Reliability Engineering and System Safety 185 (2019) 348–361

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

# Operational risk assessment model for marine vessels

Abdul Aziz[a], Salim Ahmed[a], Faisal Khan[a,*], Chris Stack[b], Annes Lind[b]

[a] Center for Risk, Integrity, and Safety Engineering (C-RISE), Faculty of Engineering & Applied Science, Memorial University, St. John's, NL A1B 3 X 5, Canada
[b] HSEQ Dept., Canship Ugland Ltd., Topsail Road, St. John's, NL A1B 3M7, Canada

ARTICLE INFO

*Keywords:*
Marine operations
Process hazards
Marine vessel reliability
Operational risk
Fault tree
Event tree

ABSTRACT

This paper presents a practical approach to quantify the risk associated with different systems in a marine vessel using the existing operational database. A structured bow-tie methodology is proposed to assess risk. The first step was the development of probable failure scenarios for four different events, namely, fire and explosion, propulsion engine failure, power failure, and maneuverability failure. The second step includes the formulation of corresponding bow-tie models representing these scenarios using vessel configuration and process information. Using the failure data for different elements obtained from the vessel's maintenance logbook and incident records, the frequency of events and failure rates of the safety barriers are estimated to quantify risk. Operational data from the vessel, a single engine ice-breaker bulk career navigating mainly in the Canadian sub-arctic region, validated the proposed model. The methodology is verified by comparing the model's observations with an alternative dataset (actual failure scenario from the ship). The proposed methodology is expected to serve as a useful tool for marine vessel's safety and risk management.

## 1. Introduction

Marine transportation is a catalyst for civilization around the globe and the lifeline of inter-continental trade [1]. To regulate safety standards for the ships operating in the international waterways, the international convention of Safety of Life at the Sea (SOLAS) was adopted [2]. There are numerous other regional and international bodies to regulate the shipping operations. Nevertheless, there are major accidents reported every year. Ships operating in arctic and sub-arctic regions are more prone to accidental loss due to extreme weather conditions. The regulatory authorities, e.g., International Maritime Organization [3] and the Ministry of Transport of Canada [4], have introduced amendments based on the geographical requirements. The polar code [5,6] now regulates ships navigating through the ice-covered arctic water. Arctic council's report [7] identifies shipping related accident types and their causes in addition to a discussion on the prospects of shipping in this region and its brief history. Shipping related accidents remain as a threat to the Arctic transportation industries.

A comprehensive study by Kum and Sahin [8] analyzed the causes of arctic marine transportation accidents in recent years. This study identifies poor weather conditions, lack of communication and navigational aid, sub-zero temperatures and remoteness as some of the challenges. Aside from weather influenced accidents, technical or operational faults have been identified as a root-cause for collision, grounding, machinery failure as well as fire and explosion related marine incidents in this region. While operating crew's training, stress management skills, navigation planning are required for competency, vessel's performance is also a factor of interest [9]. Therefore, this study mostly focuses on operational integrity or reliability of marine vessels towards excellence in performance.

Reliability assessment of process equipment or a system is a key element to asset integrity management [10]. Reliability centric maintenance (RCM) has been a well-established preventive methodology to influence maintenance decision to upgrade process reliability as well as to enhance safety [11–15]. The efficacy of knowledge-based models entirely depends on the acquisition of valid reliability data of the system, which might be challenging. Approaches for the collection of data on failure frequency, as well as reliability, have been discussed in the literature [16,17]. Failure frequency acquisition form historical data might be the most effective approach. While frequencies can be estimated using the existing database, operating experience and process diagrams provide the background for such models. Whether the corresponding plant or similar component database from the literature provides the information, a case study can validate this approach of reliability quantification as well as risk analysis.

The present study uses the bow-tie model which is a well-established and well-documented tool. It is frequently used in processing industries (mineral processing; nuclear and oil and gas). However, to

* Corresponding author.
*E-mail address:* fikhan@mun.ca (F. Khan).

https://doi.org/10.1016/j.ress.2019.01.002
Received 12 February 2018; Received in revised form 26 December 2018; Accepted 2 January 2019
Available online 03 January 2019
0951-8320/ 

