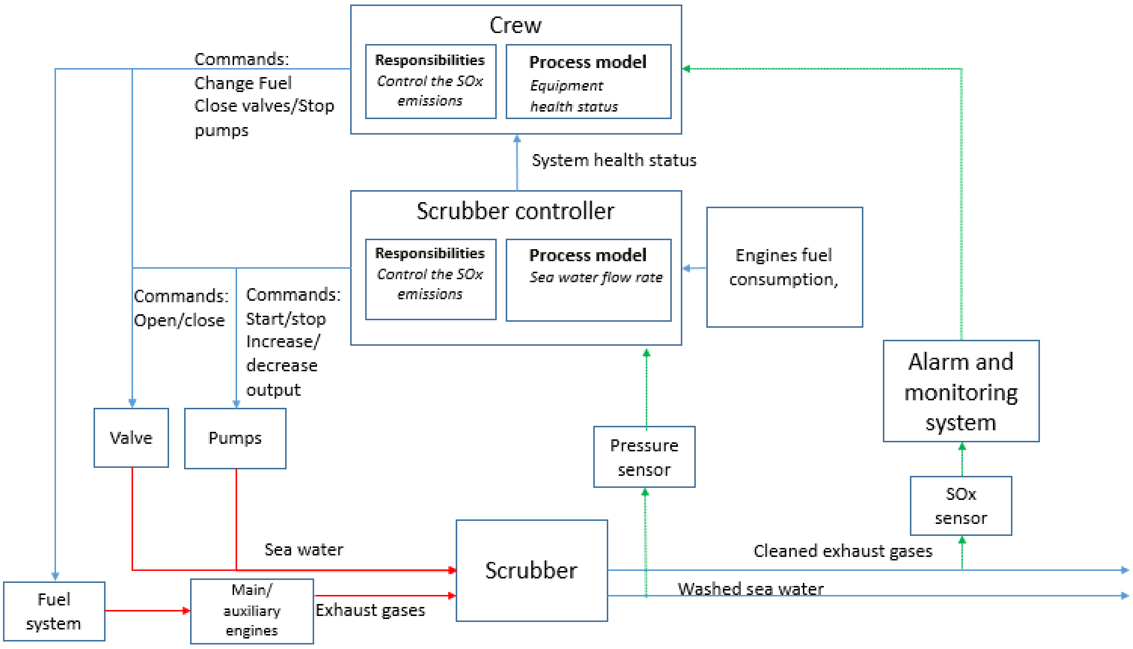


Figure 16 Scrubber control structure.

Table 16 Identified UCAs.

Control Action	Type of UCA causing hazard	UCA a/a	Description
Close valves	Providing	1	Closing valves during normal operation/faulty conditions will restrict the scrubber functionality [H-5]
Start pump	Not providing	2	Not starting the standby sea water pump when the other pump is faulty/insufficient will inhibit the scrubber operation due to lack of sea water flow [H-5]
	Providing with delay	3	Starting sea water pumps with delay will inhibit the scrubber operation due to the lack of sea water flow [H-5]
Stop pump	Providing	4	Stopping pump during normal operation will cause unavailability of sea water in scrubber [H-5]
Increase sea water flow	Not providing	5	Not providing sea water flow increase when the auxiliary/engines output increase may lead to noncompliance with regulations [H-5]
	Providing with delay	6	Providing sea water flow increase with delay when the auxiliary/engines output increase may lead to noncompliance with regulations [H-5]
Decrease sea water flow	Providing	7	Decreasing sea water flow when the auxiliary/engines output increase/stable may lead to noncompliance with regulations [H-5]
Issue alarm	Not providing	8	Not issuing alarm, when the system SOx emissions are not in compliance will lead to noncompliance with regulations [H-5]
Implement fuel change over	Not providing	9	Not changing fuel during faulty operation of the scrubber will lead to noncompliance with regulations [H-5]
Diagnose and predict scrubber failures	Not providing	10	Not diagnosing and predicting failures in scrubber may lead to operation with faulty scrubber system [H-5]

Table 17 Causal factors.

UCA a/a	Causal factors
1	Software failure, engine and auxiliary generator sets fuel sensors failure
2	Pump failure, controller hardware failure, communication failure, software failure, controller hardware failure
3	Software failure (Wrong software implementation on controller)
4	Software failure, engine and auxiliary gets load/fuel sensors erroneous measurement
5	Software failure, controller hardware failure, communication failure, engine and auxiliary gets fuel sensors erroneous measurement
6	Software failure
7	Software failure, engine and auxiliary generator sets load sensors erroneous measurement
8	SOx sensor failure
9	Human error
10	Software failure, inconsistent physical model, pressure sensor errors

5.3.2 ESI results (CASA Step 5)

The “Event Tree” derived by applying the ESI for the hazard [H-5] is provided in Figure 17, which also depicts the relations between the UCAs and the different events of “Event Tree”. As it is deduced from this figure, the UCAs support the development of the “Event Tree”. When the exhaust gas system operation does not comply with the emission regulations ([H-5]), the SOx emissions sensor provides an alarm. This can be used from the crew to switch the engine operation to the low sulphur fuel usage and simultaneously to switch off the scrubber system. If crew fails to do that, the first hazardous scenario occurs. If the SOx sensor is faulty, then the crew will be unaware of potential noncompliance with the emissions regulations (scenario 2). The developed “Event Tree” will be converted to a Fault Tree in the next step (step 6).

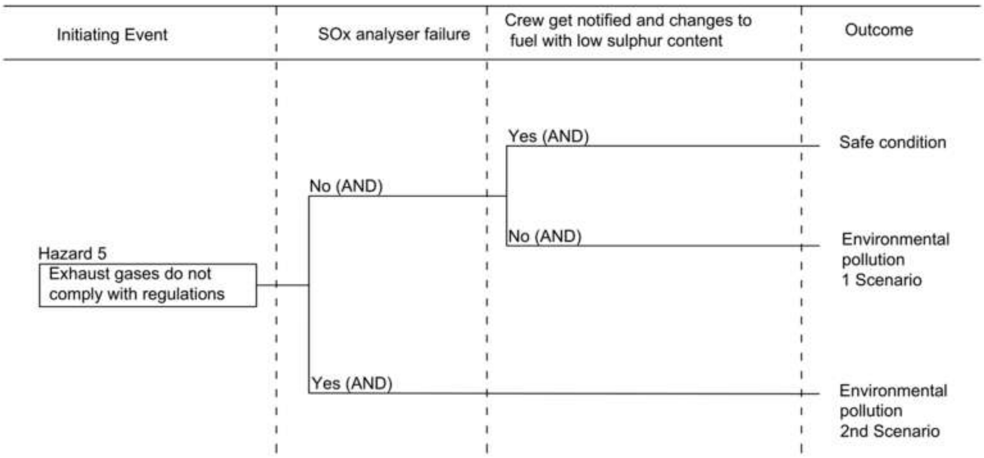

Initiating Event
SOx analyser failure
Crew get notified and changes to fuel with low sulphur content
Outcome
Yes (AND)
Safe condition
No (AND)
No (AND)
Environmental pollution 1 Scenario
Hazard 5
Exhaust gases do not comply with regulations
Yes (AND)
Environmental pollution 2nd Scenario

Figure 17 ESI results

5.3.3 STPA and ESI results integration (CASA Steps 6-8), FTA results (CASA Step 9)

Since the investigated system is simple, there are no interactions between the different developed “Event Trees”. By transforming the “Event Tree” (step 6) and enriching it with the results of STPA (step 7), the Fault Tree shown in Figure 18 is generated. As the causal factors are given in Table 17, the causal factors were not developed further in Figure 18. The developed Fault Tree includes the two scenarios leading to environmental pollution, inheriting the structure of the “Event Tree” from Figure 17. This Fault Tree is refined further in step 8.

If we ignore steps (5-6), the Fault would be developed by connecting all the UCAs by OR gate. In the hypothetical case all the UCAs (UCAs 1-10) were connected using OR gate, then either ‘Closing valves during normal operation/faulty conditions will restrict the scrubber functionality [H-5]’ (UCA 1) or ‘Not changing fuel during faulty operation of the scrubber [H-5]’ (UCA10) would lead to the hazard [H-5], that is noncompliance with regulations. However, it is known from experience that these two UCAs must occur at the same time (there is a need for AND gate). Potentially, it would be possible to identify this relationship using the safety analyst experience. Nonetheless, using the ESI adds rigor to the analysis; hence ESI was included in the CASA method.

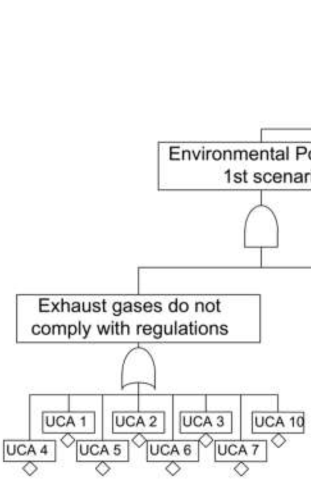

A-3
Environmental Pollution - 1st scenario
Environmental Pollution - 2nd scenario
Exhaust gases do not comply with regulations
SOx analyser failure
Exhaust gases do not comply with regulations
SOx analyser normal operation
Crew does not change fuel
UCA 1
UCA 2
UCA 3
UCA 10
UCA 4
UCA 5
UCA 6
UCA 7
UCA 8
UCA 9

Figure 18 Fault Tree populated with STPA results (Step 6)

After applying the refinement rules provided in Table 10 (step 8), the Fault Tree shown in Figure 19 is developed. As shown in Figure 19, the refinement was applied to UCAs 1-3 and 5-7 context (refinement rule 1, Table 10) and for the common causal factors to UCA 5 and 7 (erroneous measurement of fuel flow) (refinement rule 4, Table 10). The system is rather simple; hence no other refinements were required. In more complex systems, such as DEP system, more refinement rules would be applicable. The Fault Tree of step 8 is enriched with the results of FTA for physical failures, thus providing the finally developed Fault Tree (shown in Figure 18), which is the output of the CASA method qualitative analysis. The FTA (step 9) is applied to the scrubber system to identify the components that may fail. Only five scrubber unit components have been considered in the analysis. The results of the FTA are also provided in Figure 19. The results of FTA are similar to the structural breakdown of the scrubber unit. The final Fault Tree depicted in Figure 19 is used for the purpose of quantitative analysis (step 10). The results for the cases a-d are almost identical. There is no difference in structure for case a and b. The location of the optional functionality for case (c) is also provided in the modified Fault Tree in Figure 19. For case (d) instead of one sensor two sensors are provided.

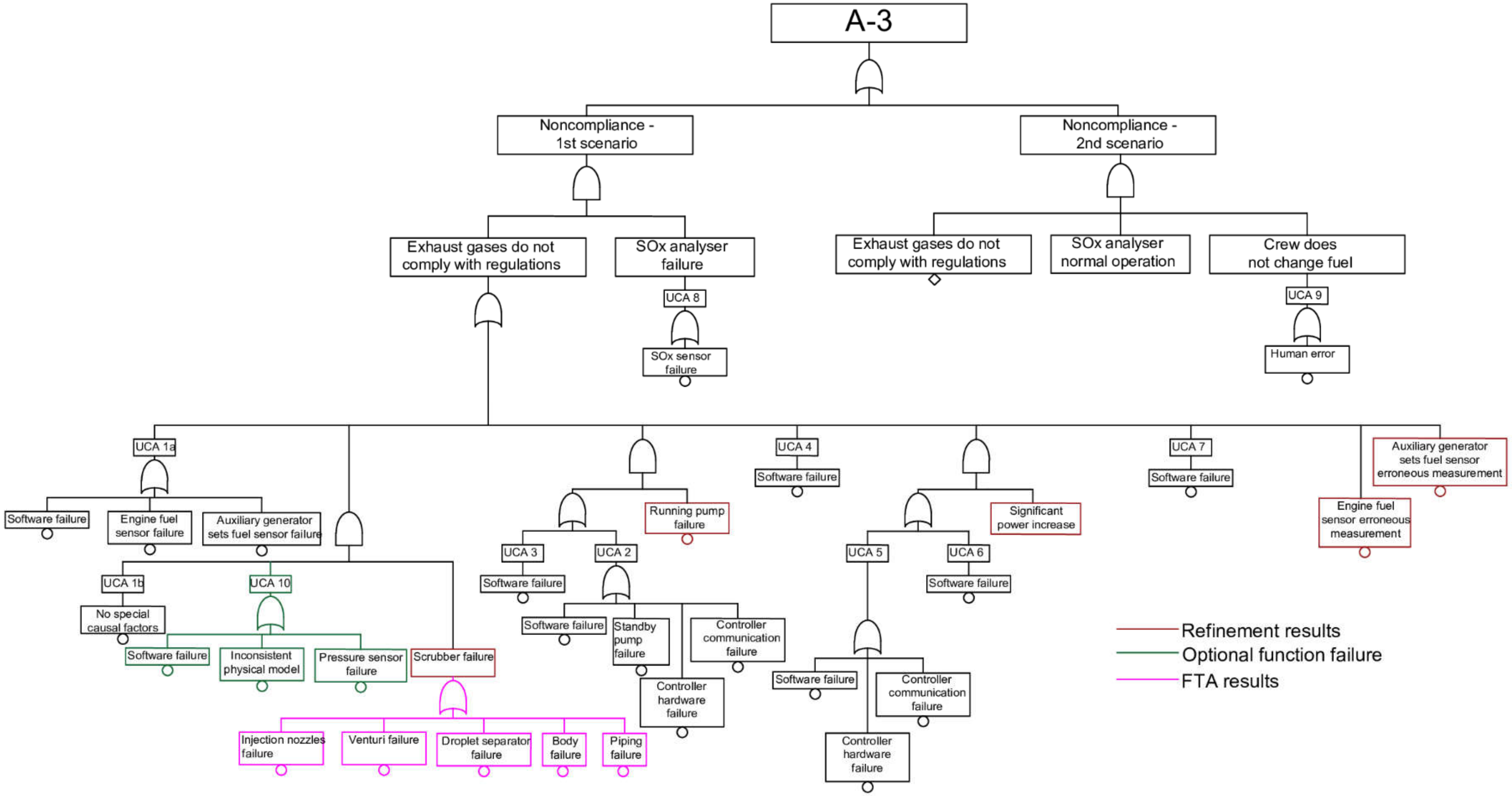

A-3
Noncompliance - 1st scenario
Noncompliance - 2nd scenario
Exhaust gases do not comply with regulations
SOx analyser failure
Exhaust gases do not comply with regulations
SOx analyser normal operation
Crew does not change fuel
UCA 8
SOx sensor failure
UCA 9
Human error
UCA 1a
Software failure
Engine fuel sensor failure
Auxiliary generator sets fuel sensor failure
UCA 1b
No special causal factors
UCA 10
Software failure
Inconsistent physical model
Pressure sensor failure
Scrubber failure
Injection nozzles failure
Venturi failure
Droplet separator failure
Body failure
Piping failure
Running pump failure
UCA 3
Software failure
UCA 2
Software failure
Standby pump failure
Controller communication failure
Controller hardware failure
UCA 4
Software failure
Significant power increase
UCA 5
UCA 6
Software failure
Software failure
Controller communication failure
Controller hardware failure
UCA 7
Software failure
Auxiliary generator sets fuel sensor erroneous measurement
Engine fuel sensor erroneous measurement
Refinement results
Optional function failure
FTA results

Figure 19 Refined Fault Tree developed in Step 9.

5.3.4 Quantitative Analysis (CASA Step 10)

The results of estimating the top event failure rate by considering the different system functionalities (cases (a) to (d) as described in Section 5.2) are provided in Table 18. The results of the importance metrics estimation (cases (a) to (d) as described in Section 4.8.2) are provided in Table 19. Only the five top failures according to each metric and system functionalities are demonstrated. The results of importance analysis are presented in a reduced ranking order, proceeding from the most critical to the less critical failures according to each importance measure.

As it can be deduced from the derived Birnbaum metric values for case a, the top event failure is sensitive to the scrubber components failures and various software failures in the system with the regular SOx sensor testing (case a). The top event failure rate will emanate from the SOx sensor failure and some scrubber unit failures as well as the scrubber controller software failure according to Fussell-Vesely metric for case a. Therefore, the system safety performance can be improved if safety measures to address the SOx emissions sensor failure are implemented.

As it can be observed from Table 18, the implementation of continuous monitoring and diagnosis of the SOx sensor failures (case b) instead of regular testing of SOx sensor will lead to significant decrease in top event failure (several orders of magnitude). However, the human error becomes a more critical failure according to the calculated Fussell Vesely metric (Table 19). The scrubber and controller failures still remain critical failures with this additional system function. Therefore, to enhance the system safety performance further, it is required to provide information for the system conditions to support the crew in making decisions.

Instead, the application of diagnosis/prognosis techniques for the scrubber failure leads to approximately 27% reduction in the top event failure rate as depicted in Table 18 (case c). In case c, the system top failure rate becomes also sensitive to failures of the sensors used to control the sea water flow (Table 19). The most probable cause of the system failure according to the Fussell-Vesely metric remains the SOx sensor failure and various scrubber components failures (Table 19). So, with this system functionality, system safety enhancement will occur when redundancy to the SOx emissions sensor measurements is provided.

Installation of two SOx sensors (instead of one) also results in a significant reduction of the top event failure rate (an order of magnitude) (Table 18). In case d, the failure of the SOx sensors (both fail) still remain critical, but their importance is reduced compared to the case with the regular SOx sensor failure (Table 19). The other importance analysis results are similar with the previous cases importance analysis results. Thus, the system safety in case c can be enhanced by closely monitoring the scrubber unit components for detecting failures.

Based on the presented results, it can be concluded that the exhaust gas open loop scrubber system compliance with the SOx emission regulations can be enhanced when functionality of the SOx emissions sensor is continuously monitored or two SOx emissions sensors (redundancy) are installed. The scrubber unit components failures seem to be critical for the normal system operation. The installation of diagnosis/prognosis technologies will lead to the system design improvement, however not as effectively as the installation of continuous monitoring system for the SOx sensor failures or an additional SOx emissions sensor. If diagnosis/prognosis techniques are employed, then the top event failure rate will become sensitive to other failures such as in fuel flow sensors, so redundancy in fuel measurements would be recommended. However the cost-effectiveness of the suggested measures is outside the scope of present study.

Table 18 Top event failure rate for different system functionalities.

Case (a) With regular testing of SOx sensor (without continuous monitoring)	Case (b) With continuous monitoring of SOx sensor failures	Case (c) With application of diagnosis/prognosis for scrubber unit failures and with regular testing of SOx sensor	Case (d) With two SOx sensors installed
1.99 10^{-6} [h^{-1}]	5.68 10^{-8} [h^{-1}]	1.44 10^{-6} [h^{-1}]	1.23 10^{-7}

Table 19 Importance metrics estimation results.

No	With regular testing of SOx sensor (without continuous monitoring)		With continuous monitoring of SOx sensor failures		With application of diagnosis/prognosis for scrubber unit failures and with regular testing of SOx sensor		With two SOx sensors installed	
	Birnbaum [-]	Fussell-Vesely [-]	Birnbaum [-]	Fussell-Vesely [-]	Birnbaum [-]	Fussell-Vesely [-]	Birnbaum [-]	Fussell-Vesely [-]
1	Injection nozzles failure 0.070	SOx sensor failure 0.972	Injection nozzles failure 0.002	Human error 0.986	Injection nozzles failure 0.039	SOx sensor failure 0.972	Injection nozzles failure 0.004	SOx sensor failure 0.543
2	Venturi failure 0.070	Controller software closing valves 0.178	Venturi failure 0.002	Controller software closing valves 0.178	Venturi failure 0.039	Controller software closing valves 0.247	Venturi failure 0.004	Human error 0.457
3	Controller software closing valves 0.035	Controller software stopping pump 0.178	Controller software closing valves 0.001	Controller software stopping pump 0.178	Controller software closing valves 0.035	Controller software stopping pump 0.247	Controller software closing valves 0.002	Controller software closing valves 0.178
4	Controller software stopping pump 0.035	Injection nozzles failure 0.163	Controller software stopping pump 0.001	Piping failure 0.140	Controller software stopping pump 0.035	Injection nozzles failure 0.124	Controller software stopping pump 0.002	Controller software stopping pump 0.178
5	Piping failure 0.035	Piping failure 0.140	Piping failure 0.001	Venturi failure 0.054	Auxiliary engine fuel sensor failure 0.035	Auxiliary engine fuel sensor failure 0.074	Piping failure 0.002	Injection nozzles failure 0.163

5.4 Discussion on the method

To the best knowledge of the authors, no article or conference paper which demonstrates results of scrubber safety analysis, is currently available. Only two master thesis have been identified focusing on this type of system safety analysis (Andersen, 2015, Pavlidis, 2018). Comparing these studies with the present is challenging due to some differences in the considered systems, the experience level of the involved safety analysts and used input data. A more robust comparison would be based on implementing a FTA for the same system, using the same data and similar expertise level teams of safety experts. Still it could be argued that the FTA guided in both cases the students to specific results, and inference about the method can be made.

It can be observed that the considered top events in the systems in these studies (Andersen, 2015, Pavlidis, 2018) are rather slightly different from the top event of the present study. In the present study, the top event was the noncompliance with the regulations, whilst in the investigated master theses one of the Fault Trees top event was improper treatment of exhaust gases (Figure 19). However, it can be observed that the Fault Tree derived by the CASA method incorporated the SOx emissions sensor failure at much higher level connected to other events using an AND gate, highlighting its importance. In the other studies Fault Trees (Andersen, 2015, Pavlidis, 2018), the SOx sensor failure was not included. Therefore, the present analysis considered more failures related to the top event. This can be attributed to the inclusion of the STPA and ESI results. STPA is a top-down approach, which guides the analysis of specific undesired events (called accidents in the STPA framework) and system states (hazards) rather than of system component failures. The ESI results can be used to demonstrate how the hazards propagate to accidents; the SOx sensors failure appeared in the Fault Tree (Figure 17) based on this approach. Human failure was also incorporated in the present analysis. However, it was out of the analyses scope analyses reported in (Andersen, 2015, Pavlidis, 2018).

In addition, several software failures were not considered in theses analyses, whereas they are considered in the present study, such as ‘scrubber control system not increasing sea water flow/ decreasing sea water flow in the system’ or ‘scrubber control system shutting down the system’. This needs to be included in the analysis, as they contribute to the improper treatment of the exhaust gases. Based on that, it can be argued that thanks to incorporation of the STPA results, new scenarios are considered in the Fault Tree structure. Therefore, it could be claimed that the proposed CASA method guides a more accurate safety analysis, which incorporates software failures, addressing the software-intensive character of the modern ICS and CPSs.

In addition, the refinement, which was applied to the identified UCAs, allowed for the better consideration of the temporal system behaviour. In specific, the consideration of probability of UCA context, such as ‘significant power increase’ allowed for the incorporation of cases where a specific

UCA can become hazardous and their consideration in the analysis quantitative step. This is often a case for ICS, as specific control actions become hazardous only in specific system context (Leveson, 2011b).

The structure of the final Fault Tree developed in step 9 of this study is different from the Fault Trees presented in other studies FTA (Andersen, 2015, Pavlidis, 2018), which can be considered as the open-loop scrubber system breakdown. In addition, they also incorporated the failures during the system start-up. In this way, failures that can occur at different operating phases without any relation were incorporated in one Fault Tree (Andersen, 2015, Pavlidis, 2018). This is not true in the actual system operation, as several factors must occur simultaneously or in a sequence, in order for a top event to occur in modern CPSs. In the present study Fault Tree, there is a logical sequence of events, which is depicted using AND gates as connectors. For instance, a failure in scrubber system together with the SOx emissions sensor failure must occur, so that the system is noncompliant with the existing SOx regulations. Therefore, it can be argued that the presented Fault Tree, thanks to the ESI, more effectively considered the system multi-points failures and temporal character.

The method allowed for the comparison of the system behaviour using quantitate metrics in cases where advances monitoring/diagnostics functionalities were considered. It was demonstrated that when including diagnosis/prognosis techniques or the SOx emissions sensor failures continuous monitoring settings changes the system safety performance significantly, overcoming this STPA limitation. This can be useful when considering the implementation of new functions in system or design alternatives during the system design phase.

Based on the preceding discussion, the expected advantages of the method are shown in Table 20.

Table 20 Expected advantages/disadvantages of new method with respect to effectiveness versus constituent methods

		STPA	FTA	ETA	FLSA	FI	CASA
Efficiency criteria	Heterogeneity (Missing interactions between heterogeneous components)	++	++	++	++	++	+++
	Interoperability (Common cause failures/ dependencies between components/architecture)	+	++	++	+++	++	+++
	Connectivity (Cyber-security threats)	++	+	+	++	++	++
	Software-intensive (Control failures)	+++	+	+	++	++	+++
	Evolution in time (Model-based approach/alterations in time)	+	+	+	+++	+++	+
	Dynamic reconfiguration (Multipoint failures/Temporal relationships)	+	++	+++	+	+++	+++
	Autonomous decision-making (Environmental context)	+	+	+	+	++	+
Utility criteria	Risk metrics estimation criteria	+	+++	+++	+++	++	+++
	Ranking criteria	+	+++	+++	+++	++	+++
	Automated safety monitoring system	+	++	++	+++	++	+++

High effectiveness: The method/study naturally leads to identification of related scenarios / risk metrics estimation / ranking based on importance criteria / development of model fit for automated safety monitoring including sensors measurements	+ + +	Moderate effectiveness: The method/study leads to identification/capturing of some related scenarios / approximate risk metrics estimation / qualitative ranking / development of model fit for some scenarios automated safety monitoring with indication of how to integrate with sensors	+ +	Low effectiveness: The method/study leads to identification of limited number of related scenarios / no risk metrics estimation / no ranking / model not fit for automated safety monitoring or no integration with sensor measurements	+

5.5 Summary

In this chapter, a novel method was applied for the safety analysis of the open loop exhaust gas scrubber system. The developed method guided and resulted in a more accurate safety analysis, compared with previous studies for the same system by incorporating the system software failures represented by the UCAs, considering the system states, probabilities, and temporal relationships. The CASA method also allowed for the investigation of the system behaviour for cases where new functions are added to the system, as was demonstrated with the diagnosis/prognosis techniques applied to the SOx sensor and scrubber. The proposed method allowed for the estimation of the top event failure rate and the identification of the most important factors and failures affecting the safety-related event guiding the safety enhancement. The implementation of diagnosis techniques for the SOx sensor failures or two SOx sensors is expected to significantly reduce the system noncompliance frequency with regulations. Implementation of diagnosis/prognosis techniques for the scrubber unit failures is expected to reduce the frequency of noncompliance, but to a much lesser extent.

This page has been intentionally left blank

6 APPLICATION CASE STUDIES - CRUISE SHIP POWER SYSTEMS DESCRIPTION

6.1 Chapter outline

In this Chapter the investigated DEP systems information is provided. First, a generic DEP system information, main subsystems, their functionalities, and main design parameters are provided. Then ship operating data, failure rates inspection and testing intervals are disclosed in the subsequent section and relevant appendices. The system and analysis assumptions are also presented. Finally, the rationale for selected investigation case studies is explained.

6.2 Cruise ship power plant subsystems description

The primary objective of the DEP plant is the generation of electrical power, the distribution of the power and its transformation in another useful form of function (propulsion, hotel load etc.). Smooth power generation, distribution and transformation requires its proper control. Based on these basic functions, the DEP system break down into subsystems, assemblies and components is given in Figure 20, whereas its detailed description is provided in Appendix A. The control structure for the main subsystems of the DEP plant is also provided in Figure 21. The main design parameters of the investigated power plants are also reported in Table 21.

In this study, a DEP system consisting of 6 diesel-generator sets was selected as the reference system for investigation. In addition, a number of alternatives considering different fuels, different number of generator sets, and various options for the energy recovery are also investigated. The investigated reference system and the list of alternatives is provided in Table 22, whilst the systems layout is illustrated in Figure 22. The investigated DEP plants require for their operation a number of auxiliary systems including the fuel system, the lubricating oil system and the cooling water systems. These auxiliary systems layouts are provided in Appendix B. The necessary information was retrieved from manufacturer drawings and where the information in drawings was inconclusive, the system description was enhanced using data from the available literature (Ådnanes, 2003, Kongsberg, 2007, Radan, 2008, MAN, 2012, Krogseth, 2013, Meyle, 2015). The alternative DEP systems have been selected on the basis of their cost-effectiveness compared to others as identified in a previous research optimisation study (Bolbot *et al.*, 2020) or on the basis of interest for their applicability to the cruise-ship DEP system as in case of batteries.

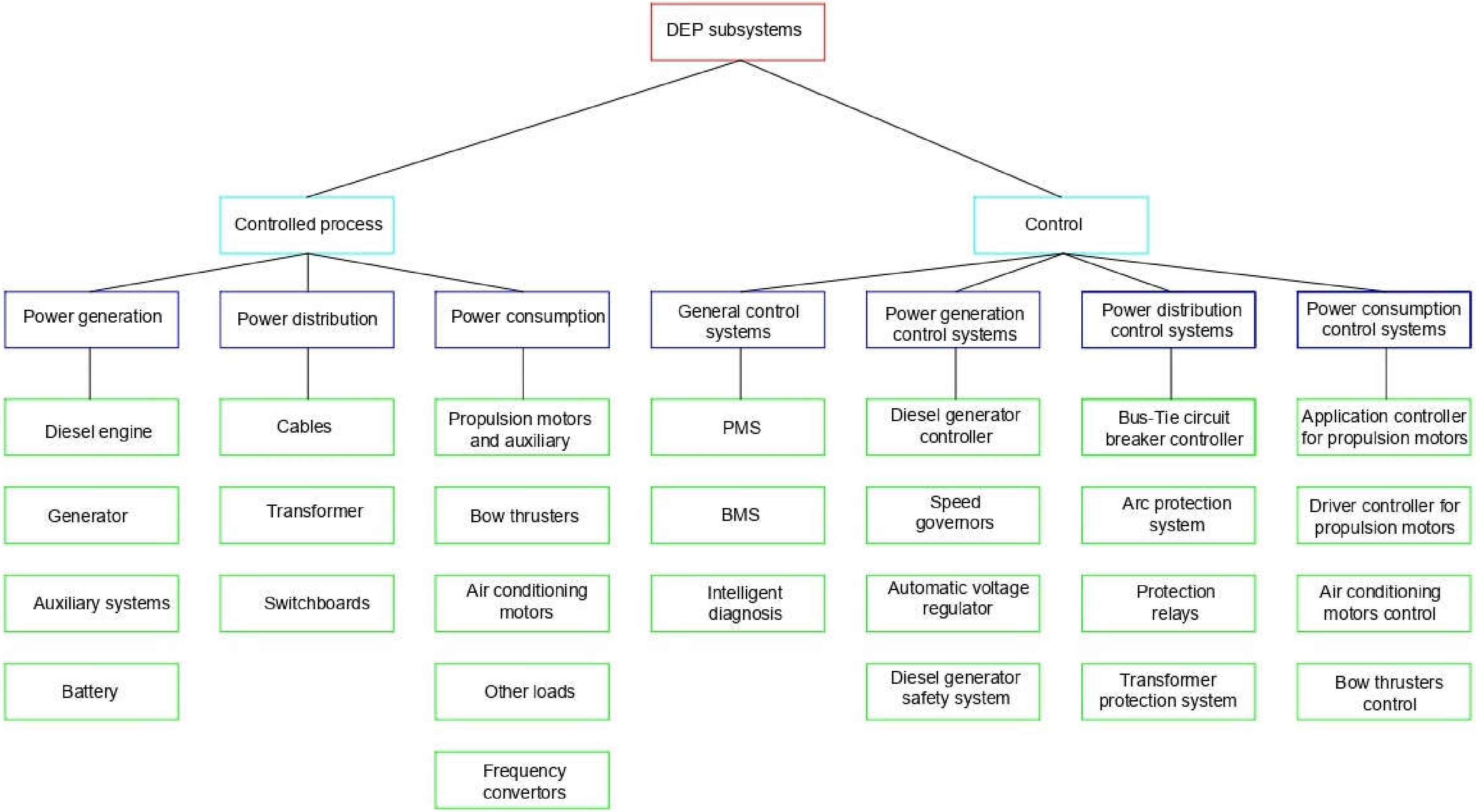

DEP subsystems
Controlled process
Control
Power generation
Power distribution
Power consumption
General control systems
Power generation control systems
Power distribution control systems
Power consumption control systems
Diesel engine
Generator
Auxiliary systems
Battery
Cables
Transformer
Switchboards
Propulsion motors and auxiliary
Bow thrusters
Air conditioning motors
Other loads
Frequency convertors
PMS
BMS
Intelligent diagnosis
Diesel generator controller
Speed governors
Automatic voltage regulator
Diesel generator safety system
Bus-Tie circuit breaker controller
Arc protection system
Protection relays
Transformer protection system
Application controller for propulsion motors
Driver controller for propulsion motors
Air conditioning motors control
Bow thrusters control

Figure 20 The main cruise ship power plant subsystems.

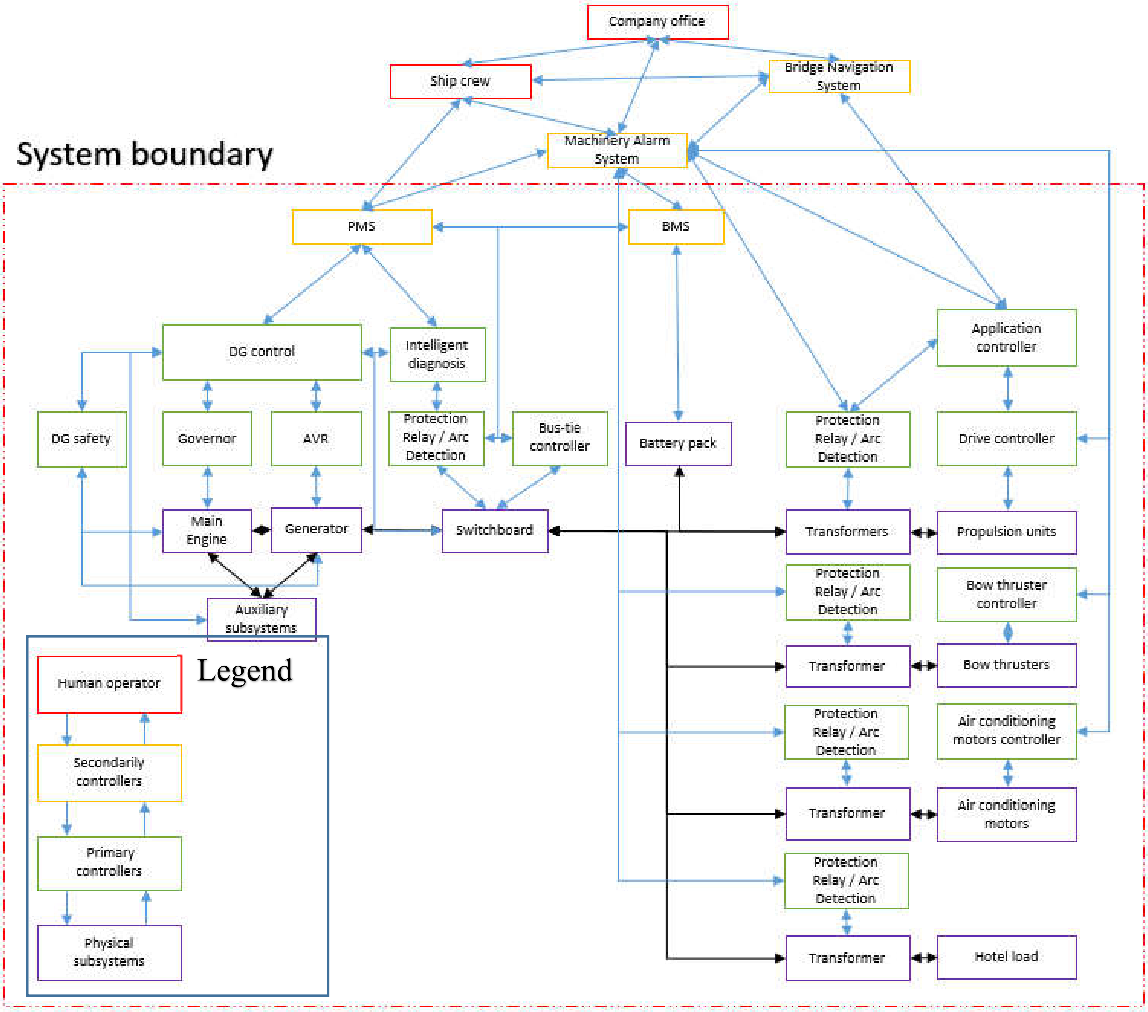


Figure 21 Cruise ship power plants network control structure.

Table 21 Used cruise ship propulsion system design parameters.

	Design feature	**Design parameters**
Generic	Network architecture	Ring
	Current type	Alternate Current
	Type of DG sets speed control	Droop
Power plant components number	Diesel Generator (DG) sets	As per investigated system
	Azipods propulsion motors	3
	Transformers per propulsion motor	2
	Switchboards	3
	Air Conditioning system compressors motors	5
	Bow thrusters	4
	Circuit breakers per DG sets and consumers	1
	Bus-Tie Breakers	6 (2 per each connection)
	Power Management System (PMS)	2
Components number for DG sets and propulsion motors	DG sets controller, Automatic Voltage Regulator (AVR), Fuel governor per DG set	1
	Speed sensors per DG set for speed control	2
	AVR sensors per DG set for voltage control	1
	Application controller per propulsion motor	1
	Drive controller per propulsion motor	1
Azipods, Bow-thrusters and DG sets maximum loads	Maximum Continuous Rating (MCR) of DG sets	As per investigated system
	Azipods propulsion motors maximum load	14 [MW]
	Bow thrusters maximum load	3 [MW]
	Maximum electrical load that can be tripped to avoid the operating DG sets overload	3 [MW]
	Maximum DG set overload limit (DNV GL, 2017)	110% of MCR
	Maximum Step Load (Radan, 2008)	33% of MCR
Batteries parameters	Batteries capacity and type (Räsänen, 2017)	1 [MWh] NMC type
	Depth of Discharge (Dimakopoulos *et al.*, 2017)	80%
	Maximum Discharge/Charge Rate (Corvus-Energy, 2019)	10C/3C
	Time required to start and connect a DG set	5 min
	Cell capacity (PV magazine, 2016)	500 [Wh]

Table 22 Investigated systems basic parameters.

a/a	Fuel type / Energy storage type	1st Engine Type				2nd Engine Type				Engine room layout
		DGT*	ERT*	No	UNP*	DGT*	ERT*	No	UNP*	
No1	HFO or LSHFO	DG sets	Not included	3	12 MW	DG sets	Not included	3	12 MW	Engine room No 1: 3 units Engine room No 2: 3 units
No2	HFO or LSHFO Batteries included	DG sets	Not included	3	12 MW	DG sets	Not included	3	12 MW	Engine room No 1: 3 units Engine room No 2: 3 units
No3	HFO or LSHFO	DG sets	SCR & Scrubber	4	10 MW	DG sets	SCR & Scrubber	4	8 MW	Engine room No 1: 2 units for each engine type Engine room No 2: 2 units for each engine type
No4	Methanol & MDO	DFG sets	Not included	4	11 MW	DFG sets	Not included	4	7 MW	Engine room No 1: 2 units for each engine type Engine room No 2: 2 units for each engine type
No5	HFO & Natural Gas & MDO	DFG sets	Not include	4	12 MW	DG sets	SCR	2	12 MW	Engine room No 1: 2 units of type 1 & 1 unit of type 2 Engine room No 2: 2 units of type 1 & 1 unit of type 2
No6	Natural gas & MDO	DFG sets	Not included	4	11 MW	DFG sets	Not included	4	7 MW	Engine room No 1: 2 units for each engine type Engine room No 2: 2 units for each engine type
No7	HFO or LSHFO	DG sets	SCR & Scrubber	4	16 MW	DG sets	SCR	4	2 MW	Engine room No 1: 2 units for each engine type Engine room No 2: 2 units for each engine type
No8	Methanol & MDO	DFG sets	Not included	4	12 MW	DFG sets	Not included	4	6 MW	Engine room No 1: 2 units for each engine type Engine room No 2: 2 units for each engine type
No9	HFO & Natural Gas & MDO	DFG sets	Not included	4	13 MW	DG sets	SCR	4	5 MW	Engine room No 1: 2 units for each engine type Engine room No 2: 2 units for each engine type
No10	Natural gas & MDO	DFG sets	Not included	4	11 MW	DFG sets	Not included	4	7 MW	Engine room No 1: 2 units for each engine type Engine room No 2: 2 units for each engine type
No11	HFO & Natural Gas & MDO	DFG sets	not included	3	16 MW	DG sets	not included	3	8 MW	Engine room No 1: 3 units of first engine type Engine room No 2: 3 units for second engine type
No12	HFO & Natural gas	DFG sets	not included	3	18 MW	DFG sets	not included	3	6 MW	Engine room No 1: 3 units of first engine type Engine room No 2: 3 units for second engine type
No13	HFO & Natural gas	DFG sets	Carbon capture	4	14 MW	DFG sets	Carbon capture	4	4 MW	Engine room No 1: 4 units of first engine type Engine room No 2: 4 units for second engine type

DGT=Diesel Generator Type; ERT=Emission reduction technology; UNP=Unit Nominal Power

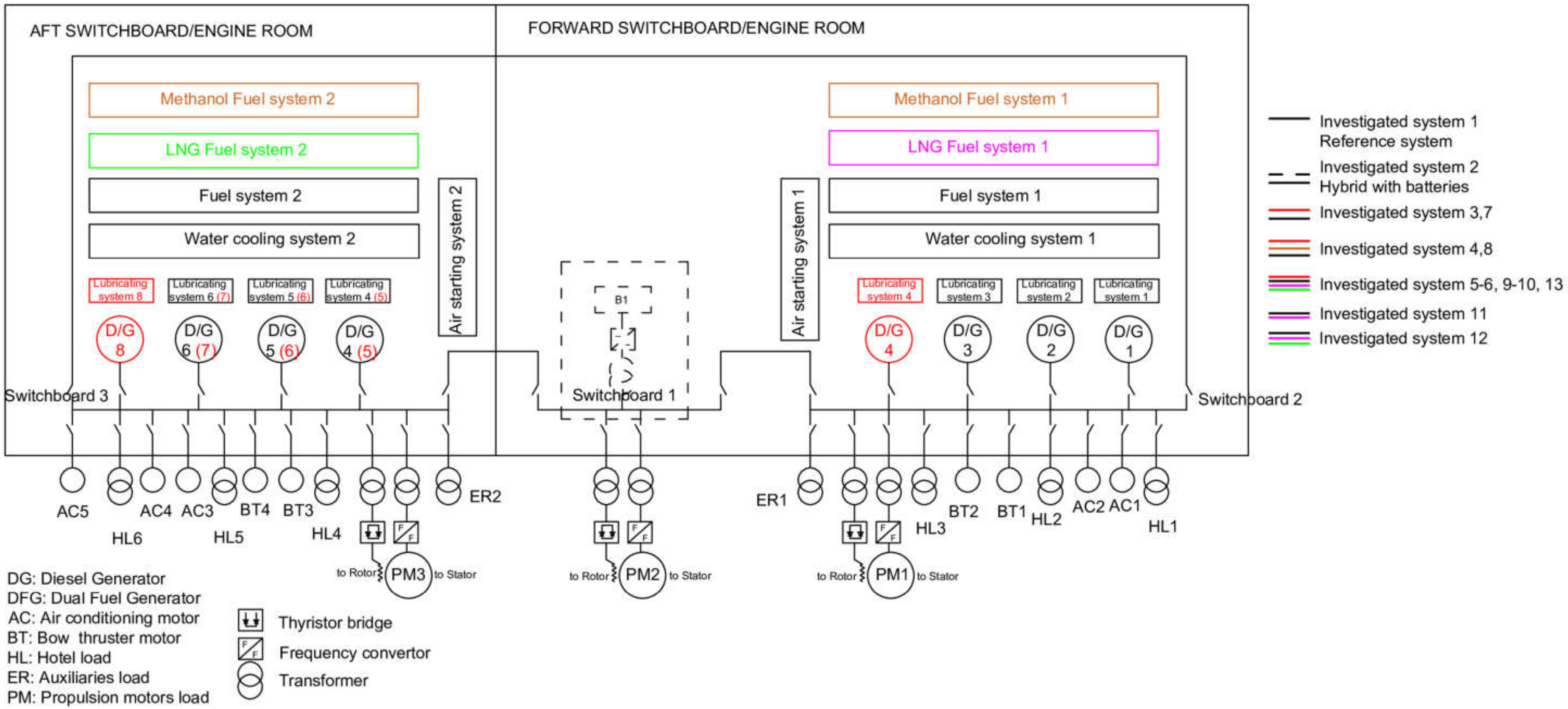


Figure 22 The investigated systems layouts.

6.3 Analysis input

6.3.1 General description of the data required

The required input for the CASA method implementation in the cases of the investigated systems is provided in Table 23. The following five types of input parameters are required: (1) the system layout and functions, the number and type of the power plant components, as well as the control structure; (2) operating data for the system and components; (3) the system components failure rates; (4) the system components maintenance and inspection intervals, and; (5) the system components maintenance duration. Whilst the system layout, functions and components number have been presented previously in the previous section as well as and in Appendices A and B, the rest of analysis input is provided in the next sections.

Table 23 Required input parameters for the implementation of the CASA method.

Type of data used for input	Maximum number of required parameters (depending on number of DG sets and type of propulsion system)	Example
Design data	61	Number of speed sensors installed on each DG set
Operating data	19	Percentage of vessel operation in the sailing mode
Maintenance inspection intervals	33	Testing of circuit breaker capability
Maintenance duration	18	Maintenance duration of each DG set
Failure rates for components	180	Failure rate for the PMS hardware

6.3.2 Maintenance inspection and duration data

The maintenance inspection intervals were retrieved from the manufacturers maintenance manuals, whilst the maintenance duration was estimated based on the data provided in (Allal *et al.*, 2017, Mennis and Platis, 2013, Reddy *et al.*, 2016), the OREDA database (OREDA, 2015) and the actual operational data. For the safety functions sensors, it was assumed that their maintenance duration is equal to 1 hour (it is expected that their failure will be immediately observed by the crew), whilst for the hardware and communication lines maintenance duration was assumed to be 20 hours (based on OREDA, 2015). The whole list of maintenance activities data is provided in Appendix F.

6.3.3 Failure rates data

The failure rates for the investigated system components were derived primary from the OREDA database (OREDA, 2015), a number of previous publications (as provided in Table 8) and the blackout accident investigation reports (provided by anonymous cruise ship operating company). The accident investigation reports (confidential data) and the Protection & Indemnity (P&I) insurance (UK P&I CLUB, 2015) clubs results were used for high level comparison of the importance metrics estimation with the results calculated for the investigated system. The PDS Data Handbook [45] and the Ohio State University report (Aldemir *et al.*, 2007) were used to identify the failure rates for the system software supported functions. The β_i values (from Section 4.8.1) for components with preventive maintenance where retrieved from a number of publications listed in Table 24. Whenever it was possible, the upper (λ_i^{upper}) and lower (λ_i^{lower}) failure rate values were estimated using the OREDA database confidence intervals (OREDA, 2015). Whenever this estimation was not available, an EF_i value of 15 was assumed for the software related failures to indicate low confidence (Schüller *et al.*, 1997), whereas an EF_i value of 7 has been assumed for the rest. A detailed list of failure rates is provided in Appendix C.

Table 24 List of sources for quantitative analysis.

Source	**Estimated parameters**
(Chai *et al.*, 2016)	Transformer failure rates, communication lines failure rates
(Aquilino, 1983)	Information on insulation failure rates in transformers
(ABB, 2005)	The current sensors failure rate
(Allal *et al.*, 2017)	Sea chest failure rate
(Anantharaman *et al.*, 2015)	The failure rate for fuel system
(Berghmans *et al.*, 2008)	The failure rate for optical sensors
(Chybowski *et al.*, 2014)	Shaft sealing system failure
(IMO, 2008, Nilsen *et al.*, 2005)	Fire failure rate in the engine room
(Menis *et al.*, 2012)	Fuel filters failure rate
(OREDA, 2015)	DG sets and electrical components failure rates
(SINTEF, 2006)	Software failure rates
(Siemens, 2013)	Arc in switchboards failure rate
(Schüller *et al.*, 1997)	Circuit breaker failure rate
(Van Ta *et al.*, 2017)	Failure rate for marine engine pistons
(Jin *et al.*, 1999, Bloch and Geitner, 2012, Mihanović *et al.*, 2016, Ossai *et al.*, 2015, Dolas and Deshmukh, 2015, Bukša *et al.*, 2009, Reliability Analytics Toolkit, 2018)	Information on β_i factors of Weibull distribution

6.3.4 Ship operating data

Based on the actual operating data collected during period of 46 months for the reference cruise ship the operational profile in Figure 23(a) has been deduced. Two different ship operating profiles were considered during analysis: (a) the original one shown in Figure 23(a), which is based on the actual operating data; (b) the operating profile shown in Figure 23(b), which was generated from the first one considering a 10% greater propulsion power demand. The port operation, which corresponds to a power range lower than 12 MW, was kept the same as the original operating profile, whereas for the remaining power range (above 12 MW), an increase of the power of 10% was applied retaining the same frequency of occurrence. The frequency of the plant operating modes (harbour, manoeuvring, sailing) and the specific system configurations (different number of DG sets operating) along with the operating Propulsion Motors (PM) and Bow Thrusters (BT) in each configuration and operating mode were estimated (Appendix D). The general mode has been also used to represent the overall, averaged plant operation.

Based on the available data, the probability density functions for the DG sets load were estimated and used as input in this analysis. They are provided in Appendix E. The switchboards and control hardware were in a continuous use. From the available operational data, the following observations were also made: (a) a request to connect an additional DG set with the ship electric network is implemented every 10 hours; (b) change over between DG sets is implemented every 20 hours; (c) the change from the harbour mode to the manoeuvring mode is implemented every 40 hours.