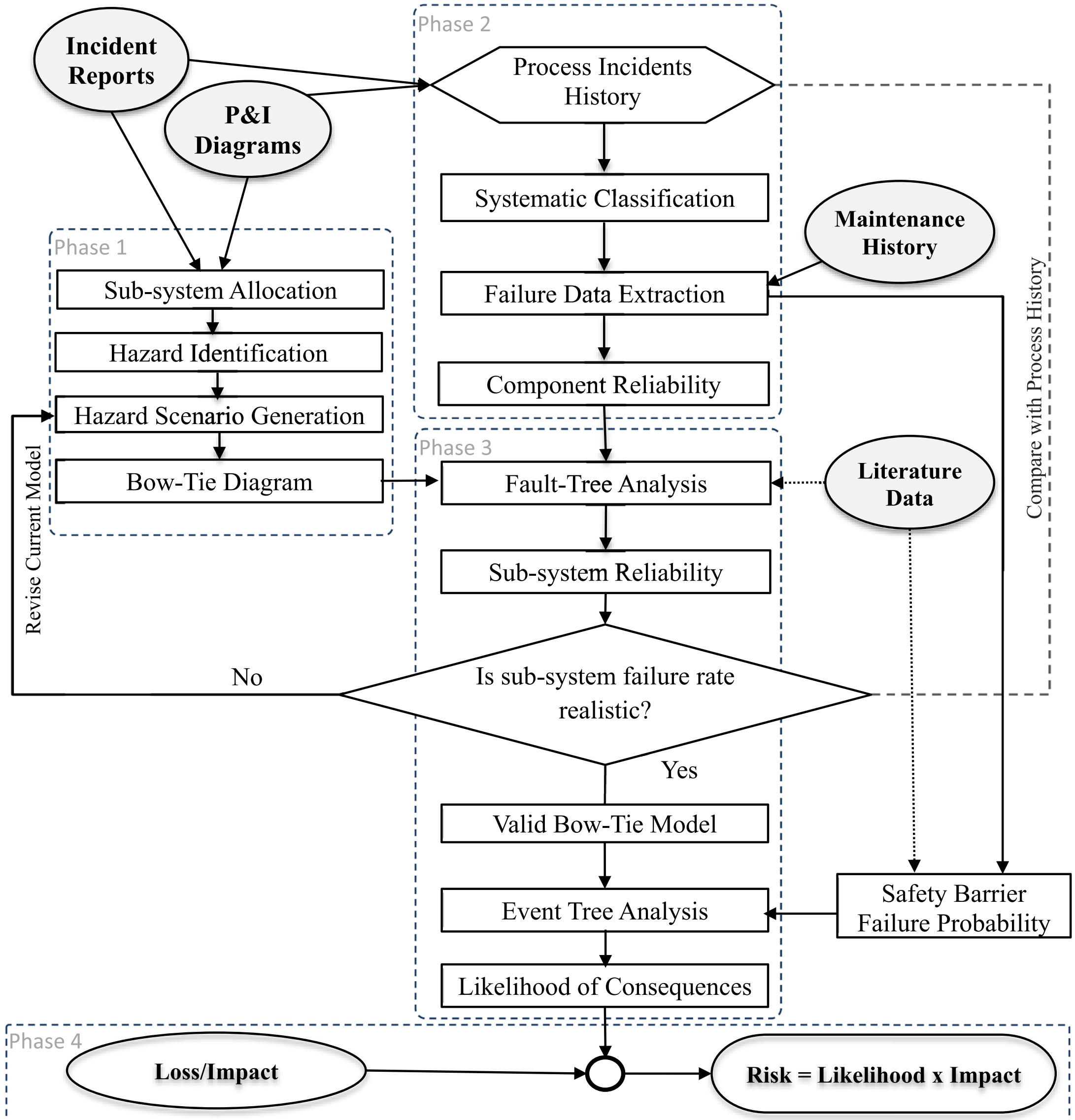


**Fig. 1.** Operational Risk Assessment methodology for a marine vessel.

the best of our knowledge, it has not been used in the shipping industry for operational risk assessment. The primary intent of this work is to demonstrate how the shipping industry could use their in-house data for their safety and integrity related decision-making. For this reason, authors have focused on a simple and tested approach. The current work is novel from three perspectives: i) First-time use of bow-tie model for ship's operational safety assessment; ii) testing and validation of risk model using the in-house data; and iii) use of the in-house data to better manage operational safety and integrity of the ship. This article introduces a case study of a marine carrier, which was brought into attention by a marine transportation industry, namely Canship Ugland Ltd., seeking the goal of excellence in safety. The database is available as "near miss" incident reports, maintenance history and supporting P&IDs. The primary purpose was to translate the operational experience into a valid scientific representation. Therefore, the primary objectives of this article are: *a)* To share the methodology adopted for reliability assessment from observed historical data of the specific marine vessel; *b)* to present hazardous event scenarios as bow-tie diagrams; c) data acquisition and estimation of failure frequencies and thus to quantify reliability from operational information; *d)* to disseminate results obtained from bow-tie analysis and methods to utilize the results.

The studied vessel is a bulk carrier mostly operating in north-eastern Canada. The ship operates around the year carrying mining equipment, supplies and metal concentrate. Due to confidentiality issues, specific details about the ship will remain undisclosed. This strengthened hull vessel with ice-breaking power navigates on a unique route in remote north Atlantic region, only in the presence of Canadian ice-surveillance airplanes. Therefore, this vessel is designed to be self-sustained, however, prone to being stranded in the case of major breakdowns. Systematic reliability assessment helps to prevent unplanned breakdown, and risk assessment results outline the adequate precautions of this vessel.

As reliability based maintenance planning and management is already a proven technique, application in specific offshore and maritime operations is not uncommon in the literature [18,19]. Some of the studies focused on the historical database for process operations, e.g. marine engine reliability or pipeline reliability [20,21] or marine fire-explosion accidents [22]. Recent studies mostly focused on risk analysis and management to reduce marine accidents [23–26] or, collisions [27,28] and applications in arctic weather [29–35]. Comparative review literature [23,36] and recent developments in marine transportation risk assessment indicates to address uncertainty using the Bayesian network (BN). Fuzzy fault tree-based models are also common in the data-scarce environment. However, this work uses the conventional bow-tie approach to accommodate available information and maximum participation of the validators.

This article includes five sections. The current section presents an introduction, relevant works and the objectives of this work. Section 2 briefs the adopted methodology for the overall procedure with a simple block diagram. Different top events with the fault propagation scenarios and possible consequences are illustrated using fault and event trees. It also describes data extraction and reliability quantification along with data sources. Section 3 presents the assessment results obtained from the historical database and a comparison with the actual scenarios. Sections 4 and 5 present discussions on results and the concluding remarks, respectively.

## 2. Operational risk assessment methodology

Most of the arctic marine vessel's construction is complex and consists of widely different types of equipment and processes. As the vessel in this case study is a self-sustainable arctic carrier, the overall design is multidimensional having powerful and complex process systems. Therefore, two basic criteria – *accessibility* and *quality* of the specific database, primarily controlled the methodology adopted to quantify system reliability. History-based data validated the sub-system reliability and consequence likelihood were projected based on the outcome. Therefore, this case specific methodology is adapted mostly with the insights of Quantitative Risk Analysis (QRA) [17] and partly System Hazard Identification, Prediction and Prevention (SHIPP) methodology [37] for process systems. However, systematic hazard identification, data mining, organization, the projection of reliability from historical failure data - are its unique features. Fig. 1 presents a complete overview of the methodology.

There are four different phases in the proposed approach, namely, scenario generation, historical data acquisition, bow-tie analysis and risk estimation. This study uses the traditional definition of risk, which is a function of the probability of hazard occurrence and its impact. There is a contemporary definition of risk focusing on the uncertainty of hazard. The interested reader may refer to relevant resources [38–40].

As risk-based approaches are mostly case-centric, database accessibility to extract historical incidents is the most influential factor in the preliminary phases of this methodology. The type of accessible database and the stored information control the workflow. The historical database may have three types of resources- safety critical or operational incident reports, process diagrams and maintenance records. These resources, in combination, provide an idea about the process, types of incidents, root-causes and severity of any plausible phenomenon. There are two major segments in the preparation stage to capture the process history. Scenarios generation or, hazard scenario model development provides the basic framework to capture and reflect upon the information using a visual model. Also, the failure database provides quantitative information for historical reliability estimation in the *data acquisition* step. Both these stages are preparatory steps and denoted as phases 1 and 2, respectively, in Fig. 1.

***Phase 1-Scenarios Generation:*** The first step in this methodology is sub-system categorization followed by hazard identification, which includes preliminary outlining of the process hazard scenarios from past incidents and accidents. Study of previous incidents and process diagrams can help to envisage the most likely event propagation scenarios. Different hazard modelling techniques are available in the literature cited earlier in this section.

This methodology adopts fault tree and event tree-based bow-tie approach for scenario generation. Upon identifying a hazardous event as the top event for each of the subsystem, fault trees are generated to capture most common primary events and event propagation. The event tree provides the accident propagation scenario and consequences, considering the available safety barriers. The bow-tie diagrams can translate a primary failure to plausible accident scenarios with the likelihood of occurrence. These models provide the basic framework for estimation of sub-system reliability and the likelihood of consequences for specific sub-systems.

***Phase 2 -Historical Data Acquisition:*** The goal of this step is to collect all the information and prepare the required data for the next step. The collected process history data is classified based on different domain/sub-systems and equipment. The sub-systems, consisting of different equipment or components, are interrelated and may share components. Once the process history database is organized based on subsystems and components, the frequency of failure is estimated based on failure counts for each component over a period. Maintenance history provides additional information about repair and maintenance of any specific component. Constant failure rate can be considered for ease of estimation, as further details might not be available for reasonably large process systems.

The failure frequency allows the estimation of component reliability. Choosing the maximum value, comparing the failure frequencies estimated from process incident history and condition-based maintenance database, provides the most likely scenario of failure.

***Phase 3-Bow tie Analysis:*** Once the tentative bow-tie models are ready, the component reliability data may be used to validate the models. Plugging in the reliability data will provide a failure rate for the specific subsystem. If the fault tree model is complete and efficient, the subsystem failure rate should be comparable to the process incident history.

A crucial challenge for bow-tie analysis might be the missing information. However, when there is no historical failure data available, literature database may be used. On-demand failure rates for the safety barriers may be considered as useful information. The event tree analysis yields a likelihood of consequences for each subsystem failure.

***Phase 4 -Risk Estimation and Mitigation:*** In most cases, likelihood of a consequence is the primary measure of associated risk. However, quantification of risk in dollar value significantly improves the effectiveness of the decision-making ability. When financial loss/impact values are assigned, risk measures in dollar values are obtained by combining impacts with their likelihood. Depending on the risk, management decisions can be made to mitigate, control or avoid hazardous situations.

This methodology is developed focusing on the vessel under consideration. In the following section, the methodology is implemented in a set of case study examples.

## 3. A case study of a marine vessel

### *3.1. Scenario generation: bow-tie diagrams*

Bow-tie models, composed of Fault Trees (FT) and Event Trees (ET), are developed to represent the possible hazard scenarios. For a hazardous event or top event, fault tree identifies the primary events and the fault propagation path; event tree represents the defensive barriers and likely consequences.

For the marine vessel in the study, all the process incidents and safety-critical events are listed as incident reports in a historical database. These provide a complete overview of the primary events, root-causes and sequential evidence for any unwanted scenario. Table 1 presents some sample incident examples. These incident reports help to build process history. Piping and Instrumentation Diagrams (P&ID) provide additional information regarding design. Basic understanding of process history accompanied by experienced professional's input is incorporated in developing each hazard scenario.

For the marine vessel under study, four different hazardous situations were outlined as significant hazards i) propulsion system failure, ii) power failure, iii) navigations and maneuverability system failure and iv) fire and explosion. The next step included envisioning of potential hazards, accident scenarios and the common operational consequences [8] - loss of propulsion, blackout, grounding/collision, fire and explosion and capsize. A set of generic bow-tie models has been developed to portray the hazardous scenarios.

**Table 1**
Sample incident scenarios reported for the marine vessel.

| Date | Subsystem | Incident | Root cause | Severity |
|---|---|---|---|---|
| 30-Jul-2009 | Main engine | Breakdown of FO purifier: #1 HFO purifier stopped running because of low speed in a bowl. #2 purifier also stopped working with the same alarm and couldn't be restarted, leaving the ship with no way to purify the HFO for the M/E. | Random failure | Near miss |
| 26-Jul-2009 | Electrical | Blackout at sea: During Pilotage, #3 Auxiliary generator L/O filter pressure dropped to alarm level and was switched over to the standby filter. While commisioning the filter again after cleaning, the oil pressure dropped enough to trigger low lube oil pressure switch to shut-down the only generator causing Black-out. | Improper procedure/ human error | Near miss |
| 17-Aug-2010 | Main engine | M/E blower failure: While travelling, an alarm rang in indicating "blower 1 Failure" and "blower 2 Failure", which caused the scavenge pressure in the engine to drop thus starving the engine for air, and slowdown. | Random failure | Near miss |
| 13-Dec-2014 | Maneuverability & navigation | Steering failure: When the vessel is approaching the port, there was an "Auto"-"Emergency Alarm" on the steering console that was immediately acknowledged. The ETA shut the auto-pilots and established local emergency control and put the rudder amidships. | Random failure | Near miss |
| 18-Dec-2015 | Fire & explosion hazard | Diesel oil spill: While Carrying out an overhaul of the Port Bunker Tank hydraulically operated suction valve, approx. One litre of diesel oil was spilled on the deck in the Pipe Tunnel. | Spill/release | Near miss |

#### *3.1.1. Fire/explosion hazard scenario*

The vessel in the case study is a bulk carrier. As such, aside from operational releases, properties of contained cargo material pose a significant threat to the vessel's safety. Potential of any combustible material release, explosive properties of the cargo material as well as the presence of ignition sources are the major contributors in this hazard scenario. Inert gas blanketing cargo, gas detectors, fire alarms, fire extinguisher and emergency fire training are the available preventive mechanisms on board the vessel.

The bow-tie diagram in separate Fault Tree (FT) and Event-Tree (ET) segments illustrates a more straightforward presentation. Fig. 2 represents the developed fault tree diagram for fire and explosion hazard in the marine vessel. Fig. 3 presenting the possible accident scenario for fire/explosion hazards with typical safety barriers.

#### *3.1.2. Propulsion system failure*

The case study vessel is a single engine direct dive diesel powered bulk carrier. Any malfunction of the propulsion engine (Main Engine) can cause the breakdown of this subsystem. The scenario is developed considering significant events, e.g., main engine trip, failure to start, and mechanical failure. With the support of the process and instrumentation diagrams (P&IDs), the scenario is developed to capture the possible equipment breakdowns as primary events for the fault tree. In applicable cases, an entire unit (e.g., fuel oil supply unit, cooling water system) is represented as individual equipment. For demonstration purpose, major root-causes like black-out or power failure, human errors are considered as primary events to capture the historical information irrespective of additional fault trees. The fault tree diagram in Fig. 4 represents a refined propulsion failure scenario. Some primary events, e.g., *ME14* or *Fuel Oil Supply* reliabilities includes smaller subsystems consisting of multiple fuel pumps, tanks, and delivery systems. For presentation purpose, the diagrams do not include similar systems in detail. Figure-5 illustrates the accident scenario for possible propulsion engine malfunction as an event tree. The accident scenario considers collision/grounding, propulsion loss and rescue with assistance as possible consequences Fig. 5.