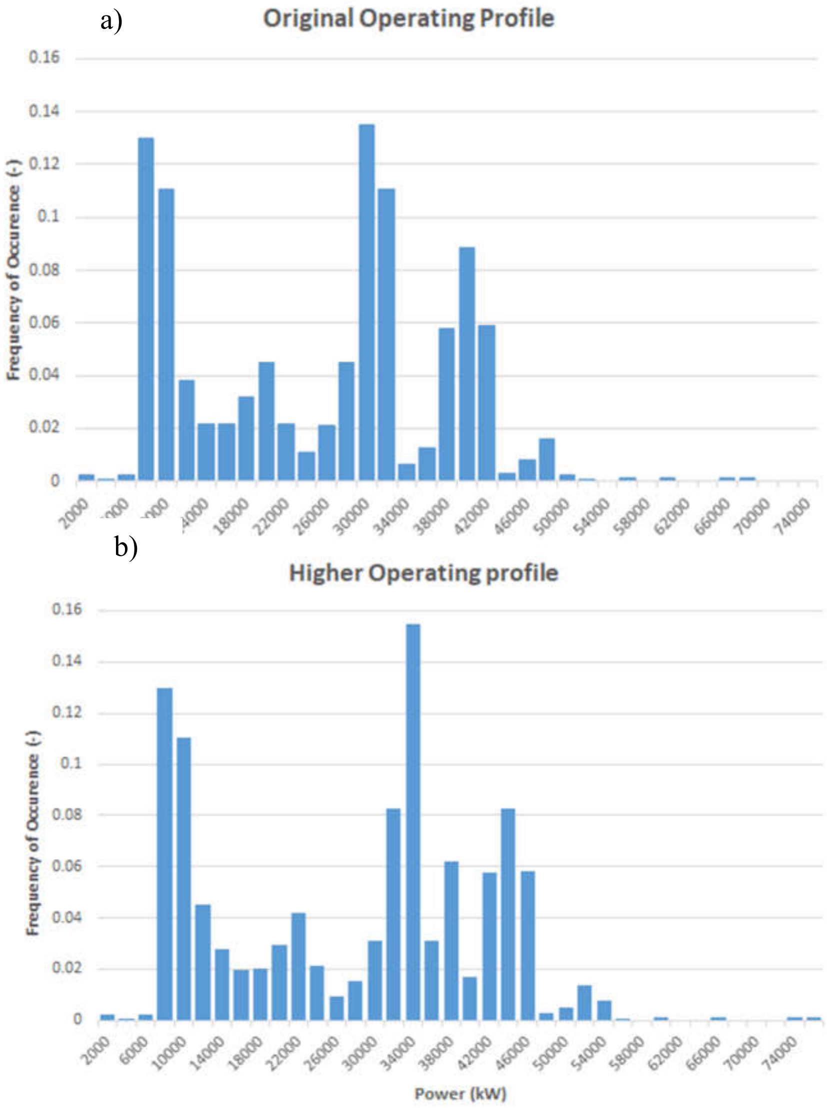


Figure 23 Considered Operational profile for the cruise ship (a) original profile; (b) operating profile with 10% higher propulsion power demand in comparison to (a)

6.4 System and analysis input assumptions

The following assumptions were considered for the purposes of the safety analysis:

Assumptions for system functions. These assumptions have a direct influence on the structure of the developed Fault Tree and practically depict the investigated system properties. They are largely based on drawings, system description in other publications and class society rules.

- The Diesel Generator (DG) sets start and connect to the ship electric network based on the ship electric power demand.
- The DG sets switchover is implemented based on the running hours of each DG set.
- The system has also the capability of changing over to another DG set in response to faults in operating DG sets.
- In cases where only one type of DG sets is considered and DG sets of different size are installed, the DG set with the smallest nominal power will be operated first.
- The load is evenly shared in proportion to the nominal power output of the generator sets among the operating generator sets.
- Each DG set can be loaded till operating at 90% of its nominal power. Above this load level (Sfakianakis and Vassalos, 2015), an additional available DG set will start and get connected to the ship electric network for covering the power demand. Only if all the DG sets are already connected, then this limit can be exceeded.
- The system includes functions for fast propulsion motors load reduction and preferential tripping of the air compressors of the Heat Ventilation Air Conditioning system (fast load reduction).
- In case of a fault in the Liquefied Natural Gas (LNG) or methanol system, the system can reconfigure, so that the generator sets engines operate by using Marine Diesel Oil (MDO) or Low Sulphur Heavy Fuel Oil (LSHFO).

Assumption for system operation. They were derived based on the operational data. Some of them have influence on the results.

- The power plant operates with the bus-tie circuit breaker connected in all operational modes. Consequently, the short circuit and load imbalance failures can be transferred between the two power sections. As the investigated vessel is cruise ship, it is not expected, that the vessel will be operated with disconnected bus-tie circuit breaker. It is a requirement for vessels with dynamic positioning capabilities.
- In the harbour mode, the propulsion motors and the bow thrusters do not operate. This is an assumption made based on operating data.

- In the manoeuvring mode, both the bow thrusters and the propulsion motors are considered to be fully operational, whereas in the sailing mode only the propulsion motors operate. This is also an assumption made based on data.
- When more than one type of fuels are considered for the power plants, the generator sets with the most environmentally friendly fuels like natural gas and methanol will be operated first. This is an operational assumption. As a result, lower blackout frequency is expected with reduced number of operating generators, due to the additional redundancy in fuel system for dual fuel generators.
- It should be noted that the system operation with 6 DG sets is very rare for the reference system (less than 1% of the total ship operational time) so it was set 1% to assess the influence of the system configuration with 6 DG set operating on the overall blackout frequency. This might slightly influence the generated results, depending though on blackout frequency/failure rate when 6 DG sets are operating.
- In addition, in general mode it was assumed that one BT and 3 PMs are operational to assess the influences of these components on frequency of blackout. As a result, more short circuits and components failures will be considered resulting in slightly increased blackout failure rate.

Safety analysis assumptions:

- The failure rates were assumed to be zero for all the STPA causal factors related to the flawed process model, except for the failure rates depicting errors related to the intelligent DG sets diagnosis responsible for identification of system load imbalances. As a result, only software failures related to software implementation are considered. It is expected, that since the system is well known and the physical problem is well understood, that this is rather a realistic approximation. If not, then slightly higher blackout frequency can be expected.
- It was assumed that any electrical load sharing imbalance can be corrected by the PMS in 90% of the cases, whereas if intelligent generator diagnosis is provided in the system, this system manages all the electrical load sharing imbalances by tripping the faulty DG set. A change in the assumption will lead to slightly higher or lower importance of failures related to load imbalance depending on its values change. This will also significantly influence the effectiveness of intelligent diagnosis system on controlling blackouts.
- It was also assumed that an uncontrolled electrical load sharing imbalance will lead to a blackout in half of the cases, whilst only one DG set will be lost for the other half. This is rather conservative assumption, as generator set safety system is likely to trip a faulty generator, which unlikely will cause a blackout. So, if more realistic assumption is made, then the load imbalance will lead to lower number of blackouts. Still it depends on the settings and functionalities of each safety system, which were unknown in the case. This assumption will influence the importance of electrical faults for the system.

- Furthermore, it was assumed that prewarning functions will allow the safe switch over to another DG set in 50% of the cases when lubrication oil low-pressure alarm, high exhaust gas temperature alarm and high cooling water temperature alarm are present in one of the operating DG sets. This is rather conservative assumption, as the effectiveness is expected to be higher. It will increase the importance of mechanical failures and blackout number due to single generator failure. This assumption will also have significant influence on results, especially when one generator is operating.
- Only short circuits that occur in bow thrusters, air conditioning compressor motors, propulsion motors, switchboards and DG sets contribute to the system blackout. This is rather realistic assumption, as the short circuits from other consumers are expected to be accepted by the power generation system due to their lower value. However, if more strong short circuits are expected to be observed in the system, it will lead to slightly higher blackout frequency.
- Any short circuit not cleared by the protection system will lead to the DG sets overcurrent and a consequent blackout. This is also a realistic assumption, as the generators safety systems are expected to shut down the engine if overcurrent is observed.
- Tripping of air conditioning motors bow thrusters and other loads causes insignificant electrical transients. Significant electrical transients are caused by the loss of operating propulsion motors and DG sets. This is also a realistic approximation as the load taken by air conditioning motors and bow thrusters is rather small, so their sudden loss will cause small transient. So, it is not expected to affect the results.
- An uncontrolled arc failure in the switchboard will cause a loss of one electric power section of the DEP plant. This is a realistic assumption, as an uncontrolled arc may result in switchboard destruction.
- Any fire in an engine room will lead to the loss of all the generator sets in this engine room. This is rather a conservative assumption, as during fire it is expected that some generators might remain operation for short period of time. However, during firefighting, it will be necessary to switch off the fuel to these generators by using the quick fuel closing valve. So, this assumption is not far away from the reality. This assumption is expected to have small influence on results.
- The failure rates for tanks (HFO tank, fuel buffer tank, lubricating oil tank, LNG fuel tank and methanol fuel tank) have been considered as zero, as the unavailability of fuel will come from wrong operational measures which has been considered to be out of the scope of present study. It is not expected that a crack in a tank and loss of fuel due that will be unnoticed by the crew.

Concluding, it can be observed, that most assumptions are either close to reality, or more conservative, so more conservative results will be estimated during the analysis.

6.5 The investigated case studies

From the functions mentioned previously, it would be worthy to investigate how the prewarning alarms effectiveness would affect the system susceptibility to blackout, as it seems to be an influencing assumption. In case their effectiveness has an impact on blackout frequency/probability, then it would be appropriate to consider the application of prognostic/diagnostic techniques for DG sets. The DG set loading is also expected to affect the potential DG overload conditions (Radan, 2008). So, for the current system, it would be interesting to investigate what will be the impact of potential increase in DG sets loading. If it is not critical, then potentially DG set size could be reduced without compromising safety.

Except that, it is well known that maintenance affects the system safety, so it would be necessary to investigate its periodicity impact on the system safety. Intelligent diagnosis is a novel concept, so it would be also noteworthy to investigate how it would affect the blackout frequency. Finally, the system is expected to trip some unnecessary consumers during blackout. It is not known though how the amount of tripped load would affect the system susceptibility to blackout. As the total number of operating DG sets varies, it would be essential to consider the variation in blackout frequency in these conditions.

In addition to the considerations above, the cruise ship is expected to operate in a number of operating modes: sailing in open sea, manoeuvring close to harbours and in harbour mode (at berth). It is therefore important to estimate the susceptibility to blackout under different operating conditions as this has direct impact on collision/contact/grounding risk. It would be also important to contemplate which are the system critical failures in each operating mode. To account though for the variation in previously functions/capabilities a general operating mode would be useful, so that fewer cases are applied, without analysing a specific operating mode separately.

Taking into account that it may be a specific challenge to acquire the accurate failure rate values for all the components and failure modes, an uncertainty analysis is required for the estimation of the Fault Tree top event (Bjerga *et al.*, 2016). It is absolutely required to estimate which is the uncertainty and which are the most uncertain failures. The most uncertain failure identification together with importance measure can support the detection of most critical failures and therefore the DEP safety enhancement. For the uncertainty analysis three different distributions for input failure rates are considered. A Lognormal (LN) distribution is assumed as the basic uncertainty distribution for failure rates, as proposed in previous studies (Schüller *et al.*, 1997, Stamatelatos *et al.*, 2011, Durga Rao *et al.*, 2007, Verma *et al.*, 2010). To assess the influence of the distribution on the uncertainty analysis of the blackout failure rate, the uncertainty analysis is repeated for triangular (TR) and uniform (UN) distributions.

At the last stage, the alternative systems blackout failure rate is estimated and insights in system design are obtained. The alternatives are used to investigate the variation in blackout frequency if some of the design parameters such as number of generators or fuel type, changes. Based on the results of the whole analysis, safety recommendations are derived.

Based on the considerations above, the case studies that were investigated in this thesis are provided in Table 25.

Table 25 The Investigated case studies.

Phase	Case study No	System No*	OM	Target / Implemented calculations	Details
1,2,3,4	i.	No1	G	Undesired event failure rate λ_p and λ^{TE} estimation in different system configurations with different DG set number operating	No prewarning alarms effective allowing a DG set switch over to a healthy DG set, when lubrication oil low-pressure alarm, high exhaust gas temperature alarm and high cooling water temperature alarm are present in every one of the operating DG sets.
	ii.	No1			Full prewarning alarms effectiveness allowing DG set switch over to health DG set when lubrication oil low-pressure alarm, high exhaust gas temperature alarm and high cooling water temperature alarm are present in one of the operating DG sets.
	iii.	No1			3 % MCR increase to the operating DG sets loading profile
	iv.	No1			10% more frequent maintenance
	v.	No1			Intelligent diagnosis added to system
	vi.	No1			50% reduced tripped load (load of air conditioning compressor motors)
	vii.	No1			Initial system design
	viii.	No1	H	Undesired event failure rate λ_p and λ^{TE} estimation	Initial system design
	ix.	No1	S		
	x.	No1	M		
5,6	xi.	No1	G	Importance metrics estimation	Estimation of I_j^B and I_j^{FV} metrics
	xii.	No1	H		
	xiii.	No1	S		
	xiv.	No1	M		
7	xv.	No1	G	Uncertainty analysis	Uncertainty assessment using Lognormal, Triangular and Uniform Probability Density Function Distribution - Estimation of λ^{TE} and $r_{\lambda^{TE}\lambda_i}$
	xvi.	No1	H		
	xvii.	No1	S		
	xviii.	No1	M		
1,2,8	xix–xxx.	No2-13	G	Undesired event failure rate λ_p, λ^{TE}estimation	Investigation in λ_p and λ^{TE} variation in different systems

OM= Operating Mode / G= General / S= Sailing / M= Manoeuvring / H= Harbour

* The system number corresponds to the details provided in Table 25.

6.6 Chapter summary

In this chapter the reference and alternative systems description, the analysis input and assumptions were provided. The investigated reference system has 6 DG sets with 2 separate engine room. Several alternative systems with varying generator set number (12 in total) were also selected. The reference to the used databases (OREDA, accident investigation reports, etc.) was made available. A number of case studies were described, the results of which allow for a progressive development, demonstration and verification of the developed method characteristics.

This page has been intentionally left blank

7 APPLICATION CASE STUDIES - CRUISE SHIP POWER SYSTEMS CASA RESULTS AND DISCUSSION

7.1 Chapter outline

In the chapter, the safety analysis results for the investigated cruise ship propulsion plants by applying the method presented in the Chapter 4 are provided. First, the results of developing the Fault Trees are provided and compared with other studies. Then, the results of quantitative analysis are provided and discussed. Based on the analysis results, the relevant safety recommendations for the cruise ship propulsion system design and operation are provided.

7.2 Fault Trees development

7.2.1 STPA results (CASA Steps 1-4)

The list of the generated sub hazards from the STPA for the investigated DEP systems that can lead to a blackout event along with the safety constraints and the existing safety measures are presented in Table 25. These hazards were identified based on publications such as (Krogseth, 2013, Karakitsos and Theotokatos, 2016, MAIB, 2011, Sfakianakis and Vassalos, 2015, Radan, 2008). The focus of this study is on the sub hazards H-1 to H-5, as the other sub hazards are external to the investigated system presented in Figure 21 and, therefore, would require significant effort and use of additional methods for safety analysis as reported in (Wheeler *et al.*, 2016). The sub hazards H-1 to H-5 are not related to the system components failures and thus their analysis would focus on the general system states. This is an advantage of this study compared to the previous studies (Chang *et al.*, 2008, Vedachalam and Ramadass, 2017, Roskilly, 2016, Menis *et al.*, 2012) that consider only the DG sets availability. The presented sub hazards are of the high-level type, and they most likely could be identified using a Preliminary Hazard Analysis (PHA) method. However, the PHA would not support the UCAs and their related causal factors identification.

The investigated DEP system control structure (CASA step 2) was developed based on the information available from the manufacturers' manuals. The developed overall control structure is presented in Figure 24(a), whereas the typical detailed description of the engine governor control structure is provided in Figure 24(b).

The STPA investigated system UCAs (CASA step 3) were derived with the support of the open source software XSTAMPP (Abdulkhaleq and Wagner, 2016), by considering all the possible failure modes of the control actions. Typical UCAs example is provided in Table 26. The list of identified UCAs is provided in Appendix G. For the investigated system No1, 78 UCAs were found. Additional 11 UCAs were found for system No2 related to Battery Management System. The results clearly demonstrate that the introduction of batteries rises the scenarios number leading to blackout due to increased number of interactions between the control part and physical part in the system N2, depicting higher system complexity. This does not necessary demonstrate that the system risk is higher. Then for systems with dual fuel supply, additional UCA has been considered referring to the reconfiguration to an alternative fuel, if failure is observed in the operating fuel system. Only one additional UCA was considered as the fuel amount control in DG sets and the safety control in fuel systems is the same no matter the fuel used.

For the investigated system No1 a large number of UCAs (19/78 or 24%) were related to the PMS functions. Proceeding from the higher to the lower controller hierarchical levels, the number of UCAs decreases, as the controller's functionalities reduce in number. The greater percentage of the UCAs (56%) was related to the DG sets overload hazard [H-3]. The incorporation of the UCAs leading to blackout for the DEP systems is one of the differentiating elements of the developed Fault Tree compared to Fault Trees presented in previous studies (Chang *et al.*, 2008, Vedachalam and Ramadass, 2017, Roskilly, 2016, Menis *et al.*, 2012). In this respect, the presented analysis more effectively captures the software intensive character of the investigated DEP system.

Table 26 The identified list of sub hazards, safety requirements and existing safety measures for the investigated system.

a/a	Sub hazards	Safety requirement	Existing safety measures
[H-1]	Unavailability of the DG sets or related equipment such as batteries and auxiliaries	DG sets/Batteries shall be always available to be connected when requested by the system	Redundancy in DG sets
[H-2]	Imbalanced power generation	The system shall always avoid imbalance in power generation	Intelligent generator diagnosis system by tripping a faulty DG set
[H-3]	Operating DG sets overload	The system must always avoid operating at conditions with overload	Fast electrical load reduction, DG sets size selection
[H-4]	Electrical load transients in the network	The system must be resilient to the presence of the transients in the network and prevent their existence in the system	Tripping functions settings proper selection, design parameters of DG sets, control over propulsion motors during the start
[H-5]	Electrical disturbances like short circuits	The system must prevent the occurrence of short circuits and do not allow the short circuit and arc fault to be uncontrolled	Protection relays, arc detection systems
[H-6]	Inappropriate interactions between humans and power network	The system must prevent the inappropriate interactions between the humans and power network	Training, operational procedures, human-machinery interface design
[H-7]	Fire in engine room	The system must prevent and extinguish fire in the engine room	Fuel quick closing valves proper operation, fire detection systems, fire-fighting systems
[H-8]	Cybersecurity attacks	The system must be protected from cyber attacks	Firewall, control and communication networks segregation
[H-9]	Flooding in engine compartments	The ship must prevent flooding from occurrence and eliminate its propagation	A wide spectrum of safety measures

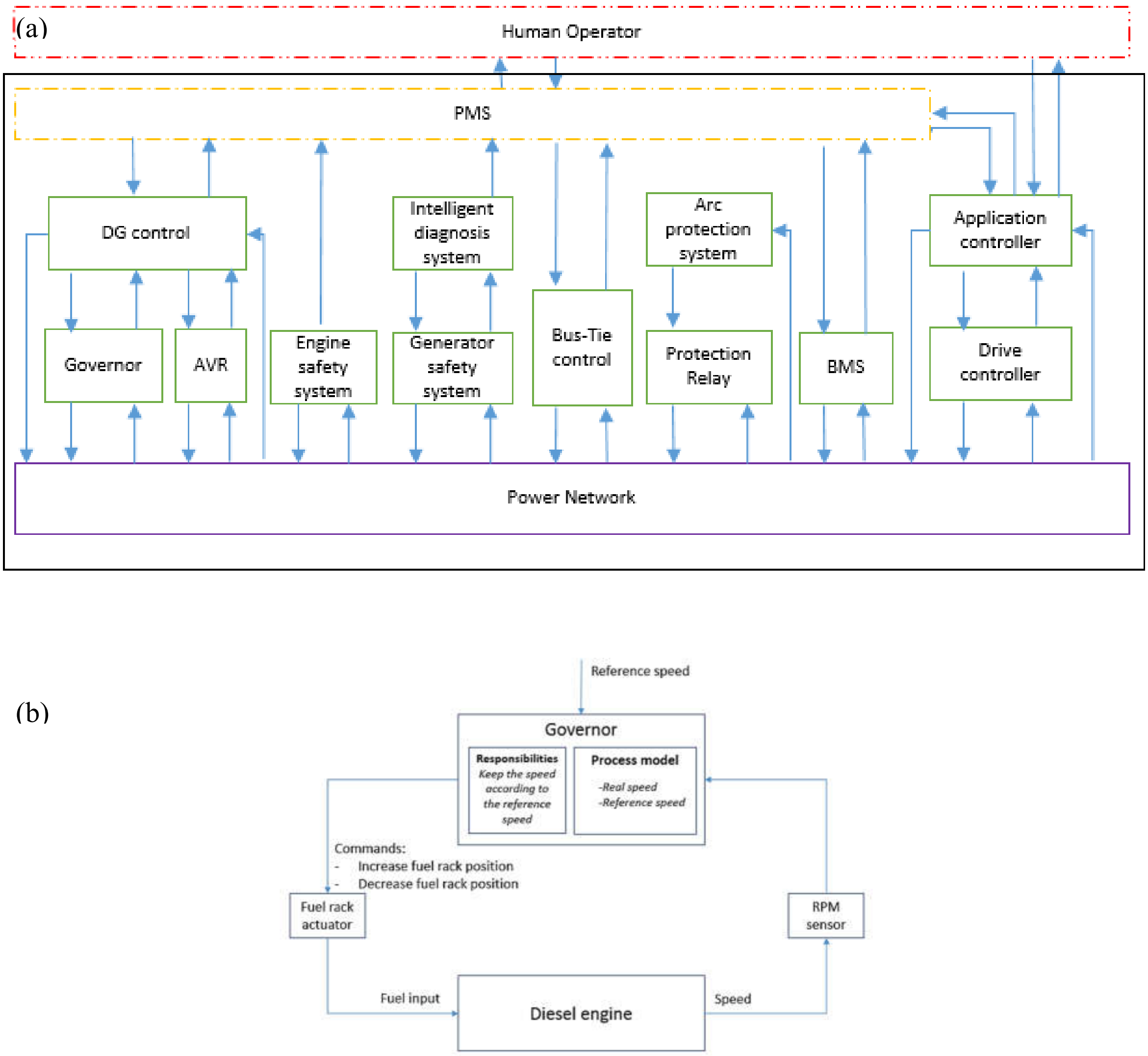


Figure 24 Investigated DEP plants control structure (a) Analysed system overall control structure; (b) Refined engine governor control structure.

Table 27 Example of UCAs in the investigated DEP systems.

Control Action	**Type of UCA**	**Description**
Start a DG set (given by PMS)	Not providing causes hazard	If the command to start a DG set is not given/followed when there is a request for higher power demand, the operating DG sets will be overloaded. [H-3]
	Providing causes hazard	Command to start a DG set, when it has specific faults or failure, may cause disturbances to the network and will lead to failure in starting a DG set, with potential overload of the operating DG sets. [H-3] [H-4] Trying to start-up an already running DG set will result in the unavailability of produced electric power when the power demand is high and failure to implement a switchover from a faulty DG set to a healthy DG set. [H-1] [H-3]
	Wrong timing or order causes a hazard	A delayed order to start a DG set will cause a delay in change over when there is a faulty DG set. This will result in the tripping of the DG set. [H-3] A delayed order to start a DG set when the power demand is higher than provided safely by other DG sets will result in overloading of the operating DG sets. [H-3]

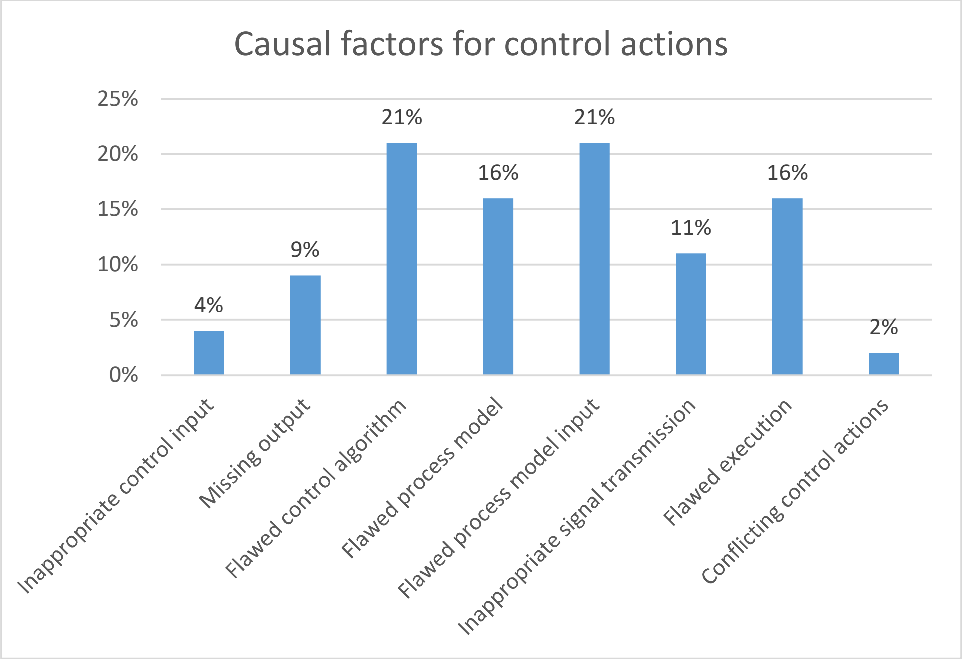


Figure 25 Distribution of causal factors.

The fourth CASA step includes identification of the causal factors contributing to the DEP systems UCAs. For each UCA, 1 to 10 causal factors were identified. The causal factors identification was supported using the guiding words available in Appendix H. This task was repeated for all the 90 UCAs. On overage, 3.9 causal factors per UCA were identified (299 for system N1, 344 for system N2, 350 in total considering all the systems). The results were similar for all the investigated systems. The distribution of all causal factors per category is shown in Figure 25. As it may be observed the dominant factors were related to: (a) the flawed control algorithm implementation; (b), the inconsistent process models; (c), the flawed process model input from sensors to controller and; (d) inappropriate transmission of the control signal to actuators. In addition, failures in actuators leading to flawed execution of control action were identified as important causal factors. Fewer causal factors were identified related to conflicting control actions, missing output from controllers due to their failure and inappropriate control input. These results can be attributed to the fact that the STPA more effectively highlights the importance of the software functions for the system, thus supporting the identification of the causal factors related to the control hardware and software including flawed control algorithms, flawed process models and flawed process model input parameters.

7.2.2 ESI results (CASA Step 5)

The sub hazards H-1 to H-5 that were identified for the investigated system were used as initiating events during the ESI "Event Trees" development phase. A resultant example ESI "Event Tree" showing the propagation of two of the sub hazards for the investigated DEP system No1, namely the DG sets unavailability and the operating DG sets overload into blackout is presented in Figure 26. The other developed "Event Trees" are provided in Appendix I. As it can be observed, the DG sets and other generator sets overload will occur when the system will fail to trip hotel load and reduce the load of propulsion motors.

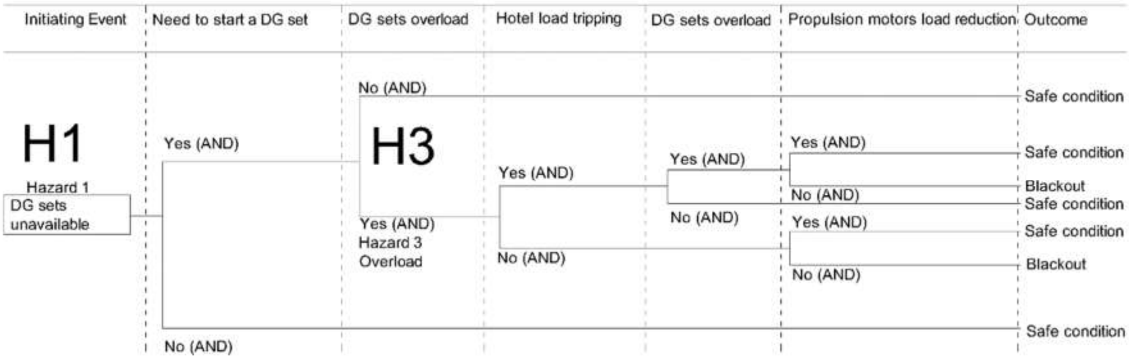


Figure 26 ESI's "Event Tree" for first and third sub hazards.

7.2.3 STPA and ESI results integration (CASA Steps 6-8)

The process of synthesis of the ESI results is done in this step (CASA step 6). The developed Fault Tree for system No1 is quite extensive and includes 13 levels, 21 AND gates, 9 OR gates and 57 undeveloped events; hence it was not possible to present it in its full extent.

After the STPA results were integrated into the developed Fault Tree (CASA step 7), its size became extremely large, as for each event of the initial "Event Trees" and consequently to the Fault Tree, two levels were added increasing exponentially the number of gates and undeveloped events corresponding to the UCAs and the causal factors, respectively. The initial mapping of the identified UCAs to different events of Event Tree is provided in Appendix J.

Refinement for the UCAs context was applied for 40 out of 78 UCAs in system No1 (CASA Step8). Similar refinement was applied for the other investigated systems. Typical examples include the UCAs for starting the DG sets and controlling the position of the bus-tie breaker. Grouping of the interconnected UCAs was applied for the UCAs related to the DG sets starting, controlling the propeller speed, and thus, the load of the electric propulsion motors as well as the UCAs for controlling the bus-tie circuit breaker position. The electrical load transients may be caused by different events (fast increase in propulsion power or sudden loss of a heavy electrical consumer), which will increase or decrease the operating DG sets power output leading to potential imbalanced load sharing between the connected DG sets. The causal factors for the occurrence of the UCAs leading to imbalanced load sharing between the DG sets in both cases are the same, so their merging can be applied. The PMS hardware failure and the DG sets speed and voltage sensors erroneous measurements were identified as common causal factors to many UCAs and were promoted to a higher level. Similar refinement was applied for other systems.

Contradiction were found in the UCAs related to the PMS functions. The PMS cannot start a DG set and cannot handle a load imbalance or overload when the PMS hardware failure occurs. An additional refinement was applied to UCAs related to the DG sets physical failures. An extract from the refined Fault Tree describing the conditions leading to blackout due to operating DG sets overload based on the "Event Tree" of Figure 26 is presented in Figure 27. As it is observed from this figure, the refinement was applied in case of (a) not starting a DG set when a DG set has a failure; (b) not starting a DG set when the load demand is high and (c) for the PMS hardware failure. The DG sets and other failures are further analysed using the FTA as described in the next section.

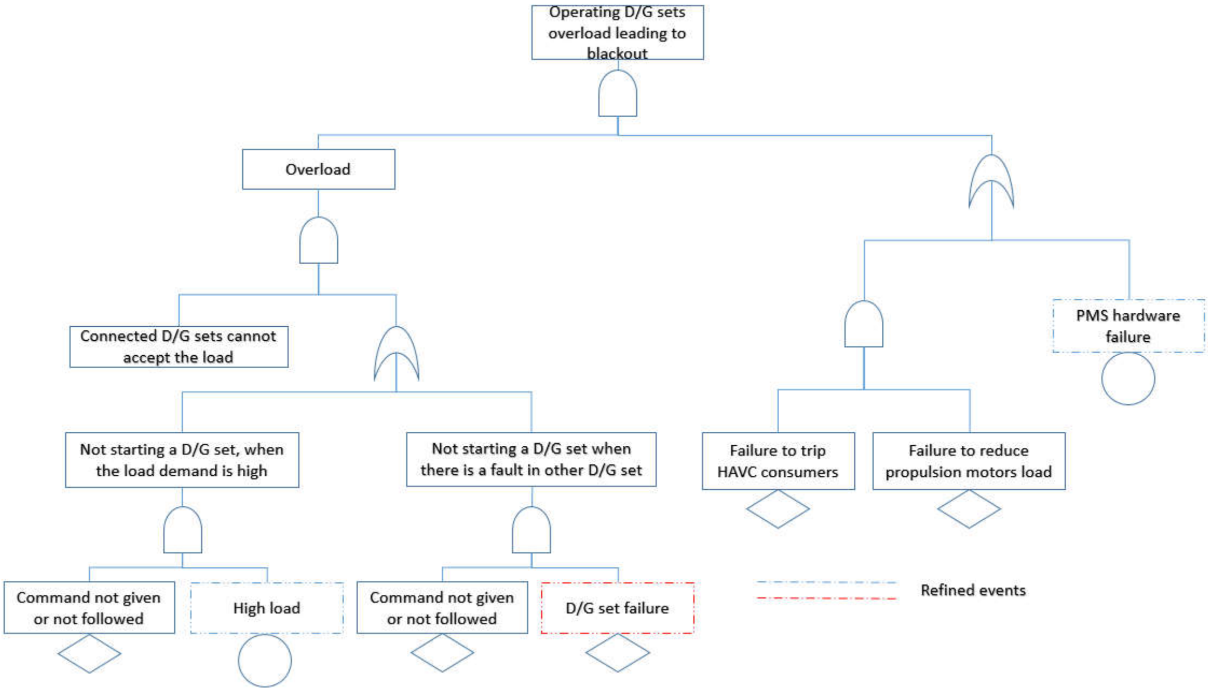

Operating D/G sets overload leading to blackout
Overload
Connected D/G sets cannot accept the load
Not starting a D/G set, when the load demand is high
Not starting a D/G set when there is a fault in other D/G set
Command not given or not followed
High load
Command not given or not followed
D/G set failure
Failure to trip HAVC consumers
Failure to reduce propulsion motors load
PMS hardware failure
Refined events

Figure 27 An extract from the refined Fault Tree.

7.2.4 FTA results (CASA Step 9)

The FTA is used to develop further some events in the refined Fault Tree of previous step; in specific, FTA was applied for the analysis of the failures in one DG set, its auxiliary systems and propulsion electric motors. The Fault Tree results are provided in Appendix K. The Fault Tree derived for the main engine failures leading to the engine shut down is presented in Figure 28. This Fault Tree was developed based on information provided in (Li *et al.*, 2010, Arcidiacono and Campatelli, 2004, Chybowski, 2002, Laskowski, 2015, Rasoulzadeh Khorasani, 2015, Garyfallos, 2016, Lazakis *et al.*, 2018). However, it differentiates from the information provided in the mentioned resources in the way the failures are organised and presented, as attention was given to the conditions leading to the engine shutdown with alarm. In this Fault Tree, the failures of the air starting system are not incorporated, as the air supply system is engaged only during engine starting procedure. In addition, failures leading to the deterioration of the system performance are not considered as a cause of the engine shutdown. The critical alarms of the system leading to the system shut down are activated by: (a) failures of the DG set control hardware; (b) high cylinder liner temperature; (c) high cooling water temperature; (d) high thrust bearing temperature; (e) high main bearing temperature; (f) low lubrication oil pressure; (g) increased oil mist concentration and; (h) other failures affecting the engine output.

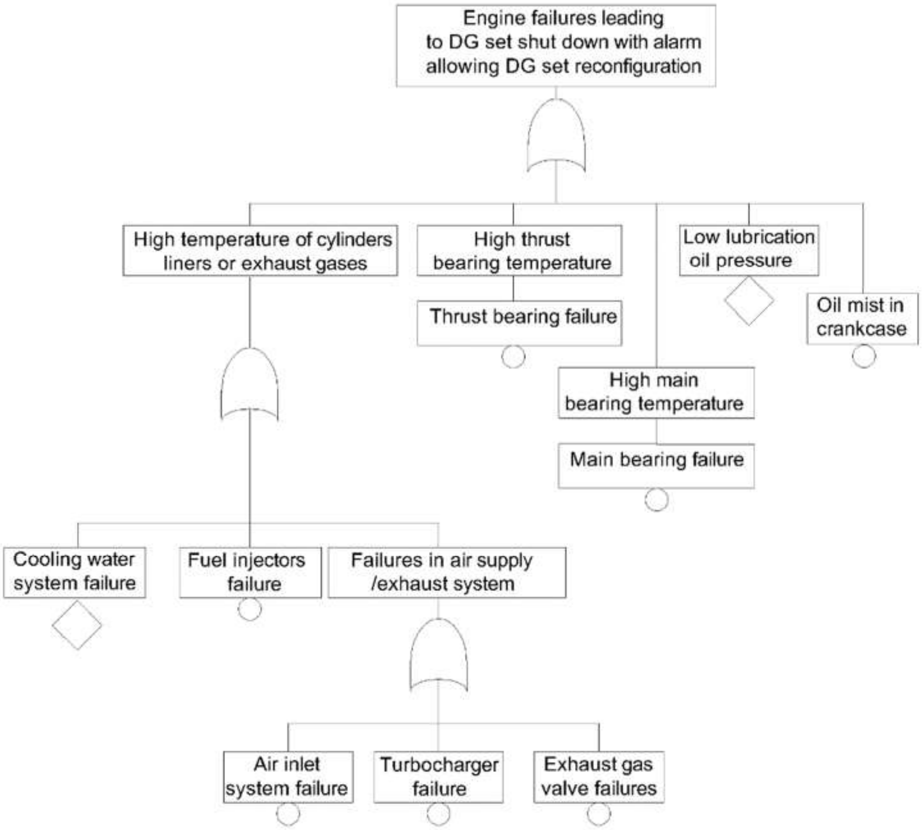

Engine failures leading to DG set shut down with alarm allowing DG set reconfiguration
High temperature of cylinders liners or exhaust gases
High thrust bearing temperature
Thrust bearing failure
Low lubrication oil pressure
Oil mist in crankcase
High main bearing temperature
Main bearing failure
Cooling water system failure
Fuel injectors failure
Failures in air supply /exhaust system
Air inlet system failure
Turbocharger failure
Exhaust gas valve failures

Figure 28 DG set failures leading to loss with alarm allowing reconfiguration to another DG set.

7.2.5 The finalised Fault Tree

The Fault Tree of the Figure 29 is a high–level depiction of the final Fault Tree that incorporates all the important intermediate events of the investigated reference and alternative systems. It demonstrates the complexity in the interactions between the different sub hazards in the investigated system. The operating DG sets overload leading to blackout event is also represented to show the relationship between the Fault Trees shown in Figure 29 and Figure 27. It can be also observed that the developed Fault Tree has a structure different from the Fault Trees presented in previous safety studies on DEP systems (Chang *et al.*, 2008, Vedachalam and Ramadass, 2017). The depicted Fault Tree may create an illusion, that all the events are connected using OR gate. However, in the reality, the final Fault Tree consist of a mixture of AND and OR gates. To account for common cause failures, the methodology includes a number of rules for refinement, provided in Section 4.6. The finally developed Fault Tree (not shown) here is quite extensive and therefore not presented in the thesis.

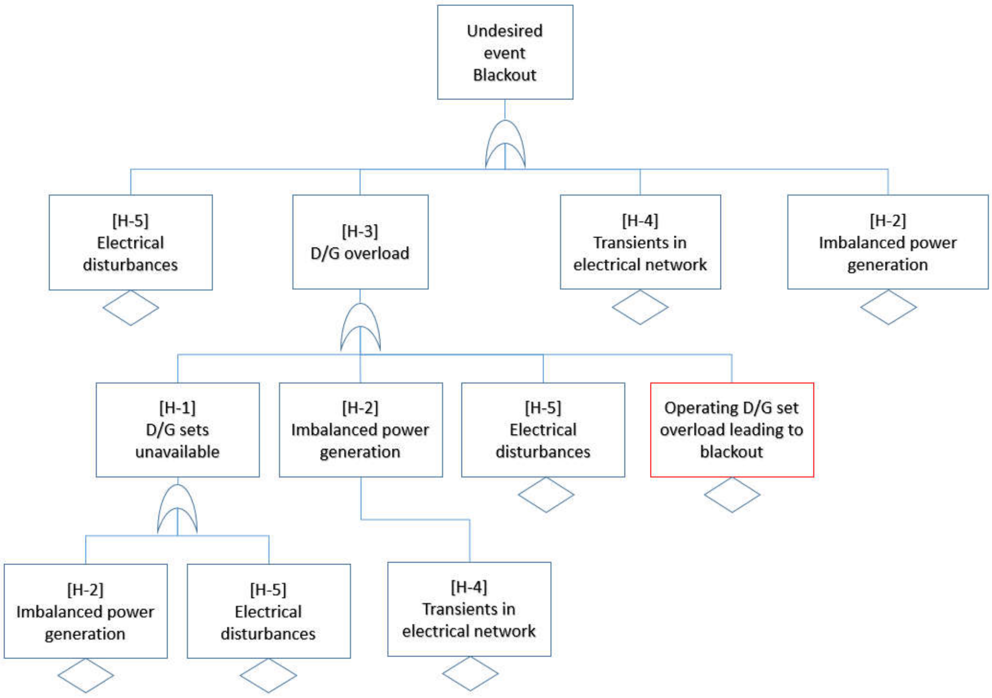

Undesired event Blackout
[H-5] Electrical disturbances
[H-3] D/G overload
[H-4] Transients in electrical network
[H-2] Imbalanced power generation
[H-1] D/G sets unavailable
[H-2] Imbalanced power generation
[H-5] Electrical disturbances
Operating D/G set overload leading to blackout
[H-2] Imbalanced power generation
[H-5] Electrical disturbances
[H-4] Transients in electrical network

Figure 29 Fault Tree showing the interconnection between hazards.

7.3 Comparison of the derived Fault Tree results with Fault Trees from previous studies

As it was discussed in Section 3.3, a number of previous studies has focused on DEP or similar systems. However, as elaborated below, their Fault Tree structure compared to the structure of the FT in Figure 29 is not as suitable for description of a blackout event; they also do not consider all the potential scenarios that lead to this event.

The Fault Tree derived by Menis *et al.* (2012) is demonstrated in Figure 30. The top event of this Fault tree is different from the investigated top event in this thesis (the blackout event). Still, for the propulsion system failure it is considered that a failure of all the DG set is required. However, a single DG operating set failure can automatically lead to a blackout. Furthermore, it is known from experience that a single DG set failure under specific loading conditions may lead to a blackout (Radan, 2008). In addition, a failure of a single Integrated Automation System (IAS) does not automatically lead to blackout, as the system has the ability to use a redundant IAS system if required. Finally, only physical failures were considered in this FT structure. Other hazardous systems events, such as short circuits events were neglected. The failure of the control functions of the subsystems were not considered as well. Therefore, the depicted Fault Tree lacks significant information related to hazard analysis and hence, it can be considered suitable only for reliability analysis. Similar criticism can be applied to the Fault Tree derived by (Vedachalam and Ramadass, 2017) that is presented in Figure 31.

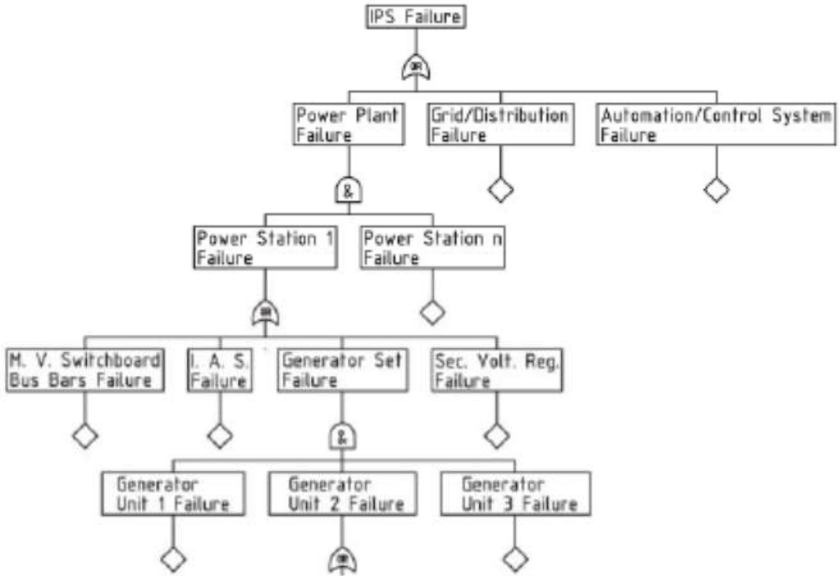


Figure 30 Fault Tree for Integrated Propulsion System (IPS) derived by Menis *et al.* (2012)

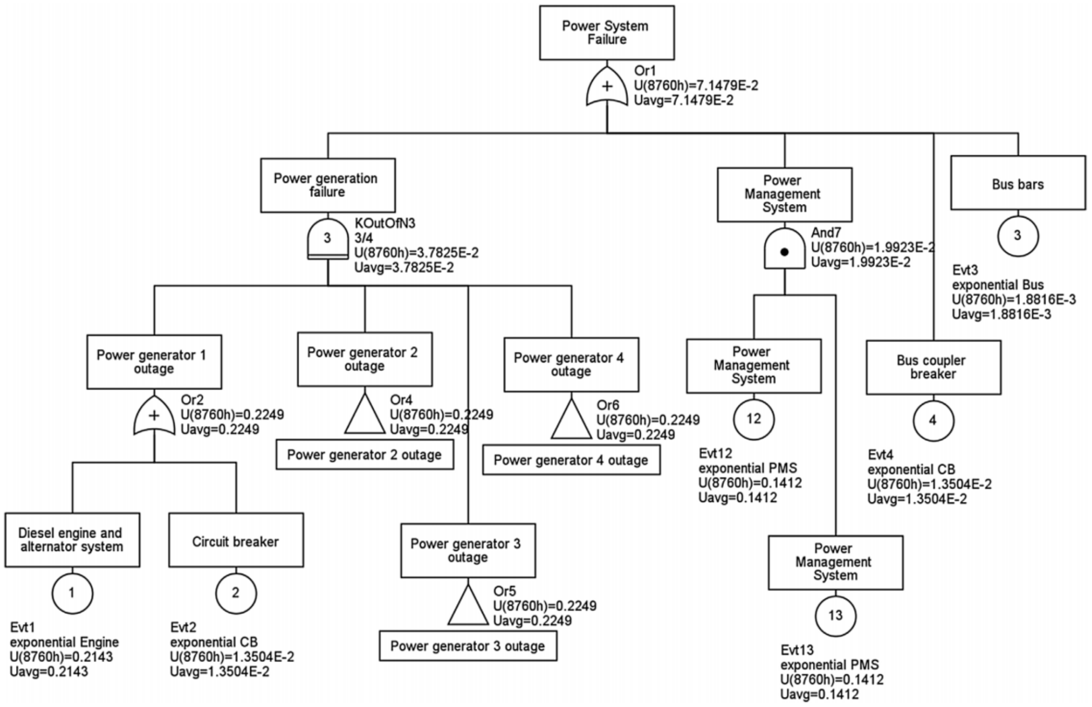


Figure 31 Fault Tree derived by (Vedachalam and Ramadass, 2017).

Another Fault Tree for the blackout event of on ice class bulk carrier was developed by Aziz *et al.* (2019); this is presented in Figure 32. This approach differentiates from the approach followed in this thesis, as it is more experiential and is based on data from accident investigations. The depicted Fault Tree incorporates some scenarios in the analysis related to the involved software failures, such as the load controller failure or the preferential trip device failure. Still, these failures are described on a high level. Potential overload conditions are not considered. The major limitation of this approach is that it does not incorporate scenarios that have never occurred before, which implies that potential future hazardous scenarios are not considered. In addition, the DG set blower failure will not necessarily lead to a blackout event, as a number of other conditions should simultaneously occur in order for a blackout to be encountered. So experiential approach of the developing Fault Tree leads to omitting potential hazardous scenarios.

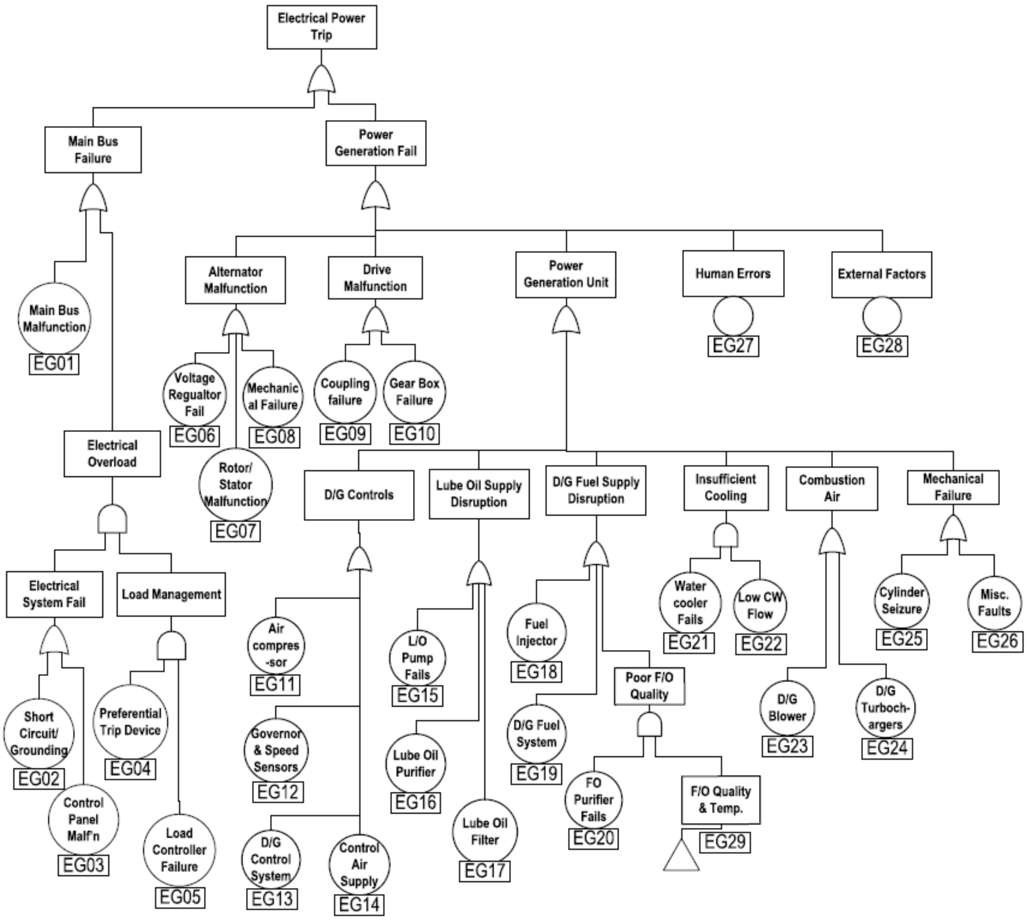


Figure 32 Blackout Fault Tree according to Aziz *et al.* (2019).

7.4 Top event frequency estimation and verification for the reference cruise ship DEP system (CASA Step 10)

For all the investigated case studies, the calculations were performed in Matlab/Simulink environment (MATLAB User’s Guide, 1998) by using the developed Fault Trees and the equations (1)-(15) provided in Section 4.8.1.

The blackout failure rate (λ^B) where the reference DEP system (consisting of 6 DG sets, system No1) employs a different number of simultaneously operating DG sets for the general mode are presented in Figure 33(a-c). The derived results for the following cases are provided by considering variation in both design and operational measures: (i) No prewarning alarms; (ii) all prewarning alarms effective; (iii) 3% MCR increase to the operating DG sets loading profile; (iv) 10% more frequent maintenance; (v) Intelligent diagnosis added to system; (vi) 50% reduced tripped load; (vii) initial system design.