#### *3.1.3. Power system failure*

Electrical power generation unit is the primary utility for a marine vessel's operations. Any blackout or disruption of electrical power may lead to multiple severe hazardous situations. As most of the equipment and controls are electrical, the case study vessel has multiple layers of redundancies for the power generation sub-system. Three diesel driven generators, one emergency diesel generator, and 24 V DC battery power-pack are essential parts of the system; which have layers of standby equipment through the main bus controller. An electrical power trip scenario has been envisaged considering main bus malfunction or in-service generator trip event. The trip scenario could be a result of any credible malfunction which represents a primary event in the fault tree (Fig. 6).

If all of the safety barriers fail, an electrical power trip can trigger a brief complete blackout, which may lead to accidents. The accident scenario is presented as in Fig. 7, considering the available preventive barriers and the emergency protocols.

#### *3.1.4. Navigation and manoeuvrability failure*

Marine vessel's stability, steering and maneuverability are integral elements for safe navigation. Our case study vessel has a sophisticated steering system, with a set of navigation equipment. A sea-water ballasting system, controlled by different monitoring components, maintains the vessel's stability. A single bow-tie model represents maneuverability, navigation and stability sub-systems, to capture the significant events and mechanisms. Steering unit, mooring and winch systems, navigation system and power dependency are the common factors in this subsystem. Fig. 8 represents the scenario as a fault tree diagram. The consequences of maneuverability and navigation system