It can be deduced from this figure that the λ^B is significantly higher when only one DG set operates, as a single point failure in the operating DG set or its auxiliary systems will lead to a blackout. In addition, due to the operational profile of the cruise ship and the DG sets loading conditions, DG sets overload conditions will occur more frequently when running with two or three DG sets (in comparison with the cases where more DG sets operate), which leads to greater λ^Bvalues in these cases. Furthermore, it can be also observed that operating with five operating DG sets provided a slightly greater λ^B in comparison with the $\lambda^B$when operating with four DG sets. This is primarily owing to the DG sets loading profile and secondarily to the fact that more components are used in the system, so it is more probable that a failure will occur.

From Figure 33, it can be also inferred that a substantial reduction in λ^B value can be achieved for a specific system configuration for the cases where prewarning functions are fully operational allowing for the switching over to a different engine in case of any critical alarm activation. This implies that the implementation of advanced prognostic and diagnostic techniques will improve the investigated DEP system safety for the case where one DG set operates, as it will allow for a reliable fault prediction and a timely system reconfiguration. In addition, it can be deduced that the λ^B is sensitive to the DG sets loading profile, since a small increase in loading (3% of Maximum Continuous Rating (MCR)) for each specific configuration leads to a considerable λ^B increase. The inspection and maintenance intervals seem to only slightly affect the $\lambda^B,$ as the maintenance and inspection of some critical components is already frequent and the influence of maintenance intervals can be investigated only for a number of the system components. The addition of intelligent diagnosis for handling load sharing errors has a positive effect on λ^B in the cases where a greater number of DG sets than three operates. According to the used operational profile, this is less frequent though, applicable to 25% of the plant operational time (Appendix D). Finally, the preferential tripping functions parameters have a direct impact on the λ^B similarly with the DG sets loading profile; the less load is tripped, the higher the λ^B.

The derived results for the case studies (viii)-(xi) (as described in Table 24) are presented in Table 28. The estimated frequency of blackout (FOB) in the general mode is higher than but relevantly close to the value of 0.1 events per ship-year, which was also reported in Friis-Hansen et al. (Friis-Hansen et al., 2008). However, in the harbour mode, the FOB is significantly higher than the FOB in the general mode. This is due to the fact that the system often operates with a single DG set connected to the ship power network. In the manoeuvring mode, a number of DG sets operate at lower loads, which leads to a lower FOB value. In the sailing mode, due to the increased number of the operating DG sets, the FOB is found to be approximately 0.003 events per ship-year and is much smaller than the respective values for the other modes. However, it must be noted that human error induced blackouts as well as blackouts caused by disconnection from the port network in the harbour mode are not considered in the blackout frequency calculations. Furthermore, the estimation of 0.1 average events per ship year and accident investigation statistics refer to the cruise ships and passenger vessels fleet and does not consider the specific differences between the different cruise ships propulsion systems, which have an important influence on the FOB calculation as discussed above.

Table 28 Comparison of λ^Bin different operating modes.

Operating Modes	λ^B $[hour^{-1}]$	FOB $[events/year]$
General (Case study (vii))	4.515 10^{-5}	0.396
Harbour (Case study (viii))	1.691 10^{-4}	1.481
Sailing (Case study (ix))	3.225 10^{-7}	0.003
Manoeuvring (Case study (x))	3.646 10^{-5}	0.319
Sailing Friis-Hansen et al. (2008)	1.141 10^{-5}	0.100
Accident investigation reports (General)	9.704 10^{-5}	0.850

It must be noted that whilst the FOB in the harbour mode is relatively high, there is no risk of collision/contact/grounding in the harbour due to blackout on the cruise ship itself. In the manoeuvring and sailing modes, the blackout duration can be short, and another DG set will be started up and connected to the ship electric network to supply the necessary power, unless there is a significant system failure. Furthermore, whilst the λ^B in the manoeuvring mode is higher than the one in the sailing mode, the percentage of time ship in manoeuvring is relatively small, which reduces the risk of collision, contact, grounding. In addition, the ship crew can apply drastic measures, such dropping anchor, if blackout occurs during manoeuvring. The detailed estimation of blackout risk is outside the scope of this study, however the blackout risk has been ranked as small by experts (Nilsen *et al.*, 2005).

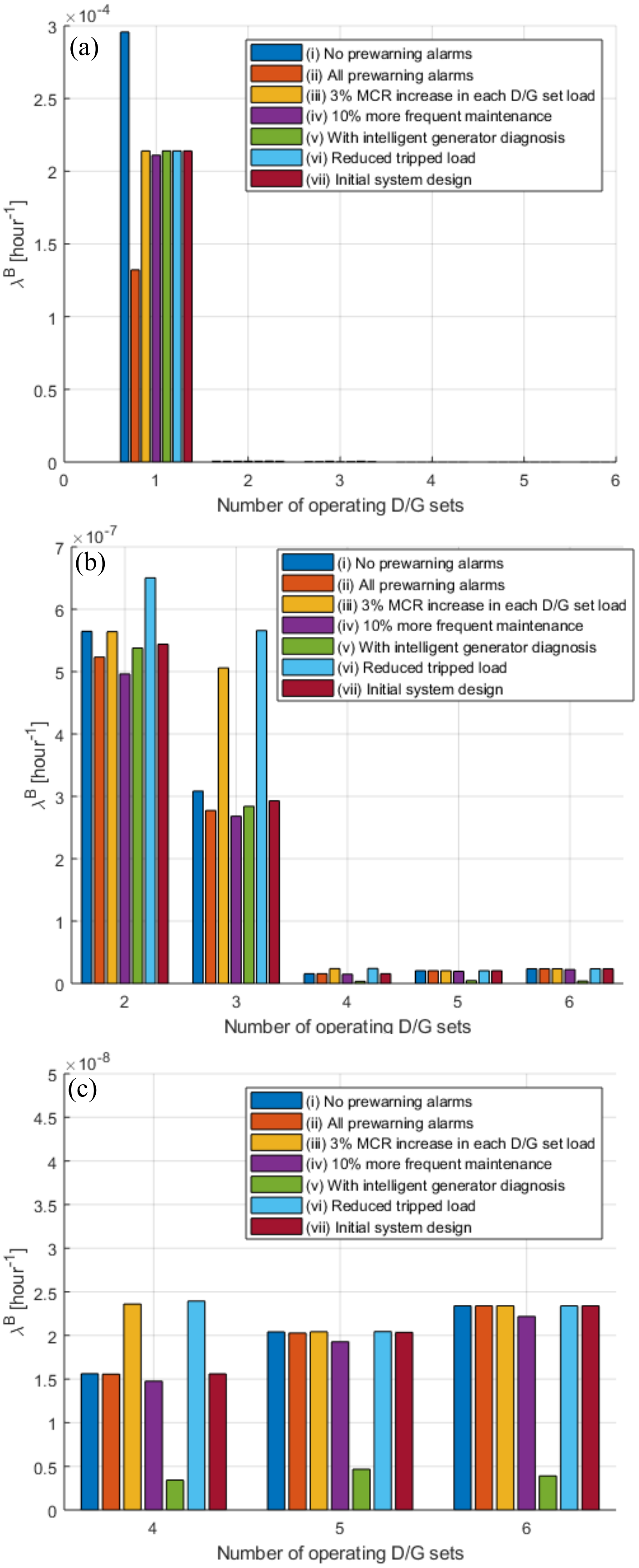


Figure 33 λ^B for different total number of DG sets operating (a) 1-6 DG sets operating; (b) 2-6 DG sets operating; (c) 4-6 DG sets operating.

7.5 Importance measures estimation and verification (CASA Step 10)

The calculated I_j^{FV} values for the general (case study xi) and the sailing (case study xiii) operating modes are presented in Table 29. The I_j^{FV} is used to represent the most probable failure leading to a blackout; higher I_j^{FV} values denote a higher probability that these failures will lead to a blackout. The results for the harbour (case study xii) and the manoeuvring operating (case study xiv) modes were similar to the results for the general operating mode. As it can be inferred from Table 29, the mechanical failures leading to loss of one DG set have a greater importance in the general operating mode than in the sailing mode. These include the failures in the cooling water and the lubricating oil systems as well as the engine failures leading to an erroneous/missing output. The blackout failure rate is adversely affected by errors in the control systems including the PMS command leading to (a) a running DG set stopping, (b) fuel quick closing valve faulty operation, (c) faulty DG set tripping by the safety systems and (d) erroneous sensor measurements of the engine bearing temperature. Failures leading to a DG set tripping without prewarning including failures in the control system hardware or shaft failures leading to a DG set stop were also identified as important. In the sailing mode, anomalies in the load sharing and control have a greater importance than in other modes. Such failures include erroneous DG set speed measurements, failures in fuel racks and failure in the propulsion motors fast load reduction. Fuel leakages and control hardware failures were also identified as important contributors to the λ^B increase.

As the I_j^{FV} metric can be used to identify the top event most probable cause, I_j^{FV} can be compared with available data from accident investigation reports and Protection & Indemnity (P&I) insurance club categories (UK P&I CLUB, 2015) by aggregating the I_j^{FV} values for the different failure categories leading to a blackout and analysing the overall contribution of each category (${I_j^{FV}}_{OM}$). The comparison of the calculated parameters with other data sources is shown in Table 30. The derived results, in general, are in line with the results derived from accident investigation reports provided by a cruise ship operator as well as the results from a published P&I club study (UK P&I CLUB, 2015). Differences in the estimated causal factors percentage in the various operating modes can be attributed to the fact that the importance of the mechanical failures changes from one operating mode to another as the mechanical failures are of greater importance when fewer DG sets operate. According to this analysis results, the mechanical, electrical and control failures have higher contribution to the λ^B value, whilst failures in the fuel system are found to contribute less to the λ^B value, in comparison to the respective contribution estimated according to the P&I results and the available accident investigation results. The observed deviations are justified by the fact that both the P&I clubs and accident investigation report results have been derived based on blackout analyses from a number of ships with different functionalities and design redundancy level, which, as it was explained in Section 4.5.1, contribute to the system performance variation. In addition, often these reports do not capture the actual accident causes. In this respect, they can be used only for a high-level comparison with the calculated results of the present study.

Table 29 Top critical failures in the investigated system.

	Failures	I_j^{FV} [-]
General mode	Lubricating oil pump failure	0.136
	High temperature water cooling pump failure	0.086
	Low temperature water cooling pump failure	0.086
	Shaft failure leading to engine stop	0.054
	Thrust bearings temperature sensors failure	0.052
	AVR hardware system failure leading to the DG set tripping	0.051
	Fuel quick closing valve faulty operation	0.046
	Generator safety faulty tripping the DG set	0.046
	Engine safety faulty tripping the DG set	0.046
	Failure in automation system – PMS stopping DG set without other set allocation	0.046
Sailing mode	DG set fuel racks failure	0.540
	Failure to reduce the propulsion motors load by the PMS	0.219
	Failure to reduce the propulsion motors load in time by PMS	0.219
	Failure to reduce the propulsion motors load by application controller	0.219
	Failure to reduce the propulsion motors load in time by application controller	0.219
	Governor speed sensors erroneous measurement	0.133
	Leakages in fuel pipes	0.085
	Load (current and voltage) sensors on azipods propulsion motors failure	0.041
	Engine safety system tripping engine with delay during failure occurrence	0.027
	AVR hardware system failure	0.026

Table 30 Comparison of the calculated results with results from P&I clubs and accident investigation reports for the distribution of causal factors.

	${I_j^{FV}}_{OM}$ estimated from external sources		Operating modes			
Failure category	UK P&I CLUB (2015)	Accident Investigation reports	General	Harbour	Manoeuvring	Sailing
Mechanical	8%	35%	49%	46%	49%	5%
Automation	22%	7%	5%	5%	5%	0%
Electrical	22%	13%	6%	6%	6%	46%
Fuel	22%	13%	7%	8%	7%	5%
Control	26%	32%	33%	35%	33%	44%

The ten failures with the greater estimated I_j^B values for the general and the sailing operating modes, indicating their 'structural' importance, are given in Table 31. The results for the harbour and the manoeuvring operating modes were similar to the results of the general operating mode. As it can be inferred from the general operating mode results, the blackout failure rate is sensitive to: (a) failures in sensors used for the DG sets tripping in case of a short circuit, and; (b) failures in the thrust bearings sensors due to multiple sensors employed. In the general mode, the blackout failure rate is also sensitive to failures leading to a sudden tripping of DG sets without prewarning, such as failure in hardware used for DG sets control, piston failures, lubricating oil pressure and fresh water cooling system temperature sensors failure. In addition, the λ^B was found sensitive to short circuits and differential current failures due to the fact that: (a) 3-phase Alternate Current electric system is used, and; (b) the short circuits occurrence leads to a DG set tripping without prewarning. In the sailing operating mode, the λ^B is sensitive to failures related to the system power reduction functions such as failures in the DG set and the propulsion motor power sensors as well as failures in sensors and actuator used for the power control in the DG sets. High λ^B sensitivity was identified with respect to design errors including overwhelming electrical transients in the system and DG sets circuit breaker failures. The proper operation of the DG set circuit breaker is important to ensure the DG set tripping when a number of failures in the DG set occurs, as otherwise it will lead to prolonged DG set maintenance.

Table 31 Calculated I_j^B indicating the system top sensitive failures.

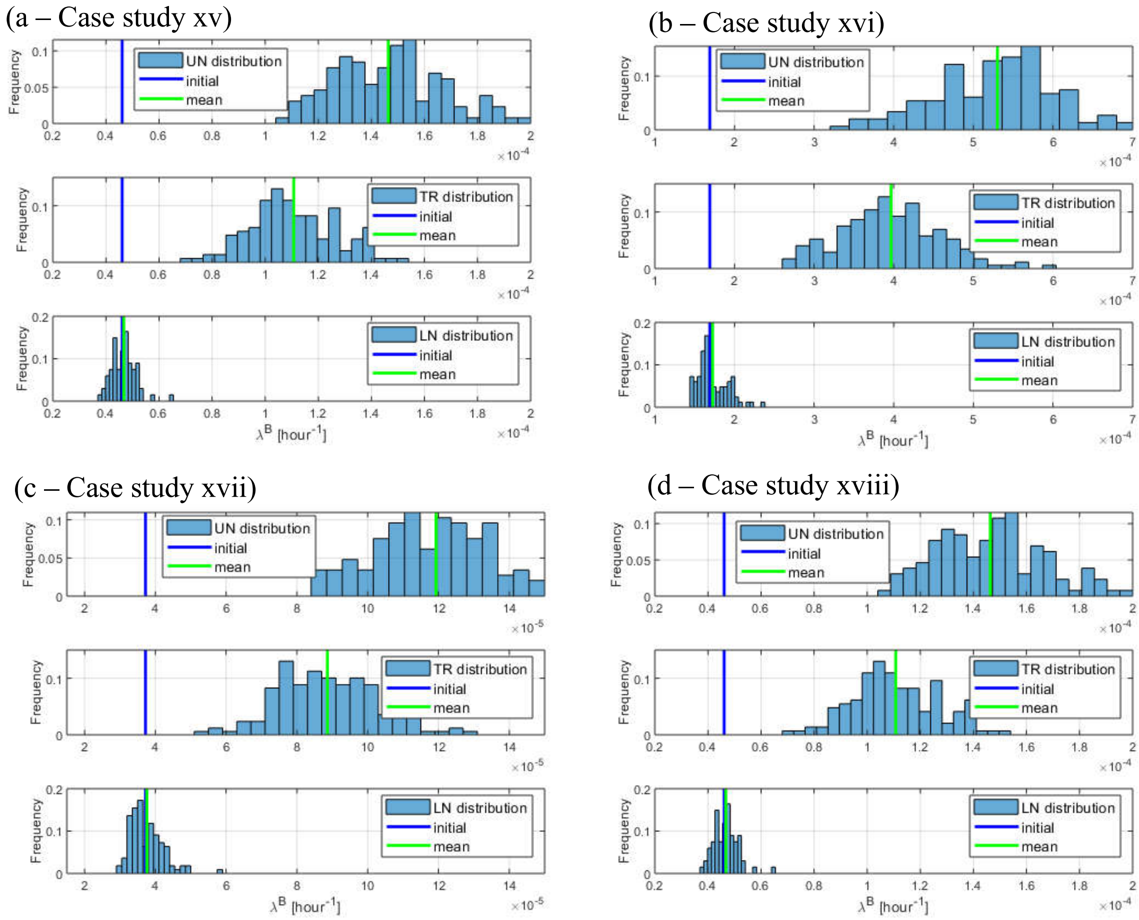
	Failures	I_j^B [-]
General mode	Generator safety system current sensors failure	0.630
	Thrust bearings temperature sensors failure	0.630
	Catastrophic engine piston failure	0.332
	Short circuit in DG sets	0.212
	AVR hardware system failure	0.212
	Fresh water-cooling system temperature sensors failure	0.212
	DG set controller hardware failure	0.212
	Governor hardware failure	0.212
	Lubricating oil pressure sensors failure	0.212
	Differential current fault in DG set	0.212
Sailing mode	Load (current and voltage) sensors on azipods propulsion motors failure	0.047
	Erroneous electrical power measurement on DG sets (current and voltage sensors failure)	0.011
	DG set fuel racks failure	0.007
	Governor speed sensors erroneous measurement	0.004
	Electrical transient is not acceptable by the system	0.003
	DG set circuit breaker not operating	0.002
	Erroneous speed measurement on propulsion motors	0.001
	Failure to reduce the propulsion motors load by the PMS	0.001
	Failure to reduce the propulsion motors load in time by the PMS	0.001

7.6 Uncertainty assessment (CASA Step 10)

The results of uncertainty analysis for case studies (xvi)-(xix) (described in Table 25) are presented in Figure 34 and Table 32. The uncertainty analysis was implemented for four operating modes (general, harbour, manoeuvring and sailing) employing the Uniform (UN), the Triangular (TR) and the Lognormal (LN) PDF distributions with a target accuracy Err_{acc} of 0.02. It can be inferred from the presented results that the λ^B mean values for the UN and the TR distributions are higher than the λ^B mean values estimated using the LN distribution and the derived λ^B values reported in Section 7.4. These differences are attributed to the different distribution types. The λ_i values dispersion is much closer to λ_i^{upper} values for the UN distribution, less closer to λ_i^{upper} values for the TR distribution and even less closer to λ_i^{upper} values for the LN distribution. As there is also a scale difference between the λ_i^{upper} and λ_i values due to selected EF_i values, the $\overline{\lambda_i^t}$ value of distribution will be close to the λ_i^{upper} value in the UN distribution, less closer to the λ_i^{upper} value in the TR distribution, and even less to the λ_i^{upper} value in the LN distribution than the case of the UN distribution. For the same reasons, the variance of λ^B value is also higher for the cases of UN and the TR distributions, whereas it is much smaller for the LN distribution. Concluding, the results demonstrate that there is significant variation in estimated λ^B and the uncertainty in the system components failure rates λ_i has significant impact on the estimated λ^B value.

Table 32 Uncertainty analysis results for various operating modes using different PDF distributions.

		mean $\lambda^B \pm 3\sigma$ for different PDF distributins $[hour^{-1}]$		
Operating Modes	λ^B $[hour^{-1}]$ (initial)	Uniform	Triangular	Lognormal
General	4.515 10^{-5}	1.464±0.607 10^{-4}	1.107±0.485 10^{-5}	4.672±1.389 10^{-5}
Harbour	1.691 10^{-4}	5.302±2.350 10^{-4}	3.967±1.900 10^{-4}	1.725±0.570 10^{-4}
Sailing	3.225 10^{-7}	4.018±4.114 10^{-6}	2.404±2.425 10^{-6}	3.255±4.435 10^{-6}
Manoeuvring	3.646 10^{-5}	1.193±0.525 10^{-4}	8.861±4.191 10^{-5}	3.761±1.430 10^{-5}
Sailing Friis-Hansen *et al.* (2008)	1.141 10^{-5}	Not Available	Not Available	Not Available
Accident investigation reports (General)	9.704 10^{-5}	Not Available	Not Available	Not Available


(a – Case study xv)

(b – Case study xvi)

(c – Case study xvii)

(d – Case study xviii)

Figure 34 Uncertainty distribution for λ^B in (a) General (b) Harbour (c) Sailing (d) Manouvering Mode.

The failures with the highest contribution to the λ^B calculation uncertainty is given in Table 16. As a basis for the analysis, the Pearson correlation coefficient ($r_{\lambda^B \lambda_i}$) from the LN distribution were selected since it is the most preferred PDF distribution as referred in 4.8.3 whilst the TR and the UN distributions were used for comparative purposes. It can be observed from the presented results that there is a difference in the $r_{\lambda^B \lambda_i}$ estimated using different distributions. The derived results are similar for the general, the harbour and manoeuvring operating modes. For this reason, only results for the general and sailing operating modes are presented. In the general operating mode, the failure rates uncertainty used for the failures leading to a loss of DG sets in one engine room (fuel quick closing valve faulty operation, clogged sea chests) and the failures leading to a DG set tripping (tripping due to oil mist fault alarm) significantly contribute to the λ^B uncertainty. For the sailing mode, the failures in the propulsion motor load reduction and the power generation control considerably affect the λ^B uncertainty. In the general and the sailing operating modes, the λ^B uncertainty increases due to components failures, which have been already identified as critical using the I_j^B and I_j^{FV} metrics (fuel quick closing valve faulty operation, failure to reduce the propulsion motors load by the PMS, DG set fuel racks failure). It can be also inferred that the software failures are a significant contributory cause to the system uncertainty, which is attributed to the selected EF_i . Some of the failures were identified as important when the LN distribution is used, however, the correlation coefficient $r_{\lambda^B \lambda_i}$ was found to be weak (close to 0.1 or even negative) or inconsistent with the uncertainty analysis results using other distributions, so these results cannot be considered as reliable.

Table 33 Uncertainty analysis results for the lognormal (LN), triangular (TR) and uniform (UN) distributions.

	Failures	$r_{\lambda^B \lambda_i}$ [-]		
		LN	*TR*	*UN*
General mode	Fuel quick closing valve faulty operation	0.668	0.263	0.433
	Generator safety current sensor failure	0.371	0.023	0.043
	Sea chest clogged	0.340	0.287	0.332
	Earth fault in DG sets	0.267	0.073	0.098
	Engine safety system faulty tripping the engine due to alleged high oil mist concentration	0.256	0.302	0.141
Sailing mode	Failure to reduce propulsion motors load by PMS	0.521	0.433	0.413
	Failure to reduce propulsion motors load by PMS in time	0.500	0.452	0.489
	Failure to reduce the propulsion motors load by application controller	0.478	0.417	0.455
	Delayed propulsion motors load reduction done by application controller	0.463	0.444	0.364
	DG sets fuel racks failure	0.236	0.339	0.390

7.7 Top event frequency estimation for alternative systems.

The estimation of top frequency and failure rate are provided in Table 34, Figure 36 and Figure 35. As it can be observed in Figure 35, the blackout failure rate with a single DG set operating in cruise ship propulsion system with batteries is lower than in the reference DEP system. Batteries increase the overall propulsion plant redundancy and allow for the system reconfiguration to include a healthy DG set in case where a fault in the operating DG set occurs. With 2 and 3 operating (connected) DG, the propulsion plant with batteries exhibit a λ^B reduced by 18 and 14 times, respectively. This is less than when one DG set operates (26 times compared to reference DEP system No1). This is because of: (a) common cause failures leading to simultaneous loss of multiple DG sets are more important when many DG sets are operating than in configuration mode with one DG set operating and they cannot be controlled by batteries; (b) due to the specific DG sets loading profile in the particular system, and; (c) the relevant (in %) batteries power contribution is reduced when more DG sets are engaged. Eventually, when more than three DG sets operate, the λ^B is quite similar with the λ^B for the case where four, five and six DG set operate due to the following reasons: (a) control failures leading to load imbalance become more important; (b) overload conditions more rarely occur due to the adequate redundancy in the system DG set, and; (c) DG sets specific loading conditions as the one provided in Appendix E. Concluding, this analysis results demonstrate that the introduction of batteries modules in an existing DEP system whilst lead to higher complexity in the system, also will lead to lower overall λ^B, thus enhancing the plant safety. However, this result must be also considered together with plant fire risk assessment (Bolbot *et al.*, 2019a), which has not been implemented in the present study.

For all the systems, as it can be deduced from Figure 35, the λ^B values for the case where one generator set operates are several orders of magnitude greater than the respective λ^B values when more generator sets operate. This is attributed to the additional redundancy in generator number in other modes. In the cases where one generator set operates, the λ^B for the various investigated solutions exhibited similar values (except the solution No2). Small λ^B variations can be attributed to the variation in failure rates for the physical components, as different fuel systems are employed in each one of the considered propulsion systems. When more than two generator sets are connected to the operating power plant, the variation in λ^B values between the different solutions are attributed to the generator sets loading conditions in each solution, which in turn is dependent on the generator sets size and the considered cruise ship operational profile. The λ^B values slightly increase when more than five generators are operating due to the fact that more components can fail in the system and there the number of operating generator sets is too limited, thus operating generator sets tripping is more prone to lead to a blackout.

Furthermore, it can be observed that when running with one DG set, the λ^B is slightly lower in systems with additional fuel systems. This is due to the higher redundancy in fuel supply system, as except for the normal fuel system, there is also LNG/methanol fuel supply system. In case where fault/failure in LNG/methanol fuel supply system occurs, the necessary fuel is taken from the normal diesel fuel supply system. Thus, slight improvements in system λ^B value can be attributed to the additional redundancy in fuel supply system.

As it can be observed from the Table 34, the incorporation of batteries reduces significantly the susceptibility to the blackout (results for system No2). The λ^B for the other systems significantly varies. However, the λ^B values lie within two ranges: one in the order of magnitude of 10^{-1} events per hour and another in the order of magnitude of 10^{-3} events per hour. The primarily parameter that influences these values is the frequency of operations with one DG set connected. In systems N7-8, 10, 12-13 the frequency of operating with one DG set is 0, which, as explained in the previous paragraph, naturally leads to a significantly reduced λ^B value.

Interesting conclusions can be derived from Figure 36 ((a) 1-8 total number of generators: (b) 2-8 total number of generators). As it can be observed from Figure 36, the dispersion of λ^Bvalues among designs with 6 and 8 generator sets is significant and similar. Designs with 6 DG sets can achieve an λ^B value similar with the system consisting of 8 DG sets and vice versa, designs with 8 DG sets can have as bad performance as systems with 6 DG sets. Thus, practically means that the increase in redundancy do not necessary leads to a significant λ^B improvement. Therefore, increased redundancy (and reliability) does not naturally translates into increased safety for power plants as other parameters can be critical, as explained previously.

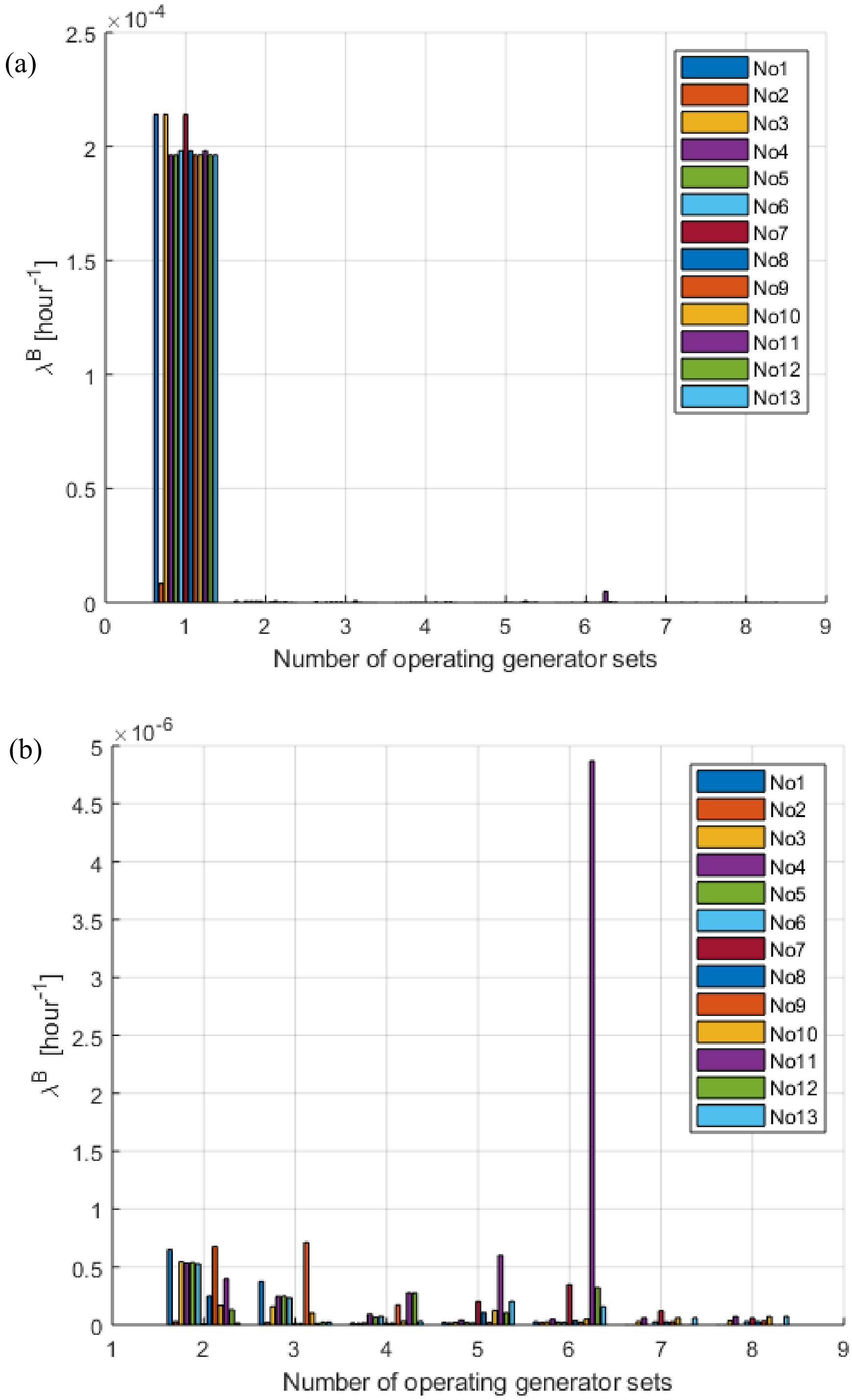


Figure 35 λ^B for different total number of operating DG sets: (a) 1-8 total number of generator sets operating; (b) 2-8 total number of generator sets operating.

Table 34 Blackout frequency estimations for different configurations

Case study No	System No	Total DG No	Fuel type / Energy storage type	OM	λ^B $[hour^{-1}]$	FOB $[events/year]$
vii.	1	6	HFO or LSHFO	G	$4.515\ 10^{-5}$	0.3955
xix.	2	6	HFO or LSHFO Batteries included	G	$1.759\ 10^{-6}$	0.0154
xx.	3	8	HFO or LSHFO	G	$3.133\ 10^{-5}$	0.2744
xxi.	4	8	Methanol & MDO	G	$4.260\ 10^{-5}$	0.3732
xxii.	5	8	HFO & Natural Gas & MDO	G	$5.151\ 10^{-5}$	0.4512
xxiii.	6	8	Natural gas & MDO	G	$4.297\ 10^{-5}$	0.3765
xxiv.	7	8	HFO or LSHFO	G	$2.286\ 10^{-7}$	$2.003\ 10^{-3}$
xxv.	8	8	Methanol & MDO	G	$8.569\ 10^{-8}$	$7.506\ 10^{-4}$
xxvi.	9	8	HFO & Natural Gas & MDO	G	$5.383\ 10^{-5}$	0.4716
xxvii.	10	8	Natural gas & MDO	G	$1.022\ 10^{-7}$	$8.957\ 10^{-4}$
xxviii.	11	6	HFO & Natural Gas & MDO	G	$6.645\ 10^{-5}$	0.5821
xxix.	12	6	HFO & Natural gas	G	$1.770\ 10^{-7}$	$1.555\ 10^{-3}$
xxx.	13	8	HFO & Natural gas	G	$1.010\ 10^{-7}$	$8.847\ 10^{-4}$
NA	Generic	NA	Friis-Hansen et al. (2008)	S	$1.141\ 10^{-5}$	0.1000

OM=Operating Mode / G = General / S = Sailing

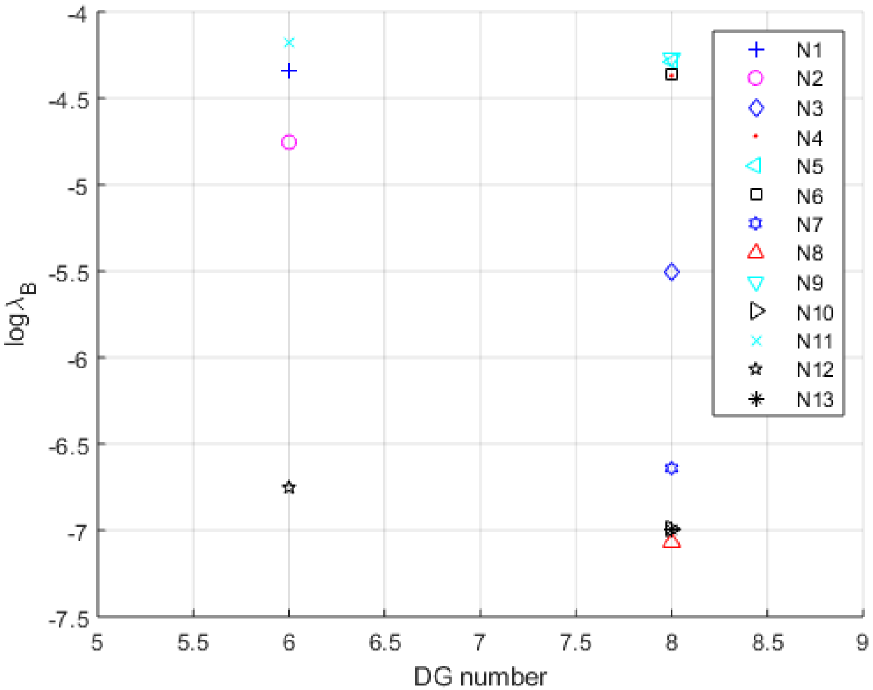


Figure 36 Blackout failure rate λ^B versus total DG number in systems N1-N13.

7.8 Safety recommendations

Overall the derived results for the employed importance and uncertainty metrics indicate that the failures of the generator sets, failures without pre-warning alarms (such as controller hardware failure, or shaft failures) and the failures that can lead to simultaneous loss of a number of generator sets are the most significant for the blackout failure occurrence rate calculation. These findings indicate that the engine room redundancy required by Safe Return to Port regulations prevents a number of scenarios leading to blackout, but it cannot address all the hazardous scenarios as explained below.

Additionally, blackout prevention requires a reliable operation of the preferential tripping and the propulsion motors load reduction functions. On the other hand, failures of the propulsion motors except for those related to the power reduction functions and failures in the electrical power network seem to be of less importance for the λ^B in the investigated DEP systems. The analysis results also indicate that the operational conditions and the generator set sizing influences significantly the generator sets loading conditions, which have a significant influence on the blackout frequency. Instead, the fuel selection has little influence on the selected systems susceptibility to blackout.

Based on this analysis results, the following safety recommendations can be provided for the design and operation for investigated system power plant, which can also be taken into consideration for other ship power plants. These are some existing and novel design and operational control measures which can reduce the blackout frequency:

- Ship operation with one generator set should be avoided as it results in considerably higher λ^Bvalues.
- The propulsion motors fast electrical power reduction function, the power increase control function and the preferential tripping function should be thoroughly examined during the system design phase and extensively tested during the ship sea trials. These software supported system functions must be also thoroughly tested after a software update.
- The employed generator sets size, loading profile and overload limits should be carefully selected to avoid overload conditions in case of one or more generator sets tripping.
- Prevention of failures leading to simultaneous loss of a number of generators sets such as a fuel quick closing valve faulty operation, a fire in engine room and clogged sea chests should be ensured.
- Meticulous design and testing of the components/subsystems with multiplicities such as piston assemblies must be ensured for generator sets.
- The systems design parameters shall be properly selected, as increased redundancy not necessary results in increased safety.

- Adequate redundancy in speed and voltage sensors should be provided or intelligent monitoring techniques should be employed to avoid failures in the electrical power control system leading to a load imbalance and a blackout.
- The condition of the generator sets fuel racks need to be closely monitored by using advanced diagnosis and prognosis techniques as it is important failure.
- Tripping of generator sets due to sensors failures can be reduced by employing relevant fault tolerance techniques allowing diagnosis and by-passing of relevant sensor failures.
- Sudden tripping of generator sets due to failures in the control system hardware can be reduced by closer monitoring of the generator set hardware health.
- Battery pack use could be considered for reducing probability of blackout in operations with one generator set.

7.9 Chapter summary

In this chapter, the results of applying the developed CASA method to several systems were provided. In total, 13 systems were investigated, and 30 case studies were implemented. The developed method guided and resulted in a more accurate safety analysis, compared with previous studies for the same system by incorporating the system software failures represented by the UCAs and considering hazardous states such as DG sets overloads, electrical transients and electrical disturbances. The method also allowed for the investigation of the system behaviour for cases where novel functions are added to the system, as was demonstrated with the prewarning functions for the DG sets in the investigated DEP plant. The STPA results demonstrated that the incorporation of batteries contributes to an increased number of hazardous scenarios. However, reduced blackout failure rate for the system with batteries was found. The importance measure estimation results demonstrated that different components and functions can be considered as critical in different operating modes. Significant variation of the blackout failure rate was also identified for the investigated systems, depending on the number of operating DG sets, the DG sets loading conditions, the tripped electrical load and the DG set overload limits. The results also demonstrated that increased redundancy does not necessary result in a reduced blackout frequency.

8 AUTOMATED BLACKOUT MONITORING SYSTEM INITIAL DEVELOPMENT

8.1 Chapter outline

In this chapter, the last major contribution of this thesis is presented – the methodology for developing an automated blackout monitoring system for enhancing the safety of cruise ship operations. Initially, the rationale for the development this system along with its basic architecture are provided. Then, the methodology that has been followed for its development and concept validation is described. The case studies that has been used to validate the concept are also demonstrated. Based on the derived results, the system advantages, disadvantages, and developmental cost are discussed.

8.2 Introduction

As it was commented in the Introduction (Chapter 0), there is a need to support the human operator in decision-making during safety-critical operations of complex systems. A potential solution regarding this challenge is the employment of new design and operational solutions, which integrate safety models, measured parameters (acquired from sensors) and the alarm monitoring system data.

This concept for the DEP automated blackout monitoring system is formulated in Figure 37. For the DEP plant, it would be possible to use sensor measurements for estimating the health indices for the plant subsystems/components, to integrate them with the available OREDA database information and to use Health Index (HI) and OREDA to update the component failure probability. The estimation of the power demand and the actual DG sets loading conditions could be used to estimate whether a DG sets overload will occur under specific system failure (in DG sets, in fuel system, etc.). The components that are presently operating and their history of maintenance from the Planned Maintenance System could be also incorporated in the safety analysis. All this information could be used to update the Fault Tree basic events probability of occurrence in time giving a real-time estimation of probability of blackout. Such an approach would allow implementation of risk assessment in time and integration of different bits of information into one metric representing the function reliability. It would be also possible to implement a dynamic importance measures estimation and support the selection of proper rectification actions enhancing the safety of ship operations.

The aim of this chapter is to demonstrate the validity of this concept and to verify its applicability to the selected cruise ship propulsion system. Its development along with the derived results are presented in the next sections.

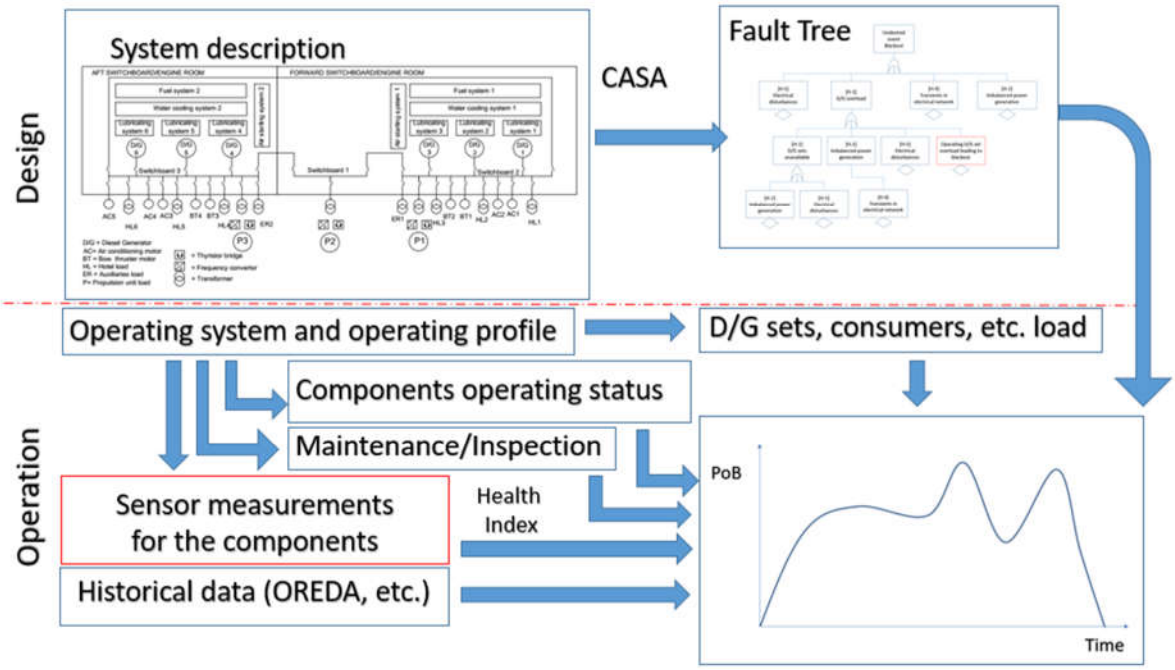

Design
System description
CASA
Fault Tree
Operating system and operating profile
D/G sets, consumers, etc. load
Components operating status
Maintenance/Inspection
Operation
Sensor measurements for the components
Health Index
Historical data (OREDA, etc.)
PoB
Time

Figure 37 The information flow for the blackout probability estimation.

8.3 Methodology

8.3.1 The general overview

The new technology development usually goes through different phases according to the Technology Readiness Levels (TRL) presented in Figure 38 (European Space Agency (ESA), 2009, EARTO, 2014). The development usually starts with observation of the basic principles at TRL 1, proceeds with technology concept/application formulation at TRL 2, and the concept validation at TRL 3 (European Space Agency (ESA), 2009, EARTO, 2014). The basic principles have been provided in the introduction (Section 1.3) and in literature review section (Section 3.4). The technology concept has been formulated in the previous section (Section 8.2). In this section, the methodology that was followed to validate the proposed concept according to TRL2-3 is described.

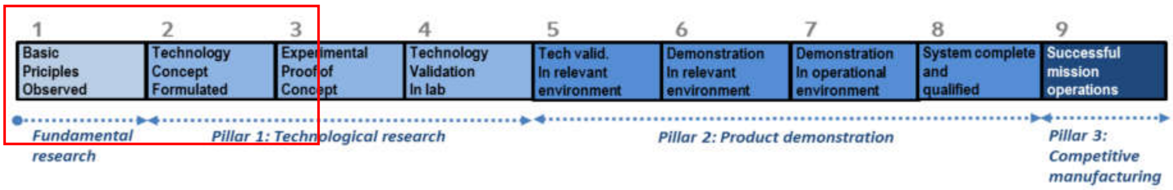

1
Basic Priciples Observed
2
Technology Concept Formulated
3
Experimental Proof of Concept
4
Technology Validation In lab
5
Tech valid. In relevant environment
6
Demonstration In relevant environment
7
Demonstration In operational environment
8
System complete and qualified
9
Successful mission operations
Fundamental research
Pillar 1: Technological research
Pillar 2: Product demonstration
Pillar 3: Competitive manufacturing

Figure 38 TRL levels adopted by European Commission (EARTO, 2014).

The general overview of the followed methodology for the development and validation of the proposed automated blackout monitoring system is provided in Figure 39. The first step includes the development of a safety model suitable for the automated safety monitoring for the investigated DEP system. In the second step, the parameters that can be monitored using sensors and data acquisition systems for the investigated cruise ship DEP system components are identified. During the third step, the failure rate is estimated based on sensor measurements. In the fourth step, the selected system parameters/sensor measurements are fused with the developed safety models. In the fifth step, the suggested safety enhancement actions for each failure/hazardous scenario are identified. In the sixth step, the system is simulated in a virtual environment and the concept is validated.

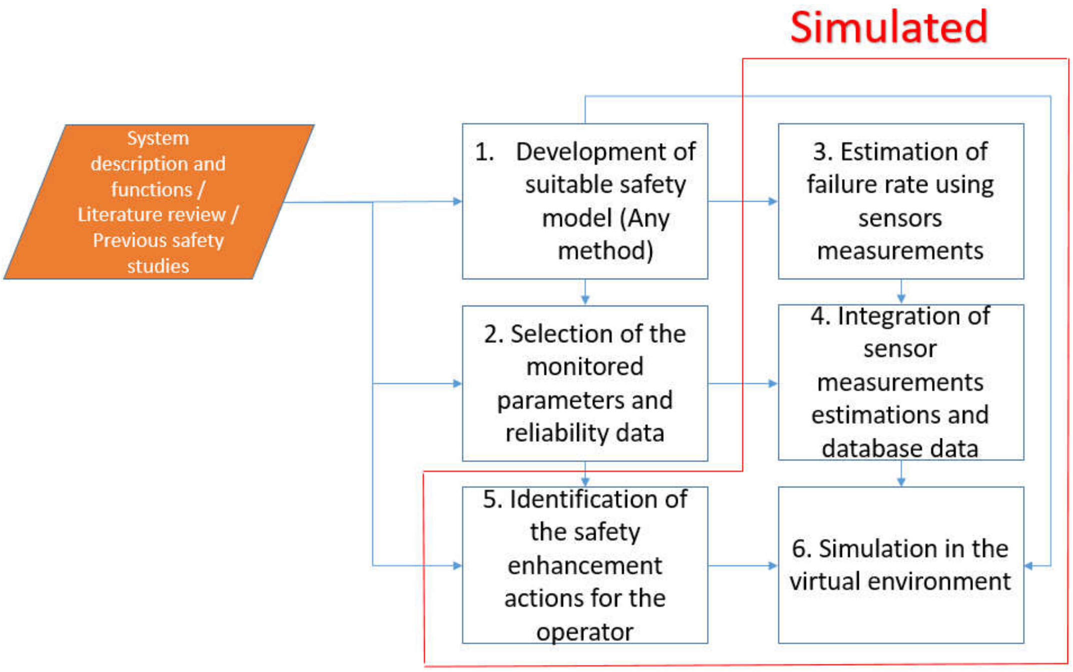

Simulated
System description and functions / Literature review / Previous safety studies
1. Development of suitable safety model (Any method)
2. Selection of the monitored parameters and reliability data
3. Estimation of failure rate using sensors measurements
4. Integration of sensor measurements estimations and database data
5. Identification of the safety enhancement actions for the operator
6. Simulation in the virtual environment

Figure 39 The flowchart followed for the development of safety monitoring system.

8.3.2 Development of the safety model (step 1)

The first step of the methodology includes the development of a suitable safety model. In general, a number of safety analysis methods can be employed for this purpose. This includes the FTA, HAZOP with Bayesian Network, BDMP as demonstrated by literature review in Section 3.4, but other methods could be also used such as Hip-HOPs for automatically deriving the Fault Tree or Dynamic Fault Trees. As shown, however, in the previous sections, the CASA method offers much more effective and comprehensive representation of the safety related events in the investigated system, thus, the CASA method has been preferred and selected for this analysis. The CASA method description was presented in Chapter 4, whereas the results derived by applying the method in two different investigated systems are discussed in Chapters 5 and 7. As this Chapter focuses on the reference cruise ship DEP system presented in Chapter 6, the Fault Tree developed at step 9 of CASA method (Figure 29) from Section 7.2.5 is used in the subsequent sections.

8.3.3 Selection of the monitored parameters and reliability data (step 2)

The following criteria are employed for selecting measured parameters for their integration with/inclusion to the developed automated safety monitoring system:

- Measured parameters that sufficiently and effectively depict/represent the actual system health based on the pertinent literature.
- Measured parameters that represent the system configuration and power demand e.g. which DG set is operating.
- Measured parameters monitored in the existing ship alarm and monitoring system.
- Measured parameters from the ship plant critical components, as identified from previous safety analyses or accident investigation data.

In addition to the required measured parameters, a number of failure rates is also required based on their availability and the relevant databases. These failure rates are used in conjunction with the sensor measurements to estimate the components failure rate. The databases such as OREDA database are selected based on their relevance to the system, availability, their trustworthiness, and publication date.

As described in the introduction of this Chapter (Section 8.2), the proposed automated safety monitoring system also incorporates the maintenance inspection intervals and the actual inspection implemented for the components. Therefore, the information from Planned Maintenance System is incorporated as well. It is desired to obtain the required input parameters for all the system components, to the focus is put on the most critical components of the investigated DEP system.

8.3.4 Estimation of failure rates using sensors measurements (step 3)

For the components, whose safety is monitored using sensor measurements, Health Indexes (HI_i) can be estimated. The HI_i are used to depict the performance and health status of component (Knutsen *et al.*, 2014, Jürgensen *et al.*, 2017, Bohatyrewicz *et al.*, 2019, Aizpurua *et al.*, 2019). The HI_i is estimated in this study as follows:

$$HI_i = \frac{|F_i - F_{alarm}|}{|F_{alarm} - F_{norm}|} \tag{21}$$

Where F_i represents a feature of for the system ith component, F_{alarm} is feature value when the component is failed (this can be the F_i value after which the component failure alarm is given to the crew) and F_{norm} is feature value under normal conditions. Features are variables indicative of component health state (Goebel *et al.*, 2017). The considered features (F_i) can be the component temperature and/or the pressure, a parameter estimated based on vibration analysis, or a combination of physical parameters, which can be considered as a reliable representation of component health state. F_i can be estimated based on the physical parameters monitored for a system component in real-time or at periodic times. Preferably F_i is a physical parameter monitored by the existing alarm and monitoring system. Based on eq. 21, when, HI_i=1, the component is fully functional, when HI_i=0, the components is failed, whilst intermediate values e.g. indicate degrading performance conditions of component.

Based on the estimation of the components HI_i, in absence of any other information, it is assumed that the components failure rates (retrieved from used database) (λ_i) can be updated, according to the following equation:

$$\lambda_{i,m} = \lambda_i^{HI_i} \tag{22}$$

The working assumption behind eq. (22) is that the closer the feature is to the alarm or failure threshold, the higher is the probability that failure will occur in the next period of time as depicted in Figure 40. It is also expected that the relationship between time and HI_i shall be of an exponential nature, as lower values of the component health index correspond to much lower component remaining useful life (Figure 40) (Hafver *et al.*, 2017, Mutunga *et al.*, 2019). This can be viewed as rather a conservative approximation for the component fault growth curve. By using the HI_i as the exponent in eq. (22), smoothness and exponential relationship in transition is ensured. In addition, the boundary conditions are satisfied. When HI_i equals to 1, the $\lambda_{i,m}$ equals to the original component failure rate (λ_i) which is only available estimation of the component probability of failure at the beginning, with no other information available. When the alarm limit is reached $(HI_i = 0)$, the component failure rate obviously equals to 1 h^{-1} and the therefore this component is considered faulty.

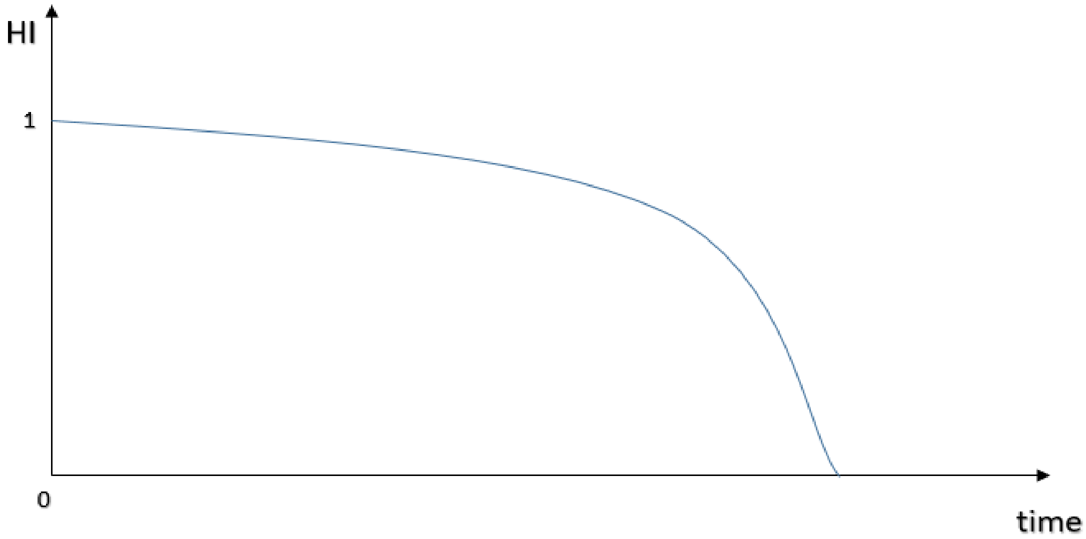


Figure 40 HI evolution in time.

8.3.5 Integration of sensor measurements estimation and database data (step 4)

For integrating the component failure rate with the health state estimated from the measured data, the following equation is used that employs the weight (w) assigned by the user or expert to different information sources in similar way as in (Aizpurua *et al.*, 2019):

$$\lambda_{i,A} = 10^{[w \log \lambda_{i,m} + (1-w) \log \lambda_{i,m}]} \tag{23}$$

The logic behind eq. (23) is that the expert/user can have different trust in the information available from the various measurements (sensors) and different trust to the information available from historical databases. w=1 denotes full reliance on the measured parameters, whereas w=0 denotes independence from measured parameters.

8.3.6 Identification of safety enhancement actions (Step 5)

For the safety enhancement during operations, the importance metrics are used to identify the critical failures and prioritise the rectification actions. The use of Birnbaum $I_i^B(t)$ and Fussel-Vesely $I_i^{FV}(t)$ importance metrics is suggested herein. The Birnbaum importance metric depicts the most sensitive component failure or components whose probability of failure slight change will impose significant changes in the Fault Tree top event probability. Therefore, these components degradation must be carefully monitored. $I_i^B(t)$ is also used to assess the top event sensitivity to some operating parameters such as number of operating DG sets or DG sets load. The Fussel-Vesely importance metric is used to identify the components whose failure most probably will occur and will lead to the blackout.

The Birnbaum importance measure is estimated according to the following equation:

$$I_i^B(t) = \frac{\partial P^{TE}}{\partial p_{i,A}} \approx \frac{\Delta P^{TE}(p_{i,A})}{\Delta p_{i,A}} \approx \frac{P^{TE}(p_{i,A}) - P^{TE}(p_{i,A}=0)}{p_{i,A}} \tag{24}$$

Where $p_{i,A}$ is probability of the basic event calculated by using $\lambda_{i,A}$.

For operating parameters, such as engine load or number of connected DG sets similar equation has been employed:

$$I_i^B(t) = \frac{\partial P^{TE}}{\partial p_{i,A}} \approx \frac{\Delta P^{TE}(OP)}{\Delta OP} \approx \frac{P^{TE}(OP\ initial) - P^{TE}(OP\ final)}{Small\ change\ in\ OP\ parameters} \tag{25}$$

As small change in the operating parameters value (ΔOP) could be considered the following: reducing the number of operating DG by 1 unit, or slightly increasing the DG set load, or reducing the number of connected electrical power consumers. This metric is used to identify if specific reconfiguration is required in the system to reduce the probability of the top event.

An averaged over time I_i^Bmetric is used to estimate the importance of each basic event in the Fault Tree based on the $I_i^B(t)$ value at different times and is estimated as follows:

$$I_i^{Bt} = \frac{1}{cr_{max}} \sum_{cr=1}^{cr=cr_{max}} I_i^B(t) \tag{26}$$

Where cr denotes a importance estimation number and cr_{max} denotes the maximum number of implemented importance estimations.

The Fussel-Vesely importance measure is estimated by using the following equation:

$$I_i^{FV}(t) = \frac{\partial P^{TE}/P^{TE}}{\partial p_{i,A}/p_{i,A}} = \frac{p_{i,A}}{P^{TE}} \frac{\partial P^{TE}}{\partial p_{i,A}} \approx \frac{p_{i,A}}{P^{TE}} \frac{\Delta P^{TE}\left(p_i^{Agg}\right)}{p_{i,A}} \approx \frac{P^{TE}(p_{i,A}) - P^{TE}(p_{i,A}=0)}{P^{TE}} \tag{27}$$

An averaged over time I_i^{FVt} metric is used to estimate the importance of each basic event based on the $I_i^{FV}(t)$ value at different times and is estimated as follows:

$$I_i^{FVt} = \frac{1}{cr_{max}} \sum_{cr=1}^{cr=cr_{max}} I_i^{FV}(t) \qquad (28)$$

The importance measures indicate which components failures /operational parameters are critical. Based on that, suggestions for system enhancement are generated. This can be the changeover to a healthier DG set to allow maintenance and repair actions to occur or increasing the number of operating DG sets or reducing the propulsion motors load (speed).

8.3.7 Simulation in the virtual environment (Step 6)

To allow simulation of the system top event and dynamic importance measures estimation, the developed Fault Tree basic events are transformed into the suitable Markovian process. This makes the developed Fault Tree structure similar with the Boolean logic Driven Markovian Process (BDMP) (Bouissou and Bon, 2003). The use of BDMP has been considered as necessary to depict some dynamic features of the systems, which are not available in the Fault Tree. This is explained in detail below.

The BDMP model can be defined by the following quadruple $\langle L, G, T, TE \rangle$ (Bouissou and Bon, 2003, Aizpurua *et al.*, 2017b), where:

- $L = \{L_i\}$ is the set of basic leaves (equivalent for basic events in the fault tree), where each leaf is represented using a Markov process P_i and can have two states Working (W_i) or Faulty (F_i).
- $G = \{G_i\}$ is the set of Fault Tree gates, which can be of two types: OR and AND.
- $T = \{T_i\}$ is the set of triggers of a BDMP model. The triggers are used to model the dynamic dependencies, i.e. the triggers are used to model the switch of one mode to another in a leaf according to the set of the selected Boolean variables in another leaf.
- TE is the modelled top event for the system.

An example of a BDMP model is provided in Figure 41.

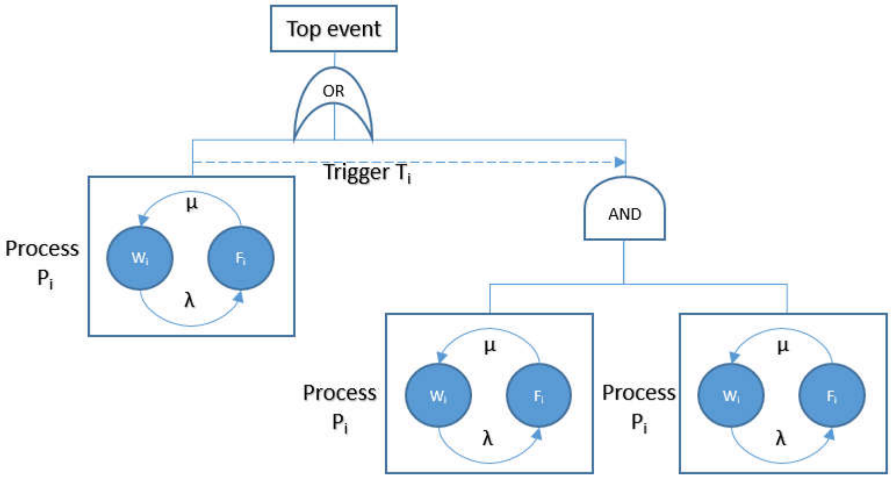


Figure 41 A BDMP example.

W_i=working state, F_i=faulty state

To allow for the simulation, some basic events of the developed Fault Tree are transformed into Markovian process, whilst the probability of failure for basic events is also modified by employing the equation provided in Table 35. For the prediction of the top event probability of occurrence in the next time step (Δt in hours), probabilities are used for calculations. However, in parallel a random function is involved to simulate probabilistically whether the component is faulty. So, in the case of a failure occurrence, the probability value of this specific basic event becomes 1. In this way, the used Fault Tree constitutes the simplest form of BDMP, as there are no triggers $\{T_i\}$ involved. The Fault Tree uses OR and AND gates for calculations, whereas different branches of the Fault Tree are activated or deactivated based on the operating status of components. Therefore, the probability of the top event is estimated as function of the combination of basic leaves following the rules for the AND and OR gates.

For the simulation of the system in the virtual environment, the investigated plant operating parameters, such as the DG sets load, the number of connected DG sets, were taken from actual historical data, which were used in the form of time series.

For the simulation purposes only, it has been assumed that the F_i is evolving according to the following equation:

$$F_i = F_i^{norm} + F_i^{deg}(t - t_i^m) + noise \qquad (29)$$

Where F_i^{norm} is the normal feature value, whilst F_i^{deg} is degradation parameter, t_i^m is the time of the last maintenance for the component i. A noise term is introduced in the analysis to account for the sensor's measurement uncertainty. However, the actual fault growth curve can differ significantly from the suggested curve and depends on the component operating conditions. These assumptions are used only for the simulation purposes.

The F_i^{deg} was assumed to be equivalent to the half of the inverse of the maintenance inspection interval. This assumption was made based on the observation that the preventative maintenance scheme in maintenance manuals quite often is implemented every half of the component useful life.

Table 35 Probabilities of basic events in the developed Fault Tree

	System components	Original Fault Tree probability estimation	Modified Fault Tree probability estimation (BDMP model)	Eq. Number
Operating components	Software, hardware, communication and sensors failures (Schüller *et al.*, 1997)	$p_{i,j}^{OC} = \lambda_i \mathrm{t}$	$p_{i,j}^{OC} = \lambda_i \Delta t$	(30)
	Other components with preventative maintenance	$p_{i,j}^{OC} = T_i^{\beta_i-1} \lambda_i^{\beta_j} t$	$p_{i,j}^{OC} = \beta_j \lambda_i^{\beta_j} t_i^{\beta_i-1} \Delta t$	(31)
	Parts with preventive maintenance where a single component failure out of r identical will lead to event occurence (based on (Schüller *et al.*, 1997))	$p_{i,j}^{OC} = \sum_1^r \binom{r}{1} \left(T_i^{\beta_i-1} \lambda_i^{\beta_j}\right)^r \left(1 - T_i^{\beta_i-1} \lambda_i^{\beta_i}\right)^{1-r} t$	Replaced with OR gate connecting components failures. Each component failure rate is modelled as in (4)	(32)
	Parts with preventive maintenance where all the r identical components must fail for event occurrence (based on (Schüller *et al.*, 1997))	$p_{i,j}^{OC} = \left[\left(T_i^{\beta_i-1} \lambda_i^{\beta_i}\right)^r + r T_i^{\beta_i-1} \lambda_i^{\beta_i} \left(\frac{\lambda_i}{\lambda_i + \mu_i}\right)^{r-1} + \left(\frac{\lambda_i}{\lambda_i + \mu_i}\right)^r\right] t$	Replaced with AND gate connecting components failures. Each component failure rate is estimated as in (4) and each component state is modelled as a Markov process.	(33)
Safety systems	Tested standby equipment failure on demand (except for software failures) (Schüller *et al.*, 1997)	$p_{i,j}^{SS} = 1 + \frac{\left(e^{-\lambda_i T_i} - 1\right)}{\lambda_i T_i}$	$p_{i,j}^{SS} = 1 + \frac{\left(e^{-\lambda_i T_i} - 1\right)}{\lambda_i T_i}$	(34)
	For safety system/functions with continuous monitoring failure on demand (Schüller *et al.*, 1997)	$p_{i,j}^{SS} = \frac{\lambda_i}{\lambda_i + \mu_i}\left(1 - e^{-(\lambda_i + \mu_i) T_i}\right)$	Modelled as Markov process	(35)
	Safety functions with periodical testing failure on demand (Schüller *et al.*, 1997)	$p_{i,j}^{SS} = 1 + \frac{\left(e^{-\lambda_i T_i} - 1\right)}{\lambda_i T_i}$	$p_{i,j}^{SS} = 1 + \frac{\left(e^{-\lambda_i T_i} - 1\right)}{\lambda_i T_i}$	(36)
	For software failures in safety functions (Schüller *et al.*, 1997)	$p_{i,j}^{SS} = PFD_i$	$p_{i,j}^{SS} = PFD_i$	(37)
	Unavailability due to periodical maintenance of standby equipment where r standby equipment are involved (based on (Schüller *et al.*, 1997))	$p_{i,j}^{SS} = \left(\frac{1/T_i}{1/T_i + \mu_i}\right)^r$	Replaced with AND gate connecting components failures. Each component failure rate is estimated as in (8) and each component state is modelled as a Markov process.	(38)

8.4 Case studies and analysis input description

The analysis has been implemented for the reference DEP system (system N1) described in Chapter 6. The Fault Tree developed in Chapter 7 is used as input. The actual operational profile time series of load and connected DG sets has been used to simulate the DEP system: The DG sets load in time, connected DG sets number, propulsion motors number, etc. The simulated case studies are provided in Table 36. The simulation run is implemented for approximately a week, whilst the blackout probability is predicted using horizon of 24 hours considering that operating conditions are stable (not changing). Considering some computational limitations, the importance measures is implemented every 24 hours at case study 4. As reference value, the annual failure rate of 0.1 blackout per year (Friis-Hansen *et al.*, 2008) has been used, which is translated now in probability. Probabilities are estimated now, as the interest in estimation of likelihood of at least one blackout occurring in the predicted horizon, not number of predicted blackouts. Except PoB the probability of a DG set loss in active system is estimated (PoDGloss)

Table 36 Simulated case studies.

a/a	Selected w [-]	Analysis conducted
1	0	Time step: Δt = 0.5 h Simulation run duration 175 Horizon prediction of 24 hours
2	0.5	As above
3	1	As above
4	0.5	As above + Importance measures estimation implemented every 24 hours.

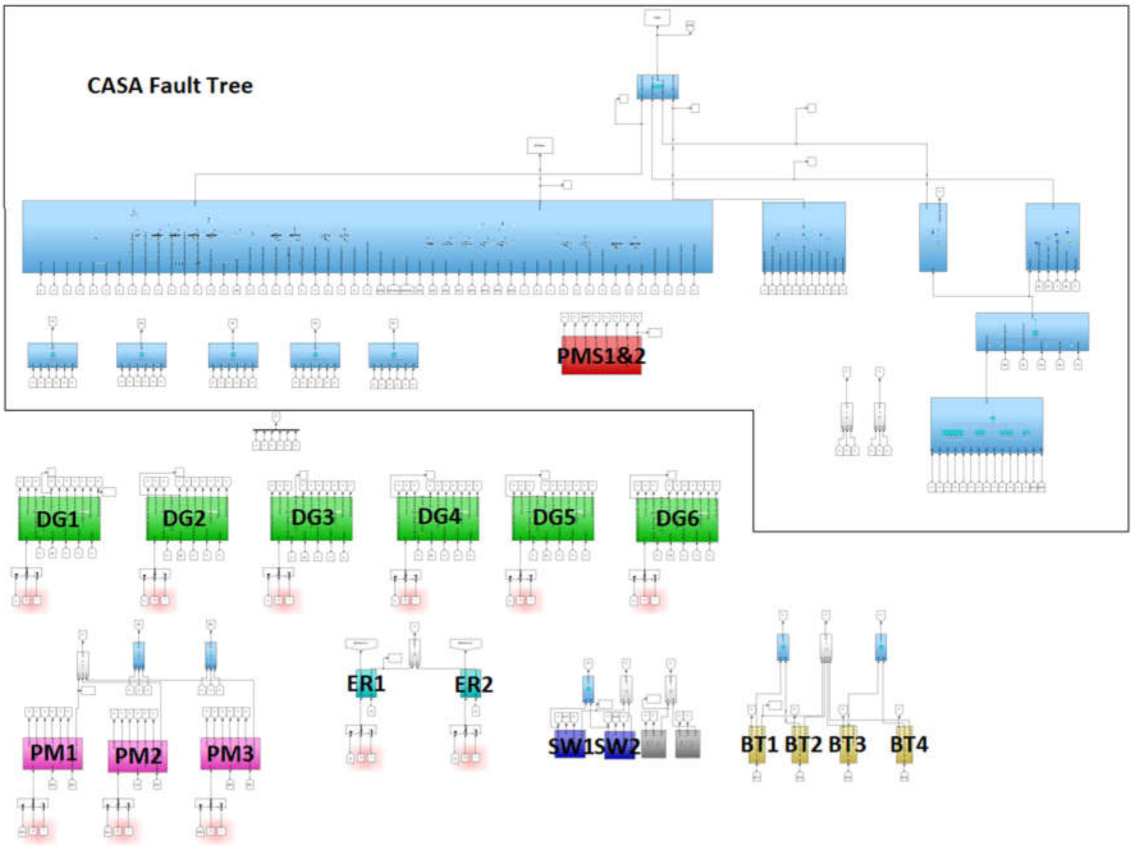


Figure 42 The developed model for blackout monitoring system simulation.

8.5 Results

8.5.1 The development of safety model for simulations (step 1)

The model that has been developed for blackout monitoring system simulation in Matlab/Simulink environment is provided in Figure 42. The Fault Tree developed by CASA in Chapter 7 can be observed there, as well the major DEP subsystems: DG sets, Propulsion Motors (PM), Engine Room (ER) components, Bow Thrusters (BTs), Switchboards (SW). The Fault Tree structure is not shown further as it is too extensive. The basic event probability for each component as well as operating status are used in the Fault Tree calculations.

8.5.2 Selection of the monitored parameters and other data (Step 2)

The features F_i that have been selected for health monitoring for some components and the maintenance intervals used to estimate F_i^{deg} are given in the Table 37. These features have been selected, since the respective measured parameters are available in the ship alarm and monitoring system and these measurements are used for monitoring of safety critical components based on the results of Section 7.5.

Table 37 Selected features for the identified critical components of the investigated cruise ship DEP system.

a/a	Component	Feature	Normal value	Alarm value	Maintenance interval
1	Engine Thrust bearings	Temperature	80ºC	100ºC	18000 hours
2	Engine Main bearings	Temperature	80ºC	100ºC	18000 hours
3	Engine high temperature cooling water pump	Pressure	4 bar	2 bar	10000 hours
4	Engine low temperature cooling water pump	Pressure	3.6 bar	2 bar	10000 hours
5	Generator low temperature cooling water pump	Pressure	3.6 bar	2 bar	10000 hours
6	Exhaust gases valve	Temperature	450	490	6000 hours
7	Turbocharger (TC)	Temperature	450	490	12000 hours
8	Engine lubricating oil cooler	Temperature	70	80	10000 hours
9	Lubricating oil pump	Pressure	4	3	5000 hours

Other parameters that are used as input to the system are:

- DG sets operating status.
- DG sets load.
- Engine room operating status (whether in use or not)
- Number of operating DG sets in each engine room
- Hotel load

- Propulsion motors operating status and load
- Bow thrusters status and load
- Whether a DG set is starting
- Whether a propulsion motor is starting

Reliability and maintenance intervals data has been selected for the DEP system simulation as well. However this data has been already presented in Section 6.3.2 and 6.3.3 and for reasons of brevity their description has been omitted.

8.5.3 Simulation in the virtual environment (application of Steps 3-6)

The simulation results of simulation for the case studies 1 to 3 are provided in Figure 43. As it can be observed the Probability of Blackout (PoB) is higher than the reference value (0.1 blackout per year) in case when only one DG set is operating. For this reason the same results are presented in Figure 43 (b), excluding the conditions with operation with one DG set. At the same time it can be observed that at these conditions the propulsion motors are disconnected, which indicates that the vessel is in harbour mode. Therefore, the PoB increases significantly in harbour mode, which is in line with previous sections results (Section 7.4).

The reference value is also exceeded when no propulsion motors are connected and the ship is propelled using bow thrusters. This can be attributed to the fact that power reduction functions for the propulsion motors are not available during this operation, and hence less safety barriers are active in the system. This occurs despite the low DG set load and the significant number of DG sets engaged. From this it can be inferred that according to this analysis the power reductions functions have a critical role for the ship safety. This is also in line with the findings from the previous Chapter 7. A potential way to improve the ship safety would be by including the power reduction functions for the bow thrusters as well.

The probability of sudden loss of a DG set (PoDGloss) in the system is also presented in Figure 43. As it can be observed, the PoDGloss follows the same pattern with the number of connected DG sets. This can be attributed to the fact that the more DG sets are connected to the system, the higher the probability that one of them will fail. However the PoB seems to be little correlated to the PoDGloss. This indicates that a number of other parameters is more critical for PoB than number of connected DG sets, except condition when only one DG set is connected.

Additionally, a variation in the PoB value can be observed if the sensor measurements are excluded from the analysis, partly included, or are included. This indicates that the incorporation of sensor measurements in this case will have a significant influence on the result of the automated blackout monitoring system.

The importance measures estimation results from the case study 4 for the selected components are provided in Table 38 and Figure 44. The importance measures estimation is implemented only every 24 hours, so the actual variation of these importance metrics is unknown between these points. However, the provision of lines offers better visibility and therefore has been preserved. The importance metrics in Table 38 is in line with results generated previously in Section 7.5. These importance measures estimation results demonstrate that not only physical failures but also failures in software functions demonstrated in Table 38 can be considered as critical for system safety during operations. Additionally, the investigation demonstrates the importance of other hazardous events e.g. arc in switchboards. Based on that consideration and ranking the system operator must pay attention to variation in sensor values/degradation of these specific components and failures, as small change in their value can have significant influence on PoB.

As it can be observed from Figure 44, the importance of each DG set varies with time. Obviously, the importance depends if the DG set is connected to the system or not. A disconnected DG set has an importance of 0. The importance variation can be observed due to the different degradation, usage of the DG sets, system configuration and system loads. The importance metric $I_i^{FV}(t)$ for DG2, DG5 and DG6 is reduced at t=120 hours as three DG sets are operating at a low load, so it is unlikely that a failure in DG sets will result in blackout. So potentially at this condition it would be possible to operate with only two DG sets with better DG load conditions, improving the energy efficiency of power plant, without sacrificing safety. The importance metric $I_i^{B}(t)$ increases for DG1, DG5 and DG6 at t=144 hours because instead the load is relatively high, so the sensitivity to failures increases. It is a situation where the crew must be on alert on potential failures / degradation of DG sets health index.

The importance metric $I_i^{FV}(t)$ for different components of the DG1 is provided in Figure 45. As it can be observed the importance of components varies with time. This relates to the configuration parameters as explained previously. In addition, the importance of each component with respect to the other varies in time e.g. Low Temperature (LT) water pump importance is less than High Temperature (HT) water pump importance at 72 hours but higher at 144 hours.

Table 38 Importance measures estimation results.

Component or software function failure	I_i^{Bt}[-]	Type of failure
PMS failure to reduce load of propulsion motors	0.0047	Software
Arc protection software failure	1.21E-09	Software
Arc in switchboards N1 and N2	0.0072	Physical
DG 1 water cooler failure	0.0004	Physical
DG 1 Engine lubricating oil cooler	0.0004	Physical

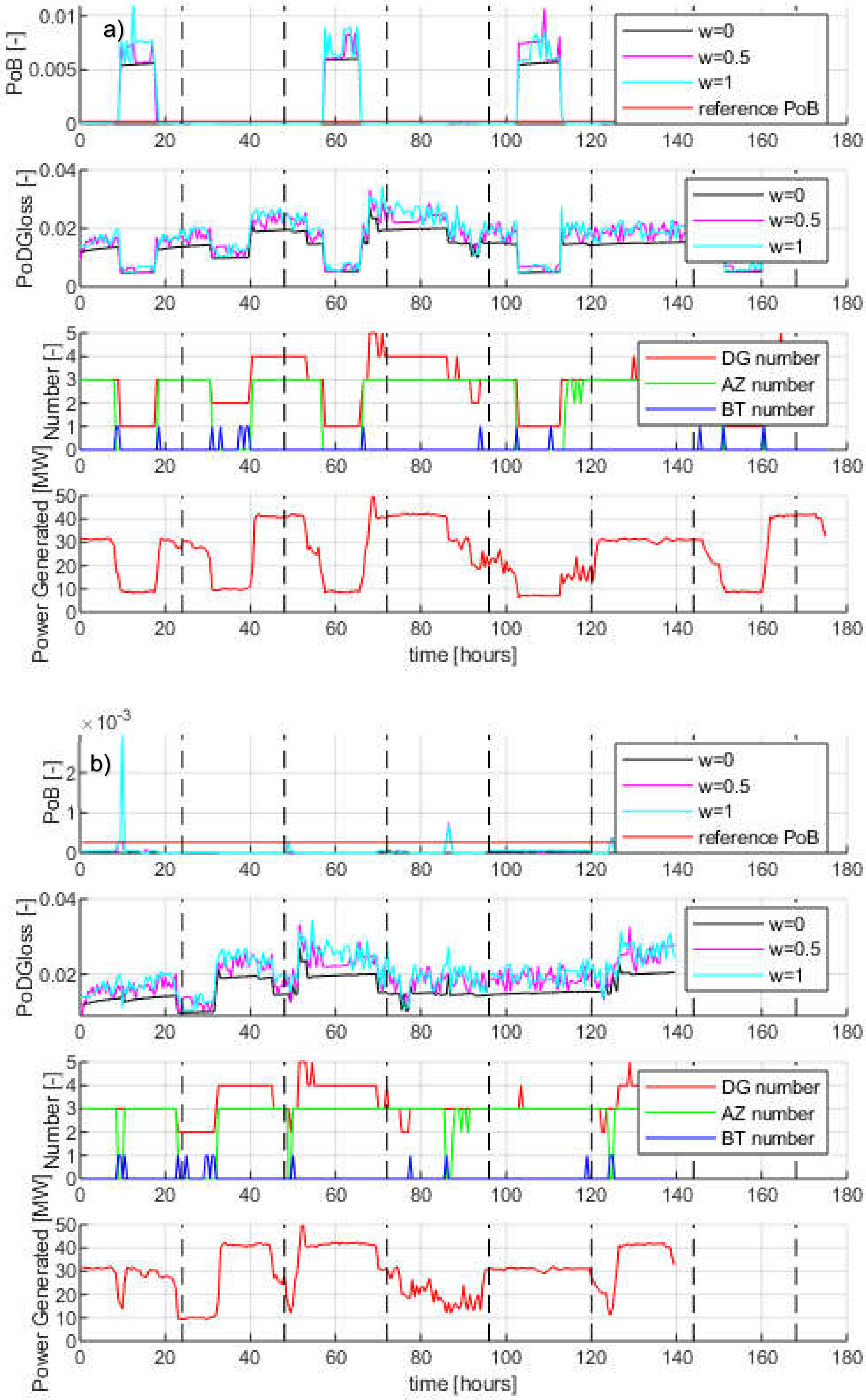


Figure 43 Estimated PoB and probability of DG loss values a) Normal b) Filtered (excluding the conditions with one DG set operating).

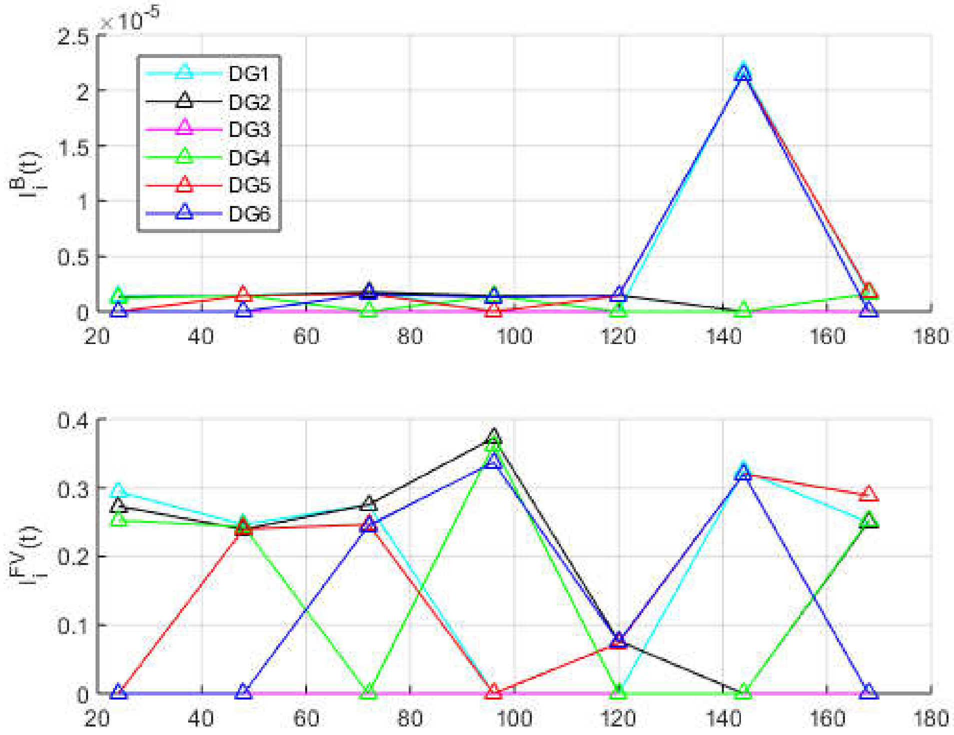


Figure 44 $I_i^B(t)$ and $I_i^{FV}(t)$ for the connected DG sets (x axis is hours).

*lines between importance measures estimation points have been added for better visibility.

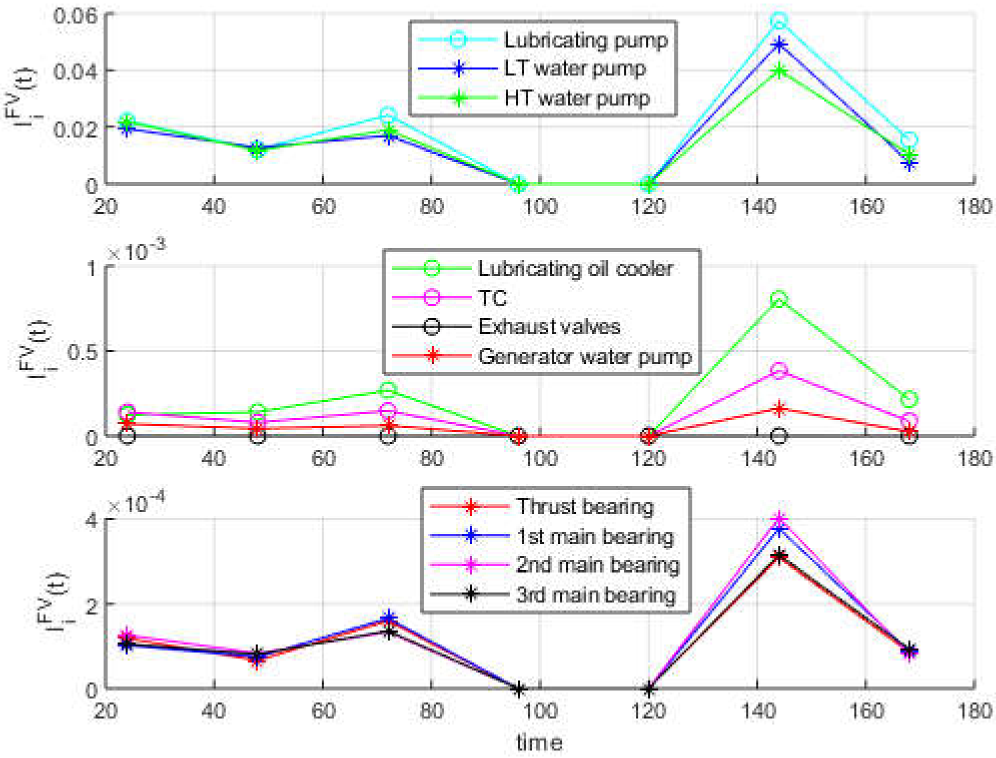


Figure 45 $I_i^{FV}(t)$ for different components for DG1 (x axis is in hours).

*lines between importance measures estimation points have been added for better visibility.

8.6 Discussion

The presented blackout monitoring system satisfies some of the automated safety monitoring system criteria (Papadopoulos and McDermid, 2001). It provides high-level functional alarm for the tested cruise ship power system based on the prevailing system operating conditions. It also allows for the organisation of the alarms/failures to reflect their present importance in the investigated DEP system. Furthermore, in this way it allows the operator to assess indirectly the impact of different failures on the ship functions and to select the components that need to be maintained or disconnected from the DEP system. Therefore, it can be inferred that this concept facilitates the cruise ship DEP management.

However, the suggested blackout safety monitoring system does not incorporate the on-line fault diagnosis including the early detection of escalating disturbances and isolation of root failures from observed anomalous symptoms. This development would require gathering significant amount of historical data related to the subsystems of the cruise ship power system or development of detailed simulation models. The use of the features F_i based on the available critical alarms contributes to the simplicity of the developed model, but at the same time it can have a number of false positive, as it does not incorporate the features values variation due to variation of the plant power demand or/and the environmental conditions. Prognostic algorithms have not been incorporated in the system, as this would require significant amount of well-treated data to be analysed and used for the design of the required relevant algorithms. The blackout monitoring system does not consider the errors in sensor measurements. In this respect, its reliability depends on the reliability of the sensors measurements and alarms used as input. Still, this constitutes the first essential step to the development of this automated blackout monitoring system.

The development and validation of this blackout monitoring system required significant resources. One man-year was required to implement the CASA analysis for the reference DEP system. Additionally, around 3 man-months were required to develop the model for dynamic simulation and validation. Extra resources would be required to address the above-mentioned drawbacks. Further time would be required to implement and verify this approach and system in the industrial environment. However, the high development cost can be attributed to the fact that novel method has been employed for Fault Tree development. Furthermore, the lack of proper system information contributed to the delays to this project. Therefore, further work or reapplication of the method to other systems would be more efficient than presented herein.

8.7 Chapter summary

In this chapter, a methodology for the development of an automated safety monitoring system for enhancing the safety of a cruise ship DEP system operations was presented. The rationale and the main steps of this methodology as well as the concept validation up to TRL2/3 level in a virtual environment were provided. The amendment of the Fault Tree derived by the CASA method was required for the methodology application for the case of the cruise ship reference DEP system. It was demonstrated that the proposed automated blackout monitoring system can identify the conditions where the probability of blackout exceeds the set thresholds and the components which failure is importance from the safety perspective. The ability to incorporate the different sensor measurements was also verified. Still, the proposed system needs to be improved to enhance accuracy by using input from diagnostics and prognostics technologies. The development cost for the blackout monitoring system proved significant, although future applications of the proposed methodology at the concept stage are not expected to be so resource-intensive.

This page has been intentionally left blank

9 DISCUSSION

9.1 Chapter outline

In this Chapter the main outcomes of PhD thesis are discussed. First the novelty of the current research is presented using bullets points. Then the advantages of the novel method are elaborated. This Section is followed by the discussion on the present research limitations. Last, the main contributions of the PhD are summarised.

9.2 PhD research novelty

The novelty of the present research includes:

- A critical review of the hazard identification methods and analysis methods identification of the safety related properties for the CPSs and investigation of how the hazard identification methods address these properties. (Resulted in a journal publication, see Research output)
- Cross-fertilisation of STPA, Event Sequence Identification (ESI) and FTA methods to develop a "Combinatorial Approach to Safety Analysis" (CASA), which is a novel safety analysis method. (Research gaps 1,4,8,9,11, Section 3.6.1)
- Safety analysis of the exhaust gas open loop scrubber system with respect to compliance to environmental rules and regulations. (Novelty supported in Section 5.4)
- Blackout failure rate estimation for the reference cruise ship DEP plant and the associated importance metrics estimation and uncertainty analysis. (Research gaps 12-14, Section 3.6.2)
- Assessment of the susceptibility to blackout with different number of DG sets running, in several operating modes, with varying design features and considering the effect of Intelligent Diagnosis for a cruise ship power plant. (Research gaps 12-14, Section 3.6.2)
- Investigation for a number of alternative DEP systems for a cruise ship in terms of their susceptibility to blackout including systems with LNG fuel system, methanol fuel system, combination of LNG and Heavy Fuel system and batteries. (Research gaps 12-14, Section 3.6.2)
- Development of new methodology for the design of the automated dynamic safety monitoring system and integration of a number of system parameters. (Research gaps 16, Section 3.6.3)
- Safety monitoring system concept development for the cruise ship DEP power plant with focus on blackout prevention on cruise ships and validation in virtual environment. (Research gaps 16, Section 3.6.3)

9.3 Method advantages

Based on the results, it was demonstrated that the proposed novel CASA method main advantage is the development of a Fault Tree of greater accuracy in comparison with the Fault Tree that can be derived using the classical FTA. The classical FTA may result in inaccuracies if applied to a modern CPS. The CASA method incorporates a wider system context, considers the software failures, thus addressing the

CPSs software-intensive character of CPSs, and incorporates the system temporal behaviour in the Fault Tree thanks to the inclusion of the ESI approach. The incorporation of the system temporal aspects is an advantage compared to other studies using FMEA (Faiella *et al.*, 2018), FTA (Wheeler *et al.*, 2016, Clark *et al.*, 2018), Bayesian Networks (Utne *et al.*, 2020) and STPA (Puisa *et al.*, 2019, Bolbot *et al.*, 2019a, Wróbel *et al.*, 2018, Valdez Banda *et al.*, 2019, Bolbot *et al.*, 2019b). The method incorporates both deductive (STPA, FTA) and inductive (ESI) thinking.

Compared to the STPA, the CASA method included the estimation of the risk and importance metrics, thus supporting a financial resources prioritisation for addressing the system safety enhancement. The importance metrics estimation is an advantage compared to Petri Nets based approaches (Zhang *et al.*, 2019, Wang *et al.*, 2016, Liu *et al.*, 2016). As it was demonstrated, in CASA method more detailed system safety model was developed than STPA based ranking approaches (Puisa *et al.*, 2019, Bolbot *et al.*, 2019a, Wróbel *et al.*, 2018, Valdez Banda *et al.*, 2019), which supports more accurate importance metrics estimation.

Another advantage of the CASA method is the quantification of the impact on the system safety of adding advanced software-based functions, which was not demonstrated in STPA based approaches (Puisa *et al.*, 2019, Wróbel *et al.*, 2018, Valdez Banda *et al.*, 2019, Bolbot *et al.*, 2019b), and only approximated in (Bolbot *et al.*, 2019a, Bolbot *et al.*, 2019b). This is an advantage a number of model-based approaches. For instance, a model based approach used for the Fault Tree development applied to a power system failed to quantify the power reduction functions impact on the system safety (Roskilly, 2016). In this respect, it can be deduced that the quantification of the advanced functionalities impact on the system safety by using FTA is questionable. Potentially, this would be possible by using Bayesian Networks or Petri Nets, and this is a topic for future research.

The fact that the method was successfully implemented for the safety analysis of a non-safety critical ship system as well safety-critical system demonstrates that it can be applied to other safety critical and non-safety critical ICS, ballast water treatment systems, nuclear control systems, industrial power systems, heat, ventilation and air conditioning control system. Forthcoming studies could also investigate if the CASA method is effective for the safety analysis of socio-technical systems and autonomous CPSs.

9.4 Limitations

As with every research, there is a number of limitations to the present research.

The identification of the CPSs related safety properties has been based on the existing literature. Whilst the literature review has been extensive, there is no guarantee that all the safety related properties have been addressed. Furthermore, not all of the existing hazard identification, hazard analysis and safety analysis methods have been reviewed as their overall number is rather overwhelming (more than 800 (Everdij and Blom, 2016)).

The increased CASA accuracy came at a significant cost. The method is not simple and has rather a large number of steps, which indicate that more time is required to apply the method than the STPA or the classical FTA. Its application to DEP system resulted in a huge number of scenarios, which were difficult to handle. This poses for a need to automate the application of the method based on formal models. It should be noted that, the CASA method heavily depends on the expertise of the safety engineer applying the method (as for the other hazard identification methods!). But CASA method is independent from any simulation results or formal system models. The CASA method also proved to be rather labour-intensive when applied to complex system, requiring significant amount of attention to avoid any implementation errors. Potentially this method needs to be enhanced or special training provided before it is used. Concluding, the complex problem was addressed in a complex way rather than in a simple way.

The accidents, hazards and sub hazards are treated independently in the CASA method. This contributes to the amount of resources required for the CASA application. Furthermore, the estimation of risk metric is implemented for each of the accident / hazards independently from the other hazards. The estimated risk metric in CASA is the frequency/failure rate which focuses on the left side of the Bow Tie diagram, excluding potential consequences. No cost-benefit analysis guidelines have been provided in the present study. A more comprehensive decision-making and safety enhancement approach would incorporate the consequences and risk control measures cost in it. However, this implementation would require much more time than allowed in a single PhD.

In this respect it should be noted that the safety analysis was implemented by a single person under close monitoring of his supervisor. Feedback on the results was provided by DNV GL, at relevant conferences and during the articles review process. However, it would be more correct if a team of safety engineers and experts would work together on deriving the scenarios and the Fault Tree structure. This would improve the quality of results. However, this might not be always possible in the real life.

An additional limitation is the use of OREDA and other databases as source of failure rates. This is a well-known constraint on the studies of marine systems. Potentially the results would be worse (less safe) considering the maintenance quality on the ships.

The blackout monitoring system was developed only at its initial stages and it considers only one risk metric. Due to some computational constraints the importance measures estimation has been implemented in Matlab/Simulink only every 24 hours. The considered fault growth curve for components is independent from historical sensors data available for the same components. This limitation could be overcome through closer cooperation with industry and method application on other computational platforms.

These limitations pose directions and suggestions for new research, which are provided in the next Chapter.

9.5 Impact and contribution

This research constitutes a significant contribution to the academia as:

- It offered systematic mapping of the CPSs safety-related properties (Chapter 2). This mapping can be used as basis for other systematic literature review analysis of the CPSs.
- The state of the art and novel safety analysis methods have been analysed for their effectiveness in addressing the safety-related CPSs properties (Chapter 2). This analysis offers directions for improvement of existing research methods.
- A novel method (CASA) has been developed which overcomes the limitations of existing safety analysis methods (Chapter 4). The method can offer ideas on how to overcome the different problems in safety analyse and inspire for even better safety analysis methods.
- A novel methodology for the development of automated safety monitoring system has been demonstrated (Chapter 8). This methodology can support the development of new methodological approaches for automated safety monitoring systems.
- A novel automated safety monitoring system principles and functions have been presented (Chapter 8). These principles can be used to inspire the development of similar monitoring systems for other marine systems.

The implemented research has also significant implications for the industry as:

- The new developed method can be used as a tool for the safety analysis and enhancement of other complex industrial CPSs (Chapter 4).
- The safety analysis results for the investigated systems and the derived safety recommendations presented in Chapters 5, 7 and Section 10.2 can be used to enhance the DEP and open loop scrubber exhaust gas systems design and operation.
- The automated blackout monitoring system can be developed further into a new product for enhanced safety operations. Similar automated safety monitoring systems can be developed for other marine systems as well (Chapter 8).

9.6 Chapter summary

In this Chapter the results of the PhD thesis are discussed. As it was demonstrated a number of research gaps was covered in this research, rendering it a novel contribution. The CASA method main advantage includes its more detailed Fault Tree structure and ability to estimate safety metrics. However, the method proved to be rather labour intensive. In addition, the quality of results and methodology could be improved by obtaining a more detailed feedback from industry. Nevertheless, the contribution of this thesis can be considered in the CASA method, insights gained into marine systems through CASA application and the novel automated blackout monitoring system.

10 CONCLUSIONS

10.1 Chapter outline

In this Chapter the main conclusion of the present thesis, reflections on the achieved objectives as well as suggestions for further research are provided.

10.2 Conclusions and main findings

The main conclusions and findings of the present thesis with respect to the safety of CPSs, the presented method, the investigated systems and the proposed safety monitoring system can be summarised as follows:

With respect to the CPSs safety.

- New systems are being developed which introduce new accident scenarios due to their complexity, which need to be properly addressed (Chapter 1&2).
- The complexity in CPSs can be attributed to a number of their properties, including these systems a) Heterogeneity, b) Interoperability, c) Connectivity, d) Software-intensiveness, e) The presence of humans in the loop, f) Their evolving character g) Ability to reconfigure, h) Autonomous decision making (Chapter 2).
- One of the ways to enhance the CPSs safety is by ensuring the completeness and accuracy of identified scenarios. However, the most popular hazard identification methods have been criticised on how they do support the hazard identification process analysis (Chapter 2).

With respect to the new developed method:

- The developed CASA method guided and resulted in a more accurate safety analysis, compared with previous studies for the similar systems by incorporating the system software failures represented by UCAs and considering the system hazardous states, such as DG sets overloads, etc. (Chapter 5 & 7).
- The method also allowed for the investigation of the system behaviour for cases where new functions are added to the system, as was demonstrated with the pre-warning functions for the DG sets in the investigated reference DEP plant (Chapter 7) and with condition monitoring in open loop scrubber system (Chapter 5).
- The proposed method allowed for the estimation of the safety-related event failure rate with the associated uncertainty and the identification of the most important factors and failures affecting the safety-related event (Chapter 5 and Chapter 7).
- In addition, the developed approach allowed for the investigation of the safety-related event failure rate under different operating modes, considering the number of connected DG sets and changes in the DG sets loading profile (Chapter 7).

- The proposed approach proved to be tedious, resulting in a quite substantial number of UCAs, process variables, causal factors, and branches in "Event Trees" for complex system such as reference DEP system. The integration of methods also required specific attention to avoid any issues and errors during the Fault Tree refinement and integration phase (Chapters 7 and 9).

With respect to the investigated application case studies:

- Use of more than one SOx sensors or their condition monitoring can significantly reduce the non-compliance cases for SOx scrubber system (Chapter 5).
- The estimated blackout frequency for the investigated cruise ship power plant was estimated to be around 0.4 events per ship-year, whilst the estimated blackout frequency varies in different operating modes from 0.003 events per ship-year in the sailing mode to 1.5 per ship-year in the harbour mode (Chapter 7).
- The DG set loading conditions and the number of DG sets connected to the ship electric network have significant influence on the blackout failure rate, and therefore the blackout frequency can be reduced by controlling them (Chapter 7).
- It was found that the reliable operation of the PMS fast electrical load reduction, the prewarning and reconfiguration functions is important for avoiding a blackout event (Chapter 7).
- When a number of DG sets operate, failures in the components used for the electrical power generation control, such as the DG sets fuel racks, the electric power sensors or/and the propulsion motors load reduction functions become more important. The mechanical components failures, such as lubrication oil or cooling water system failures become more important in cases where a small number of DG sets operates. Failures leading to simultaneous loss of multiple DG sets are also important from blackout perspective when a smaller DG set number operates (Chapter 7).
- The number of hazardous scenarios leading to blackout increases in HEP system due to higher system complexity (Chapter 7).
- The blackout frequency in the system with batteries is significantly reduced when three or less DG sets are connected to the network as batteries are acting as an additional barrier to DG set overload leading to a blackout, allowing quick system reconfiguration without consumers' power reduction. This leads to a lower blackout susceptibility in the HEP system than in the conventional DEP system (Chapter 7).
- Slight improvements of the blackout frequency and failure in power plant configurations with DF engines, can be attributed to the addition of another fuel system, leading to increased redundancy in fuel supply (Chapter 7).

- Increase in DG set number does not necessary results in reduced blackout frequency, as other parameters are also important for the cruise ship safety. Therefore, systems with lower redundancy can have similar safety level depending on the safety metric (Chapter 7).

With respect to the developed automated blackout monitoring system and the reference DEP system:

- The developed blackout monitoring system provides high-level functional alarm for a cruise ship power system based on the current system operating conditions and operational status. It also has the potential to improve the organisation of the alarms/components failures to reflect their present importance in the DEP system (Chapter 8).
- The developed blackout monitoring system was able to assess the importance of different failures based on the present configuration and load conditions (Chapter 8).
- Specific operational parameters as the DG sets load and the number of connected DG sets need be used as input into the blackout monitoring system, as it influences the blackout probability (Chapter 8).
- An operation with a single DG set increases the PoB above the suggested threshold of 0.1 blackout per year. The PoB when propulsion motors are disconnected but bow thrusters are operating is also higher than threshold (Chapter 8).
- Failures in operating components can increase the PoB also above the desired threshold, however their importance is varying in time dependent on the system other parameters (Chapter 8).

10.3 Suggestions for future research

Based on the present research main findings and limitations, the following recommendations for future research are provided:

- Further improvement of the available hazard identification methods and usage of advanced hazard identification techniques to ensure the completeness of the identified accident scenarios.
- Automation of STPA based on a formal system representation in similar way with FLSA methods for technical systems.
- Investigation on the proposed CASA method automation based on formal models and formal system representation.
- Application of the CASA method to case studies other than open-loop exhaust gas scrubber system or DEP system blackout event could be examined.
- Easy integration of different accidents / hazards in CASA results could be pursued.
- Other undesired events could be also considered for the analysis for the same system using the same methodology including the events of partial blackouts, propulsion load reduction, electric

shock to the crew or passengers, insufficient propulsion, inability to cover the electric hotel load, etc.