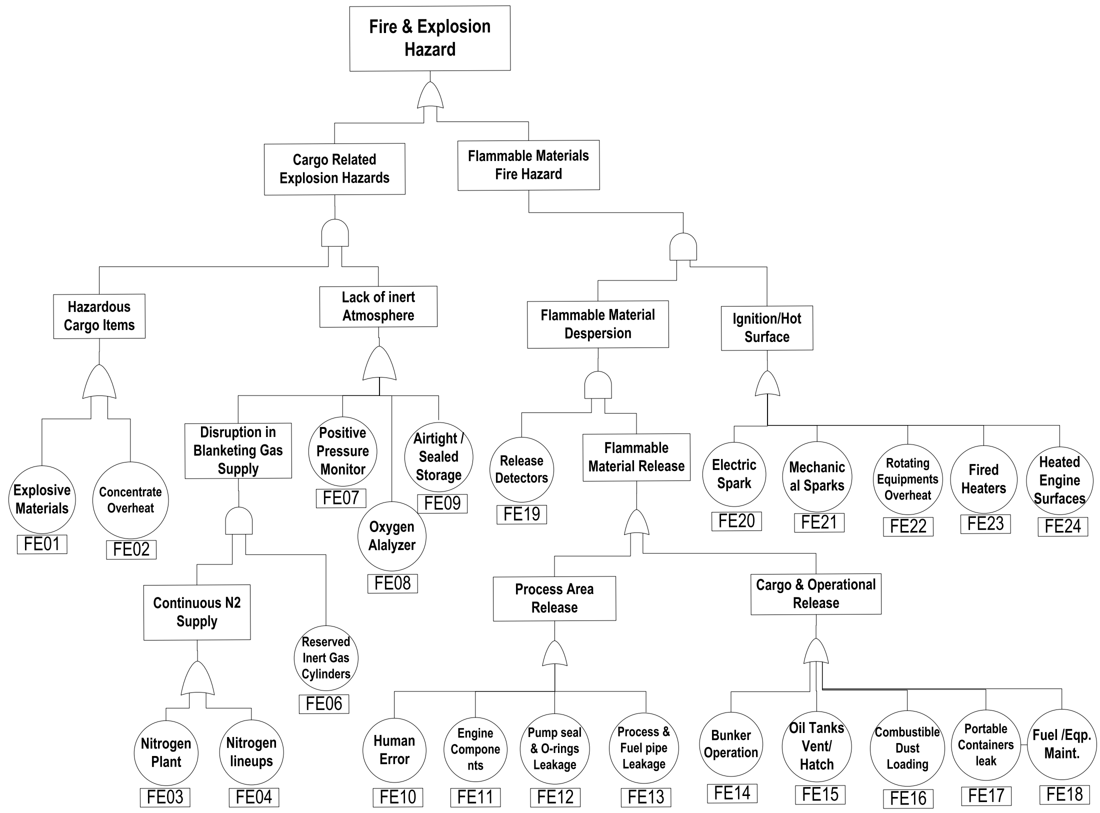


**Fig. 2.** Fire and explosion hazard fault tree.

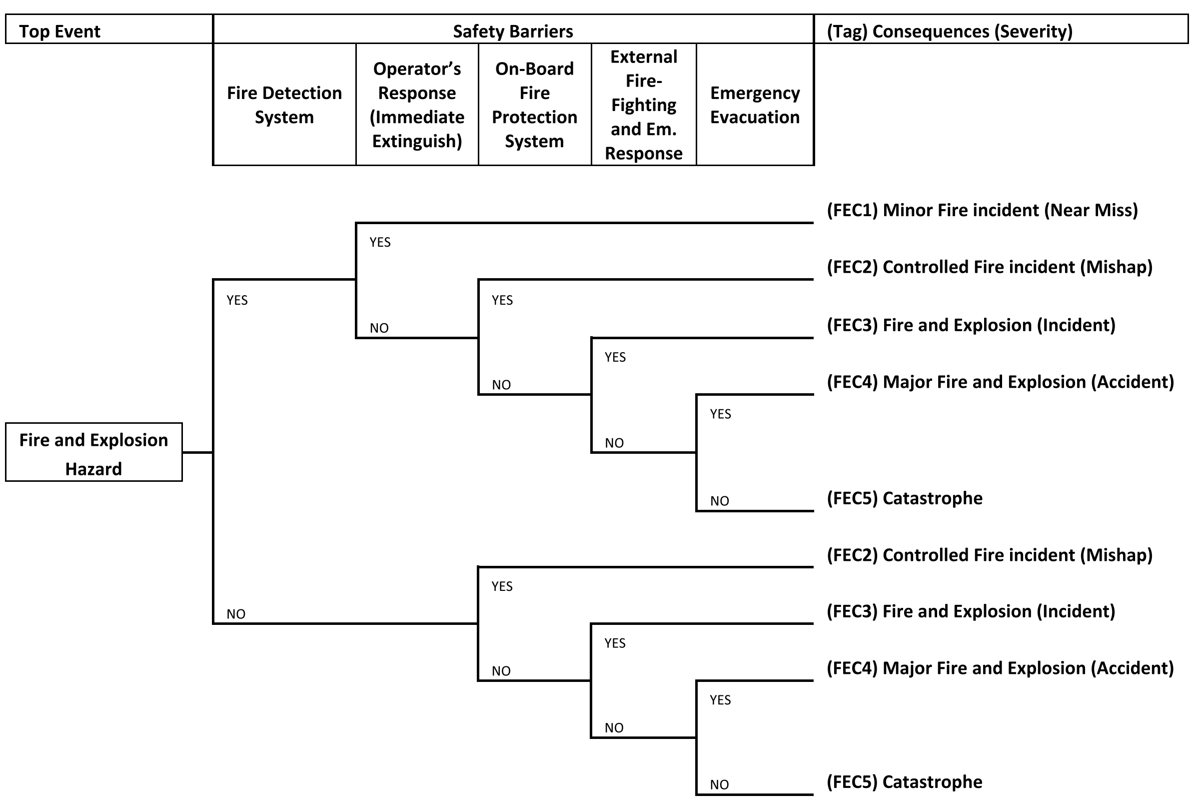


**Fig. 3.** Fire and explosion hazard event tree for a marine vessel.

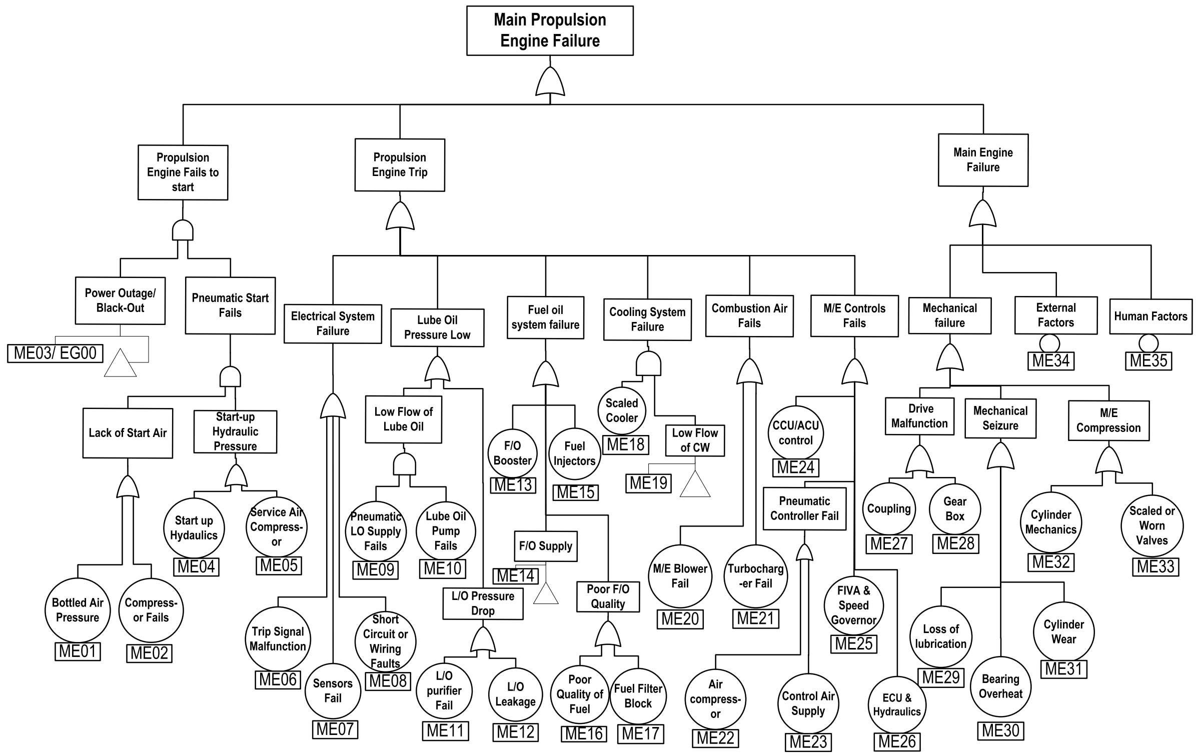


Fig. 4. Propulsion failure hazard scenario in a fault tree diagram.

failure can be from grounding to collision resulting catastrophe. The event tree diagram in Fig. 9 represents the maneuverability and navigation failure accident scenario.

### 3.2. Historical data acquisition

Alongside the production and logistics data, any industrial database usually contains the safety-critical incidents, maintenance history, inventories and so on. A well-organized database with necessary detailed information can be used for more accurate risk analysis, to maintain consistency within projects and to demonstrate to industry standards [41]. As a part of the excellent safety initiatives, Canship Ugland Ltd. maintains a dynamic database for all safety-critical incident reports, maintenance reports, job lists and management actions.

Incident reports in this case study are a collection of near miss and safety-sensitive incidents which include operational incidents, human injury or health-related incidents and potential safety hazards. For the vessel under consideration, 383 incidents were recorded over 8.25 years, where 304 incidents were processed/operational incidents and the remaining related to potential human injury or health hazards. The failure database was developed based on these reports to determine equipment-wise failure data.

While incident reports listed the process incidents due to premature or unprecedented failure of process equipment, the degradation of process equipment prevented through prior maintenance was not reflected in this database. Therefore, maintenance history was essential to

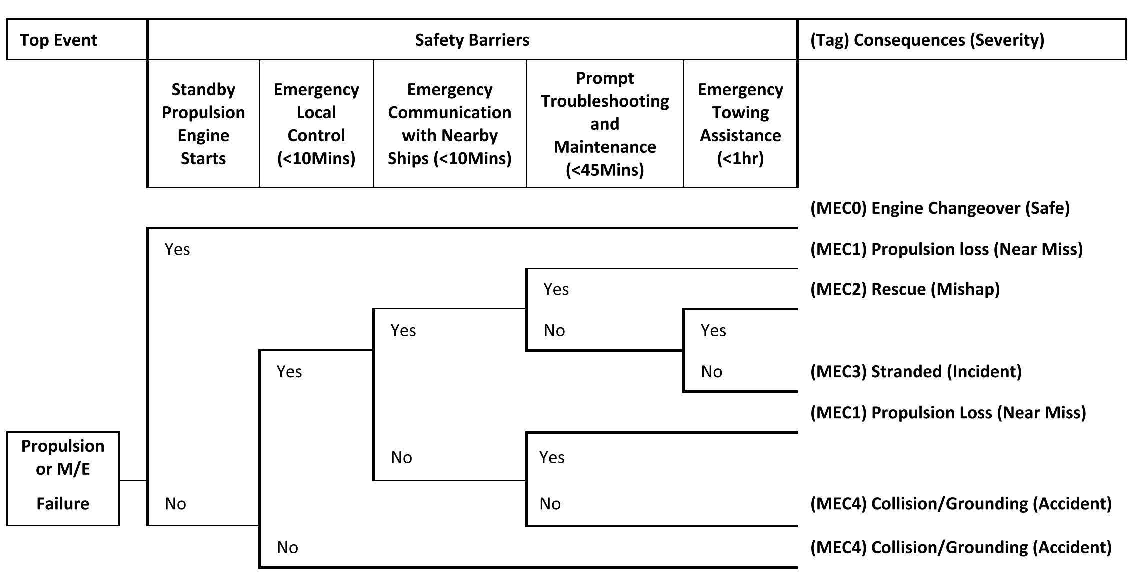


Fig. 5. Propulsion engine failure accident scenario.