- The comparison of fire and overall risk between the standard DEP system and DEP system with batteries could be pursued.
- Cost-benefit assessment for the different suggested safety improving solutions.
- Integration with diagnostic and prognostic measurements of the automated safety monitoring system could be pursued.
- It would be nice to validate the automated safety monitoring system concept using actual sensor measurements on a ship.

10.4 Review of research objectives

In this section it is discussed how effectively the research objective have been covered in this PhD thesis.

Objective 1: *To investigate and critically review the challenges with related to the CPSs safety and how the hazard identification methods address them.*

This objective was covered in in Chapters 2 and 3. A list of safety-related sources of complexity in the CPSs was identified based on the literature review. This list made simpler the critical review of hazard identification and analysis methods with respect to their application to the CPSs. There is a limitation in the number of investigated research studies and methods. However, this is a common limitation to every research study. Therefore, this objective can be considered as fulfilled.

Objective 2: *To propose and develop a novel safety analysis method by addressing gaps in existing methods.*

This objective was addressed primary in Chapter 4. The literature review guided in the identification of specific hazard analysis methods limitations and gaps in Chapter 2 and 0. These gaps and limitations were used to suggest the combination of existing methods for the development of novel method in Chapter 0. The novel method steps were presented and elaborated in Chapter 4. The method can be considered as complex, but also results in a Fault Tree of greater accuracy. Therefore, this objective can be also considered as fulfilled.

Objective 3: *To demonstrate the effectiveness of the developed novel safety analysis method by applying it to modern marine CPSs.*

This objective was addressed in Chapters 5, 6 and 7. The method was applied to the exhaust gas open-loop scrubber system and to a number of cruise ship power plants. Based on the analysis results, it could be observed that expected method effectiveness is improved compared to other used safety analysis methods. A number of novel method limitations has been also identified thanks to the application case studies. There is a limitation with respected to quality of results, as limited number of experts were involved in analysis process. However, it is not always possible to involve many safety engineers due to high human cost. Therefore, this objective can be also considered with some limitations as fulfilled.

Objective 4: *To develop an automated blackout monitoring system supporting decision-making during a marine CPS operation based on the new method results and recent CPSs developments with application to the DEP system.*

This objective was covered in Chapter 8. The main principles and functions were provided for the automated blackout monitoring system. The selected monitored parameters were also provided. The system simplifies the system monitoring to one metric and to critical components. Still there is a need to develop this system further by increasing its TRL and incorporating more information in the analysis as discussed in Section 8.6. Yet, this would require a significant amount of resources resulting in another or several other PhDs. Therefore, this objective can be considered as justifiably partially fulfilled.

Objective 5: *To summarise the main findings, conclusions, and contribution of this research and to propose new directions for further research.*

This objective was addressed in Chapter 9 and 10. The main findings and contributions were summarised using bullet points. Based on the study limitations suggestions for further research were provided. Therefore, this objective can be also considered as fulfilled.

Concluding, it can be noted that the overall aim of finding simplicity in complexity is only partially satisfied. The safety related CPSs properties were identified supporting the CPSs safety methods enhancement. The developed method combines the simple thinking of deducting and inductive processes. Yet, the method constitutes of many steps and its application to complex system resulted in a number of scenarios, which are difficult to handle.

The potential body for research in marine CPSs seems to be unlimited and new methods, design, operational solutions enhancing safety of CPSs can be realised. That's why I would like to conclude my thesis by a famous quote from Isaac Newton: "I do not know what I may appear to the world, but to myself I seem to have been only like a boy playing on the seashore, and diverting myself in now and then finding a smoother pebble or a prettier shell than ordinary, whilst the great ocean of truth lay all undiscovered before me".

10.5 Chapter summary

In this chapter the main conclusions, reflections and recommendations for future research based on this thesis results were provided. Whilst the developed method seems to offer more comprehensive scenarios identification, there is a need to develop it further to allow automated method application. Integration of automated blackout monitoring system with condition-based monitoring data is also required. This poses directions for further research.

This page has been intentionally left blank

REFERENCES

ABB (2005) 'Reliability calculation in accordance with RDF93 model from CNET'. Available at: http://www.5scomponents.com/pdf//CS-range-MTBF-1-0.pdf (Accessed: 08/08/2018).

ABB (2010) *ABB life expectancy analysis program (ABB LEAP) for stator windings of high voltage rotating machines.* Available at: https://library.e.abb.com/public/4c0c0063b5426efdc1257b2f003d522d/ABB_brochure_LEAP_low%20res1.pdf (Accessed: 25/04/2020).

ABB (2011a) *Marine services maintenance optimization through condition monitoring.* Available at: https://library.e.abb.com/public/2b7743e51a114f7bc1257b23004aa37d/Condition%20Monitoring.pdf (Accessed: 03/12/2019).

ABB (2011b) *Propulsion product services - azipod condition monitoring retrofit.* Available at: https://library.e.abb.com/public/b91bdf24f4d54253c1257850002e7148/15333%20Azipod%20Condition%20Monitoring%20Retrofit_lowres_2.3.pdf (Accessed: 03/12/2019).

ABB (2012) *Condition monitoring solutions for motors and generators - Enabling the right maintenance at the right time.* Available at: https://library.e.abb.com/public/6b2d254d287d8d96c1257b2f003d8db2/Condition%20monitoring_LR.pdf (Accessed: 03/12/2019).

Abdulkhaleq, A. and Wagner, S. (2013) Published. 'Integrating state machine analysis with System-Theoretic Process Analysis'. *Gesellschaft fur Informatik,* 2013 Koblenz, Germany. pp.501-514.

Abdulkhaleq, A. and Wagner, S. (2015) 'A controlled experiment for the empirical evaluation of safety analysis techniques for safety-critical software'. *Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering.* Nanjing, China, ACM.

Abdulkhaleq, A. and Wagner, S. (2016) 'XSTAMPP 2.0: new improvements to XSTAMPP Including CAST accident analysis and an extended approach to STPA'. *5th STAMP Workshop.* United Kingdom, Cambridge, Available at: http://dx.doi.org/10.18419/opus-8749.

Abdulkhaleq, A., Wagner, S. and Leveson, N. (2015) 'A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA'. *Procedia Engineering,* 128 2-11.

Adler, R., Domis, D., Höfig, K., Kemmann, S., Kuhn, T., Schwinn, J.-P. and Trapp, M. (2010) Published. 'Integration of component fault trees into the UML'. *International Conference on Model Driven Engineering Languages and Systems,* 2010 Oslo, Norway. Springer, pp.312-327.

Ådnanes, A.K. (2003) *Maritime electrical installations and diesel electric propulsion.* Norway, Oslo: ABB.

AIBN (Accident Investigation Board Norway) (2019) 'Interim report on the investigation into the loss of propulsion and near grounding of Viking Sky'. Available at: https://www.iims.org.uk/wp-content/uploads/2019/11/AIBN-Interim-report-12-November-on-the-investigation-into-the-loss-of-propulsion-and-near-grounding-of-viking-sky.pdf (Accessed: 01/12/2019).

Aizpurua, J.I., Catterson, V.M., Papadopoulos, Y., Chiacchio, F. and D'Urso, D. (2017a) 'Supporting group maintenance through prognostics-enhanced dynamic dependability prediction'. *Reliability Engineering & System Safety,* 168 171-188.

Aizpurua, J.I., Catterson, V.M., Papadopoulos, Y., Chiacchio, F. and Manno, G. (2017b) 'Improved Dynamic Dependability Assessment Through Integration With Prognostics'. *IEEE Transactions on Reliability,* 66 (3), pp. 893-913.

Aizpurua, J.I., Stewart, B.G., McArthur, S.D., Jajware, N. and Kearns, M. (2019) 'Towards a hybrid power cable health index for medium voltage power cable condition monitoring'. *37th IEEE Electrical Insulation Conference.* Calgary, Canada.

Aldemir, T., Stovsky, M., Kirschenbaum, J., Mandelli, D., Bucci, P., Mangan, L., Miller, D., Sun, X., Ekici, E. and Guarro, S. (2007) 'Dynamic reliability modeling of digital instrumentation and control systems for nuclear reactor probabilistic risk assessments'. Available at: https://www.nrc.gov/docs/ML0730/ML073030092.pdf (Accessed: 26/03/2018).

Alemzadeh, H. (2016) *Data-driven resiliency assessment of medical cyber-physical systems.* Ph.D. Thesis. University of Illinois at Urbana-Champaign.

Alfa Laval (2017a) '*Maintenance manual'*.

Alfa Laval (2017b) '*PureSOx Design Guide'*.

Allal, A.A., Mansouri, K., Youssfi, M. and Qbadu, M. (2017) 'Toward a reliable sea water central cooling system for a safe operation of autonomous ship'. *International Conference on Recent Innovation in Engineering and Technology.* Berlin, Germany.

Allen, C., Alston, G., Angerer, O., Barr, S., Barrett, J., Barth, T., Battiston, R., Beard, B.L., Begault, D.R., Benson, E., Bertels, C., Bertrand, R., Bjorvatn, B., Calvelli, V., Canepa, G., Dillinger, T., Dischinger, H.C.J., Dittemore, G., Dorneich, M.C., England, S., Watts-Englert, J., Ferrante, M., Fodroci, M., Garbino, A., Giraudo, M., Gohmert, D., Goodman, J., Gore, B.F., Groen, E., Grohmann, E. and Grosveld, F.W. (2018) *Space Safety and Human Performance.* United Kingdom, Oxford: Elsevier Ltd.

Anantharaman, M., Khan, F., Garaniya, V. and Lewarn, B. (2015) 'Reliability of Fuel Oil System Components Versus Main Propulsion Engine: An Impact Assessment Study'. *Safety of Marine Transport: Marine Navigation and Safety of Sea Transportation,* 175.

Andersen, M.L. (2015) *Formal Safety Assessment of an Open Loop System.* Master Thesis Norwegian University of Science and Technology.

Aquilino, J.W. (1983) 'Report of transformer reliability survey-industrial plants and commercial buildings'. *IEEE transactions on industry applications,* IA-19 (5), pp. 858-866.

Arcidiacono, G. and Campatelli, G. (2004) 'Reliability improvement of a diesel engine using the FMETA approach'. *Quality and Reliability Engineering International,* 20 (2), pp. 143-154.

Asare, P., Lach, J. and Stankovic, J.A. (2013) Published. 'FSTPA-I: A formal approach to hazard identification via system theoretic process analysis'. *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems,* 2013. ACM, pp.150-159.

Axelrod, C.W. (2013) 'Managing the risks of cyber-physical systems'. *IEEE Long Island Systems, Applications and Technology Conference (LISAT).* New York, United States.

Aziz, A., Ahmed, S., Khan, F., Stack, C. and Lind, A. (2019) 'Operational risk assessment model for marine vessels'. *Reliability Engineering & System Safety,* 185 348-361.

Bagade, P., Banerjee, A. and Gupta, S.K.S. (2017) 'Validation, verification, and formal methods for Cyber-Physical Systems*'*. In*:* Rawat, D.B., Jeschke, S. and Brecher, C. (eds.) *Cyber-Physical Systems.* Boston: Academic Press, pp. 175-191.

Baier, C. and Katoen, J.-P. (2008) *Principles of model checking.* Cambridge, Massachusets: MIT press.

Banerjee, A., Venkatasubramanian, K.K., Mukherjee, T. and Gupta, S.K.S. (2012) 'Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems'. *Proceedings of the IEEE,* 100 (1), pp. 283-299.

Baumgart, S., Froberg, J. and Punnekkat, S. (2018) Published. 'Can STPA be used for a System-of-Systems? Experiences from an Automated Quarry Site'. *2018 IEEE International Systems Engineering Symposium (ISSE),* 2018. IEEE, pp.1-8.

Becker, C. and Van Eikema Hommes, Q. (2014) 'Transportation systems safety hazard analysis tool (SafetyHAT) user guide (version 1.0)'. Available at: https://rosap.ntl.bts.gov/view/dot/12034 (Accessed: 01/08/2018).

Becker, U. (2018) 'STPA Guided Systems Engineering'. *International Conference on Computer Safety, Reliability, and Security.* Västerås, Sweden, Springer.

Berghmans, F., Eve, S. and Held, M. (2008) 'An introduction to reliability of optical components and fiber optic sensors*'*. *Optical Waveguide Sensing and Imaging.* Springer, pp. 73-100.

Bjerga, T., Aven, T. and Zio, E. (2016) 'Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM'. *Reliability Engineering & System Safety,* 156 203-209.

Blandine, A. (2013) *System theoretic hazard analysis applied to the risk review of complex systems: an example from the medical device industry. PhD Thesis.* Doctor of Philosophy Massachusetts Institute of Technology.

Bliznakov, Z., Mitalas, G. and Pallikarakis, N. (2007) 'Analysis and Classification of Medical Device Recalls'. *World Congress on Medical Physics and Biomedical Engineering 2006.* Berlin, Heidelberg, Springer Berlin Heidelberg.

Bloch, H.P. and Geitner, F.K. (2012) *Machinery failure analysis and troubleshooting: practical machinery management for process plants.* Oxford, United Kingdom: Butterworth-Heinemann.

Bohatyrewicz, P., Płowucha, J. and Subocz, J. (2019) 'Condition Assessment of Power Transformers Based on Health Index Value'. *Applied Sciences,* 9 (22), pp. 4877.

Bolbot, V., Puisa, R., Theotokatos, G., Boulougouris, E. and Vassalos, D. (2019a) 'A comparative safety assessment for DC and DC with hybrid power systems in a windfarm SOV using STPA'. *European STAMP Workshop & Conference.* Helsinki, Finland.

Bolbot, V., Theotokatos, G., Boulougouris, E. and Vassalos, D. (2019b) 'Comparison of diesel-electric with hybrid-electric propulsion system safety using System-Theoretic Process Analysis'. *Propulsion and Power Alternatives.* London, United Kingdom, Royal Institute of Naval Architects.

Bolbot, V., Trivyza, N.L., Theotokatos, G., Boulougouris, E., Rentizelas, A. and Vassalos, D. (2020) 'Cruise ships power plant optimisation and comparative analysis'. *Energy,* 196 (MOSES special issue), pp. 117061.

Bouissou, M. and Bon, J.-L. (2003) 'A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes'. *Reliability Engineering & System Safety,* 82 (2), pp. 149-163.

British Standards Institution (BSI) (2004) '*Functional safety - Safety instrumented systems for the process industry sector -IEC-61511'. Part 3: Guidance for determination of the required safety integrity levels.* London, United Kingdom: British Standards Instituition.

BSI (2006) '*Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) EN 60812'.* London, United Kingdom: British Standards Instituition.

Buede, D.M. and Miller, W.D. (2016) *The engineering design of systems: models and methods.* John Wiley & Sons.

Bujorianu, M.L. and Piterman, N. (2015) 'A Modelling Framework for Cyber-Physical System Resilience'. In*:* Mousavi, M.R. and Berger, C. (eds.) *Cyber Physical Systems. Design, Modeling, and Evaluation: 5th International Workshop, CyPhy 2015, Amsterdam, The Netherlands, October 8, 2015, Proceedings.* Cham: Springer International Publishing, pp. 67-82.

Bukša, A., Šegulja, I. and Tomas, V. (2009) 'Ship Machinery Maintenance Concept Adjustment and Design'. *Strojarstvo: časopis za teoriju i praksu u strojarstvu,* 51 (3), pp. 227-238.

Bures, T., Weyns, D., Berger, C., Biffl, S., Daun, M., Gabor, T., Garlan, D., Gerostathopoulos, I., Julien, C., Krikava, F., Mordinyi, R. and Pronios, N. (2015) 'Software Engineering for Smart Cyber-Physical Systems -- Towards a Research Agenda: Report on the First International Workshop on Software Engineering for Smart CPS'. *SIGSOFT Softw. Eng. Notes,* 40 (6), pp. 28-32.

Chai, M., Reddy, D.B., Sobrayen, L., Panda, K.S., Die, W. and Xiaoqing, C. (2016) Published. 'Improvement in efficiency and reliability for diesel- electric propulsion based marine vessels using genetic algorithm'. *2016 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific),* 1-4 June 2016 2016. pp.180-184.

Chang, D., Rhee, T., Nam, K., Chang, K., Lee, D. and Jeong, S. (2008) 'A study on availability and safety of new propulsion systems for LNG carriers'. *Reliability Engineering & System Safety,* 93 (12), pp. 1877-1885.

Chen, M., Wang, L., Hu, J. and Feng, T. (2018) Published. 'An Extraction Method of STPA Variable Based on Four-Variable Model'. *International Conference on Intelligent and Interactive Systems and Applications,* 2018. Springer, pp.375-381.

Chybowski, L. (2002) 'Auxiliary installations' fault tree model for operation analysis of vessel's power plant unit'. *Балттехмаш-2002, KGTU Kaliningrad, Czerwiec,* 299-301.

Chybowski, L., Idziaszczyk, D. and Wiśnicki, B. (2014) 'A comparative components importance analysis of a complex technical system with the use of different importance measures'. *Systemy Wspomagania w Inżynierii Produkcji,* (1 (7)), pp. 23--33.

Clark, A.J., Williams, A.D., Muna, A. and Gibson, M. (2018) 'Hazard and Consequence Analysis for Digital Systems–A New Approach to Risk Analysis in the Digital Era for Nuclear Power Plants'. *Transactions of the American Nuclear Society.* Orlando Florida.

Corvus-Energy (2019) *FAQ-Frequently Asked Questions.* Available at: https://corvusenergy.com/faq-frequently-asked-question/ (Accessed: 05-04-2019).

Cruise Lines International Association (CLIA) (2016) '2017 cruise industry outlook'. Available at: https://www.cruising.org/docs/default-source/research/clia-2017-state-of-the-industry.pdf?sfvrsn=0 (Accessed: 01/12/2017).

Dakwat, A.L. and Villani, E. (2018) 'System safety assessment based on STPA and model checking'. *Safety Science,* 109 130-143.

Dawson, L.A., Muna, A.B., Wheeler, T.A., Turner, P.L., Wyss, G.D. and Gibson, M.E. (2015) 'Assessment of the Utility and Efficacy of Hazard Analysis Methods for the Prioritization of Critical Digital Assets for Nuclear Power Cyber Security'. Available at: https://www.osti.gov/servlets/purl/1252915 (Accessed: 01/12/2017).

Delange, J., Pautet, L. and Feiler, P.H. (2009) 'Validating safety and security requirements for partitioned architectures'. *Reliable Software Technologies.* Ada-Europe, Lecture Notes in Computer Science, vol 5570, Springer.

Denson, W., Chandler, G., Crowell, W., Clark, A. and Jaworski, P. (1994) *Nonelectronic parts reliability data 1995.* Rome, NY, United States: Ft. Belvoir Defense Technical Information Cente.

Dimakopoulos, I., Menegakis, P., Lampris, N., Gkinis, S. and Panagoulias, G. (2017) 'Replacement of a Diesel Generator with a containerised battery system on-board a containership'. *Power and Propulsion Alternatives for Ships.* Rotterdam, Netherlands, The Royal Institution of Naval Architects.

DNV GL (2015) 'Technology outlook 2025'.

DNV GL (2016) 'Guidance for safe return to port projects'. Available at: https://rules.dnvgl.com/docs/pdf/DNVGL/CG/2016-04/DNVGL-CG-0004.pdf (Accessed: 01/06/2017).

DNV GL (2017) '*Rules for classification'. In:* DNV GL (ed.) *Part 4 Chapter 3 Section 1.* DNV GL AS.

Dogramadzi, S., Giannaccini, M.E., Harper, C., Sobhani, M., Woodman, R. and Choung, J. (2014) 'Environmental hazard analysis-a variant of preliminary hazard analysis for autonomous mobile robots'. *Journal of Intelligent & Robotic Systems,* 76 (1), pp. 73-117.

Dokas, I.M., Feehan, J. and Imran, S. (2013) 'EWaSAP: An early warning sign identification approach based on a systemic hazard analysis'. *Safety Science,* 58 11-26.

Dolas, D.R. and Deshmukh, S. (2015) 'Reliability Ananlysis of Cooling System of Diesel Engine'. *Universal Journal of Mechanical Engineering,* 3 (2), pp. 57-62.

Dubey, A., Santoso, S. and Arapostathis, A. (2015) 'Reliability analysis of three-dimensional shipboard electrical power distribution systems'. *2015 IEEE Electric Ship Technologies Symposium (ESTS).* Washington DC, USA.

Durga Rao, K., Kushwaha, H.S., Verma, A.K. and Srividya, A. (2007) 'Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies'. *Reliability Engineering & System Safety,* 92 (7), pp. 947-956.

EARTO (2014) 'The TRL Scale as a Research & Innovation Policy Tool, EARTO Recommendations'. Available at: https://www.earto.eu/wp-content/uploads/The_TRL_Scale_as_a_R_I_Policy_Tool_-_EARTO_Recommendations_-_Final.pdf (Accessed: 01/12/2019).

Electropaedia (2019) *Battery Reliability and How to Improve it.* Available at: https://www.mpoweruk.com/reliability.htm (Accessed: 01/04/2019).

Elks, C.R. (2012) 'Development of a fault injection-based dependability assessment methodology for digital and I & C systems'. Available at: https://www.nrc.gov/docs/ML1300/ML13003A015.pdf (Accessed: 01/02/2018).

Eloranta, S. and Whitehead, A. (2016) 'Safety aspects of autonomous ships'. *6th International Maritime Conference.* Germany, Hamburg.

Engell, S., Paulen, R., Reniers, M.A., Sonntag, C. and Thompson, H. (2015) Published. 'Core research and innovation areas in cyber-physical systems of systems'. *Cyber Physical Systems. Design, Modelling, and Evaluation,* 2015 Netherlands, Amsterdam. Lecture Notes in Computer Science, vol 9361, Springer, pp.40-55.

European Space Agency (ESA) (2009) 'Technology readiness levels handbook for space applications'. Available at: https://artes.esa.int/sites/default/files/TRL_Handbook.pdf (Accessed: 01/02/2020).

Everdij, M.H.C. and Blom, H.A.P. (2016) 'Safety methods database'. Available at: https://www.nlr.nl/downloads/safety-methods-database.pdf (Accessed: 01/11/2017).

Faiella, G., Parand, A., Franklin, B.D., Chana, P., Cesarelli, M., Stanton, N.A. and Sevdalis, N. (2018) 'Expanding healthcare failure mode and effect analysis: A composite proactive risk analysis approach'. *Reliability Engineering & System Safety,* 169 (Supplement C), pp. 117-126.

Federal Office for Information Security (2014) 'The IT security in Germany 2014'. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile/ (Accessed: 01/01/2018).

Flaus, J.-M. (2019) *Cybersecurity of industrial systems.* London, United Kingdom: ISTE Ltd.

Fleming, C.H. (2015) *Safety-driven Early Concept Analysis and Development.* Citeseer.

Fricks, R.M. and Trivedi, K.S. (2003) Published. 'Importance analysis with Markov chains'. *Annual Reliability and Maintainability Symposium* 27-30 Jan. 2003 2003. pp.89-95.

Friis-Hansen, P., Ravn, E. and Engberg, P. (2008) 'Basic modelling principles for prediction of collision and grounding frequencies'. *IWRAP Mark II Working Document,* 1-59.

Gamble, C., Pierce, K., Fitzgerald, J. and Bos, B. (2014) 'Co-modelling of faults and fault tolerance mechanisms'. In: Fitzgerald, J., Larsen, P.G. and Verhoef, M. (eds.) *Collaborative Design for Embedded Systems: Co-modelling and Co-simulation.* Berlin, Heidelberg: Springer, pp. 185-197.

Garyfallos, I. (2016) *Reliability and criticality assesssment of four-stroke dual-fuel engine. Master Thesis.* Master of Engineering The University of Strathclyde.

Geertsma, R.D., Negenborn, R.R., Visser, K. and Hopman, J.J. (2017) 'Design and control of hybrid power and propulsion systems for smart ships: A review of developments'. *Applied Energy,* 194 30-54.

Ghosh, S., Lincoln, P., Tiwari, A., Zhu, X. and EDU, W. (2016) 'Trusted Machine Learning for Probabilistic Models'. *Reliable Machine Learning in the Wild at ICML*.

Glomsrud, J.A. and Xie, J. (2019) 'A Structured STPA Safety and Security Co-analysis Framework for Autonomous Ships'. *European Safety and Reliability conference.* Germany, Hannover.

Glossop, M., Loannides, A. and Gould, J. (2000) 'Review of hazard identification techniques'. Available at: https://www.hse.gov.uk/research/hsl_pdf/2005/hsl0558.pdf (Accessed: 01/02/2019).

Goebel, K., Daigle, M., Saxena, A., Sankararaman, S., Roychoudhury, I. and Celaya, J.R. (2017) *Prognostics The science of prediction.* USA: Create Space Independent Publishing Platform.

Goerlandt, F., Khakzad, N. and Reniers, G. (2016) 'Validity and validation of safety-related quantitative risk analysis: A review'. *Safety Science,* 99 (November), pp. 127-139.

Gomes, J.P.P., Rodrigues, L.R., Galvão, R.K.H. and Yoneyama, T. (2013) Published. 'System level RUL estimation for multiple-component systems'. *Proceedings of the 2013 Annual conference of the prognostics and health management society,* 2013. pp.74-82.

Gomez, C. (1996) 'Importance measures'. *Workshop on "PSA Applications".* Sofia, Bulgaria, Available at: https://inis.iaea.org/collection/NCLCollectionStore/_Public/28/059/28059559.pdf (Accessed: 01/03/2018).

Guillén, A., Crespo, A., Macchi, M. and Gómez, J. (2016) 'On the role of Prognostics and Health Management in advanced maintenance systems'. *Production Planning & Control,* 27 (12), pp. 991-1004.

Guiochet, J. (2016) 'Hazard analysis of human–robot interactions with HAZOP–UML'. *Safety science,* 84 225-237.

Guiochet, J., Machin, M. and Waeselynck, H. (2017) 'Safety-critical advanced robots: A survey'. *Robotics and Autonomous Systems,* 94 43-52.

Gunes, V., Peter, S., Givargis, T. and Vahid, F. (2014) 'A survey on concepts, applications, and challenges in cyber-physical systems'. *KSII Transactions on internet and information systems,* 8 (12), pp. 4242-4268.

Gurgel, D.L., Hirata, C.M. and Bezerra, J.d.M. (2015) Published. 'A rule-based approach for safety analysis using STAMP/STPA'. *IEEE/AIAA 34th Digital Avionics Systems Conference (DASC),* 2015. pp.7B2-1-7B2-8.

Hafver, A., Pedersen, F.B., Jakopanec, I., Oliveira, L., Domingues, J., Eldevik, S. and Lindberg, D.V. (2017) 'Dynamic risk management for enhanced safety'. Available at: https://www.dnvgl.com/oilgas/download/position-paper-maintaining-confidence-dynamic-risk-management-for-enhanced-safety.html (Accessed: 01/03/2017).

Hamann, R., Papanikolaou, A., Eliopoulou, E. and Golyshev, P. (2013) 'Assessment of safety performance of container ships'. *Proceedings of the IDFS,* 18-26.

Han, X., Tang, T. and Lv, J. (2019) 'A hierarchical verification approach to verify complex safety control systems based on STAMP'. *Science of Computer Programming,* 172 117-134.

Hehenberger, P., Vogel-Heuser, B., Bradley, D., Eynard, B., Tomiyama, T. and Achiche, S. (2016) 'Design, modelling, simulation and integration of cyber physical systems: Methods and applications'. *Computers in Industry,* 82 273-289.

Hetherington, C., Flin, R. and Mearns, K. (2006) 'Safety in shipping: The human element'. *Journal of Safety Research,* 37 (4), pp. 401-411.

Hollnagel, E. (2012) *FRAM, the functional resonance analysis method: modelling complex socio-technical systems.* Surrey, England: Ashgate Publishing Ltd.

Hossain, M.A., Kelly, S.J., Ahmed, M.F. and Roa, M.J. (2013) Published. 'Cause and effect of catastrophic failure of shipboard and offshore vessel/platform power sources'. *Petroleum and Chemical Industry Technical Conference (PCIC), 2013 Record of Conference Papers Industry Applications Society 60th Annual IEEE,* 2013. IEEE, pp.1-8.

Hu, J., Zhang, L., Ma, L. and Liang, W. (2010) 'An integrated method for safety pre-warning of complex system'. *Safety Science,* 48 (5), pp. 580-597.

Hu, J., Zhang, L., Ma, L. and Liang, W. (2011) 'An integrated safety prognosis model for complex system based on dynamic Bayesian network and ant colony algorithm'. *Expert Systems with Applications,* 38 (3), pp. 1431-1446.

Huang, X., Kwiatkowska, M., Wang, S. and Wu, M. (2017) 'Safety verification of deep neural networks'. *Computer Aided Verification 2017.* Heidelberg, Germany, Lecture Notes in Computer Science, vol 10426, Springer

Hulin, B. and Tschachtli, R. (2011) Published. 'Identifying software hazards with a modified CHAZOP'. *PESARO 2011 First Int. Conf. Performance, Saf. Robustness Complex Syst. Appl,* 2011. pp.7-12.

IATA (International Air Transport Association) (2018) 'IATA Safety report 2017'. Available at: https://aviation-safety.net/airlinesafety/industry/reports/IATA-safety-report-2017.pdf (Accessed: 01/02/2019).

IMO (2008) 'Formal Safety Assessment - Cruise ships - MSC 85/INF.2'. Available at: http://www.safedor.org/resources/MSC_85-INF-2.pdf (Accessed: 01/10/2017).

IMO (2018) 'Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process'. Available at: http://research.dnv.com/skj/IMO/MSC-MEPC%202_Circ%2012%20FSA%20Guidelines%20Rev%20III.pdf (Accessed: 01/06/2019).

INCOSE (2015) *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities.* Fourth Edition edn. USA, New Jersey: John Wiley & Sons, Inc., Hoboken.

International Agency for Research on Cancer (2012) 'IARC: Diesel engine exhaust carcinogenic'. *Press release,* 213.

Ishimatsu, T., Leveson, N.G., Thomas, J., Katahira, M., Miyamoto, Y. and Nakao, H. (2010) 'Modeling and hazard analysis using STPA'. *Fourth IAASS conference.* USA, Alabama.

ISO (2009) '*Risk management — Risk assessment techniques'*. *ISO 31010.* Switzerland, Geneva: International Organization for Standardization.

ISO (2010) '*Functional safety of electrical/electronic/programmable electronic safety-related systems - IEC 61508'*. *Part 1: General requirements.* United Kingdom, London: British Standard Institution.

ISO (2011) '*ISO 26262: Road vehicles — Functional safety'*. *Part 1: Vocabulary.* United Kingdom, London: British Standard Industries.

ISO (2018) '*Risk management - Guidelines - ISO 31000'*. United Kingdom, London: British Standards Institution.

Jaskolka, J. and Villasenor, J. (2017) Published. 'Identifying Implicit Component Interactions in Distributed Cyber-Physical Systems'. *Proceedings of the 50th Hawaii International Conference on System Sciences,* 2017.

Jeong, B., Oguz, E., Wang, H. and Zhou, P. (2018) 'Multi-criteria decision-making for marine propulsion: Hybrid, diesel electric and diesel mechanical systems from cost-environment-risk perspectives'. *Applied Energy,* 230 1065-1081.

Jin, X., Wang, C., Chen, C., Cheng, T. and Amancio, A. (1999) Published. 'Reliability analyses and calculations for distribution transformers'. *Transmission and Distribution Conference, 1999 IEEE,* 1999. IEEE, pp.901-906.

Johansen, I.L. and Rausand, M. (2014a) 'Defining complexity for risk assessment of sociotechnical systems: A conceptual framework'. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* 228 (3), pp. 272-290.

Johansen, I.L. and Rausand, M. (2014b) 'Foundations and choice of risk metrics'. *Safety Science,* 62 (Supplement C), pp. 386-399.

Jokioinen, E., Pokonen, J., Hyv ö nen, M., Kolu, A., Jokela, T., Tissari, J., Paasio, A., Ringbom, H., Collin, F., Viljanen, M., Jalonen, R., Tuominen, R., Wahlstr ö m, M., Saarni, J., Nordbelg-Davies, S. and Makkonen, H. (2016) 'Remote and autonomous ships The next steps'. Available at: http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf (Accessed: 01/06/2017).

Joshi, A., Whalen, M. and Heimdal, M.P.E. (2006) 'Model-Based Safety Analysis final report'. Available at: https://shemesh.larc.nasa.gov/fm/papers/Model-BasedSafetyAnalysis.pdf (Accessed: 01/08/2017).

Jürgensen, J.H., Godin, A.S. and Hilber, P. (2017) 'Health index as condition estimator for power system equipment: a critical discussion and case study'. *CIRED-Open Access Proceedings Journal,* 2017 (1), pp. 202-205.

Kabir, S., Walker, M., Papadopoulos, Y., Rüde, E. and Securius, P. (2016) 'Fuzzy temporal fault tree analysis of dynamic systems'. *International Journal of Approximate Reasoning,* 77 20-37.

Kaplan, S. and Garrick, B.J. (1981) 'On the quantitative definition of risk'. *Risk analysis,* 1 (1), pp. 11-27.

Karakitsos, I. and Theotokatos, G. (2016) Published. 'Modelling of diesel electric propulsion'. *Energy Efficient Ships,* 2016 United Kingdom, London. The Royal Institution of Naval Architects.

Kevin Anthony, H. and Masooda, B. (2014) 'Trust in automation: integrating empirical evidence on factors that influence trust'. *Human Factors,* 57 (3), pp. 407-434.

Khan, F.I. and Abbasi, S.A. (1998) 'Techniques and methodologies for risk analysis in chemical process industries'. *Journal of Loss Prevention in the Process Industries,* 11 (4), pp. 261-277.

Kim, H., Lee, S.-H., Park, J.-S., Kim, H., Chang, Y.-S. and Heo, G. (2015) 'Reliability data update using condition monitoring and prognostics in probabilistic safety assessment'. *Nuclear Engineering and Technology,* 47 (2), pp. 204-211.

Kim, K.D. and Kumar, P.R. (2012) 'Cyber–Physical Systems: a perspective at the centennial'. *Proceedings of the IEEE,* 100 (Special Centennial Issue), pp. 1287-1308.

Knegtering, B. and Pasman, H. (2013) 'The safety barometer: How safe is my plant today? Is instantaneously measuring safety level utopia or realizable?'. *Journal of Loss Prevention in the Process Industries,* 26 (4), pp. 821-829.

Knutsen, K., Manno, G. and Vartdal, B. (2014) 'Beyond condition monitoring in the maritime industry'. *DNV GL Strategic Research & Inovation Position Paper*.

Komite Nasional Keselamatan Transportasi (2019) 'Aircraft Accident Investigation Report'. Available at: http://knkt.dephub.go.id/knkt/ntsc_aviation/baru/2018%20-%20035%20-%20PK-LQP%20Final%20Report.pdf (Accessed: 01/12/2019).

Kong, S., Lu, M. and Li, L. (2017) Published. 'Fault propagation analysis in software intensive systems: A survey'. *2017 Second International Conference on Reliability Systems Engineering (ICRSE),* 10-12 July 2017 2017. pp.1-9.

Kongsberg (2007) *Power Management System.* Available at: https://www.km.kongsberg.com/ks/web/nokbg0397.nsf/AllWeb/B759133464F70B12C1256DEB0039EBCD/$file/AD-00447B_PMS_datasheet.pdf?OpenElement (Accessed: 01/06/2017).

Kretschmann, L., Rødseth, Ø., Fuller, B.S., Noble, H., Horahan, J. and McDowell, H. (2012) 'D9.3: Quantitative assessment'. Available at: http://www.unmanned-ship.org/munin/wp-content/uploads/2015/10/MUNIN-D9-3-Quantitative-assessment-CML-final.pdf (Accessed: 02/02/2018).

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M. and Halgand, Y. (2015) 'A survey of approaches combining safety and security for industrial control systems'. *Reliability Engineering & System Safety,* 139 156-178.

Kristiansen, S. (2013) *Maritime transportation: safety management and risk analysis.* New York, USA: Routledge.

Krogseth, I.B. (2013) *Dynamic fault-detection in shipboard electric load sharing.* Master Thesis Norwegian University of Science and Technology.

Laskowski, R. (2015) 'Fault Tree Analysis as a tool for modelling the marine main engine reliability structure'. *Zeszyty Naukowe Akademii Morskiej w Szczecinie,* (41 (113)), pp. 71--77.

Lazakis, I., Raptodimos, Y. and Varelas, T. (2018) 'Predicting ship machinery system condition through analytical reliability tools and artificial neural networks'. *Ocean Engineering,* 152 404-415.

Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., King, A., Mullen-Fortino, M., Park, S., Roederer, A. and Venkatasubramanian, K.K. (2012) 'Challenges and research directions in medical Cyber-Physical Systems'. *Proceedings of the IEEE,* 100 (1), pp. 75-90.

Leveson, N. (2004) 'A new accident model for engineering safer systems'. *Safety science,* 42 (4), pp. 237-270.

Leveson, N. (2011a) *Engineering a safer world: Systems thinking applied to safety.* London, England: The MIT press.

Leveson, N. (2011b) *Engineering a safer world: Systems thinking applied to safety.* Cambridge, Massachusetts, USA: MIT press.

Leveson, N. (2012) 'Complexity and Safety'. *Complex Systems Design & Management 2011.* Germany, Berlin, Springer.

Leveson, N. and Thomas, J. (2018) 'STPA Handbook'. Available at: http://sunnyday.mit.edu/STPA-Primer-v0.pdf (Accessed: 01/02/2019).

Li, S. and Li, X. (2014) 'Study on generation of fault trees from Altarica models'. *Procedia Engineering,* 80 140-152.

Li, Y.-h., Shao, W.-z. and Zhang, J. (2010) Published. 'Fuzzy grey fault tree analysis on diesel engine reliability'. *Fuzzy Systems and Knowledge Discovery (FSKD), 2010 Seventh International Conference on,* 2010. IEEE, pp.1263-1267.

Lipsith, G. (2019) *Smarter than human? How AI is revolutionising maintenance.* Available at: https://www.rivieramm.com/opinion/smarter-than-human-how-ai-is-revolutionising-maintenance-22104 (Accessed: 03/12/2019).

Lisagor, O., McDermid, J. and Pumfrey, D. (2006) Published. 'Towards a practicable process for automated safety analysis'. *24th International system safety conference,* 2006. pp.607.

Liu, J.T., Tang, T., Zhu, J.B. and Zhao, L. (2016) 'An extended system-theoretic hazard analysis method for the safety of high-speed railway train control systems'. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit,* 231 (8), pp. 821-834.

Liu, Y., Peng, Y., Wang, B., Yao, S. and Liu, Z. (2017) 'Review on cyber-physical systems'. *IEEE/CAA Journal of Automatica Sinica,* 4 (1), pp. 27-40.

Luft, J. and Ingham, H. (1961) 'The johari window'. *Human Relations Training News,* 5 (1), pp. 6-7.

MAIB (2011) 'Report on the investigation of the catastrophic failure of a capacitor in the aft harmonic filter room on board RMS Queen Mary 2 while approaching Barcelona 23 September 2010'. Available at: https://assets.publishing.service.gov.uk/media/547c6fa6ed915d4c10000031/QM2Report.pdf (Accessed: 01/12/2017).

Malone, T., Kirkpatrick, M., Mallory, K., Eike, D., Johnson, J. and Walker, R. (1980) 'Human factors evaluation of control room design and operator performance at Three Mile Island-2'. Available at: https://tmi2kml.inl.gov/Documents/2c-L2-NUREG/NUREGCR-1270,%20Vol.%201,%20Human%20Factors%20Evaluation%20of%20Control%20Room%20Design%20and%20Operator%20Performance%20at%20TMI-2%20(1980-01).pdf (Accessed: 01/06/2018).

MAN (2012) 'Diesel-electric Propulsion Plants'. Available at: https://marine.man.eu/docs/librariesprovider6/marine-broschures/diesel-electric-drives-guideline.pdf (Accessed: 01/08/2017).

Martins, M.R. and Schleder, A.M. (2012) 'Reliability analysis of the regasification system on board of a FSRU using Bayesian networks'. *Natural Gas: Extraction to End Use.* Pennsylvania, USA: INTECH Open Science, pp. 143-158.

Marwedel, P. and Engel, M. (2016) 'Cyber-Physical Systems: Opportunities, Challenges and (Some) Solutions'. *Management of Cyber Physical Objects in the Future Internet of Things.* Springer, pp. 1-30.

MATLAB User's Guide (1998) 'The mathworks'. *Inc., Natick, MA,* 5 333.

Menis, R., da Rin, A., Vicenzutti, A. and Sulligoi, G. (2012) 'Dependable design of all electric ships integrated power system: Guidelines for system decomposition and analysis'. *Electrical Systems for Aircraft, Railway and Ship Propulsion (ESARS).* Bologna, Italy, IEEE.

Mennis, E. and Platis, A. (2013) 'Availability assessment of diesel generator system of a Ship: A case study'. *International Journal of Performability Engineering,* 9 (5), pp. 561-567.

Meyle (2015) *Arc Detection System.* Available at: http://www.meyle.com.cn/pdf/arc-detection-systems.pdf (Accessed: 01/09/2017).

Mihanović, L., Komar, I. and Gržan, M. (2016) 'Methodology analysis using exploitation reliability with the use of the RTOP main diesel engine'. *NAŠE MORE: znanstveno-stručni časopis za more i pomorstvo,* 63 (2), pp. 48-55.

Möller, D.P. (2016) *Guide to computing fundamentals in Cyber-Physical Systems.* Switzerland: Springer International Publishing.

Murashov, V., Hearl, F. and Howard, J. (2016) 'Working safely with robot workers: Recommendations for the new workplace'. *Journal of Occupational and Environmental Hygiene,* 13 (3), pp. D61-D71.

Mutunga, J.M., Kimotho, J.K. and Muchiri, P. (2019) 'Health-Index Based Prognostics for a Turbofan Engine using Ensemble of Machine Learning Algorithms'. *Journal of sustainable research in engineering,* 5 (2), pp. 50-61.

National Transportation Safety Board (NTSB) (2017) 'Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida May 7, 2016 '. Available at: https://www.ntsb.gov/investigations/AccidentReports/Reports/HAR1702.pdf (Accessed: 02/03/2018).

Nilsen, O.V., Johansen, C.B., Knight, M., Hoffman, P. and Skjong, R. (2005) 'FSA for Cruise Ships - Task 4.1.1 - Hazid identification'. Available at: http://www.safedor.org/resources/SAFEDOR-D-04.01.01-2005-10-31-DNV-HAZID-Cruise-vessels.pdf (Accessed: 01/11/2017).

Oberle, W. (2015) 'Monte Carlo Simulations: Number of Iterations and Accuracy'. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a621501.pdf (Accessed: 01/06/2018).

OREDA (2002) *Offshore reliability data handbook.* 4th edn. Norway, Hovik: OREDA participants.

OREDA (2009) *Offshore reliability data handbook.* 5th edn. Norway, Hovik: OREDA participants.

OREDA (2015) *Offshore reliability data handbook.* 6th edn. Norway, Hovik: OREDA participants.

Ossai, C.I., Boswell, B. and Davies, I.J. (2015) 'Estimation of internal pit depth growth and reliability of aged oil and gas pipelines—A Monte Carlo simulation approach'. *Corrosion,* 71 (8), pp. 977-991.

Panasiuk, I. and Turkina, L. (2015) 'The evaluation of investments efficiency of SOx scrubber installation'. *Transportation Research Part D: Transport and Environment,* 40 87-96.

Papadopoulos, Y. and McDermid, J. (1999) 'Hierarchically performed hazard origin and propagation studies'. *Computer safety, reliability and security.* Toulouse, France, Lecture Notes in Computer Science, vol. 1698, Springer.

Papadopoulos, Y. and McDermid, J. (2001) 'Automated safety monitoring: A review and classification of methods'. *International journal of COMADEM,* 4 (4), pp. 14-32.

Papadopoulos, Y., Walker, M., Parker, D., Sharvia, S., Bottaci, L., Kabir, S., Azevedo, L. and Sorokos, I. (2016) 'A synthesis of logic and bio-inspired techniques in the design of dependable systems'. *Annual Reviews in Control,* 41 170-182.

Park, S., Rogers, W.J. and Pasman, H.J. (2018) 'Is HAZOP a Reliable Tool? What Improvements are Possible?'. *Journal of Korean Institute of Gas,* 22 (2), pp. 1-20.

Patriarca, R., Di Gravio, G. and Costantino, F. (2017) 'A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM) to assess performance variability in complex systems'. *Safety Science,* 91 49-60.

Pavlidis, A. (2018) *Techno-economic and safety analysis of installation of a scrubber in oil tankers.* Masters University of Strathclyde.

Peeters, J.F.W., Basten, R.J.I. and Tinga, T. (2018) 'Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner'. *Reliability Engineering & System Safety,* 172 36-44.

Perrow, C. (1999) *Normal accidents: Living with high risk technologies.* Princeton, New Jersey: Princeton University Press.

Petnga, L. and Austin, M. (2013) 'Ontologies of time and time-based reasoning for MBSE of Cyber-Physical Systems'. *Procedia Computer Science,* 16 403-412.

Placke, S., Thomas, J. and Suo, D. (2015) 'Integration of multiple active safety systems using STPA'. *SAE Technical Paper,* (2015-01-0277), pp.

Procter, S. and Hatcliff, J. (2014) Published. 'An architecturally-integrated, systems-based hazard analysis for medical applications'. *2014 Twelfth ACM/IEEE Conference on Formal Methods and Models for Codesign (MEMOCODE),* 19-21 Oct. 2014 2014. pp.124-133.

Puisa, R., Bolbot, V. and Ihle, I. (2019) 'Development of functional safety requirements for DP-driven servicing of wind turbines'. *European STAMP Workshop & Conference 2019.* Helsinki, Finland.

PV magazine (2016) *PV magazine award für großen Verteilnetz-Speicher.* Available at: https://www.pv-magazine.de/2016/03/07/pv-magazine-award-fr-groen-verteilnetz-speicher/ (Accessed: 05/04/2019).

Qureshi, Z.H. (2007) Published. 'A review of accident modelling approaches for complex socio-technical systems'. *Workshop on Safety critical systems and software and safety-related programmable systems,* 2007 Australia, Adelaide. Australian Computer Society, Inc., pp.47-59.

Radan, D. (2008) *Integrated control of marine electrical power systems.* PhD Thesis. Norwegian University of Science and Technology.

Rajhans, A., Bhave, A., Ruchkin, I., Krogh, B.H., Garlan, D., Platzer, A. and Schmerl, B. (2014) 'Supporting heterogeneity in cyber-physical systems architectures'. *IEEE Transactions on Automatic Control,* 59 (12), pp. 3178-3193.

Ramos, M.A., Thieme, C.A., Utne, I.B. and Mosleh, A. (2020) 'Human-system concurrent task analysis for maritime autonomous surface ship operation and safety'. *Reliability Engineering & System Safety,* 195 106697.

Räsänen, J.-E. (2017) 'Current and future scale limitation for alternative marine power and propulsion solutions'. *Power & Propulsion Alternatives for Ships.* Rotterdam, Netherlands, The Royal Institution of Naval Architects.

Rasoulzadeh Khorasani, V. (2015) *Risk assessment of diesel engine failure in a dynamic positioning system.* Master Thesis. University of Stavanger, Norway.

Raspotnig, C. and Opdahl, A. (2013) 'Comparing risk identification techniques for safety and security requirements'. *Journal of Systems and Software,* 86 (4), pp. 1124-1151.

Rausand, M. (2013) *Risk assessment: theory, methods, and applications.* John Wiley & Sons.

Reddy, B.D., Lingeshwaren, S., Chai, M., Babu, Y.D., Chuhan, P.J., Kamala, S.R., Panda, S.K., Die, W. and Qing, C.X. (2016) 'Investigations on LVAC architectures of diesel electric propulsion based marine vessels for improved power quality and reliability'. *2016 IEEE 8th International Power Electronics and Motion Control Conference (IPEMC-ECCE Asia).*

Reimann, M., Rückriegel, C., Mortimer, S., Bageritz, S., Henshaw, M., Siemieniuch, C., Sinclair, M., Palmer, P., Fitzgerald, J., Ingram, C., Servat, D., Stock, D., Rauschecker, U., Götz, B., Ordóñez, D., Butler, T., de Lama, N., Rico, J. and Alonso, J. (2017) *Road2CPS. Priorities and recommendations for research and innovation in Cyber-Physical Systems.* Stuttgart: Steinbeis-Edition.

Reliability Analytics Toolkit (2018) *Failure rate estimates for mechanical components.* Available at: https://reliabilityanalyticstoolkit.appspot.com/mechanical_reliability_data (Accessed: 2018/04/26).

Rokseth, B., Utne, I.B. and Vinnem, J.E. (2017) 'A systems approach to risk analysis of maritime operations'. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* 231 (1), pp. 53-68.

Rokseth, B., Utne, I.B. and 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.

Roskilly, T. (2016) 'INOMANS2HIP Final publishable report'. Available at: https://trimis.ec.europa.eu/sites/default/files/project/documents/9809/final1-inomanship_public-final-report_unew_v1.pdf (Accessed: 03/03/2018).

Sabaliauskaite, G., Liew, L.S. and Cui, J. (2018) 'Integrating autonomous vehicle safety and security analysis using STPA method and the Six-Step model'. *International Journal on Advances in Security,* 11 (1&2), pp. 160-169.

SafeCOP (2016) 'State of the art on safety assurance'. Available at: http://www.safecop.eu/wp-content/uploads/2017/06/D2.1-Public.pdf (Accessed: 01/11/2017).

Safety of Autonomous Systems Working Group (SASWG) (2020) '*Safety assurance objectives for autonomous systems'. Version 2. (SCSC-153A).* Safety Critical Systems Society.

Sampigethaya, K. and Poovendran, R. (2013) 'Aviation Cyber–Physical Systems: foundations for future aircraft and air transport'. *Proceedings of the IEEE,* 101 (8), pp. 1834-1855.

Santoso, S., Arapostathis, A., Abdelwahed, S., Amgai, R., Cartes, D., Soman, R., Vu, T., Stevens, B. and Shi, J. (2015) 'Improving reliability of MVDC ship power system'.

Scharl, A., Stottlar, K. and Kady, R. (2014) '*Functional Hazard Analysis (FHA) methodology tutorial'.* St. Louis, Missouri: NAVSEA, warfare centers , Dahlgren.