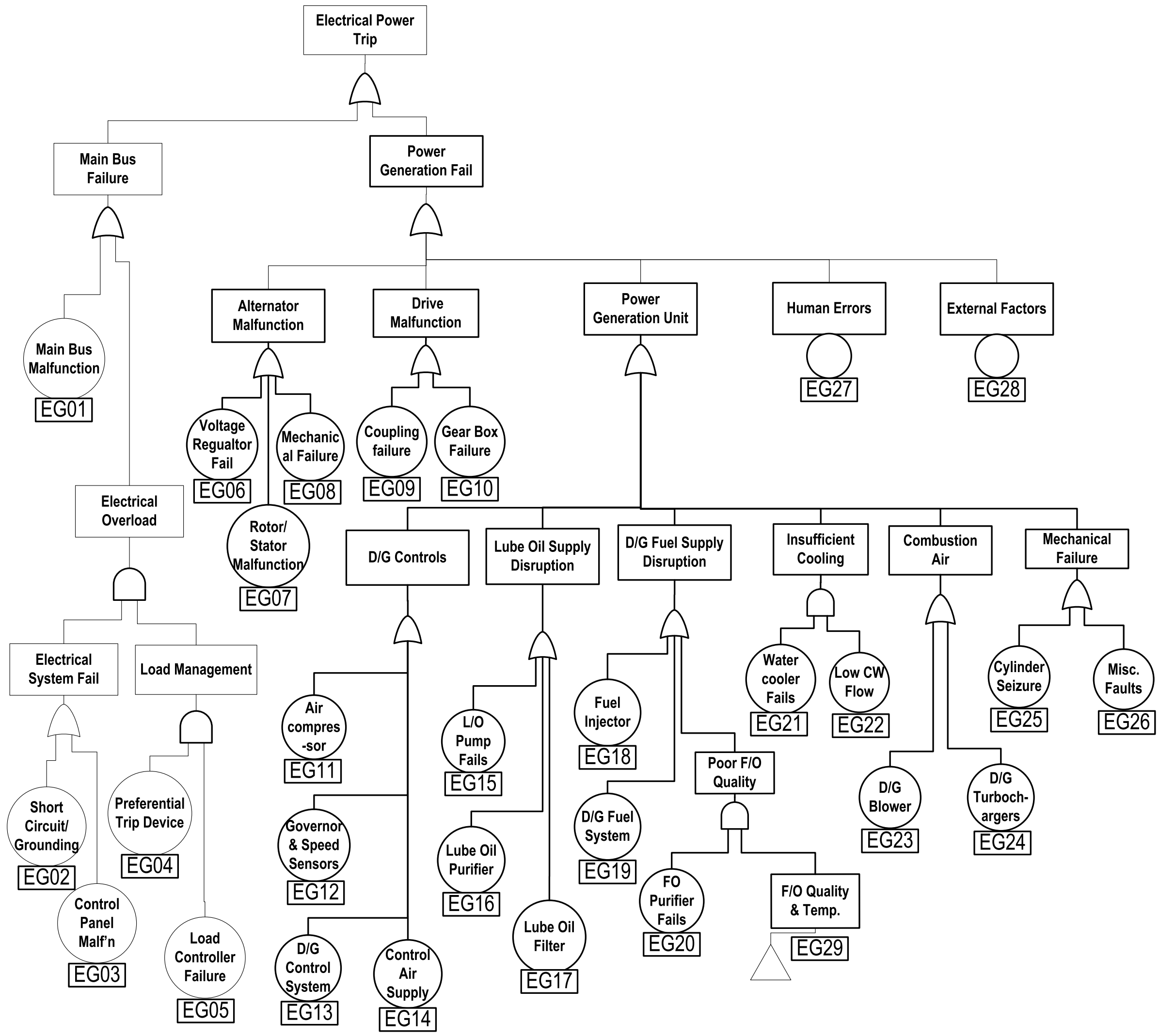


**Fig. 6.** Electrical power trip scenario in a fault tree diagram.

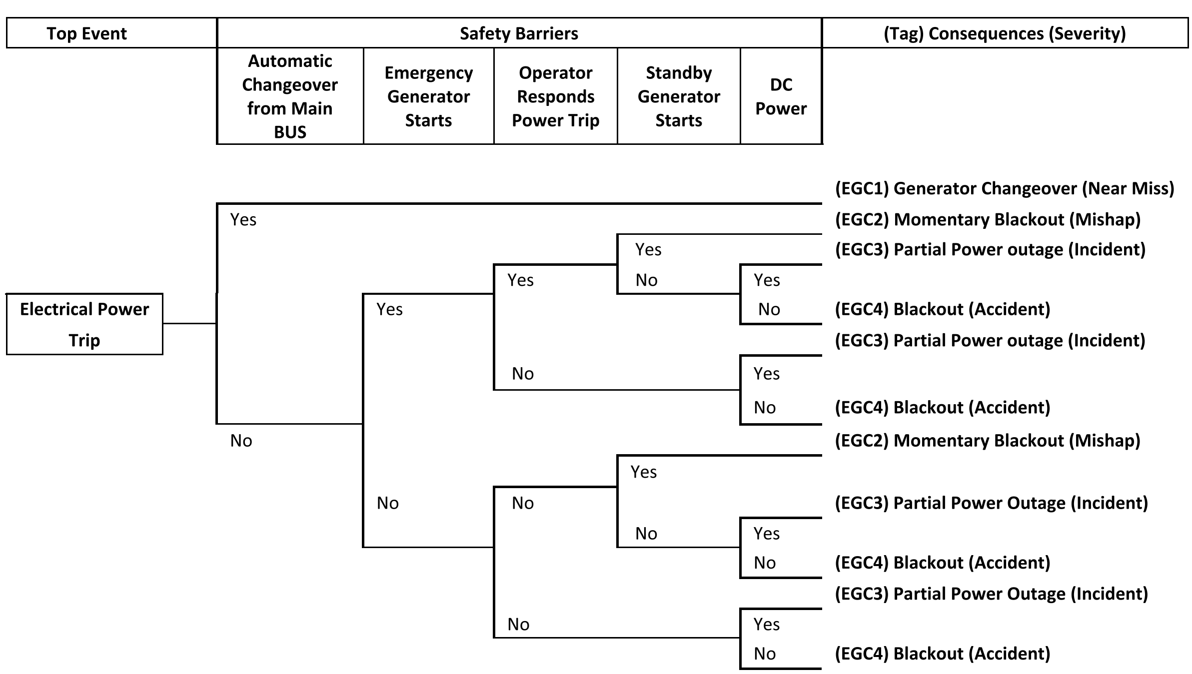


**Fig. 7.** Accident scenario in event tree for the electrical power trip.

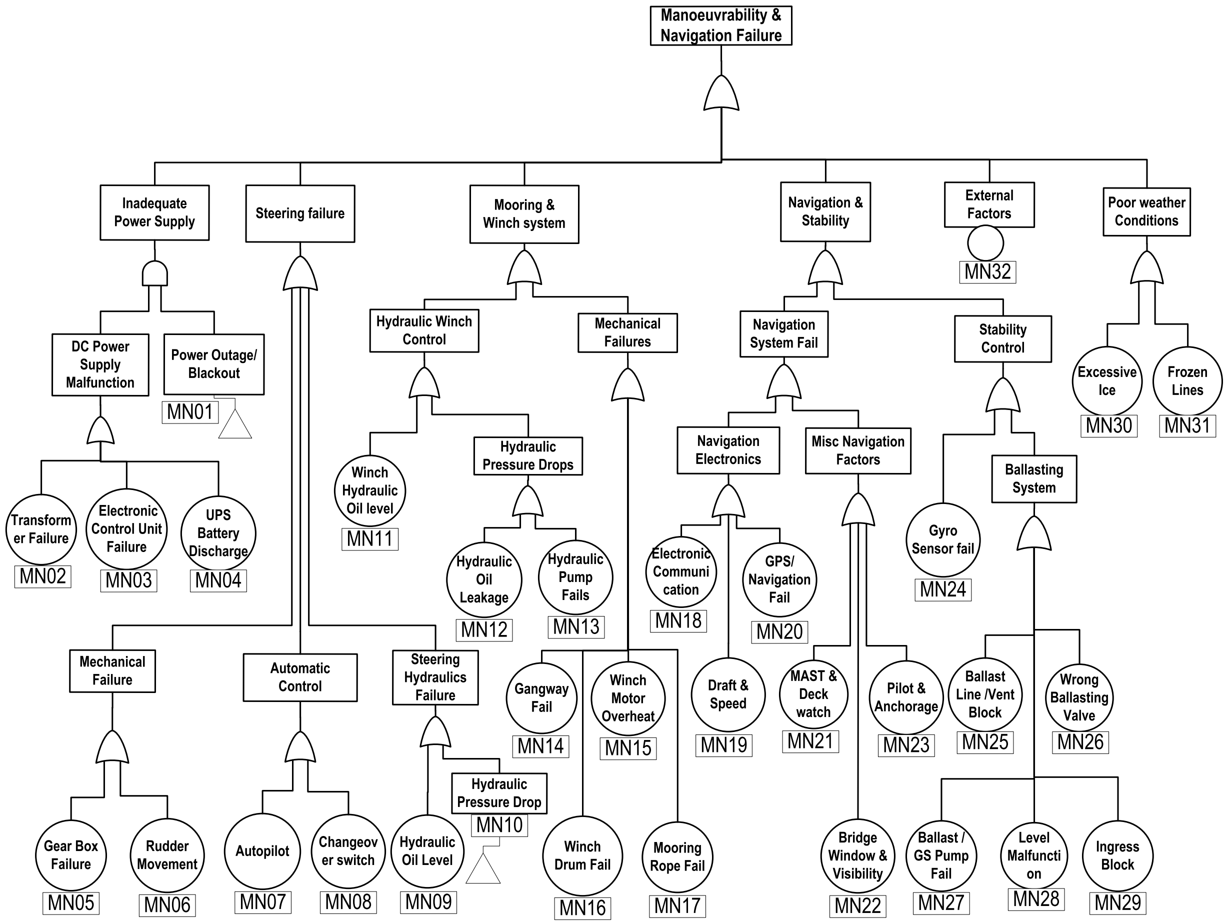


**Fig. 8.** Maneuverability and navigation system failure scenario in fault tree diagram.

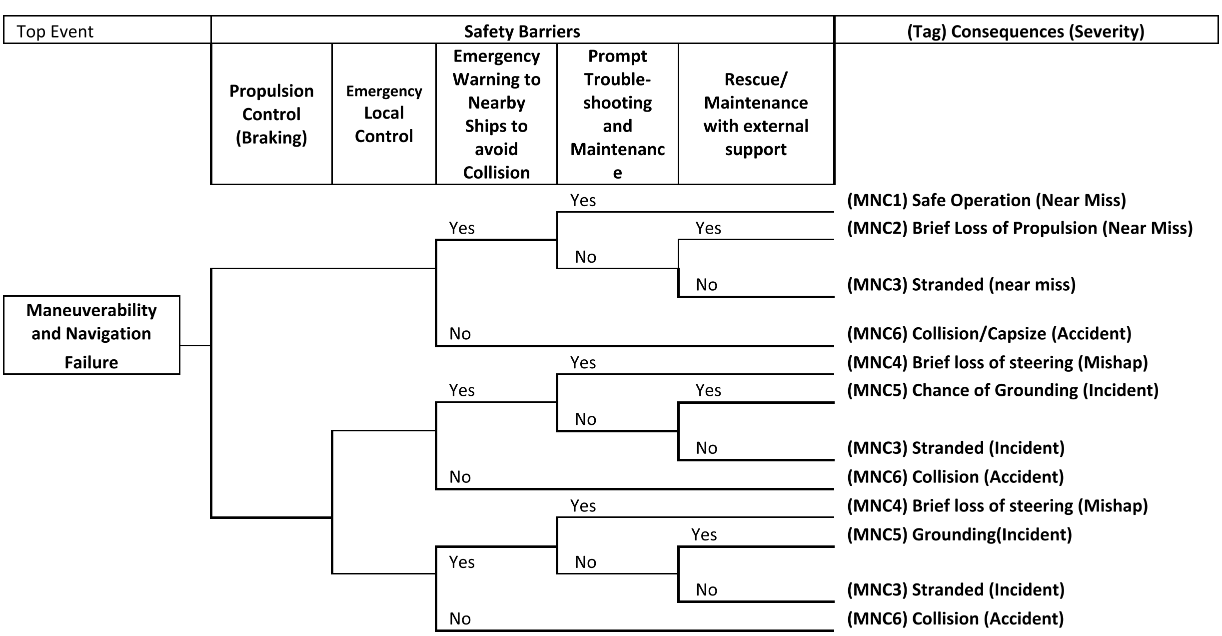


**Fig. 9.** Maneuverability and navigation failure scenario event tree diagram.

support the failure database. Canship Ugland Ltd. maintains a well-organized maintenance database for individual equipment based on maintenance criteria. This historical database includes the operating time, maintenance schedule, conditions, job lists and recommendations. Therefore, it provides vital support to the failure database with additional information on operating hours, degradation rate, equipment replacement or restoration, redundancies etc. A yearly database is prepared based on the condition-based history. The chronological degradation of any equipment has a numeric score, which marks equipment condition to describe the conditions and recommendations in