Schmittner, C., Ma, Z., Schoitsch, E. and Gruber, T. (2015) 'A case study of FMVEA and CHASSIS as safety and security co-analysis method for automotive Cyber-Physical Systems'. *1st ACM Workshop on Cyber-Physical System Security.* Singapore, Republic of Singapore, 2732204: ACM.

Schüller, J., Brinkman, J., Van Gestel, P.J. and Van Otterloo, R. (1997) *Methods for Determining and Processing Probabilities: Red Book.* Committee for the Prevention of Disasters.

Sfakianakis, K. and Vassalos, D. (2015) 'Design for safety and energy efficiency of the electrical onboard energy systems'. *2015 IEEE Electric Ship Technologies Symposium.* Washington DC, USA.

Sharvia, S., Kabir, S., Walker, M. and Papadopoulos, Y. (2016) 'Model-based dependability analysis: State-of-the-art, challenges, and future outlook'. In*:* Soley, R. *et al.* (eds.) *Software Quality Assurance.* Boston: Morgan Kaufmann, pp. 251-278.

Siemens (2013) '*Arcing faults in medium-voltage and low-voltage switchgear'*.

Sierla, S., O'Halloran, B.M., Karhela, T., Papakonstantinou, N. and Tumer, I.Y. (2013) 'Common cause failure analysis of cyber–physical systems situated in constructed environments'. *Research in Engineering Design - Theory, Applications, and Concurrent Engineering,* 24 (4), pp. 375-394.

Sinha, K. (2014) *Structural complexity and its implications for design of cyber-physical systems.* PhD Thesis. Massachusetts Institute of Technology.

SINTEF (2006) *Reliability data for safety instrumented systems PDS Data Handbook.*

Sputnik (2016) *Super-realistic robot Sophia threatens to destroy humans.* Available at: https://sputniknews.com/world/201603181036498584-hanson-robotics-super-robot-sophia-destroy-humans/ (Accessed: 01/02/2018).

Stamatelatos, M., Dezfuli, H., Apostolakis, G., Everline, C., Guarro, S., Mathias, D., Mosleh, A., Paulos, T., Riha, D. and Smith, C. (2011) *Probabilistic risk assessment procedures guide for NASA managers and practitioners.* 2nd edn. Washington DC, USA: NASA Center for AeroSpace Information.

Stefani, A. (2013) *An introduction to ship automation and control systems.* United Kingdom, London: Institute of Marine Engineering, Science & Technology.

Steffen, P. (2017) *Steffen Peter personal web page.* Available at: http://www.ics.uci.edu/~steffenp/ (Accessed: 01/03/2017).

Sulaman, S.M., Beer, A., Felderer, M. and Höst, M. (2017) 'Comparison of the FMEA and STPA safety analysis methods–a case study'. *Software Quality Journal,* 1-39.

Teikari, O., Valkonen, J. and Virkkunen, R. (2014) 'CORSICA Task 4.1 Hazard analysis methods of digital I&C systems'. Available at: https://www.semanticscholar.org/paper/CORSICA-Task-4.1-Hazard-analysis-methods-of-digital-Valkonen/da9e170edaf486cb3753e5390d00e6c0d7926332 (Accessed: 01/02/2019).

Thomas, J. (2013) *Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis.* PhD thesis. Massachusetts Institute of Technology.

Thompson, H., Paulen, R., Reniers, M., Sonntag, C. and Engell, S. (2015) 'D2.4 Analysis of the State-of-the-Art and Future Challenges in Cyber-physicalSystems of Systems'. Available at: https://cordis.europa.eu/docs/projects/cnect/5/611115/080/deliverables/001-D24Stateoftheartandfuturechallengesincyberphysicalsystemsofsystems.pdf (Accessed: 01/05/2017).

Tian, J., Wu, J., Yang, Q. and Zhao, T. (2016) 'FRAMA: A safety assessment approach based on Functional Resonance Analysis Method'. *Safety Science,* 85 41-52.

Triginer, J.M.C., Martin, H., Winkler, B. and Marko, N. (2020) 'Integration of safety and cybersecurity analysis through combination of systems and reliability theory methods'. *European Congress Embedded Real Time Systems.* Toulouse, France.

UK P&I CLUB (2015) 'Risk Focus: Loss of power'. Available at: https://www.ukpandi.com/fileadmin/uploads/uk-pi/Documents/Brochures/Risk%20Focus%20-%20Loss%20of%20Power.pdf (Accessed: 01/03/2017).

Ullah, Z., Waldrop, T. and Chavez, N. (2019) *Helicopters sent to rescue 1,300 passengers from cruise ship off Norway.* Available at: https://edition.cnn.com/2019/03/23/europe/norway-cruise-ship-evacuation/index.html (Accessed: 30/09/2019).

United States Environmental Protection Agency (2019) *What is Acid Rain?* Available at: https://www.epa.gov/acidrain/what-acid-rain.

US Department of Defence (1980) '*MIL-STD-1629A - Military Standard - Procedures for performing a failure mode, effects and criticality analysis'*.

US Department of Defence (2012) '*Department of defense standard practice: System safety MIL-STD-882E'*. U.S. Department of Defense.

Utne, I.B., Rokseth, B., Sørensen, A.J. and Vinnem, J.E. (2020) 'Towards supervisory risk control of autonomous ships'. *Reliability Engineering & System Safety,* 196 106757.

Valdez Banda, O.A., Kannos, S., Goerlandt, F., van Gelder, P.H.A.J.M., Bergström, M. and Kujala, P. (2019) 'A systemic hazard analysis and management process for the concept design phase of an autonomous vessel'. *Reliability Engineering & System Safety,* 191 106584.

Van Ta, T., Thien, D.M. and Cang, V.T. (2017) 'Marine Propulsion System Reliability Assesment by Fault Tree Analysis'. *International Journal of Mechanical Engineering and Applications,* 5 (4-1), pp. 1-7.

Van Wesel, P. and Goodloe, A.E. (2017) 'Challenges in the Verification of Reinforcement Learning Algorithms'. Available at: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20170007190.pdf (Accessed: 01/02/2018).

Vedachalam, N. and Ramadass, G.A. (2017) 'Reliability assessment of multi-megawatt capacity offshore dynamic positioning systems'. *Applied Ocean Research,* 63 251-261.

Verma, A.K., Srividya, A. and Karanki, D.R. (2010) *Reliability and safety engineering.* Springer.

Wang, R., Zheng, W., Liang, C. and Tang, T. (2016) 'An integrated hazard identification method based on the hierarchical Colored Petri Net'. *Safety Science,* 88 166-179.

Wartsila (1999) '*Maintenance manual for Wartsila 46 engine*'.

Wheeler, T.A., Williams, A.D., Turner, P.L., Muna, A.B. and Schulz, P.V. (2016) 'A New Look at Cyber Security for Nuclear Power Plants: The Cyber Hazards Analysis Risk Methodology (CHARM)-Slides'. Available at: https://www.osti.gov/servlets/purl/1530052 (Accessed: 01/12/2017).

Winther, R., Johnsen, O.-A. and Gran, B.A. (2001) Published. 'Security assessments of safety critical systems using HAZOPs'. *International Conference on Computer Safety, Reliability, and Security,* 2001. Springer, pp.14-24.

Wolf, M. and Serpanos, D. (2018) 'Safety and security in Cyber-Physical Systems and Internet-of-Things systems'. *Proceedings of the IEEE,* 106 (1), pp. 9-20.

Wróbel, K., Montewka, J. and Kujala, P. (2018) 'Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels'. *Reliability Engineering & System Safety,* 178 209-224.

Xing, J., Zeng, Z. and Zio, E. (2019) 'A framework for dynamic risk assessment with condition monitoring data and inspection data'. *Reliability Engineering & System Safety,* 191 106552.

Xu, J. and Xu, L. (2017) *Integrated System Health Management: Perspectives on Systems Engineering Techniques.* Academic Press.

Yang, H., Jiang, B. and Cocquempot, V. (2010) 'Fault Tolerant Control and Hybrid Systems'. *Fault Tolerant Control Design for Hybrid Systems.* Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1-9.

Yang, Q., Tian, J. and Zhao, T. (2017) 'Safety is an emergent property: Illustrating functional resonance in Air Traffic Management with formal verification'. *Safety Science,* 93 162-177.

Yanmar (2013) '*Operation manual*'.

Young, W. and Leveson, N.G. (2014) 'An integrated approach to safety and security based on systems theory'. *Communnications of the ACM,* 57 (2), pp. 31-35.

Zhang, J., Kim, H., Liu, Y. and Lundteigen, M.A. (2019) 'Combining system-theoretic process analysis and availability assessment: A subsea case study'. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* 233 (4), pp. 520-536.

Zhong, D., Wu, N., Wang, Q. and Sun, R. (2015) Published. 'A multi-view extended software control structure modeling and safety analysis method'. *2015 Prognostics and System Health Management Conference (PHM),* 21-23 Oct. 2015 2015. pp.1-5.

Zhu, D., Tan, H. and Yao, S. (2018) 'Petri Nets-based method to elicit component-interaction related safety requirements in safety-critical systems'. *Computers & Electrical Engineering,* 71 162-172.

Zio, E. (2016a) 'Challenges in the vulnerability and risk analysis of critical infrastructures'. *Reliability Engineering & System Safety,* 152 137-150.

Zio, E. (2016b) 'Some challenges and opportunities in reliability engineering'. *IEEE Transactions on Reliability,* 65 (4), pp. 1769-1782.

APPENDIX A DEP SUBSYSTEMS FUNCTIONS

The DEP subsystems along with their functions, assemblies and components are provided in Tables A.1-7.

Table A. 1 Power generation subsystems.

Subsystem	Function	Assemblies and components
Diesel Engine	The main function of Diesel Engine (DE) is to transform chemical energy into kinetic.	Piston rod assembly, cylinder assembly, fuel supply assembly on engine, lubricants assembly on engine, turbocharger assembly, crankshaft assembly, thrust and main bearings, exhaust gas system.
Auxiliary systems	The main function of auxiliary subsystem is to support the transformation of chemical energy into kinetic in the Diesel Engine and the transformation of kinetic energy into electrical in the Generator.	Fuel supply system, lubricants supply system, air supply system, cooling water supply system, starting air system, air cooling system for generator.
Generator	The main function of Generator is to transform kinetic energy into electrical. Diesel Engine and Generator constitute a Diesel Generator (DG).	Stator, rotor, damper windings, exciter stator, exciter rotor, rectifier, shaft, sleeve bearings.
Battery	The main function of Battery is storage of generated electrical power and its provision to the power network under the following conditions DG sets are operating at low load inefficient load Power demand is higher than can be accepted by the connected DG sets	Batteries pack, associated ventilation, and cooling system

Table A. 2 Power distribution subsystems.

Subsystem	Function	Assemblies and components
Switchboard	The primary goal of switchboard is to distribute the generated power among the consumers.	Bus, circuit breakers, case, cables.
Transformer	The main function of transformers is to reduce the voltage level of generated electrical power to a level suitable for consumers. Other functions include galvanic separation of different voltage levels, adjustment of short-circuits currents, increase of pulse number of drives.	Enclosure, liquid oil used for cooling, winding, cores, bushings, cooling systems.
Cables	Transfer of electrical power from DG to consumers	Just cables

Table A. 3 Power consumption subsystems.

Subsystem	Function	Assemblies and components
Propulsion Motors and associated systems	The propulsion motors are the largest by far consumers of the generated power, responsible for propulsion of a cruise vessel. They are considered to constitute from synchronous motors.	Air cooling system, electrical motor bearings, propeller, shaft seals, shaft, installation block, drainage system, oil supply system for bearings.
Air Conditioning Motors	Air conditioning motors are the consumers necessary for the air conditioning of accommodation places on cruise ship to ensure comfort of passengers and represent significant part of Heat, Ventilation, Air Conditioning consumers (HVAC).	Electrical motors, cooling systems.
Bow Thrusters	An important consumer, necessary during Dynamic Positioning and Manoeuvring.	Air cooling system, bearings electrical motor, propeller, sealing's, installation block, oil supply system for bearings.
Other Loads	Primary hotel load, also including auxiliaries' systems load.	Motors, auxiliary systems, electrical devices, etc.
Frequency converters	Transformation of Alternate Current frequency with the objective of propulsion motors speed control	Frequency converters

Table A. 4 Subsystems used for system control.

Subsystem	Function	Assemblies and components
Power Management System	The central Power Management System (PMS) is supposed to have the following functions (Ådnanes, 2003) & (Radan, 2008): Automatic start/stop of DG based on the load demand and running hours. Control of restart procedures after blackout. Control of load sharing between DGs. Change over from DG with fault. Tripping of non-essential consumers (Fast load reduction). Control of load increase in propulsion motors. Load reduction in propulsion motors (Fast load reduction). Network configuration control and connection of bus-tie with other parts of network.	Programmable Logic Controller (PLC) (Ådnanes, 2003), power supply, circuit breaker status sensors, networking cables, running hours counter.

Intelligent Generator Diagnosis	Intelligent diagnosis of fault in governor and AVR of the system leading to imbalanced power generation and tripping of the faulty generator (Krogseth, 2013).	PLC, power supply, communication lines, frequency sensors, voltage and current sensors.
Battery Management System	Monitoring of the actual battery health state, the battery and cell load and control of the battery cells operating status, charging status, the discharging/charging rate, the converters power output and the battery auxiliary systems.	PLC, power supply, communication lines, frequency sensors, voltage and current sensors, circuit breakers.

Table A. 5 Power generation control systems.

Subsystem	**Function**	**Assemblies and components**
Diesel Generator Controller	The DG control has the following functions (Kongsberg, 2007): Control of starting and stopping sequence of a DG Automatic synchronization to the network Setting reference values to Governor and Automatic Voltage Regulator (AVR)	Programmable Logic Controller (PLC), power supply, communication networks, frequency sensors, voltage and current sensors at the both sides of DG circuit breaker.
Speed Governor	Frequency/speed control through the fuel amount provided to the prime mover (Ådnanes, 2003).	Programmable Logic Controller (PLC), power supply, communication networks, two touch-free, inductive proximity switches, power supply to sensors, fuel racks in fuel pumps of fuel injection system, actuators for movement of fuel racks.
Automatic Voltage Regulator	Voltage control through the actuator excitation current control (Ådnanes, 2003).	PLC, power supply, voltage sensors, stator exciter, excitation current limiter, pulse width modulators.
Diesel Safety System	Switching off the DG set, in case of hazardous abnormal situation (Kongsberg, 2007): Over speed Very low lubrication pressure Very high freshwater cooling temperature Very high cylinder liner temperature Very high thrust and bearing temperature High oil mist concentration in the crankcase Failure in control components In case of deviations, the system gives an alarm to the crew for prompt maintenance activities and	PLC, power supply, voltage sensors, lubricants temperature sensors, fresh water temperature sensors, cylinder liner temperature sensors, thrust and bearing temperature sensors, oil mist sensors, lubricants pressure sensors, fresh water pressure sensors, exhaust gases sensors at relevant positions, generator bearing temperature sensors, tripping lever, current sensors, voltage sensors, frequency sensors, power supply, communication lines, circuit breaker.

	the PMS conducts the changeover to another DG set. The conditions considered are: Low lubrication oil pressure High lubrication oil temperature Low freshwater pressure High freshwater temperature High exhaust gases temperature at cylinder valve, before and after turbine High cylinder liner temperature High main/thrust bearings temperature High exhaust gas deviation Engine safety may also give order to reduce the load of a DG set in case: High cylinder cooling water temperature High exhaust gas temperature Detection of misfiring Generator safety system ensures that the circuit breaker is tripped in the following cases (Kongsberg, 2007): Overcurrent detection Short circuit Reverse current and load detection Overload Over and under voltage Over and under frequency Differential current Earth fault High generator bearing temperature	

Table A. 6 Power distribution control systems.

Subsystem	Function	Assemblies and components
Bus-tie circuit breaker controller	The main objective of bus-tie controller is to ensure proper synchronization conditions for connecting bus-tie breakers (Kongsberg, 2007).	PLC, power supply, circuit breakers, frequency, current and voltage sensors.
Arc Protection	The purpose of arc detection and protection system is to observe the arc in the Switchboards and to trigger a circuit breaker much sooner that typical protection relays (Meyle, 2015).	PLC, power supply, optical sensors, circuit breakers.

Protection Relays	The objective of protection relays is to trigger the circuit breaker, in case overcurrent or short circuit is observed.	Circuit breaker, protection relay, current sensor.
Transformers Protection System	The purpose of transformer protection is to trigger the relevant circuit breaker, in case of observance of (MAN, 2012): Earth fault. Under voltage. Differential current fault. Thermal overload. Short circuit. Overcurrent.	Circuit breaker, temperature sensors, voltage sensors, current sensors.

Table A. 7 Power consumption control systems.

Subsystem	**Function**	**Assemblies and components**
Application Controller	The main objective of application controller is to cooperate with PMS on the load requested by propulsion units from the electrical network, to avoid overload of DG (Radan, 2008). Secondarily the application controller implements safety functions for the propulsion motors. It triggers the necessary circuit breaker in case of: Short circuit. Over current. Under voltage. Earth fault. High water cooling temperature for motors. Motor windings and bearings over temperature. Over speed. Diagnosed faults. Thirdly the application controller selects the source of reference speed.	Programmable Logic Controller (PLC), power supply, communication networks, sensors, voltage and current sensors, temperature sensors for propulsion units and associated transformers, speed sensor.
Drive Controller	The objective of drive controller is to control the firing order of thyristors in converters and in this way speed control.	PLC, power supply, communication network, speed sensor, thyristors bridge, frequency converters.

Air Conditioning Motors Controller	The control that was of interest here was that related to safety functions of air conditioning motors. The safety system would cause tripping in the following cases (MAN, 2012): Earth fault. Under voltage. Thermal overload. Stalling. Motor windings over temperature. Bearings over temperature. High water-cooling temperature.	PLC, temperature sensors, currents sensors, voltage sensors, communication lines, power supply.
Bow Thrusters Controller	The main functionalities of the bow thrusters control are considered to be similar with those of air conditioning units. The safety system would cause tripping in the following cases (MAN, 2012): Earth fault. Under voltage. Thermal overload. Stalling. Motor windings over temperature. Bearings over temperature. High water cooling temperature.	PLC, temperature sensors, currents sensors, voltage sensors, communication lines, power supply.

APPENDIX B AUXILIARY SYSTEMS LAYOUT

The DG sets' auxiliary systems are provided in Figure B1 to Figure B5.

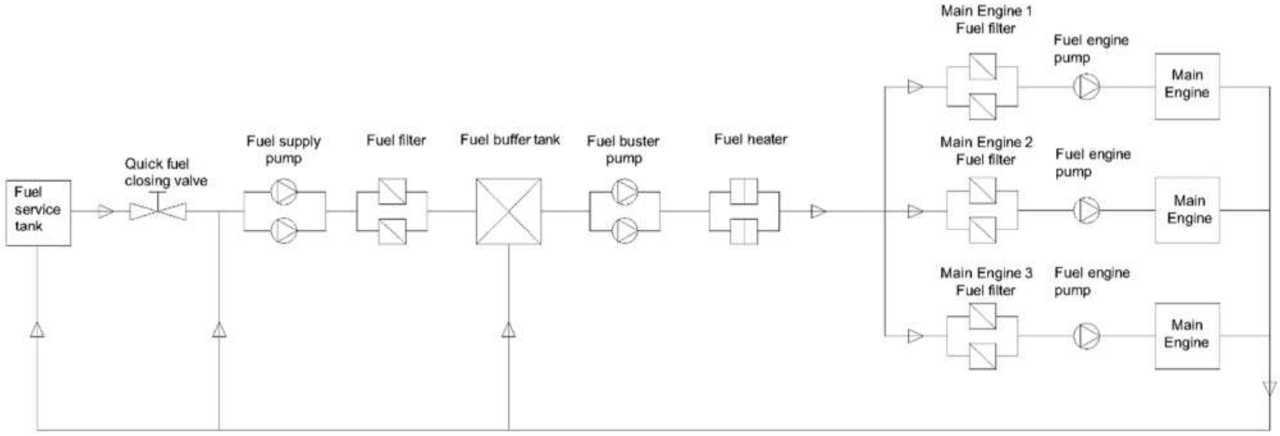


Figure B. 1 Fuel system diagram.

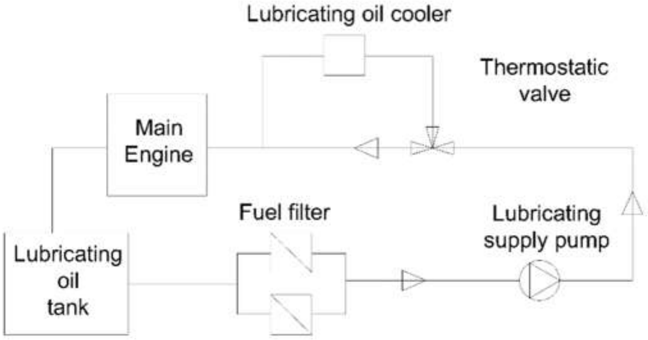
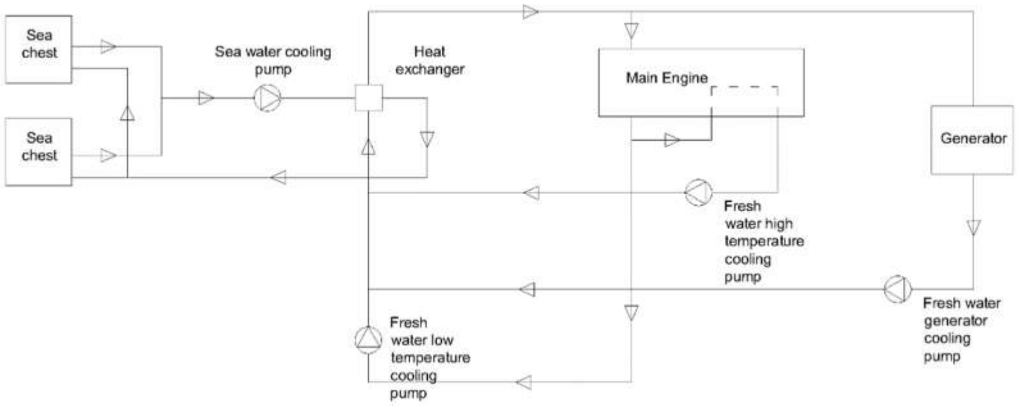


Figure B. 3 Lubricating system diagram.



Sea chest
Sea water cooling pump
Heat exchanger
Main Engine
Sea chest
Generator
Fresh water high temperature cooling pump
Fresh water generator cooling pump
Fresh water low temperature cooling pump

Figure B. 2 Cooling system diagram.

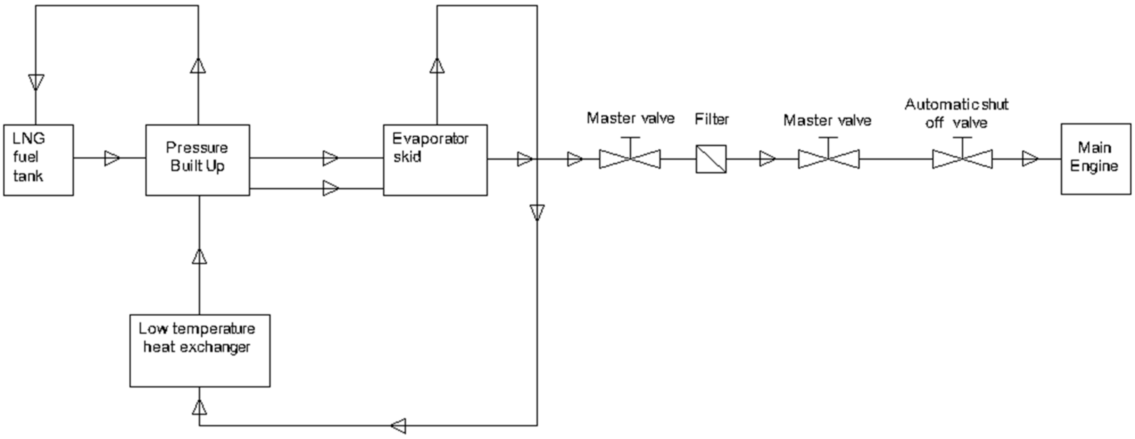


Figure B. 4 LNG feed system diagram.

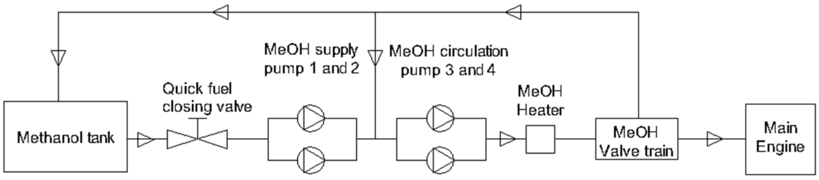


Figure B. 5 Methanol feed system diagram.

APPENDIX C RELIABILITY DATA INPUT

The failure rates that have been used as input to the analysis are provided in Table C. 1.

Table C. 1 Failure rates and beta factors used as input to analysis.

a/a	Failure	λ_i [h^{-1}]	λ_i^{upper}[h^{-1}]	λ_i^{lower}[h^{-1}]	EF_i	Source	β [−]	Source for β factors
1	Earth faults in DG set	2.79E-06	1.04E-05	7.45E-07	3.7	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
2	Overcurrent in DG set	2.79E-06	1.04E-05	7.45E-07	3.7	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
3	Differential current fault in DG set	2.79E-06	1.04E-05	7.45E-07	3.7	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
4	Short circuit in DG sets	2.79E-06	1.04E-05	7.45E-07	3.7	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
5	Engine failure	1.77E-03	3.24E-03	9.65E-04	1.8	(OREDA, 2015)	1	No data
6	Failure to start on demand the engine	1.80E-03	3.30E-03	9.82E-04	1.8	(OREDA, 2015)	NA	NA
7	Failure to start on demand the generator	4.80E-03	1.80E-02	1.28E-03	3.7	(OREDA, 2015)	NA	NA
8	DG set thrust bearings failure	2.78E-06	1.94E-05	3.97E-07	7.0	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
9	DG set main bearings failure	2.78E-06	1.94E-05	3.97E-07	7.0	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
10	Water pipelines on engine failure	1.18E-05	2.17E-05	6.46E-06	1.8	(OREDA, 2015)	1.24	(Ossai *et al.*, 2015)
11	Engine air supply failure	3.01E-06	5.51E-06	1.64E-06	1.8	(OREDA, 2015)	1	No data
12	High lubrication oil mist presence in engine crankcase	1.72E-05	1.21E-04	2.46E-06	7.0	(OREDA, 2015)	1.24	(Reliability Analytics Toolkit, 2018)
13	Turbocharger failure	4.74E-09	8.68E-09	2.58E-09	1.8	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
14	Engine exhaust valves failure	1.87E-08	3.42E-08	1.02E-08	1.8	(OREDA, 2015)	2.23	(Bukša *et al.*, 2009)

15	Engine injection system failure	2.34E-08	4.29E-08	1.28E-08	1.8	(OREDA, 2015)	1.552	(Mihanović *et al.*, 2016)
16	DG set controller hardware failure	3.77E-06	9.43E-06	1.51E-06	2.5	(OREDA, 2015)	NA	NA
17	DG set controller not starting the DG set when required	5.00E-05	7.50E-04	3.33E-06	15.0	(SINTEF, 2006)	NA	NA
18	DG set controller not synchronising the DG set when required	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
19	DG set controller implementing extra attempts to synchronise	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
20	DG set controller not coordinating AVR and DG set controller as required	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
21	DG set controller software faulty failure to coordinate Governor and DG controller	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
22	DG set controller implementing wrong starting sequence	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
23	DG set controller starting DG set longer than required	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
24	DG set controller providing wrong reference speed during start	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
25	DG set controller providing too fast speed increase command	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
26	DG controller communication lines failure	2.50E-08	1.75E-07	3.57E-09	7.0	(Chai *et al.*, 2016)	NA	NA
27	Generator frequency sensors failure	1.19E-06	2.98E-06	4.74E-07	2.5	(OREDA, 2015)	NA	NA
28	Turning gear status sensor failure	1.40E-06	9.80E-06	2.00E-07	7.0	(SINTEF, 2006)	NA	NA
29	Fuel temperature sensor failure	3.77E-06	9.43E-06	1.51E-06	2.5	(OREDA, 2015)	NA	NA
30	Fuel pressure sensor failure	1.25E-06	3.14E-06	5.02E-07	2.5	(OREDA, 2015)	NA	NA

31	Lubricating oil level sensor failure	1.40E-06	9.80E-06	2.00E-07	7.0	(SINTEF, 2006)	NA	NA
32	Air starting system air pressure sensors failure	5.32E-06	2.32E-05	1.22E-06	4.4	(OREDA, 2015)	NA	NA
33	Governor hardware faulty	3.77E-06	9.43E-06	1.51E-06	2.5	(OREDA, 2015)	NA	NA
34	Governor not responding to changes	1.00E-06	1.50E-05	6.67E-08	15.0	(Aldemir *et al.*, 2007)	NA	NA
35	Governor fails to synchronise to network	1.00E-06	1.50E-05	6.67E-08	15.0	(Aldemir *et al.*, 2007)	NA	NA
36	Governor communication lines failure	2.50E-08	1.75E-07	3.57E-09	7.0	(Chai *et al.*, 2016)	NA	NA
37	Governor speed sensors erroneous measurement	1.18E-05	3.26E-05	4.31E-06	2.7	(OREDA, 2015)	NA	NA
38	DG set fuel racks failure	2.37E-05	4.34E-05	9.31E-06	1.8	(OREDA, 2015)	1.1	(Reliability Analytics Toolkit, 2018)
39	Governor fuel limiter failure	6.27E-07	1.57E-06	2.51E-07	2.5	(OREDA, 2015)	NA	NA
40	AVR fails to synchronise to network	1.00E-06	1.50E-05	6.67E-08	15.0	(Aldemir *et al.*, 2007)	NA	NA
41	AVR does not change the voltage level when required	1.00E-06	1.50E-05	6.67E-08	15.0	(Aldemir *et al.*, 2007)	NA	NA
42	AVR voltage sensor erroneous measurement	5.08E-07	1.90E-06	1.36E-07	3.7	(OREDA, 2015)	NA	NA
43	AVR hardware system failure	1.11E-05	4.17E-05	2.98E-06	3.7	(OREDA, 2015)	NA	NA
44	AVR excitation bridge failure	2.63E-07	6.10E-07	1.14E-07	2.3	(OREDA, 2015)	1	No data
45	AVR communication failure	2.50E-08	1.75E-07	3.57E-09	7.0	(Chai *et al.*, 2016)	NA	NA
46	Engine safety system hardware failure	1.00E-05	7.00E-05	1.43E-06	7.0	(SINTEF, 2006)	NA	NA
47	Engine safety system fault tripping of engine	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
48	Engine safety system not tripping the DG set when required	5.00E-04	7.50E-03	3.33E-05	15.0	(SINTEF, 2006)	NA	NA

49	Engine safety system tripping the DG set with delay when required	5.00E-04	7.50E-03	3.33E-05	15.0	(SINTEF, 2006)	NA	NA
50	Engine safety system lubricating oil pressure sensors failure	1.25E-06	3.14E-06	5.02E-07	2.5	(OREDA, 2015)	NA	NA
51	Engine safety system thrust bearings temperature sensors failure	3.77E-06	9.43E-06	1.51E-06	2.5	(OREDA, 2015)	NA	NA
52	Engine safety system cooling water temperature sensors failure	3.77E-06	9.43E-06	1.51E-06	2.5	(OREDA, 2015)	NA	NA
53	Engine safety system exhaust gas temperature sensors failure	3.77E-06	9.43E-06	1.51E-06	2.5	(OREDA, 2015)	NA	NA
54	Engine safety system main bearings temperature sensors failure	3.77E-06	9.43E-06	1.51E-06	2.5	(OREDA, 2015)	NA	NA
55	Engine safety system oil mist detector sensor failure	5.80E-07	4.06E-06	8.29E-08	7.0	(Berghmans *et al.*, 2008)	NA	NA
56	Engine safety system speed sensor failure	1.88E-06	4.70E-06	7.53E-07	2.5	(OREDA, 2015)	NA	NA
57	Engine safety system actuator failure	1.30E-06	9.10E-06	1.86E-07	7.0	(SINTEF, 2006)	1.1	(Reliability Analytics Toolkit, 2018)
58	Engine safety system communication failure	2.50E-08	1.75E-07	3.57E-09	7.0	(Chai *et al.*, 2016)	NA	NA
59	Generator safety system hardware failure	1.00E-05	7.00E-05	1.43E-06	7.0	(SINTEF, 2006)	NA	NA
60	Generator safety system not tripping the DG set when required	5.00E-04	7.50E-03	3.33E-05	15.0	(SINTEF, 2006)	NA	NA
61	Generator safety system generator faulty tripping	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
62	Generator safety system current sensor failure	5.32E-07	3.72E-06	7.60E-08	7.0	(ABB, 2005)	NA	NA

63	Generator safety system frequency sensor failure	8.82E-07	4.16E-06	1.87E-07	4.7	(OREDA, 2015)	NA	NA
64	Cylinders failure	1.68E-10	3.07E-10	9.14E-11	1.8	(OREDA, 2015)	NA	NA
65	DG set fuel pump failure	3.35E-10	6.14E-10	1.83E-10	1.8	(OREDA, 2015)	NA	NA
66	Engine shaft failure leading to engine stop	1.68E-10	3.07E-10	9.14E-11	1.8	(OREDA, 2015)	NA	NA
67	Engine piston failure	2.61E-06	1.83E-05	3.73E-07	7.0	(Van Ta *et al.*, 2017)	1.552	(Mihanović *et al.*, 2016)
68	Governor speed sensors failure	2.37E-05	4.34E-05	1.29E-05	1.8	(OREDA, 2015)	NA	NA
69	AVR voltage sensor failure	5.08E-07	1.90E-06	1.36E-07	3.7	(OREDA, 2015)	NA	NA
70	Engine safety system faulty tripping the engine due to alleged high oil mist concentration	7.39E-06	1.11E-04	4.93E-07	15.0	AIR	1	No data
71	Failure of current sensors on DG set	5.32E-07	1.87E-06	1.51E-07	3.5	(ABB, 2005)	NA	NA
72	Failure of voltage sensors on DG set	6.73E-07	2.36E-06	1.91E-07	3.5	(OREDA, 2015)	NA	NA
73	Lubricating oil pipelines failure	7.47E-08	1.37E-07	4.07E-08	1.8	(OREDA, 2015)	1.24	(Ossai *et al.*, 2015)
74	Lubricating oil filter failure	3.35E-10	6.14E-10	1.83E-10	1.8	(OREDA, 2015)	1.1	(Reliability Analytics Toolkit, 2018)
75	Lubricating oil pump failure	1.01E-11	1.85E-11	5.52E-12	1.8	(OREDA, 2015)	1.2	(Reliability Analytics Toolkit, 2018)
76	Starting air system failure	6.28E-06	1.15E-05	3.43E-06	1.8	(OREDA, 2015)	1	No data
77	Fuel supply system during start failure	6.27E-07	1.15E-06	3.42E-07	1.8	(OREDA, 2015)	1	No data
78	Water cooler failure	2.51E-06	4.60E-06	1.37E-06	1.8	(OREDA, 2015)	1.88	(Dolas and Deshmukh, 2015)
79	Fuel pipes failure/leakages	1.34E-05	2.46E-05	7.31E-06	1.8	(OREDA, 2015)	1.24	(Ossai *et al.*, 2015)
80	Engine fuel filter failure	3.35E-10	6.14E-10	1.83E-10	1.8	(OREDA, 2015)	1.1	(Reliability Analytics Toolkit, 2018)

81	High temperature water cooling pump failure	3.02E-05	5.54E-05	1.65E-05	1.8	(OREDA, 2015)	1.2	(Reliability Analytics Toolkit, 2018)
82	Low temperature water cooling pump failure	3.02E-05	5.54E-05	1.65E-05	1.8	(OREDA, 2015)	1.2	(Reliability Analytics Toolkit, 2018)
83	Generator low temperature water pump failure	1.02E-06	3.80E-06	2.72E-07	3.7	(OREDA, 2015)	1.2	(Reliability Analytics Toolkit, 2018)
84	Oil cooler failure	1.34E-05	2.46E-05	7.31E-06	1.8	(OREDA, 2015)	1.88	(Dolas and Deshmukh, 2015)
85	Fuel supply pump failure	7.56E-06	5.29E-05	1.08E-06	7.0	(Anantharaman *et al.*, 2015)	1.2	(Reliability Analytics Toolkit, 2018)
86	Fuel filter in supply system failure	6.96E-06	4.87E-05	9.94E-07	7.0	(Anantharaman *et al.*, 2015)	1.1	(Reliability Analytics Toolkit, 2018)
87	Fuel heater failure	4.27E-06	2.99E-05	6.10E-07	7.0	(Anantharaman *et al.*, 2015)	1.552	(Mihanović *et al.*, 2016)
88	Fuel booster pump failure	8.28E-06	5.80E-05	1.18E-06	7.0	(Anantharaman *et al.*, 2015)	1.2	(Reliability Analytics Toolkit, 2018)
89	Sea chest clogged	7.00E-04	4.90E-03	1.00E-04	7.0	(Allal *et al.*, 2017)	1.3	(Reliability Analytics Toolkit, 2018)
90	Fuel quick closing valve faulty operation	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
91	Electrical transient is not acceptable by the system	3.35E-08	2.35E-07	4.79E-09	7.0	AIR	NA	NA
92	Fire in engine room	6.60E-07	4.62E-06	9.43E-08	7.0	(IMO, 2008, Nilsen *et al.*, 2005)	NA	NA
93	Failure in communication lines	2.50E-08	1.75E-07	3.57E-09	7.0	(Chai *et al.*, 2016)	NA	NA
94	Intelligent diagnosis does not identify and correct load sharing	1.00E-02	7.00E-02	1.43E-03	7.0	*	NA	NA
95	Failure of Intelligent Diagnosis hardware	3.02E-05	2.11E-04	4.31E-06	7.0	(OREDA, 2015)	NA	NA

96	Short circuit in air conditioning motors	3.28E-07	7.32E-07	1.47E-07	2.2	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
97	Arc in switchboards	1.14E-08	7.99E-08	1.63E-09	7.0	(Siemens, 2013)	1.3	(Reliability Analytics Toolkit, 2018)
98	Short circuits in transformers	4.81E-07	3.37E-06	6.87E-08	7.0	(Chai *et al.*, 2016, Aquilino, 1983)	1.3	(Reliability Analytics Toolkit, 2018)
99	DG set, Bus-Tie, Air conditioning motors, Bow Thrusters circuit breaker not operating	2.50E-06	1.75E-05	3.57E-07	7.0	(Schüller *et al.*, 1997)	NA	NA
100	DG set, Bus-Tie, Air conditioning motors, Bow Thrusters, circuit breaker spurious operation	1.20E-06	8.40E-06	1.71E-07	7.0	(Schüller *et al.*, 1997)	NA	NA
101	Transformer failure	1.75E-06	1.22E-05	2.50E-07	7.0	(Chai *et al.*, 2016)	1.93	(Jin *et al.*, 1999)
102	Arc protection hardware failure	1.50E-05	1.05E-04	2.14E-06	7.0	(OREDA, 2015)	NA	NA
103	Arc protection software not operating	5.00E-04	7.50E-03	3.33E-05	15.0	(SINTEF, 2006)	NA	NA
104	Arc protection sensors failure	5.80E-07	4.06E-06	8.29E-08	7.0	(Berghmans *et al.*, 2008)	NA	NA
105	Fault tripping of arc protection	1.50E-05	1.05E-04	2.14E-06	7.0	(OREDA, 2015)	NA	NA
106	PMS hardware faulty	1.50E-05	1.05E-04	2.14E-06	7.0	(SINTEF, 2006)	NA	NA
107	Failure to reduce the propulsion motors load by the PMS	5.00E-05	7.50E-04	3.33E-06	15.0	(SINTEF, 2006)	NA	NA
108	Failure to reduce the propulsion motors load in time by PMS	5.00E-05	7.50E-04	3.33E-06	15.0	(SINTEF, 2006)	NA	NA
109	Failure to trip heavy consumers	5.00E-05	7.50E-04	3.33E-06	15.0	(SINTEF, 2006)	NA	NA
110	Fault tripping of propulsion motors	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
111	PMS Failure to start a DG when required	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
112	PMS starting an already running DG set	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA

113	PMS starting a faulty DG set	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
114	PMS stopping DG set without other set allocation	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
115	PMS connecting bus-tie breaker to a section with electrical fault	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
116	PMS starting a DG set with delay	5.00E-05	7.50E-04	3.33E-06	15.0	(SINTEF, 2006)	NA	NA
117	PMS allowing load increase, when inadequate DG set number is connected	1.00E-06	1.50E-05	6.67E-08	15.0	(SINTEF, 2006)	NA	NA
118	Short circuit in propulsion motors or bow thrusters	3.28E-07	7.32E-07	1.47E-07	2.2	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
119	Overcurrent in propulsion motors	2.79E-06	1.04E-05	7.45E-07	3.7	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
120	Differential current fault in propulsion motors	2.79E-06	1.04E-05	7.45E-07	3.7	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
121	Application controller not reducing propulsion motors load during DG sets overload conditions	5.00E-05	7.50E-04	3.33E-06	15.0	(SINTEF, 2006)	NA	NA
122	Application controller generates unacceptable electrical transients during start of propulsion motors	5.00E-05	7.50E-04	3.33E-06	15.0	(SINTEF, 2006)	NA	NA
123	Application controller not timely reducing propulsion motors load during DG sets overload conditions	5.00E-05	7.50E-04	3.33E-06	15.0	(SINTEF, 2006)	NA	NA
124	Faulty tripping of propulsion motors by application controller	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA

125	Application controller not controlling power increase	1.00E-05	1.50E-04	6.67E-07	15.0	(SINTEF, 2006)	NA	NA
126	Drive controller not reducing propulsion motors load during DG sets overload conditions	1.00E-06	1.50E-05	6.67E-08	15.0	(Aldemir *et al.*, 2007)	NA	NA
127	Drive controller not timely reducing propulsion motors load during DG sets overload conditions	1.00E-06	1.50E-05	6.67E-08	15.0	(Aldemir *et al.*, 2007)	NA	NA
128	Drive controller not controlling power increase	1.00E-05	1.50E-04	6.67E-07	15.0	(Aldemir *et al.*, 2007)	NA	NA
129	Temperature sensors on cycloconverter failure	3.63E-06	1.39E-05	9.46E-07	3.8	(OREDA, 2015)	NA	NA
130	Temperature sensors on winding of motors failure	2.63E-07	6.10E-07	1.14E-07	2.3	(OREDA, 2015)	NA	NA
131	Temperature sensors on cooling water system of propulsion motors failure	2.63E-07	6.10E-07	1.14E-07	2.3	(OREDA, 2015)	NA	NA
132	Temperature sensors on bearings of propulsion motors failure	2.63E-07	6.10E-07	1.14E-07	2.3	(OREDA, 2015)	NA	NA
133	Speed sensors on propulsion motors erroneous measurement	2.63E-07	6.10E-07	1.14E-07	2.3	(OREDA, 2015)	NA	NA
134	Radial bearings on motors failure	3.28E-07	7.32E-07	1.47E-07	2.2	(OREDA, 2015)	1.3	(Reliability Analytics Toolkit, 2018)
135	Propulsion motors air supply system failure	2.63E-06	5.86E-06	1.18E-06	2.2	(OREDA, 2015)	1.2	Assumption
136	Propulsion motors water cooling system failure	2.30E-06	5.13E-06	1.03E-06	2.2	(OREDA, 2015)	1.2	Assumption
137	Electrical motor failure	4.38E-05	9.76E-05	1.96E-05	2.2	(OREDA, 2015)	1.2	(Reliability Analytics

								Toolkit, 2018)
138	Electrical motor shaft failure	1.00E-06	7.00E-06	1.43E-07	7.0	*	2	(Reliability Analytics Toolkit, 2018)
139	Azipods sealing failure	2.92E-05	2.04E-04	4.17E-06	7.0	(Chybowski *et al.*, 2014)	1.4	(Reliability Analytics Toolkit, 2018)
140	Load (current and voltage) sensors on azipods propulsion motors	2.63E-07	6.10E-07	1.14E-07	2.3	(OREDA, 2015)	NA	NA
141	Rectifier failure	4.34E-06	3.04E-05	6.20E-07	7.0	(OREDA, 2015)	1	No data
142	Converter failure	1.43E-04	1.00E-03	2.05E-05	7.0	(OREDA, 2015)	1	No data
143	Pressure built up unit in LNG feed system	4.51E-06	NA	NA	NA	(OREDA, 2015)	1.88	(Dolas and Deshmukh, 2015)
144	Evaporator skid failure	4.51E-06	NA	NA	NA	(OREDA, 2015)	1.88	(Dolas and Deshmukh, 2015)
145	Master valve failure	3.91E-05	NA	NA	NA	(OREDA, 2015)	1	(Reliability Analytics Toolkit, 2018)
146	LNG filter failure	4.16E-07	NA	NA	NA	(Martins and Schleder, 2012)	1	(Reliability Analytics Toolkit, 2018)
147	Low temperature heat exchanger failure	4.03E-05	NA	NA	NA	(OREDA, 2015)	1.88	(Dolas and Deshmukh, 2015)
148	Master valve 2 failure	3.91E-05	NA	NA	NA	(OREDA, 2015)	1	(Reliability Analytics Toolkit, 2018)
149	Automatic shut off valve faulty tripping	1.00E-05	NA	NA	NA	(SINTEF, 2006)	NA	NA
150	Pipelines failure	6.70E-09	NA	NA	NA	(Martins and Schleder, 2012)	1.24	(Ossai *et al.*, 2015)
151	LNG to fuel reconfiguration command not provided	5.00E-05	NA	NA	NA	(SINTEF, 2006)	NA	NA
152	LNG Fuel open valve faulty	1.30E-06	NA	NA	NA	(SINTEF, 2006)	NA	NA
153	Methanol quick fuel valve faulty tripping	1.00E-05	NA	NA	NA	(SINTEF, 2006)	NA	NA

154	Methanol supply pump	3.99E-04	NA	NA	NA	(OREDA, 2009)	1.2	(Reliability Analytics Toolkit, 2018)
155	Methanol circulating pump	3.99E-04	NA	NA	NA	(OREDA, 2009)	1.2	(Reliability Analytics Toolkit, 2018)
156	Methanol heater	7.54E-05	NA	NA	NA	(OREDA, 2009)	1.88	(Dolas and Deshmukh, 2015)
157	Methanol Valve train	3.91E-05	NA	NA	NA	(OREDA, 2009)	1	(Reliability Analytics Toolkit, 2018)
158	Methanol to fuel reconfiguration command not provided	5.00E-05	NA	NA	NA	(SINTEF, 2006)	NA	NA
159	BMS not disconnecting faulty batteries when	5.00E-05	7.50E-04	3.33E-06	6.5	(SINTEF, 2006)	NA	NA
160	BMS current sensor failure	5.32E-07	1.87E-06	3.21E-09	0.8	(ABB, 2005)	NA	NA
161	BMS voltage sensor failure	6.73E-07	2.36E-06	4.06E-09	0.8	(OREDA, 2015)	NA	NA
162	BMS temperature sensor failure	2.63E-07	6.10E-07	5.18E-08	0.3	(OREDA, 2015)	NA	NA
163	BMS communication failure	2.50E-08	1.75E-07	3.57E-09	2.6	(Chai *et al.*, 2016)	NA	NA
164	BMS circuit breaker failure	2.50E-06	1.75E-05	3.57E-07	2.6	(Schüller *et al.*, 1997)	NA	NA
165	BMS disconnecting faulty batteries with delay	5.00E-05	7.50E-04	3.33E-06	6.5	(SINTEF, 2006)	NA	NA
166	BMS not disconnecting faulty batteries due to conflicting control actions	5.00E-05	7.50E-04	3.33E-06	6.5	(SINTEF, 2006)	NA	NA
167	BMS disconnecting fault batteries with delay due to conflicting control actions	5.00E-05	7.50E-04	3.33E-06	6.5	(SINTEF, 2006)	NA	NA
168	BMS cell failure rate	2.00E-07	3.00E-06	1.33E-08	6.5	(Electropaedia, 2019)	NA	NA
169	BMS faulty batteries tripping	1.00E-05	1.50E-04	6.67E-07	6.5	(SINTEF, 2006)	NA	NA

170	BMS charging batteries when faulty	1.00E-05	1.50E-04	6.67E-07	6.5	(SINTEF, 2006)	NA	NA
171	BMS discharging batteries when faulty	1.00E-05	1.50E-04	6.67E-07	6.5	(SINTEF, 2006)	NA	NA
172	BMS hardware failure	1.50E-05	1.05E-04	2.14E-06	2.6	(SINTEF, 2006)	NA	NA
173	BMS not charging batteries during normal conditions	5.00E-05	7.50E-04	3.33E-06	6.5	(SINTEF, 2006)	NA	NA
174	BMS not discharging batteries when in normal condition	5.00E-05	7.50E-04	3.33E-06	6.5	(SINTEF, 2006)	NA	NA
175	Batteries frequency converter faulty	6.85E-07	4.79E-06	9.78E-08	2.6	(Santoso *et al.*, 2015)	NA	NA
176	Batteries faulty transformer	1.75E-06	1.22E-05	2.50E-07	2.6	(Chai *et al.*, 2016)	NA	NA
177	BMS overcharging batteries when in norm	1.00E-05	1.50E-04	6.67E-07	6.5	(SINTEF, 2006)	NA	NA
178	BMS over discharging batteries when in norm	1.00E-05	1.50E-04	6.67E-07	6.5	(SINTEF, 2006)	NA	NA
179	BMS charging batteries when power generation capacity is not available	1.00E-05	1.50E-04	6.67E-07	6.5	(SINTEF, 2006)	NA	NA
180	BMS charging batteries when power generation capacity is not available due to conflict with PMS	1.00E-05	1.50E-04	6.67E-07	6.5	(SINTEF, 2006)	NA	NA

*Assumption

AIR=Accident Investigation Reports

APPENDIX D GENERIC OPERATING DATA

The detailed operational information for the investigated cruise ship systems is provided in Table D. 1.

Table D. 1 Operational information for the investigated cruise ship systems.

System No	Case study	OM / OP	Operating DG sets total number (specific system configuration)								% time per annum	Electric Power Consumers Engaged	
			1	2	3	4	5	6	7	8			
			Operational time %									PM	BT
1, 2	*i-vii, xi, xv, xix*	*G/ (a)*	21	19	35	22	2	1	NA	NA	100	3	1
1	*viii, xii, xvi*	*H / (a)*	74	22	4	0	0	0	NA	NA	28	0	0
1	*ix, xiii, xvii,*	*S / (a)*	0	17	48	31	3	1	NA	NA	69	3	0
1	*x, xiv, xviii*	*M / (a)*	17	41	39	3	0	0	NA	NA	3	2	1
3	*xx*	*G / (a)*	4	21	17	12	17	17	10	2	100	3	1
4	*xxi*	*G / (a)*	5	25	16	17	12	16	7	2	100	3	1
5	*xxii*	*G / (a)*	7	25	17	23	25	3	NA	NA	100	3	1
6	*xxiii*	*G / (a)*	5	25	16	17	12	16	7	2	100	3	1
7	*xxiv*	*G / (b)*	0	0	0	1	36	35	25	3	100	3	1
8	*xxv*	*G / (b)*	0	22	8	7	13	29	20	1	100	3	1
9	*xxvi*	*G / (b)*	25	16	25	27	4	3	0	0	100	3	1
10	*xxvii*	*G / (b)*	0	26	7	9	24	19	14	1	100	3	1
11	*xxviii*	*G/ (a)*	31	23	43	3	0	0	NA	NA	100	3	1
12	*xxix*	*G / (a)*	0	26	7	42	25	0	NA	NA	100	3	1
13	*xxx*	*G / (a)*	0	6	20	5	16	40	13	0	100	3	1

OM= Operating Mode /OP=Operating Profile /G= General /S= Sailing /M= Manoeuvring /H= Harbour

This page has been intentionally left blank

APPENDIX E OPERATIONAL DATA INPUT

The load frequency distribution for different operating modes and investigated systems in provided in Figures E1 to Figure E15.

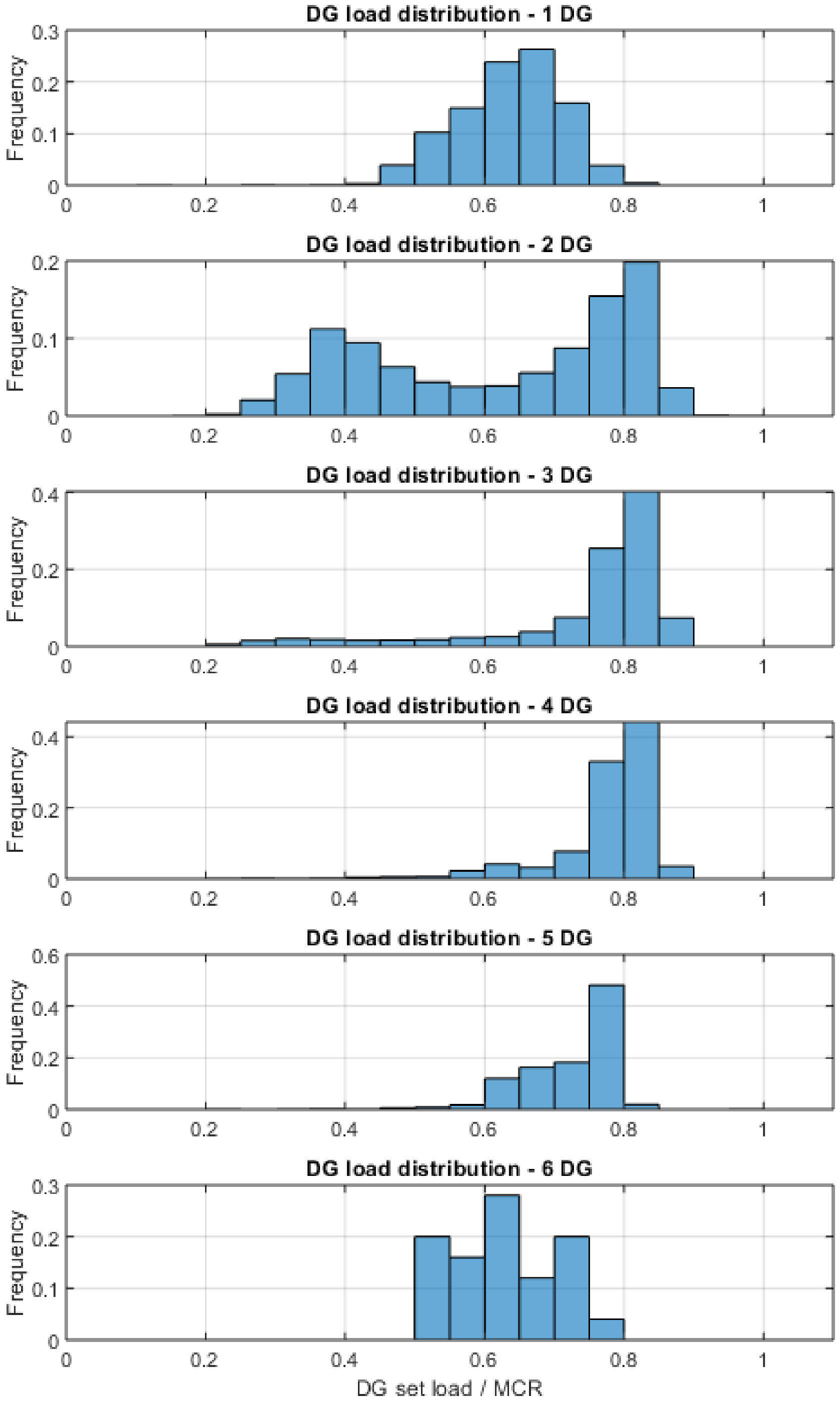


Figure E. 1 DG load frequency distribution for general operating mode for investigated system No1 and No2.

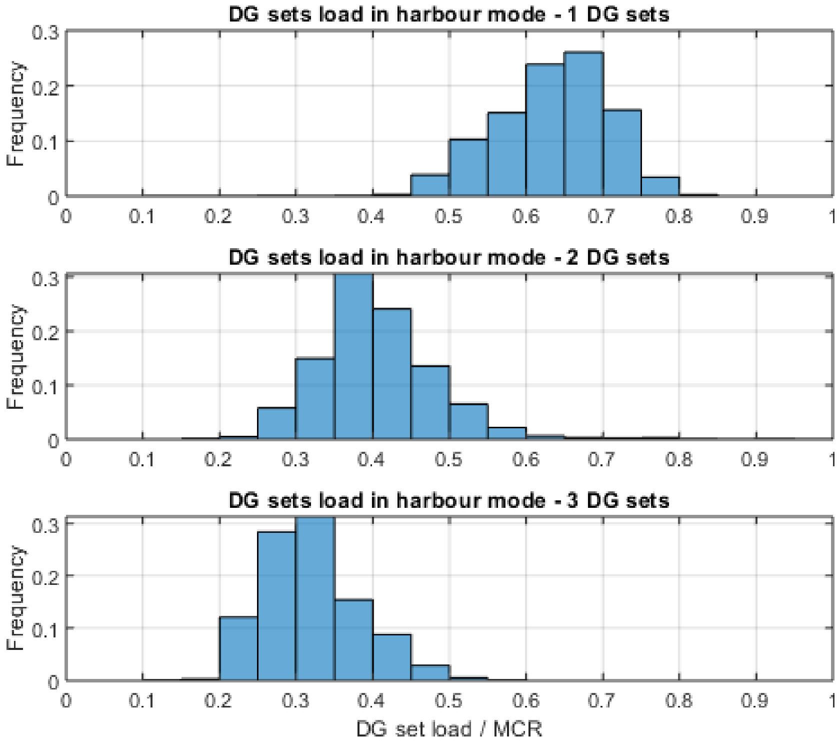


Figure E. 3 DG load frequency distribution for harbour operating mode for investigated system No1.

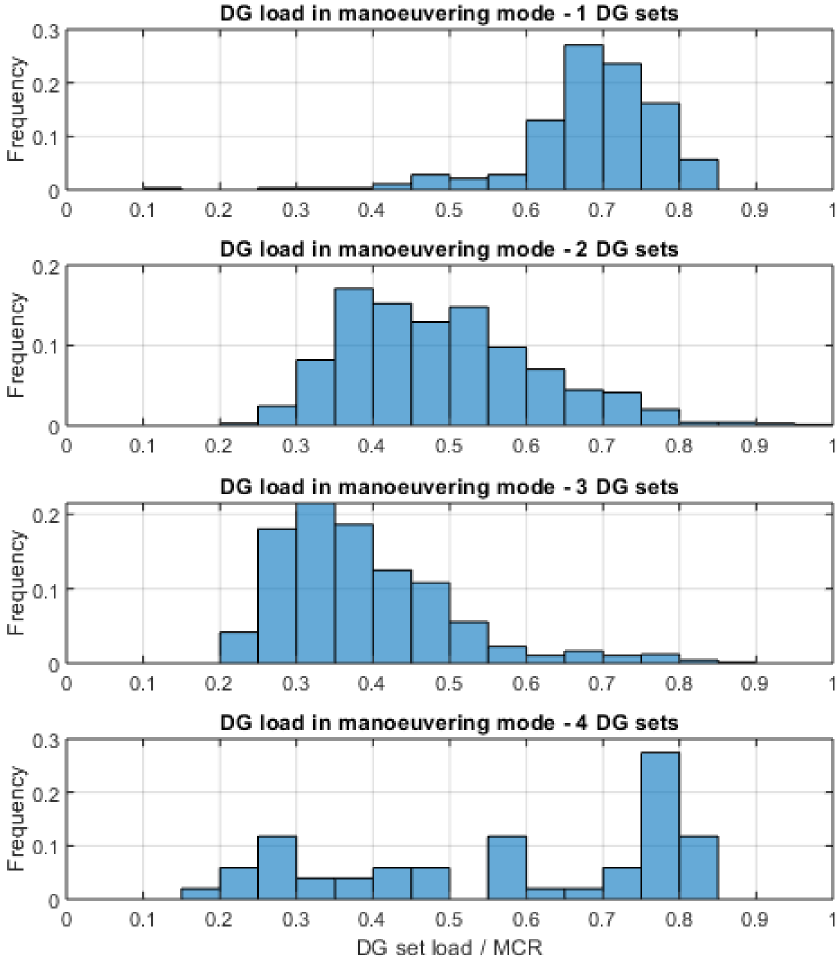


Figure E. 2 DG load frequency distribution for manoeuvering operating mode for investigated system No1.

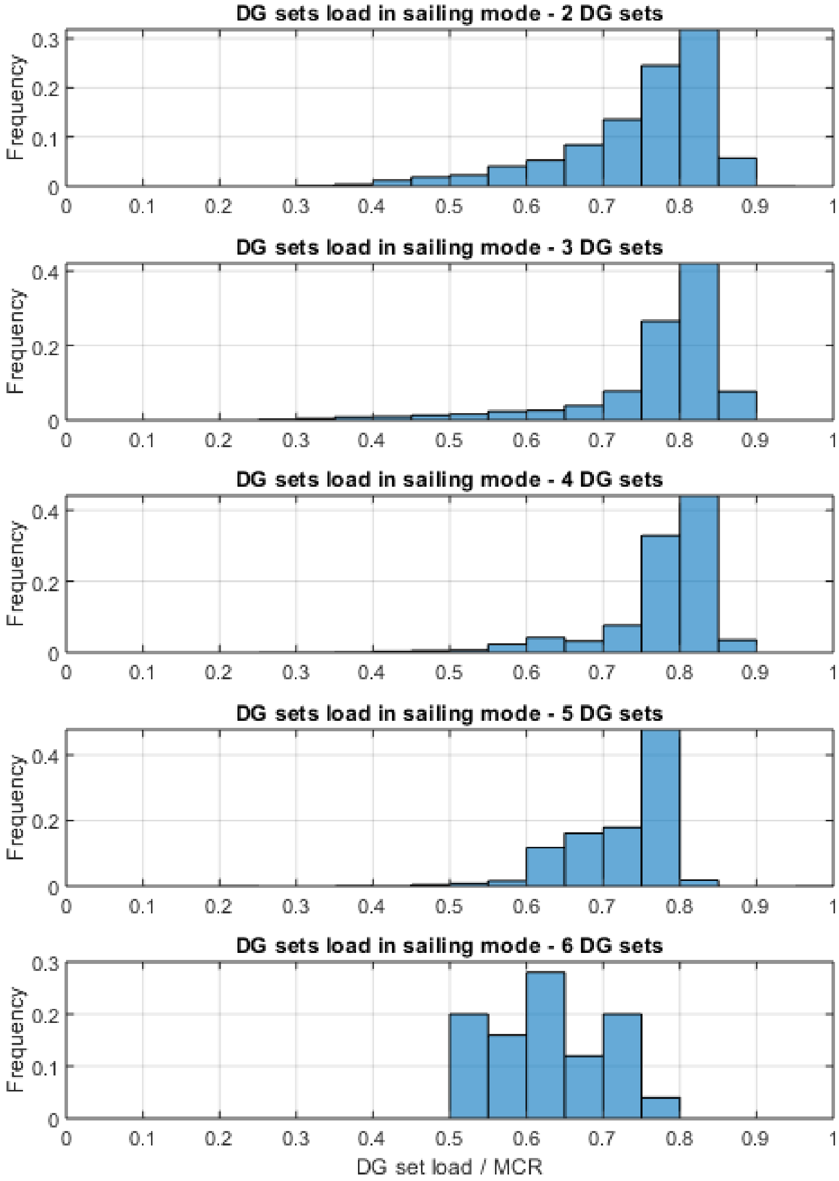


Figure E. 4 DG load frequency distribution for sailing operating mode for investigated system No1.

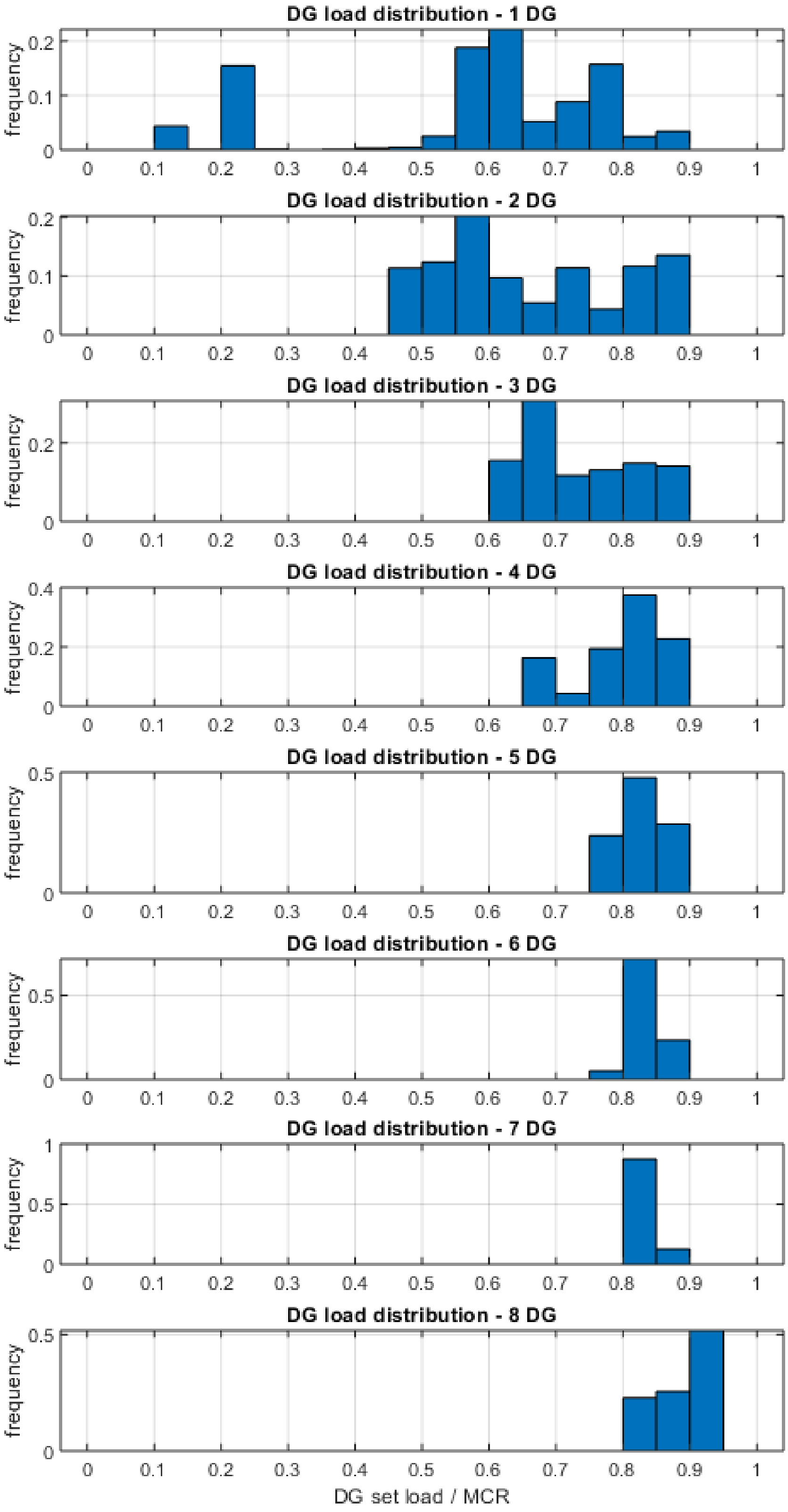


Figure E. 6 DG load frequency distribution for general operating mode for investigated system No4.

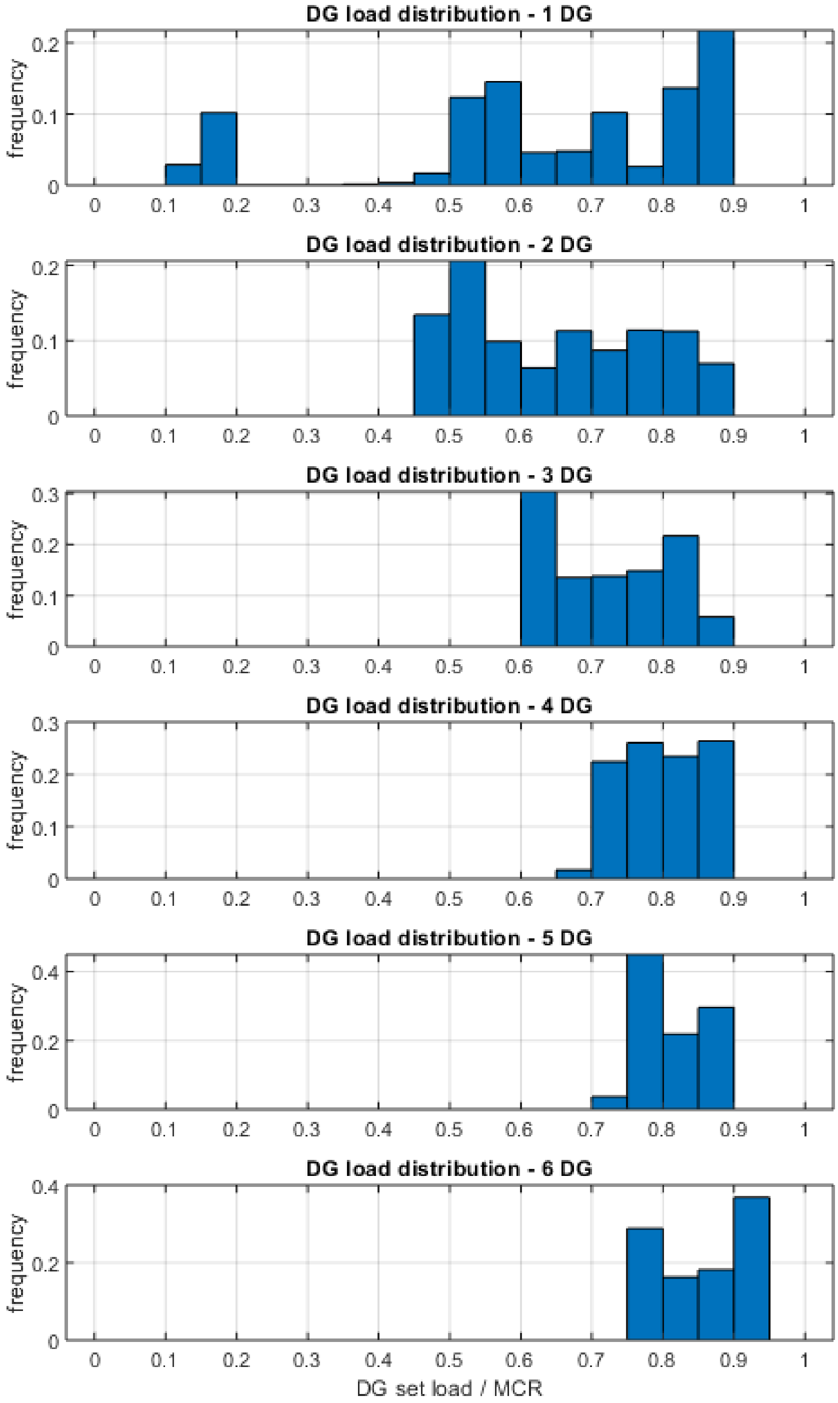


Figure E. 7 DG load frequency distribution for general operating mode for investigated system No5.

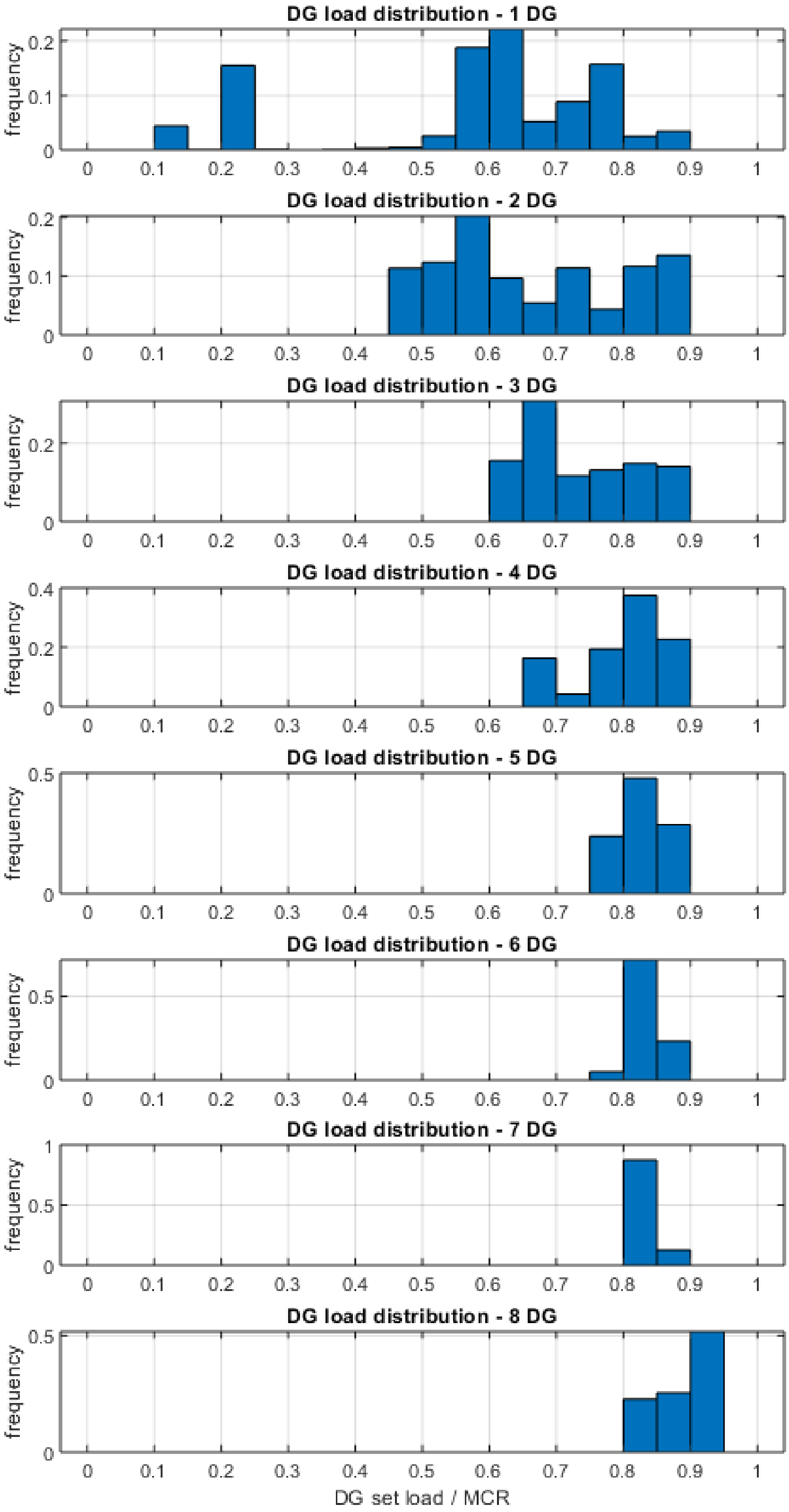


Figure E. 8 DG load frequency distribution for general operating mode for investigated system No6.

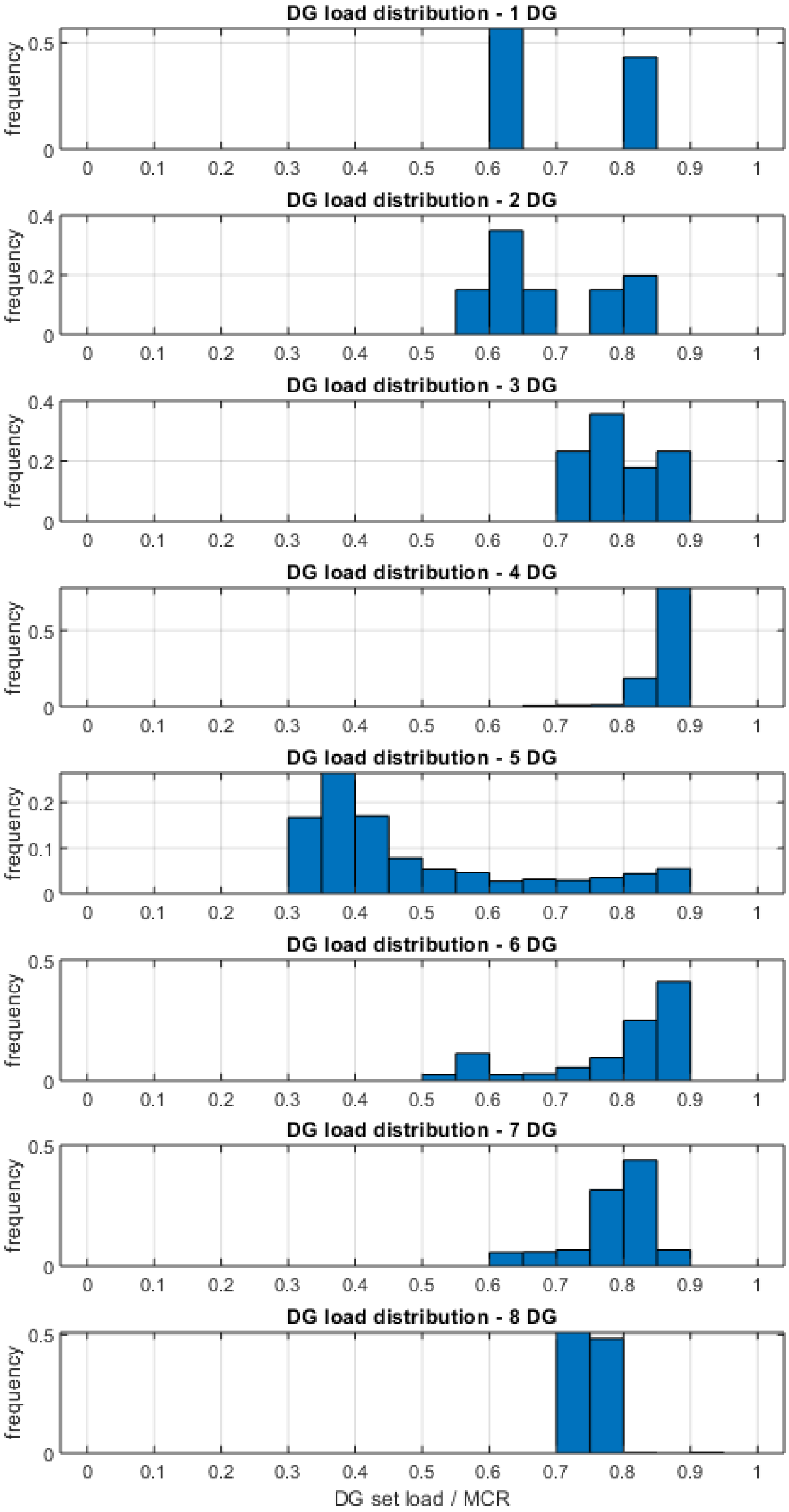


Figure E. 9 DG load frequency distribution for general operating mode for investigated system No7.

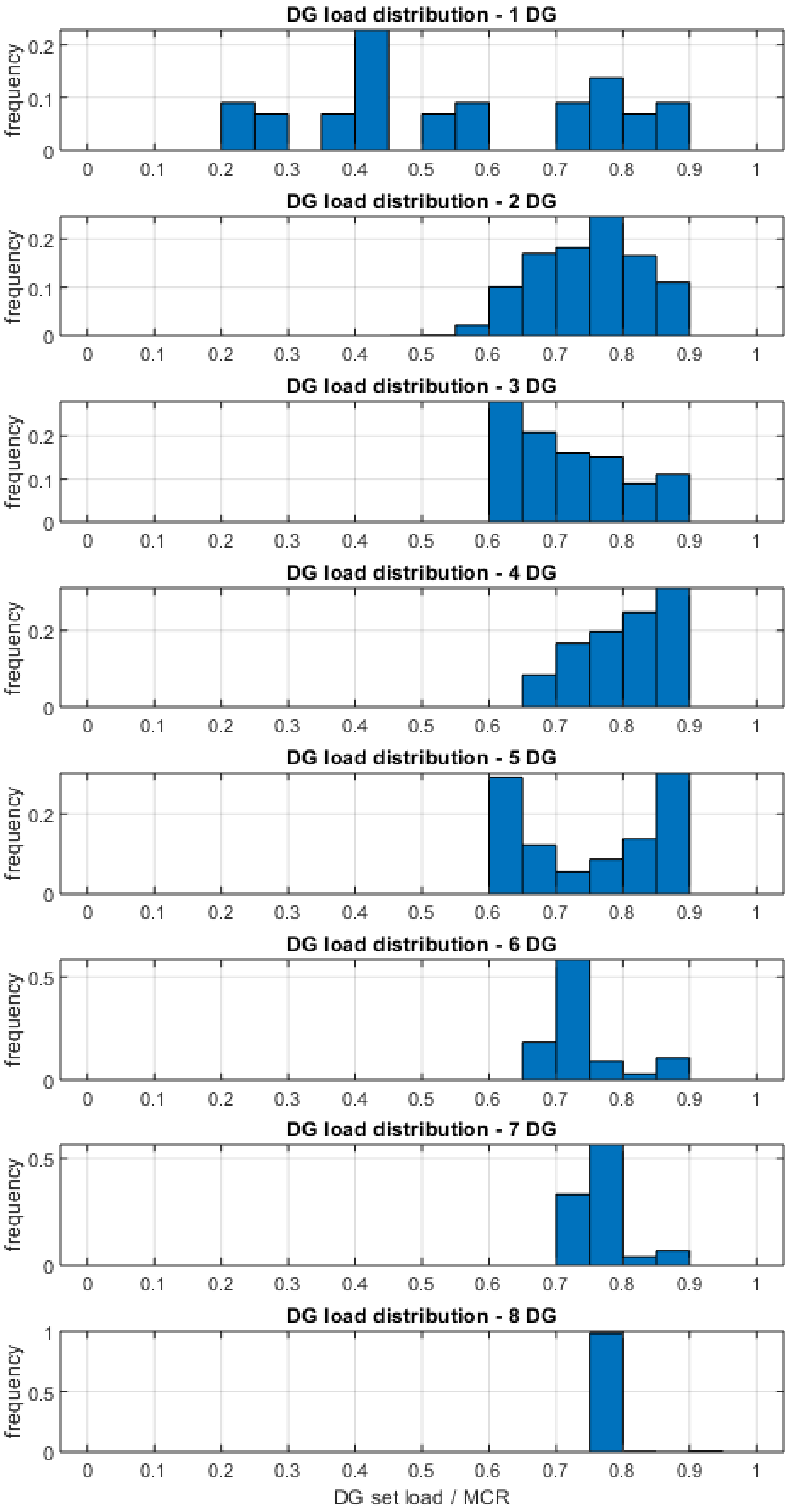


Figure E. 10 DG load frequency distribution for general operating mode for investigated system No8.

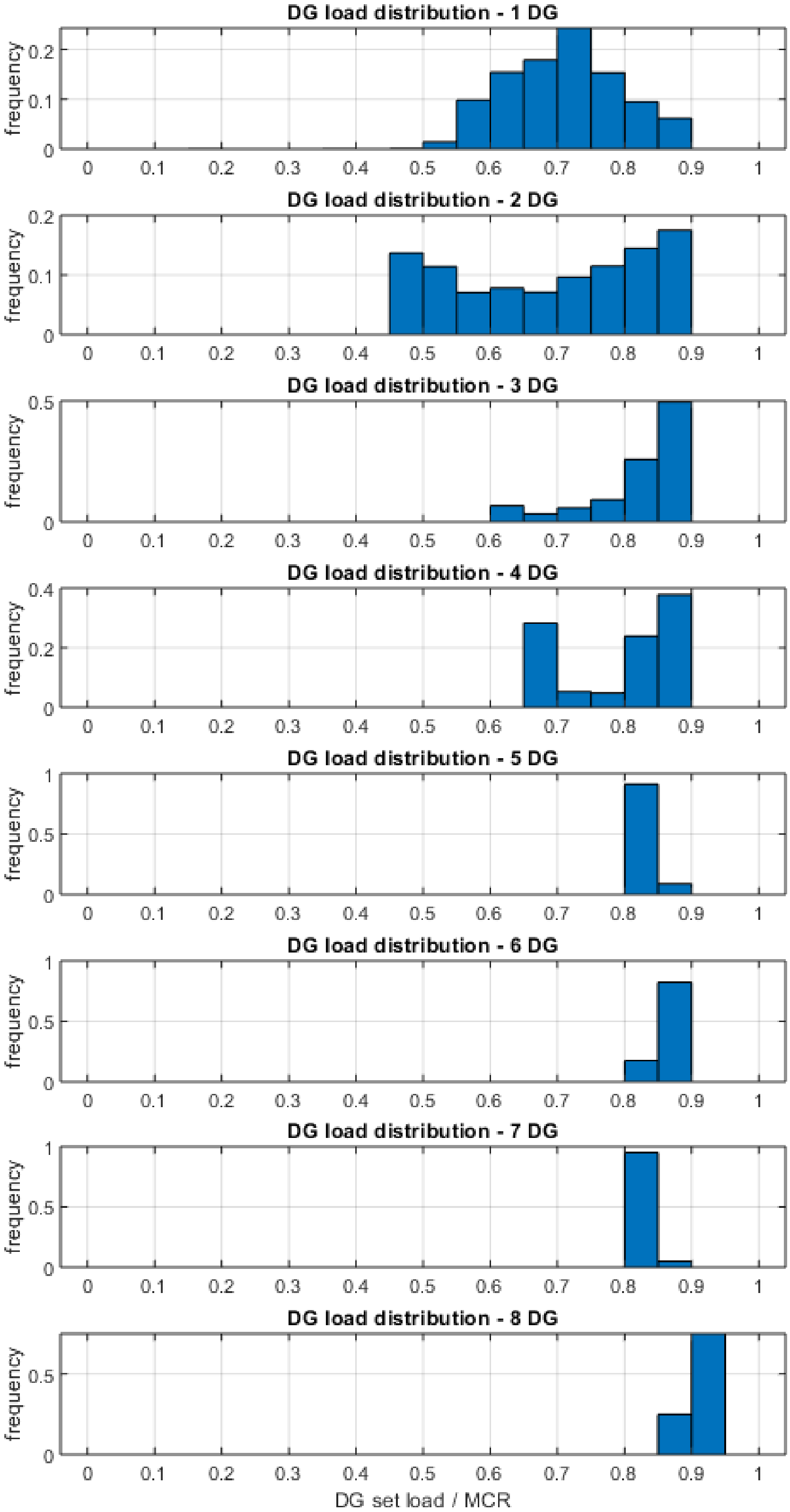


Figure E. 11 DG load frequency distribution for general operating mode for investigated system No9.

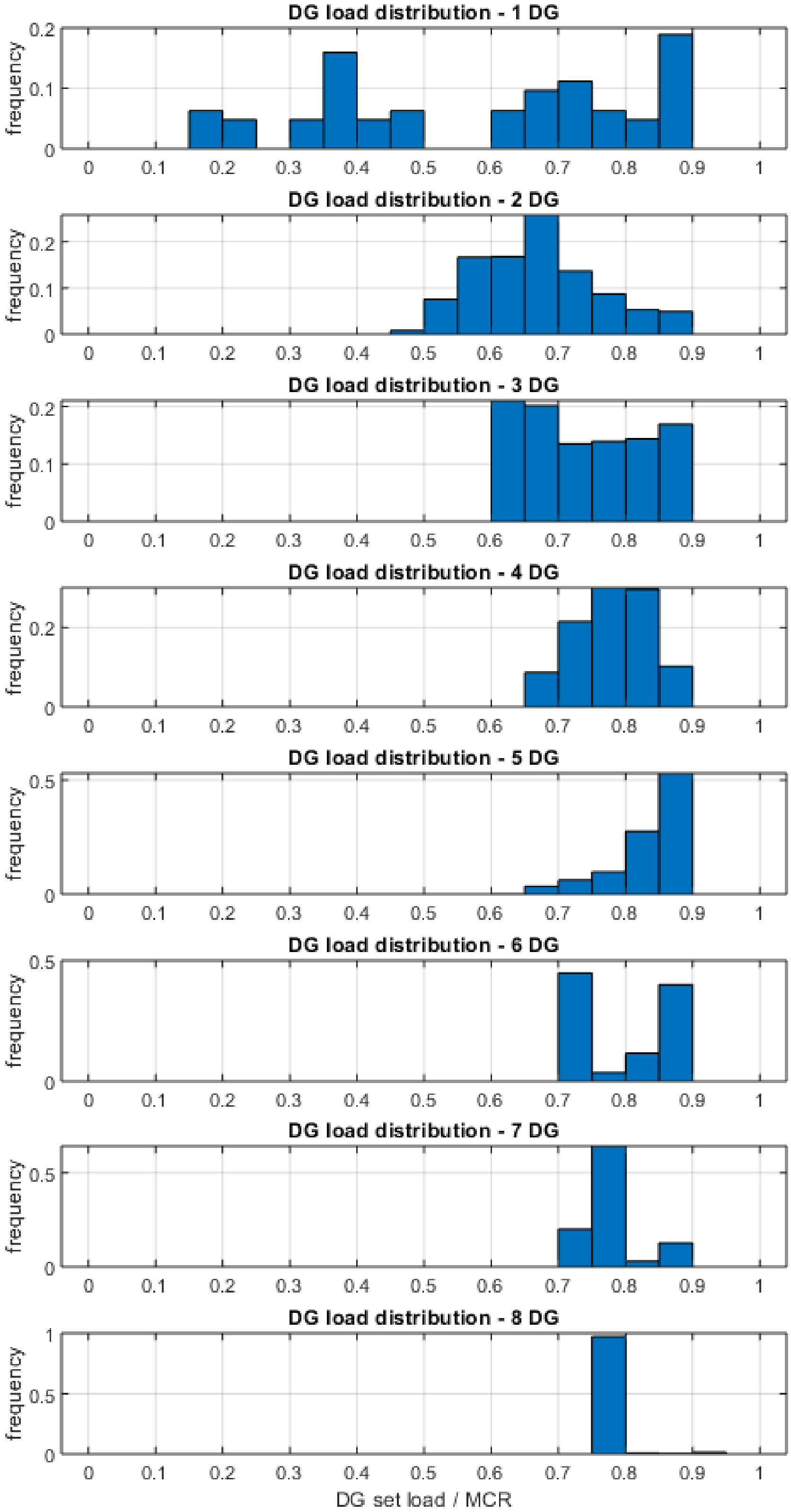


Figure E. 12 DG load frequency distribution for general operating mode for investigated system No10.

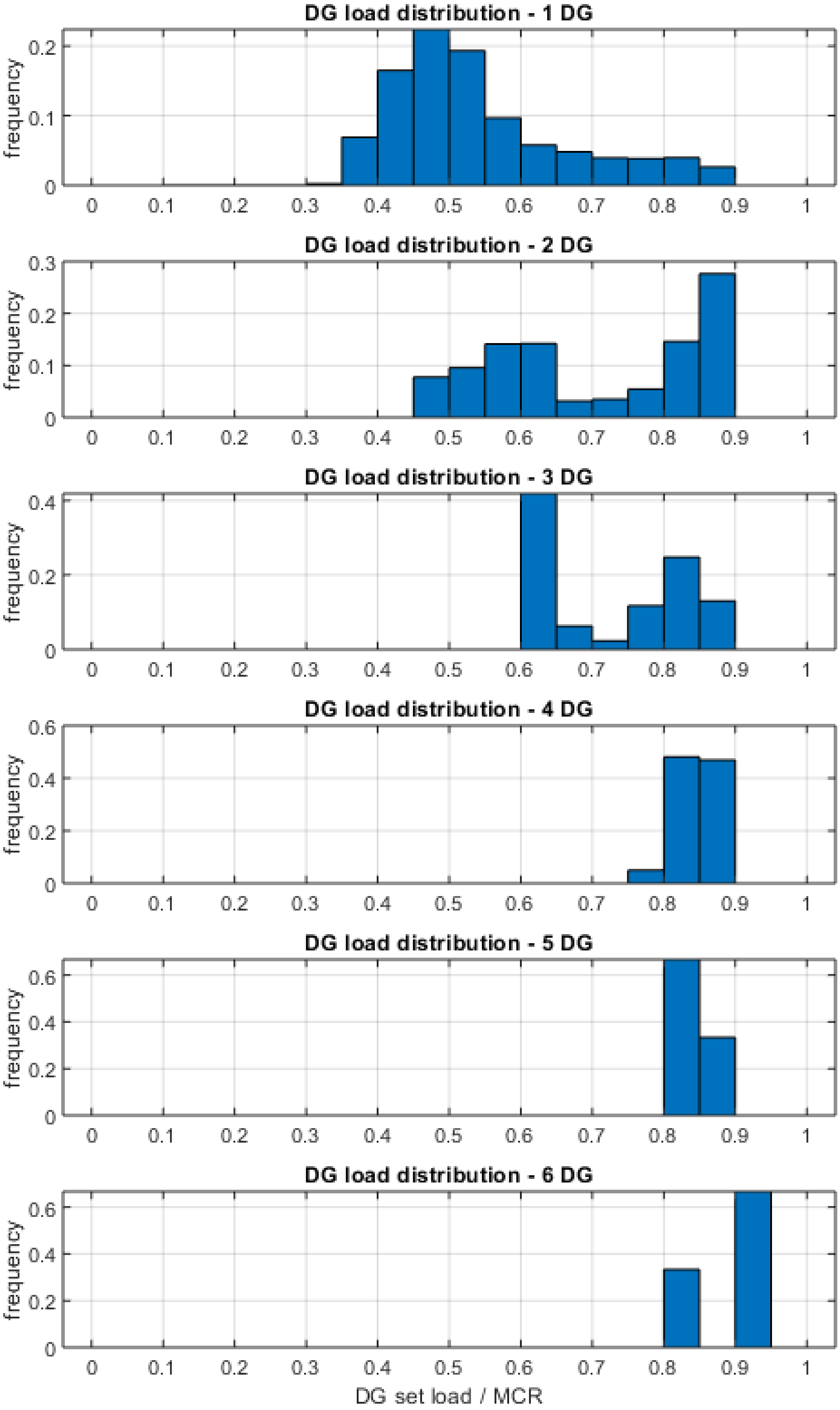


Figure E. 13 DG load frequency distribution for general operating mode for investigated system No11.

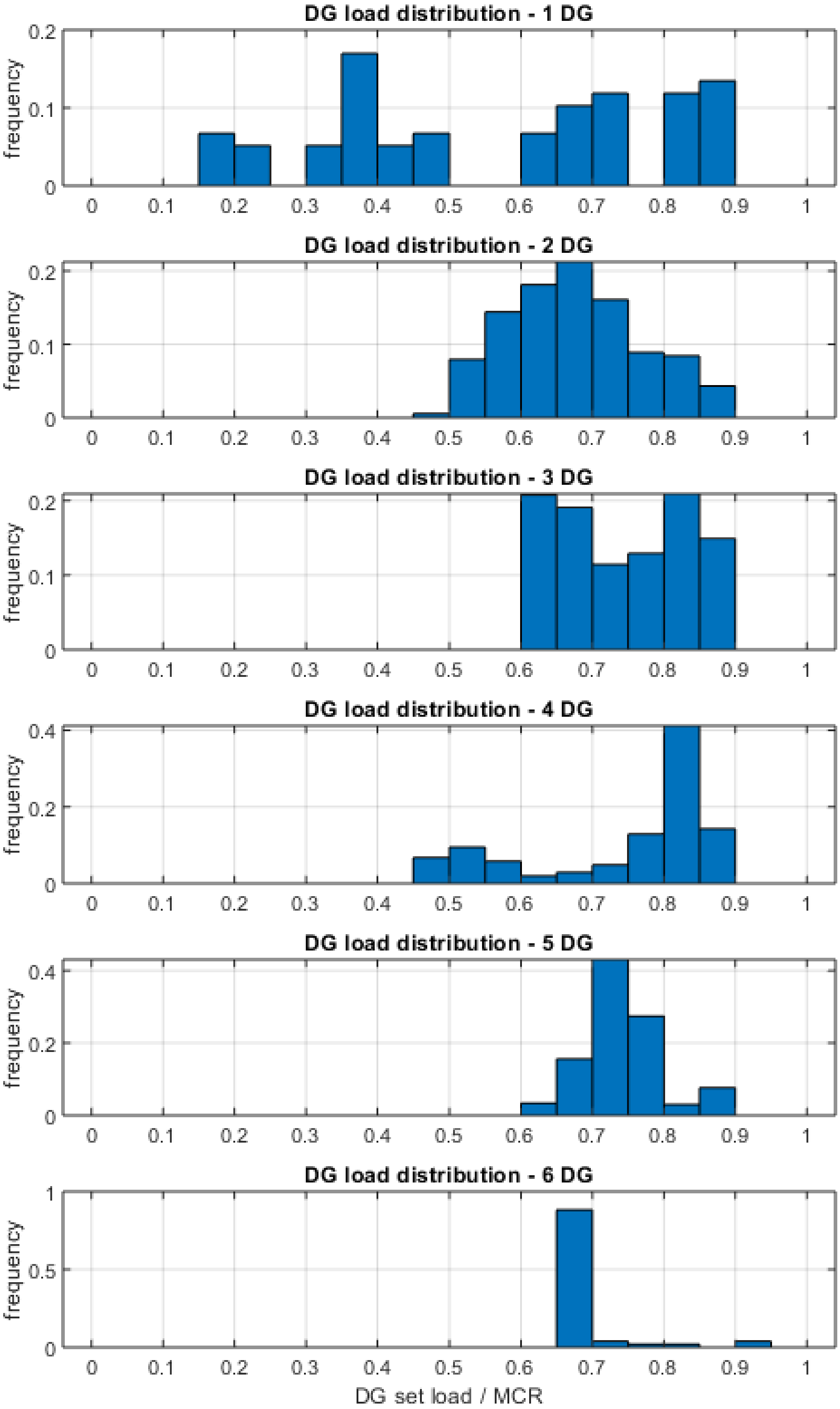


Figure E. 14 DG load frequency distribution for general operating mode for investigated system No12.

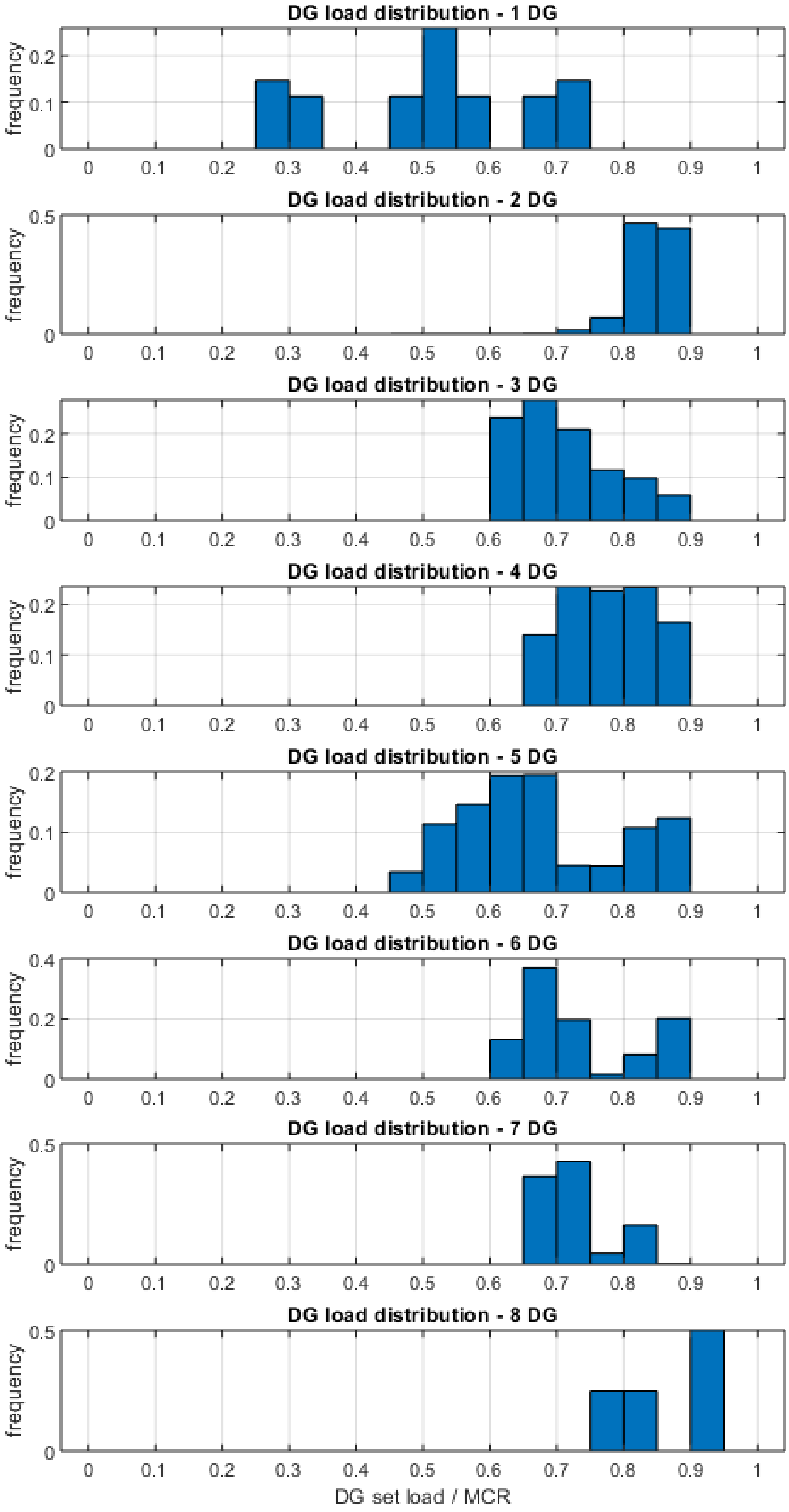


Figure E. 15 DG load frequency distribution for general operating mode for investigated system No13.

This page has been intentionally left blank

APPENDIX F MAINTENANCE ACTIVITIES

The maintenance intervals and duration used as input are provided in Table F. 1-2.

Table F. 1 Inspection/maintenance intervals.

a/a	Description of maintenance activities	MI*	Units	Source
1	Annual inspection and testing of circuit breakers	8760	hours	Assumption
2	5-year testing of arc protection system	43800	hours	Actual data
3	Test of safety system	1000	hours	(Yanmar, 2013, Wartsila, 1999)
4	Over speed test	2000	hours	(Yanmar, 2013, Wartsila, 1999)
5	Test of thrust/main bearings	18000	hours	(Yanmar, 2013, Wartsila, 1999)
6	Test of internal cooling system of main engine	50	hours	(Yanmar, 2013, Wartsila, 1999)
7	Test of air filters	1000	hours	(Yanmar, 2013, Wartsila, 1999)
8	Test of oil pump	500	hours	(Yanmar, 2013, Wartsila, 1999)
9	Test/inspection of exhaust valves	6000	hours	(Yanmar, 2013, Wartsila, 1999)
10	Inspection for excessive fuel/oil leakages	50	hours	(Yanmar, 2013, Wartsila, 1999)
11	Inspection for turbo charger	12000	hours	(Yanmar, 2013, Wartsila, 1999)
12	Inspection for injection valves	3000	hours	(Yanmar, 2013, Wartsila, 1999)
13	Inspection interval for disconnected engine	168	hours	(Yanmar, 2013, Wartsila, 1999)
14	Test of control functions of engine systems	1000	hours	(Yanmar, 2013, Wartsila, 1999)
15	Operating time of an engine	20	hours	Actual data
16	Maintenance interval for propulsion units	4380	hours	Assumption
17	Inspection interval for water coolers	1000	hours	(Yanmar, 2013, Wartsila, 1999)
18	Maintenance of engine every 2000 hours	2000	hours	(Yanmar, 2013, Wartsila, 1999)
19	Maintenance of engine every 3000 hours	3000	hours	(Yanmar, 2013, Wartsila, 1999)
20	Maintenance of engine every 4000 hours	4000	hours	(Yanmar, 2013, Wartsila, 1999)
21	Maintenance of engine every 6000 hours	6000	hours	(Yanmar, 2013, Wartsila, 1999)
22	Maintenance of engine every 12000 hours	12000	hours	(Yanmar, 2013, Wartsila, 1999)
23	Inspection interval for fuel filters	50	hours	(Yanmar, 2013, Wartsila, 1999)
24	Inspection interval for emergency fuel pump	720	hours	Assumption of monthly inspection period
25	Inspection interval for sea chests	4320	hours	According to Planned Maintenance System of other companies
26	Inspection interval for governor	250	hours	(Yanmar, 2013, Wartsila, 1999)
27	Inspection interval for AVR	250	hours	(Yanmar, 2013, Wartsila, 1999)
28	Inspection interval for heavy fuel supply pump	500	hours	(Mennis and Platis, 2013)
29	Inspection interval for heavy fuel filter	500	hours	(Mennis and Platis, 2013)
30	Inspection interval for heavy fuel oil heater	500	hours	(Mennis and Platis, 2013)
31	Inspection interval for heavy fuel booster pump	500	hours	(Mennis and Platis, 2013)
32	Inspection interval for methanol supply pump	500	hours	Assumption that it is the same for heavy fuel
33	Inspection interval for methanol circulating pump	500	hours	Assumption that it is the same for heavy fuel

*MI=Maintenance and testing intervals

Table F. 2 Maintenance activities duration.

a/a	Description of maintenance activities	MD*	Units	Source
1	Maintenance of engine every 2000 hours	3	hours	Actual data (based on actual maintenance data)
2	Maintenance of engine every 3000 hours	3	hours	Actual data (based on actual maintenance data)
3	Maintenance of engine every 4000 hours	3	hours	Actual data (based on actual maintenance data)
4	Maintenance of engine every 6000 hours	7	hours	Actual data (based on actual maintenance data)
5	Maintenance of engine every 12000 hours	15	hours	Actual data (based on actual maintenance data)
6	Maintenance of hardware	20	hours	Assumption
7	Maintenance of communication lines	20	hours	Assumption
8	Maintenance of current sensors	1	hours	Assumption
9	Maintenance of voltage sensors	1	hours	Assumption
10	Maintenance of frequency sensors	1	hours	Assumption
11	Maintenance of propulsion unit load sensors	1	hours	Assumption
12	Maintenance of propulsion unit speed sensors	1	hours	Assumption
13	Maintenance of engine safety sensors	1	hours	Assumption
14	Maintenance of circuit breakers	10	hours	(Reddy *et al.*, 2016)
15	Maintenance of failures in ME	15	hours	(OREDA, 2015)
16	Maintenance of critical failures in ME	234	hours	(OREDA, 2015)
17	Maintenance of fuel system	3	hours	(Mennis and Platis, 2013)
18	Maintenance of sea chest	2	hours	(Allal *et al.*, 2017)

MD*=Maintenance duration

APPENDIX G STPA RESULTS

The list of identified UCAs for the different investigated systems is provided in Table G.1. The different sub hazards numbers (provided in brackets) are elaborated in the section 7.2.1 of the present thesis.

Table G.1 List of Unsafe Control Actions identified for different systems

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
1	Connect (PMS to Bus-Tie Controller)		Order to connect to a section when there is an uncontrolled electrical fault will cause the transfer of disturbances and instability to the rest of the network.		
			[H-5] – UCA 1.1		
2	Disconnect (PMS to Bus-Tie Controller)	If the faulty section of the power network is not disconnected, the problems will be transferred to the rest of the power network.	Disconnection of the section, when the power generation is in one and the power demand is in the other will cause overload in the section with high power demand. This will result in temporal unavailability of DG sets as well.		
		[H-2][H-5] – UCA 1.2	[H-1][H-3] – UCA 1.3		

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
3	Tripping of heavy consumers (PMS to protection relays)	Not tripping of heavy consumers, when an overload occurs will result in blackout due to overload.		Tripping of heavy consumers with delay, when an overload occurs, may result in tripping of DG sets due to overload.	
		[H-3] – UCA 1.4		[H-3] – UCA 1.5	
4	Start DG (PMS to DG controllers)	If the order to start a DG set is not given when there is a request for higher power production and the power demand is on increase will result in overload.	Giving an order to start a faulty DG set will cause disturbances to the network or failure to connect a DG set to the network.	A delayed order to start a DG set when there is a faulty DG set connected to the power network will cause a delay in change over and potential sudden loss of a DG set.	
		[H-3] – UCA 1.6	[H-2][H-3] – UCA 1.7	[H-3] – UCA 1.8	
		Not starting a DG set, when a fault is observed in a DG set, will result in a loss of a DG set and potential overload.	Trying to turn on an already running DG set, when a connected DG set is faulty, may result in overload due to disconnection of DG set by safety functions.	A delayed order to start a DG set, when there is a request for higher power production and the power demand is on increase will result in overload.	
		[H-3] – UCA 1.9	[H-3] – UCA 1.10	[H-3] – UCA 1.11	

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
5	Stop DG (PMS to DG controllers)		Stopping a DG set when there is high power demand may result in overload.		
			[H-3] – UCA 1.12		
6	Increase the load of DG set (PMS to DG controller)	Not increasing a load of a DG set, when it is lower than the other DG set load, will result in uneven load sharing and potential loss of a DG set or total blackout.	Increasing the load of a DG set, when the load is already high may result in loss of a DG set and overload. This will also cause unequal load sharing, which if remains uncontrolled will result in blackout.		
		[H-2][H-3] – UCA 1.13	[H-2][H-3] – UCA 1.14		
7	Decrease the load of DG set (PMS to DG controller)	Not decreasing the load of a DG set when in equal will result in unequal load sharing and potential tripping of DG sets.	Decreasing the load of a DG set, when there is already high load, may result in overload of other DG sets. It may also result in in equal load sharing and false tripping.		
		[H-2][H-3] – UCA 1.15	[H-2][H-3] – UCA 1.16		
8	Reduce the load (PMS to propulsion motors)	Not reducing the load of propulsion motors, when an	Reducing too quickly the power demand when stopping the propulsion motors or at	If the order to reduce the necessary power comes too late, when an overload occurs, it may	

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
		overload occurs, will cause blackout due to overload.	emergency condition will cause transient in the network.	result in blackout due to overload.	
		[H-3] – UCA 1.17	[H-4] – UCA 1.18	[H-3] – UCA 1.19	
9	Start (DG controller to engine and auxiliaries)	If the order to start the DG set is not provided, when the DEP system is going to state of higher power demand, then an DG overload may occur.		If the DG controller doesn't follow the appropriate starting sequence, when the system is going to state of higher power demand, it will result in failure to start a DG set and potential DG sets overload.	If the system continues giving starting order, when there is a failure in the system it will deplete the available quantity of pressurised air and may delay the starting of other DG sets in this way leading to potential DG sets overload conditions.
		[H-3] – UCA 1.20		[H-3] – UCA 1.21	[H-1][H-3] – UCA 1.22
10	Synchronisation to network (DG controller to DG circuit breaker)	If an order to synchronize a DG set is not provided, when the system is going to state of higher power demand, then a DG sets overload may occur.		The connection to the network should be done at proper time. If the synchronization is not properly done, then power network instability can be created and resulting in delay in connection of DG set to the network.	If synchronisation lasts for too long, it will delay the addition of the DG set to the network with possibility to cause overload when the system is going to the state of higher load.
		[H-3] – UCA 1.23		[H-3][H-4] – UCA 1.24	[H-3] – UCA 1.25

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
				Synchronization of the DG set, when the engine has not reached its full power yet, may result in reverse power generation and tripping of the DG set. As a result the connection to the network will be failed, a transient will be caused and a DG sets overload may occur.	
				[H-3][H-4] – UCA 1.26	
11	Increase RPM reference (DG to governor)	Not increasing the RPM reference during a DG set starting procedure will lead to failure to connect a DG set.	Increasing the RPM reference during a DG set starting procedure too quickly will lead to failure to connect a DG set.		Not increasing the RPM reference during a DG set starting procedure will lead to failure to connect a DG set.
		[H-3] – UCA 1.27	[H-3] – UCA 1.28		[H-3] – UCA 1.29
12	Decrease RPM reference (DG to governor)		Decreasing the load too abruptly during stopping procedures may lead to inappropriate transient and load sharing abnormalities.		
			[H-4] – UCA 1.30		

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
13	Increase fuel flow (Governor to actuator)	Not increasing fuel flow, when there is a demand for significantly higher load (transient coming from consumers) will result in tripping of the DG engine due to overload. When the power demand is high it may result in overload.	Increasing fuel flow, when there is no increase in power demand will result in unequal load sharing.	Increasing fuel flow too slow under conditions of increased power demand will result in temporal unequal load sharing.	
		[H-3] – UCA 1.31	[H-2] – UCA 1.32	[H-2] – UCA 1.33	
		Not increasing fuel flow, when there is a small increase in power demand will result in unequal DG sets loading.			
		[H-2] – UCA 1.34			
14	Decrease fuel flow (Governor to actuator)	Not decreasing fuel flow, during transient (observed during loss of large consumer such as an Azipod propulsion motor) may result in tripping of the DG engine due to overvoltage/overspeed. When	Decreasing the fuel flow under normal conditions will result in unequal loading sharing between DG sets.	Decreasing the fuel flow too slow will result in a temporal unequal load sharing.	

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
		the power demand is high it may result in the DG sets overload due to tripping.			
		[H-3] – UCA 1.35	[H-2] – UCA 1.36	[H-3] – UCA 1.37	
		Not decreasing fuel flow, when there is a small decrease in power demand, will result in unequal load sharing among DG sets.			
		[H-2] – UCA 1.38			
15	Increase excitation current (AVR to actuator)	Not increasing excitation current, during transient, will result in tripping of the DG set, which may lead to DG sets overload.	Increasing excitation current under normal conditions will result in unequal load sharing among DG sets.	Increasing excitation current with delay during transient may result in tripping of the DG set and subsequent overload.	
		[H-3] – UCA 1.39	[H-2] – UCA 1.40	[H-3] – UCA 1.41	
		Not increasing excitation current, when there is a small increase in power demand will result in unequal loading among DG sets.			

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
		[H-2] – UCA 1.42			
16	Reduce excitation current (AVR to actuator)	Not decreasing excitation current during transient (owed to a loss of big consumer such as Azipod propulsion motors), will result in tripping of the DG set, which may lead to overload.	Decreasing excitation current under normal conditions will result in unequal load sharing.	Decreasing of excitation current with delay during transient may result in tripping of the DG set and subsequent overload.	
		[H-3] – UCA 1.43	[H-4] – UCA 1.44	[H-3] – UCA 1.45	
		Not decreasing excitation current, when there is a small decrease in power demand will result in unequal load sharing among DG sets.			
		[H-2] – UCA 1.46			
17	Switch off the engine (Engine safety to DG set)	Not switching off the DG set, when faulty will cause the unavailability of DG for longer period of time.	Switching off a DG set, when faulty or healthy will reduce abruptly the available power in network and an overload may occur.		
		[H-1] – UCA 1.47	[H-3] – UCA 1.48		

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
			Fast disconnection of a DG set, when faulty or healthy, will result in a quick reduction of power and transient.		
			[H-4] – UCA 1.49		
18	Connect a DG set (Engine safety to Power Management System)	If order to connect DG set is not given, the safety function will not switch off the defective engine early. As a result, higher damage will be incurred and the DG safety finally will cause tripping of the DG set without additional DG set allocated to the ship power network.		A delay in connecting a DG set will result in delay of implementation of other steps and consequently slower allocation of power generation to the network and tripping of the DG set. When the system is going to the state of higher power demand, it might cause the DG sets overload. It will also incur higher damage to the DG set with result a DG set being unavailable for longer time.	
		[H-1][H-3] – UCA 1.50		[H-1][H-3] – UCA 1.51	
19	Reduce load of a DG set (Engine safety to Power Management System)	Not reducing the load of a DG when faulty will cause damages		Reducing the load of a DG when connected will cause unequal load sharing.	

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
	(This control action is not applicable to the DEP)	to the system and lower DG set availability.			
		[H-1] – UCA 1.52		[H-2] – UCA 1.53	
20	Trip the DG set (Generator safety to Circuit Breaker)	Not tripping a DG set, when faulty may cause greater damage to the DG set.	Disconnecting a DG set, when faulty or healthy during high power demand may result in DG sets overload.		
		[H-1] – UCA 1.54	[H-3] – UCA 1.55		
21	Trip the DG set (Intelligent diagnosis to Circuit Breaker)		Disconnecting a DG set, when healthy or faulty might cause overload if the power demand is high.	Disconnecting a faulty DG set, before the necessary healthy DG set is allocated when the power demand is high may result in overload of DG sets.	
			[H-3] – UCA 1.56	[H-3] – UCA 1.57	
22	Connect DG (Intelligent diagnosis to PMS)	If the order to connect a DG set is not provided during faulty conditions, a DG set might be tripped and when the power demand is high this will result in overload of connected DG sets.		Delay to give order to connect a DG set may result in tripping of a faulty DG set and when the power demand is high this might result in overload of the connected DG sets.	
		[H-3] – UCA 1.58		[H-3] – UCA 1.59	

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
23	Trip command (Intelligent diagnosis to Circuit Breaker Controller)	Not tripping of faulty section of the ship power network may result in propagation of network instability due to unbalanced power generation to the rest of power network.	Tripping, when there is low power generation in one network section and high-power generation in another network section will cause overload in one power section and partial blackout.		
		[H-2] – UCA 1.60	[H-3] – UCA 1.61		
24	Connect Bus-Tie Breaker (Circuit Breaker Controller to Bus-Tie Breaker)			If the control action is provided when the proper synchronizing conditions have not been ensured, it will cause instability and transients in the network.	
				[H-4] – UCA 1.62	
25	Disconnect Bus-Tie Breaker (Circuit Breaker Controller to Bus-Tie Breaker)	Failure to disconnect the bus-tie breaker during electrical fault, will facilitate the transfer of disturbances from one faulty network section to a healthy network section.			
		[H-2] [H-5] – UCA 1.63			

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
26	Trip command (Arc Detection to protection relays)	If tripping is not provided when arc is present, then catastrophic failure in switchboards will occur, which will impair the ability to connect DG sets to the network. It will cause transients and loss of DG sets connected to the network with a potential DG sets overload.	Tripping of switchboard under normal conditions will cause drop in power generation and transients.		
		[H-1][H-3][H-4] – UCA 1.64	[H-3][H-4] – UCA 1.65		
27	Trip command (Arc Detection to Circuit Breaker Controller)	Not tripping of bus-tie breaker, when there is a fault in the switchboard may result in blackout due to transfer of transients.	Tripping, when there is low power generation in one power network section and high power generation in another power network section will cause overload in one power section and partial blackout.		
		[H-4] – UCA 1.66	[H-3] – UCA 1.67		

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
28	Trip command (Protection Relay to Circuit Breaker)	If not provided, it will allow the transfer of short circuit to the rest of the network and consequent cascading tripping of the DGs due to DG sets overload.	Tripping, when there is low power generation in one power network section and high-power generation in another power network section might cause overload in a section and partial blackout.		
		[H-5] – UCA 1.68	[H-3] – UCA 1.69		
29	Trip command (Application controller to Circuit Breaker)		If tripping of propulsion unit is provided, when either faulty or healthy, a sudden drop in consumed power will result in transients in the ship power network.		
			[H-4] – UCA 1.70		
30	Increase output (Application Controller to Drive Controller)		If the limiting rate for power increase in propulsion motors is inappropriate, then the power increase may be too fast leading to tripping of the engines due to under frequency/under voltage.		

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
			[H-4] – UCA 1.71		
			Increasing power demand, when inadequate number of DG sets is allocated, (failure of limiting function) will result in the connected DG sets overload.		
			[H-3] – UCA 1.72		
31	Decrease output (Application Controller to Drive Controller)	Not decreasing output, when there is insufficient power generating capacity available, will result in overload.	Decreasing too quickly the speed during emergency will cause electrical transients in the network.	Decreasing the output too late, during overload, may result in blackout due to overload of connected DG sets in the ship power system.	
		[H-3] – UCA 1.73	[H-4] – UCA 1.74	[H-3] – UCA 1.75	
32	Increase speed (Drive Controller to Thyristor Bridge)		If the power increase limiting rate is set inappropriately, then the power increase may be too fast leading to tripping of the connected DG sets due under frequency / under voltage.		
			[H-4] – UCA 1.76		
			Increasing power demand, when inadequate number of DG sets is		

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
			connected to the power network (failure of limiting function) will result in the connected DG sets overload.		
			[H-3] – UCA 1.77		
33	Decrease speed (Drive Controller to Thyristor Bridge)	Not decreasing output, when there is insufficient power generation capacity is available, might result in DG sets overload.	Decreasing too quickly the speed during emergency will cause electrical transient in the power network.	Decreasing output too late, if inadequate power generating capacity is available, may result in the connected DG sets overload.	
		[H-3] – UCA 1.78	[H-4] – UCA 1.79	[H-3] – UCA 1.80	
34	Disconnect (Battery Management System to Batteries)	Not disconnecting batteries when the batteries are faulty, will lead to higher unavailability of batteries due to damage	Disconnecting batteries during charging and healthy conditions will lead to unnecessary batteries unavailability.	Disconnecting batteries with delay when the batteries are faulty, will lead to higher unavailability of batteries due to damage	
		[H-1] – UCA 1.81	[H-1] – UCA 1.82	[H-1] – UCA 1.83	
			Disconnecting batteries when the batteries are providing to the network and healthy conditions will lead to unnecessary batteries		

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
			unavailability and potential DG sets overload.		
			[H-1] [H-3] – UCA 1.84		
35	Charge (receive electrical power from the ship power network) (Battery Management System to Batteries)	Not charging healthy batteries when relevant power generation capacity is available will lead to higher batteries unavailability.	Charging batteries, when they are faulty may lead to higher unavailability of batteries.		
		[H-1] – UCA 1.85	[H-1] – UCA 1.86		
			Charging batteries, when the relevant capacity on batteries is not available (overcharge) may lead to higher unavailability of batteries.		
			[H-1] – UCA 1.87		
			Charging batteries, when the relevant generating capacity is not available (overcharge) may result in connected DG sets overload.		
			[H-1] – UCA 1.88		

a/a	Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long causes hazard
36	Discharge (provide electrical power to the ship power network) (Battery Management System to Batteries)	Not discharging batteries when they have the relevant capacity and healthy will result in their unavailability during ship operations.	Discharging faulty batteries, may lead to their greater damage.	Discharging batteries with delay when they have the relevant capacity and healthy will result in their unavailability during ship operations.	
		[H-1] [H-3]– UCA 1.89	[H-1] – UCA 1.90	[H-1] [H-3]– UCA 1.91	
37	Reconfigure to another system (PMS to fuel system)	Not reconfiguring to another fuel system, when a fault is present in the fuel system will cause loss of fuel supply to a number of DG sets and subsequent DG sets loss with potential overload			
		[H-1] [H-3]– UCA 1.92			

APPENDIX H THE CAUSAL FACTORS FOR UCAS

Tables H1 and H2 of Appendix H list the generic causal factors that were used during the causal factors identification in the 4th step of the CASA method.

Table H1. Causal factors for the provided UCAs.

Scenario description	Causal factors
Inappropriate control input	Missing control input
	Inadequately timed control input
	Provided wrong control input
Missing output (Flawed hardware)	Undiagnosed or on-demand hardware failure
	Undiagnosed or on-demand power supply failure
Flawed control algorithm (Flawed software)	Missing rules
	Wrong rules
	Wrong clock and time schedule
Flawed process model	Missing process variables
	Inconsistency of the process model with the system due to system deterioration
	Inconsistency of the process model with the system due to system modification
	Inconsistency of the process model with the system due to environmental disturbances
	Inconsistency of process model with the system due to the improper representation of mode changes
Flawed process model input	Delays due to measurement delays
	Delays due to communication delays
	Delays due to inadequate integration with other controllers
	Inadequate information transmission due to interferences
	Inadequate information transmission due to noise in sensors
	Inadequate information transmission due to inaccurate measurements
	Inadequate information transmission due to incorrect installation of sensors
	Inadequate information due to communication with other controllers
	Missing information transmission due to communication failures (Hardware open, short circuits, sensor failure and failure in power supply to sensors, failure of other controllers)
	Missing information transmission due to errors in design (Communication bus errors, intermittent faults, incorrect installation of sensors, errors in other controllers)

Table H2. Causal factors for the followed UCAs.

Scenario description	Causal factors
Inappropriate signal transmission	Faulty transmission (Hardware open, short circuit, interferences)
	Communication bus error
	Incorrect connection
	Inadequately timed
Flawed execution (Faults in the physical process)	No execution, delayed execution, wrong execution due to actuator failure
	No execution, wrong execution due to incorrect mounting of the actuator
	Failure in power supply to actuator
	Flawed execution due to inappropriate process input (missing, wrong, delayed)
	Control action not followed by the lower controller
Conflicting control actions	Different data available to controllers or priorities are not appropriately set

APPENDIX I ESI RESULTS

The Event Trees of the analysis are provided in Figure I. 1-4.

For [H-2] (Figure I.2) first PMS will implement some tuning in the DG sets load. If it fails, then intelligent diagnosis will trip the faulty DG set. In case of intelligent diagnosis failure, there is chance that DG safety system will recognise the problem and will connect a healthy DG set and trip the faulty DG set. If not, then blackout will occur. Also when a faulty DG set is tripped, it is necessary to check if DG set overload conditions will occur and if the transient can be accepted by the system

For [H-4] (Figure I.3) it is well know that a number of electrical load transients are happening. However, it might be that the design cannot accept electrical load transient as in cased described by (MAIB, 2011). There is though very low probability for that to happen. If a DG set does not correct the load output due to failure in control equipment (governor, AVR), then an imbalanced load generation [H-2] will be observed.

For short circuits [H-5] (Figure I.4), local protection should be able to trip the faulty components. However, if it fails then overcurrent will be observed in the system. Then the bus-tie breaker should be able to trip the faulty section. If it succeed, blackout will occur when there is DGs overload in the healthy section due to specific load conditions in the DEP section. If bus-tie breaker fails, then blackout will occur due to overcurrent in the DEP system, as DG sets safety systems will trip the DG sets. If DG sets safety systems fail to trip the DG sets, then DG sets will be damaged and the DEP system will shut down due to DG sets failure. DG sets loss obviously leads to DG sets electrical transient and DG sets unavailability.

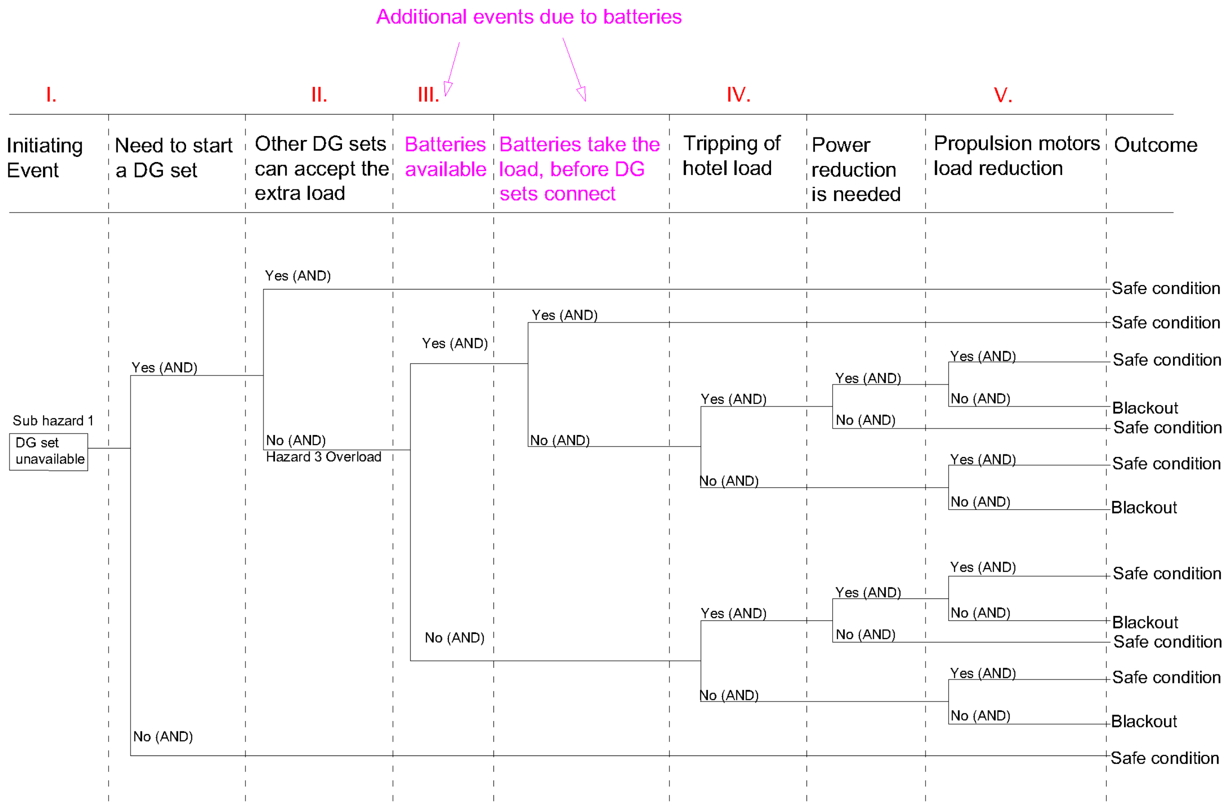


Figure I. 1 ESI's "Event Tree" for first and third sub hazards

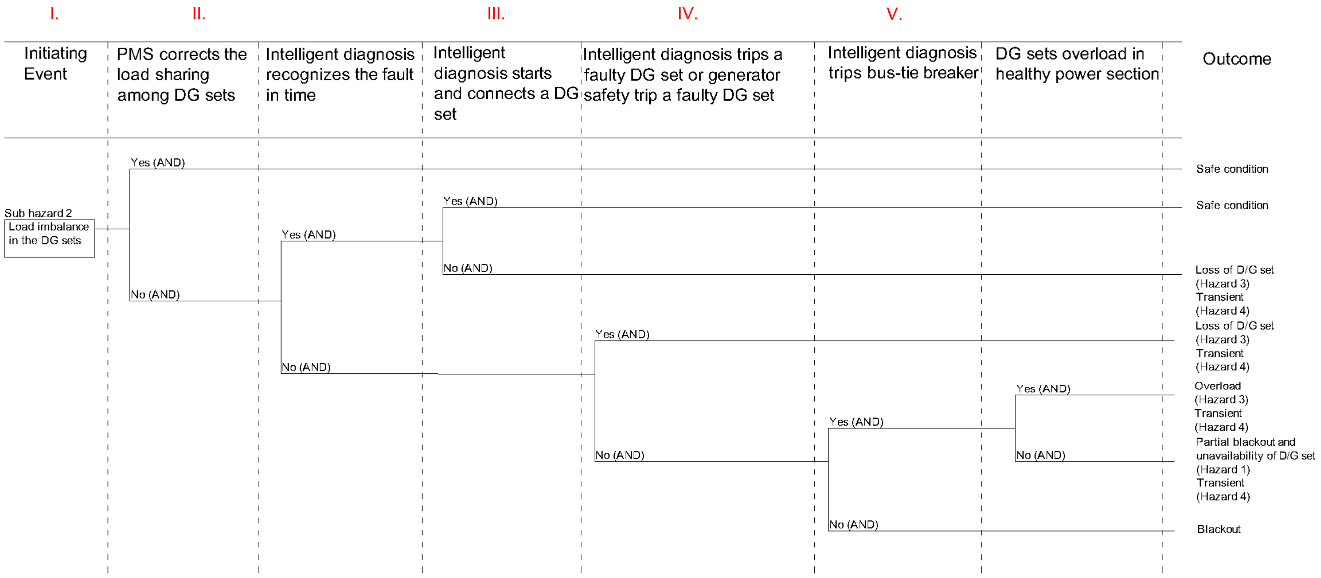

I.
II.
III.
IV.
V.
Initiating Event
PMS corrects the load sharing among DG sets
Intelligent diagnosis recognizes the fault in time
Intelligent diagnosis starts and connects a DG set
Intelligent diagnosis trips a faulty DG set or generator safety trip a faulty DG set
Intelligent diagnosis trips bus-tie breaker
DG sets overload in healthy power section
Outcome
Sub hazard 2
Load imbalance in the DG sets
Yes (AND)
No (AND)
Safe condition
Safe condition
Loss of D/G set (Hazard 3) Transient (Hazard 4)
Loss of D/G set (Hazard 3) Transient (Hazard 4)
Overload (Hazard 3) Transient (Hazard 4)
Partial blackout and unavailability of D/G set (Hazard 1) Transient (Hazard 4)
Blackout

Figure I. 2 ESI's "Event Tree" for second sub hazard.

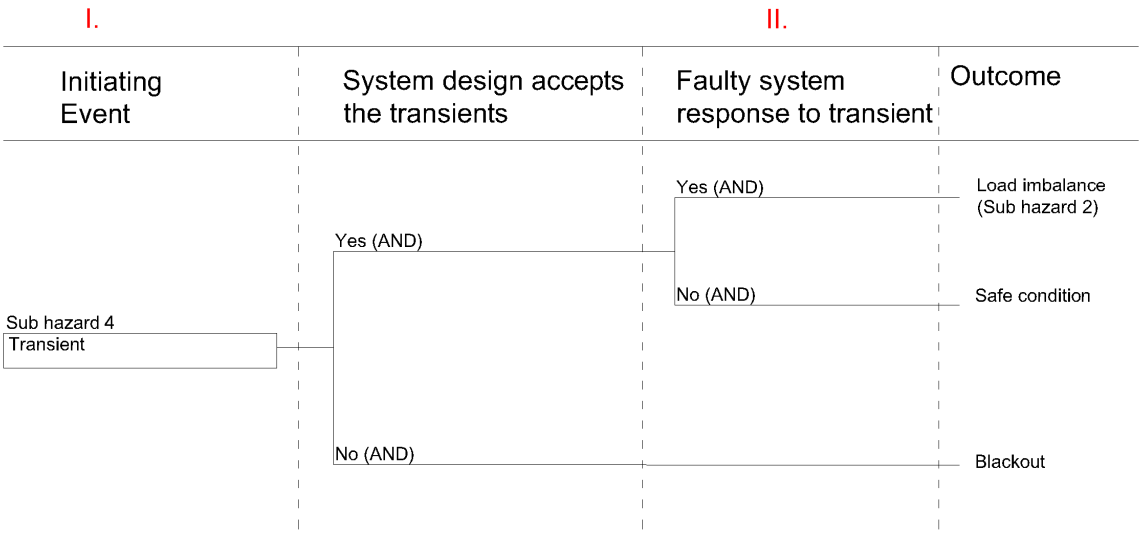


Figure I. 3 ESI’s “Event Tree” for forth sub hazard.

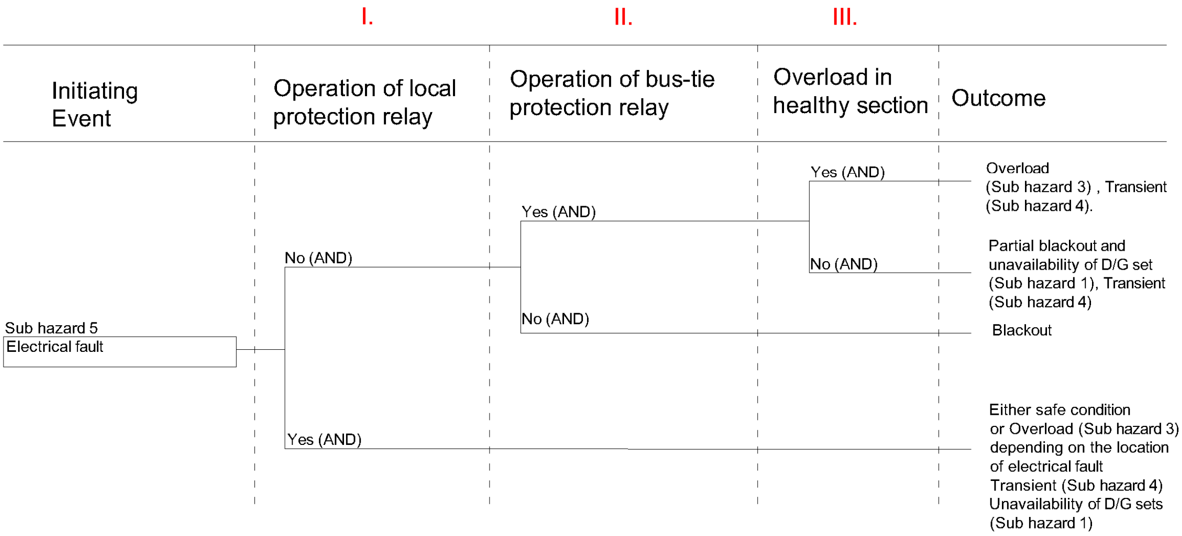

I.
II.
III.
Initiating Event
Operation of local protection relay
Operation of bus-tie protection relay
Overload in healthy section
Outcome
Sub hazard 5
Electrical fault
No (AND)
Yes (AND)
Yes (AND)
No (AND)
Yes (AND)
No (AND)
Overload (Sub hazard 3) , Transient (Sub hazard 4).
Partial blackout and unavailability of D/G set (Sub hazard 1), Transient (Sub hazard 4)
Blackout
Either safe condition or Overload (Sub hazard 3) depending on the location of electrical fault Transient (Sub hazard 4) Unavailability of D/G sets (Sub hazard 1)

Figure I. 4 ESI’s “Event Tree” for fifth sub hazard.

This page has been intentionally left blank

APPENDIX J MAPPING OF THE IDENTIFIED UCAS TO DIFFERENT EVENTS OF EVENT TREES

The mapping of different UCAs for the DEP system to the Event Trees of Appendix I is provided in Table J. 1.

Table J. 1 UCAs association with events in Event Trees.

Event Tree	Event	UCAs
Figure I. 1 ESI's "Event Tree" for first and third sub hazards	I.	UCA 1.22, UCA 1.50, UCA 1.51, (UCA 1.52 not applicable to the DEP), UCA 1.54, UCA 1.64, UCA 1.92.
	II.	UCA 1.3, UCA 1.6, UCA 1.7, UCA 1.8, UCA 1.9, UCA 1.10, UCA 1.11, UCA 1.12, UCA 1.14, UCA 1.20, UCA 1.21, UCA 1.22, UCA 1.23, UCA 1.24, UCA 1.25, UCA 1.26, UCA 1.27, UCA 1.28, UCA 1.29, UCA 1.48, UCA 1.50, UCA 1.51, UCA 1.55, UCA 1.67, UCA 1.72, UCA 1.77, UCA 1.88.
	III.	UCA 1.81,UCA 1.82, UCA 1.83, UCA 1.84, UCA 1.85, UCA 1.86, UCA 1.87, UCA 1.88, UCA 1.89, UCA 1.90, UCA 1.91.UCA 1.85UCA 1.82
	IV.	UCA 1.4, UCA 1.5.
	V.	UCA 1.17, UCA 1.19, UCA 1.73, UCA 1.75, UCA 1.78, UCA 1.80.
Figure I. 2 ESI's "Event Tree" for second sub hazard.	I.	UCA 1.7, UCA 1.14, UCA 1.16, UCA 1.32, UCA 1.33, UCA 1.34, UCA 1.36, UCA 1.37, UCA 1.38, UCA 1.40, UCA 1.42, UCA 1.44, UCA 1.46, (UCA 1.53 not applicable to the DEP), UCA 1.74.
	II.	UCA 1.13, UCA 1.15.
	III.	UCA 1.58, UCA 1.59.
	IV.	UCA 1.56, UCA 1.57.
	V.	UCA 1.56, UCA 1.2, UCA 1.60, UCA 1.61, UCA 1.63.
Figure I. 3 ESI's "Event Tree" for forth sub hazard.	I.	UCA 1.18, UCA 1.24, UCA 1.26, UCA 1.30, UCA 1.49, UCA 1.62, UCA 1.64, UCA 1.65, UCA 1.70, UCA 1.71, UCA 1.76, UCA 1.79.
	II.	UCA 1.31, UCA 1.35, UCA 1.39, UCA 1.41, UCA 1.43, UCA 1.45, UCA 1.47.
Figure I. 4 ESI's "Event Tree" for fifth sub hazard.	I.	UCA 1.68.
	II.	UCA 1.1, UCA 1.2, UCA 1.63, UCA 1.66.
	III.	UCA 1.69.

This page has been intentionally left blank

APPENDIX K FTA RESULTS

The Fault Trees of different systems for section 7.2.4 are presented in Figures K1 to K7.

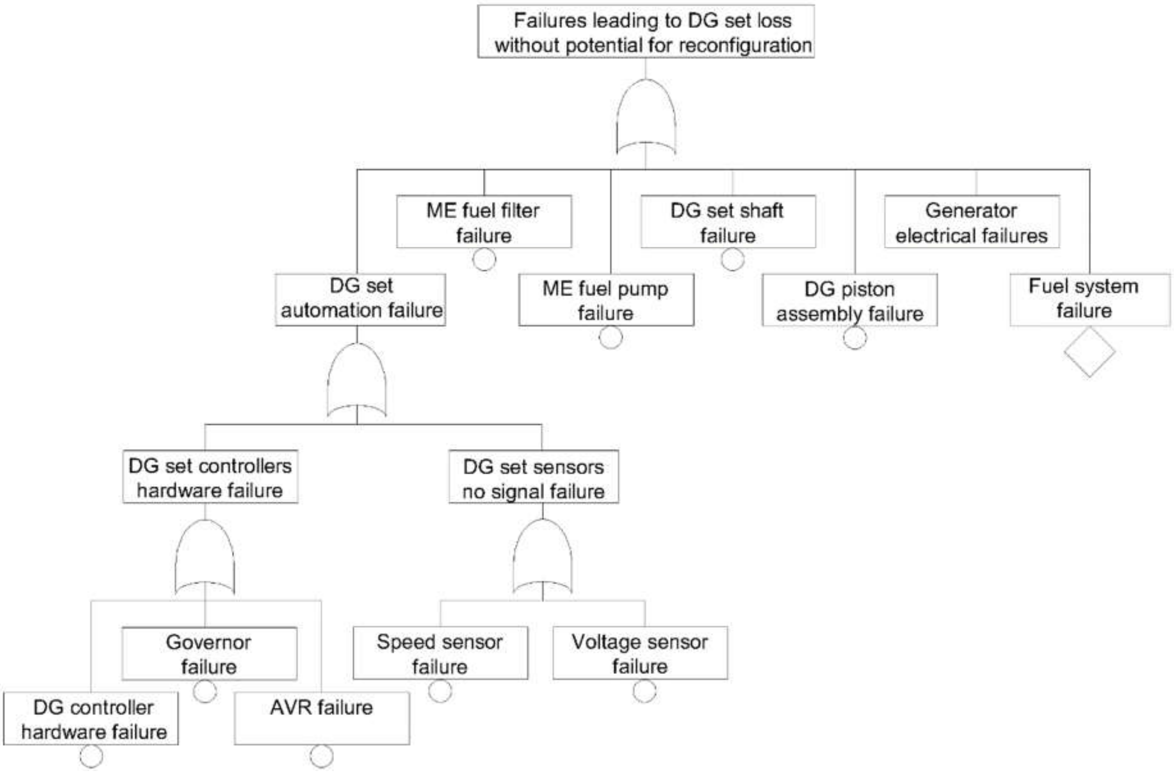

Failures leading to DG set loss without potential for reconfiguration
ME fuel filter failure
DG set shaft failure
Generator electrical failures
DG set automation failure
ME fuel pump failure
DG piston assembly failure
Fuel system failure
DG set controllers hardware failure
DG set sensors no signal failure
Governor failure
Speed sensor failure
Voltage sensor failure
DG controller hardware failure
AVR failure

Figure K. 1 DG set failures leading to loss without potential for reconfiguration.

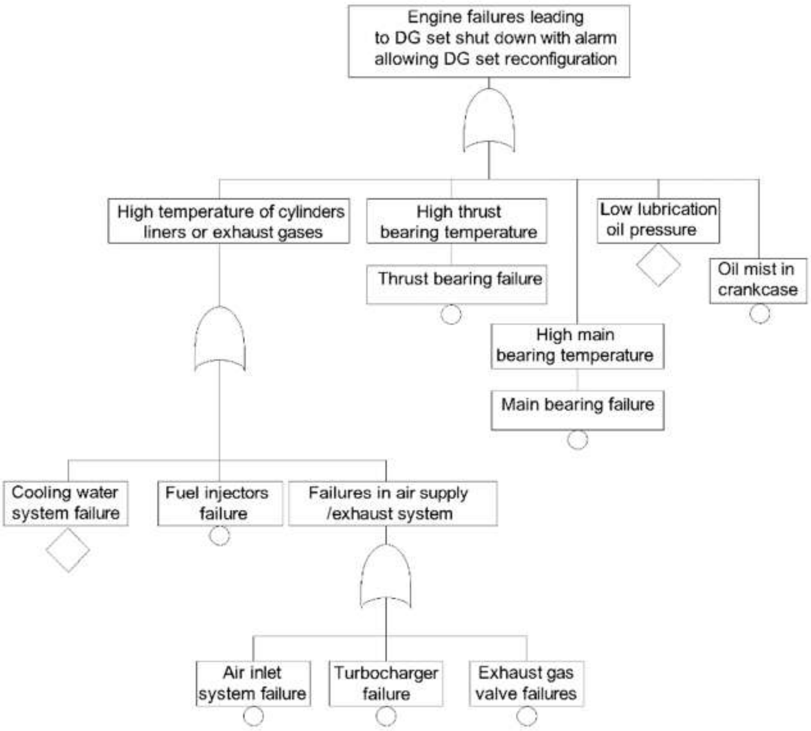

Engine failures leading to DG set shut down with alarm allowing DG set reconfiguration
High temperature of cylinders liners or exhaust gases
High thrust bearing temperature
Low lubrication oil pressure
Thrust bearing failure
Oil mist in crankcase
High main bearing temperature
Main bearing failure
Cooling water system failure
Fuel injectors failure
Failures in air supply /exhaust system
Air inlet system failure
Turbocharger failure
Exhaust gas valve failures

Figure K. 2 DG set failures leading to loss with alarm allowing reconfiguration to another DG set.

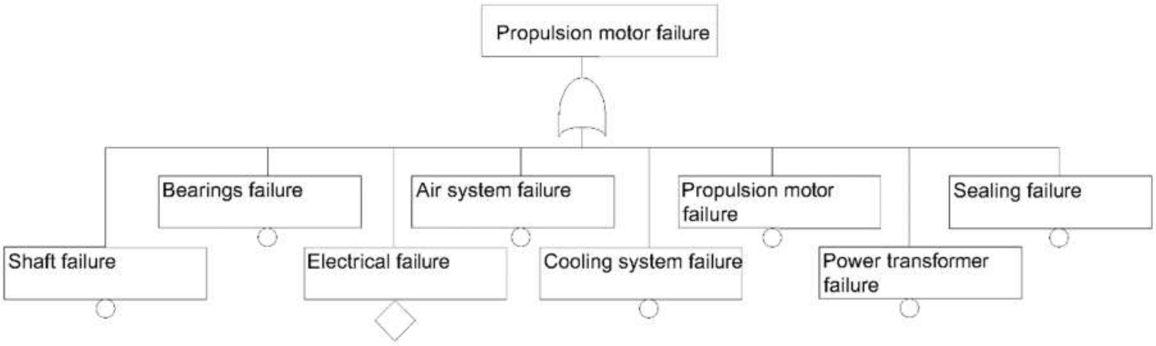


Figure K. 3 Fault Tree for propulsion motors.

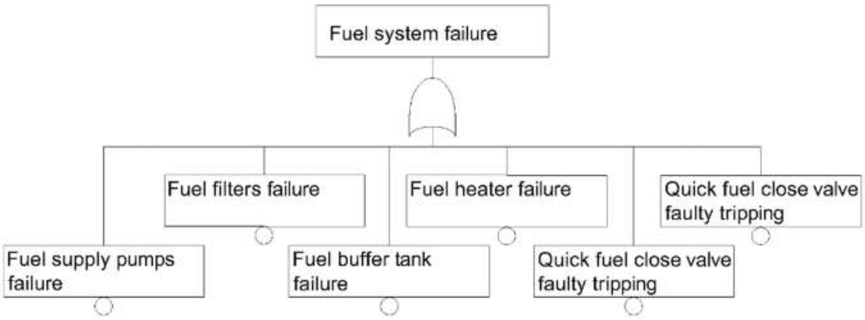

Fuel system failure
Fuel filters failure
Fuel heater failure
Quick fuel close valve faulty tripping
Fuel supply pumps failure
Fuel buffer tank failure
Quick fuel close valve faulty tripping

Figure K. 4 Fault Tree for the heavy fuel system.

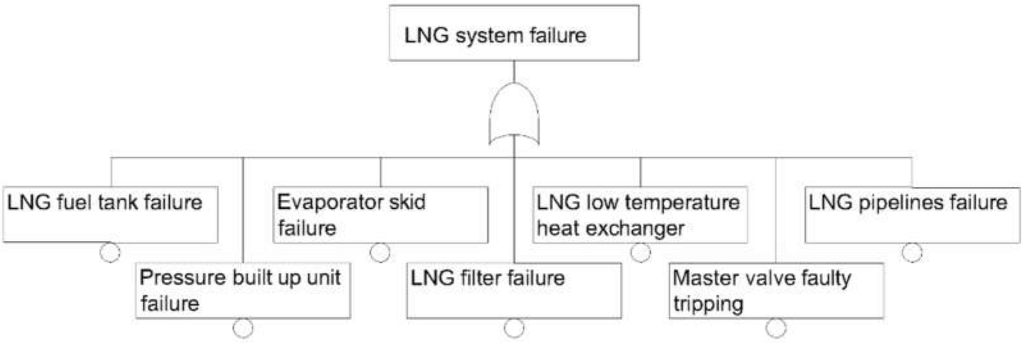


Figure K. 5 Fault Tree for the LNG fuel system.

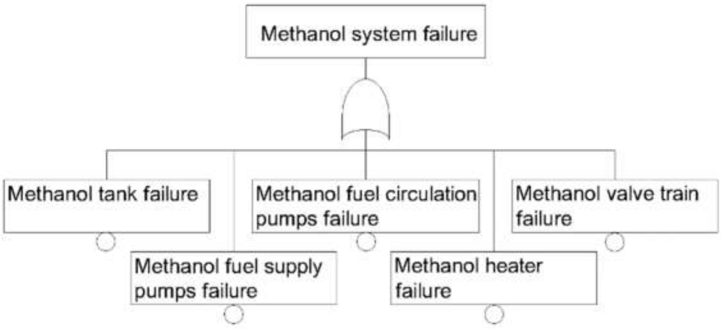

Methanol system failure
Methanol tank failure
Methanol fuel circulation pumps failure
Methanol valve train failure
Methanol fuel supply pumps failure
Methanol heater failure

Figure K. 6 Fault Tree for the methanol fuel system.

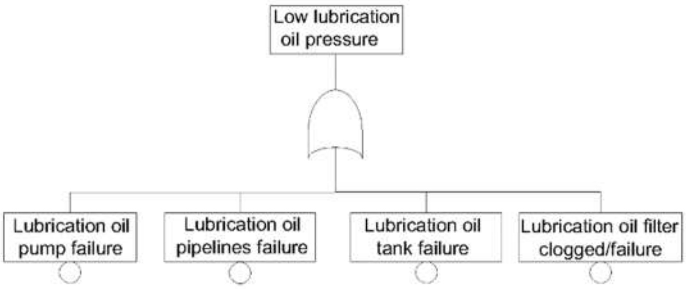

Low lubrication oil pressure
Lubrication oil pump failure
Lubrication oil pipelines failure
Lubrication oil tank failure
Lubrication oil filter clogged/failure

Figure K. 7 Fault Tree for low lubrication pressure failure event.