**Table 2**
Condition based maintenance ranking.

| Score | Condition | Recommended actions | Failure frequency weightage |
|---|---|---|---|
| 1 | Good | Normal state | 0 |
| 2 | Average | Frequent monitoring | 0.25 |
| 3 | Below average | Require maintenance on next stop | 0.50 |
| 4 | Poor | Immediate repair/replace | 0.75 |
| 5 | Breakdown | Urgent repair/replace with spare | 1 |

brief (Table 2). Knowledge acquired from the P&ID was used to support this failure database using the required design criteria- redundancies, connections, basic process controls, and safety system.

The failure database was developed based on equipment, where a set of components with functional accessories grouped as single equipment, to match primary events of the hazard scenario. Only the constant failure rate has been considered in the calculations to avoid complexities in such a big system. The frequency was estimated using the period between failures considering any deviation from a normal state as a failure. To develop the failure model and assess reliability for the long duration, authors have used the product of the weight (Table 2) and failure rate for the known specific period. It is done to address the continuous degradation of the equipment. The failure model of each equipment was different depending on the type of equipment (e.g. electrical components, rotating/stationary) and available data (incident reports/maintenance frequency/literature values). Although the Reliability values are based on 8.25 years of data, failure rates were calculated based on quarterly or, yearly frequency (depending on inspection intervals) and then formulated into a failure model. For example, in the case of electrical components (random failure) the maximum values were considered; while, for other mechanical equipment, the average failure rates were considered. In situations, where failure data is available from both incident reports and maintenance history, the higher failure rate data were used to reflect the worst-case scenario. For interested readers, general formulations and failure modes can be found in the literature [16].

For unobserved failures, different resources were used based on literature [42]. The failure database provides sufficient resources for reliability estimation for further analysis. In the case of observed failures, the maximum failure rate is interpreted as the worst-case scenario, which is more credible for calculations. However, when there was no observed failure, literature values for similar components were assigned. If the vendor information is available, using the vendor database is more practical. In this case study, the existing reliability database in OREDA handbook [43] and Lee' Loss Prevention [44] provided the literature values. However, in rare cases, as an alternative approach, it can be assumed that the component is at 70% of the way to fail [16] while estimating reliabilities. Table 3 lists a sample historical reliability database for fire & explosion hazard scenario. Relevant additional lists of databases are available in the Appendix.

As the preventive barriers or safety barriers in the bow-tie analysis require failure data, the failure probabilities are calculated from the historical database only if sufficient information is available. Calculation of the probability of failure on demand was kept straightforward. As the information about demand was available from testing frequency, demands and observed failures during the period, deterministic estimates provided the failure probabilities. If there is no failure observed, generic values from the literature are assigned. Table 4 presents a sample of estimated failure probabilities for fire and explosion preventive barriers.

### 3.3. Subsystem reliability estimation (Bow-tie analysis)

Bow-tie analysis is the principal step to visualize the outcomes of this methodology. Once the historical reliability database is ready, the bow-tie models were used to quantify the sub-system reliabilities and accident likelihood estimation. This step also involves the validation of the models. The model results are evaluated with the observed sub-system failure frequencies to update the fault tree models. Fig. 10 illustrates the fire and explosion fault tree analysis. Conventional fault tree analysis has been followed for the calculations addressing redundancies, series and parallel sequences.

**Table 3**
Historical Reliability database for Fire & Explosion Hazard Scenario.

| Historical reliabilities<br>Event No. | Fire & explosion basic events | Reliability |
|---|---|---|
| FE03 | Nitrogen plant | 0.368 |
| FE04 | Nitrogen supply lineup | 0.846 |
| FE06 | Reserved inert gas | 0.368 |
| FE09 | Hatch seals/vents leak(inert) | 0.875 |
| FE10 | Human error (process spill) | 0.887 |
| FE11 | Engine component leakage | 0.717 |
| FE12 | Pump/seal leakage | 0.951 |
| FE13 | Process & fuel line leakage | 0.705 |
| FE14 | Bunker operation (spill) | 0.135 |
| FE15 | Oil tanks vent/hatch (spill) | 0.368 |
| FE17 | Portable container storage | 0.135 |
| FE18 | Maintenance operation spills | 0.990 |
| FE19 | Gas release detectors | 0.513 |
| FE22 | Rotating equipment overheat | 0.905 |
| FE23 | Fired heaters | 0.513 |
| FE24 | Heated surface | 0.905 |
| **Un-observed failures/ assigned reliabilities**<br>Event No. | Fire explosion basic event | Reliability |
| FE01 | Explosive materials | 0.497 |
| FE02 | Concentrate overheat | 0.791 |
| FE07 | Positive pressure monitor | 0.9546 |
| FE08 | Oxygen analyzer | 0.5134 |
| FE16 | Combustible dust | 0.6065 |
| FE20 | Electric spark | 0.972 |
| FE21 | Mechanical spark | 0.999 |

**Table 4**
Probability of failure on demand fire & explosion preventive barriers.

| Safety barriers | Observed failures | The probability of failure on demand (P = n/D) |
|---|---|---|
| Fire fighting (pump & lineup) | 1 | 0.010101 |
| Fire detectors (from CBM) | 1 | 0.083 |
| Fire extinguishers | 1 | 0.0020 |
| Emergency evacuation (lifeboat) | 2 | 0.0303 |

Fig. 11 shows a sample calculation of even tree analysis for potential fire and explosion hazard. Historical failure probabilities are utilized to estimate likelihood probabilities.

Similar bow-tie analysis provided an estimation of sub-system reliabilities for all four models developed. The results section discusses further the outcomes from the analysis.

### 3.4. Risk estimation

Bow-tie analysis results provide the circumstantial likelihood of the consequences for each scenario. The impact or loss values based on the severity of the consequence can provide risk estimation. As no concrete financial information was available for the vessel in the case study, the scope of this current work does not cover the financial risk estimation. The following section includes the likelihood results and comparison with the observed scenario.

### 3.5. Results

Table 5 represents the results from the fault-tree analysis, including estimated historical sub-system reliabilities and failure frequencies for each hazard scenarios.

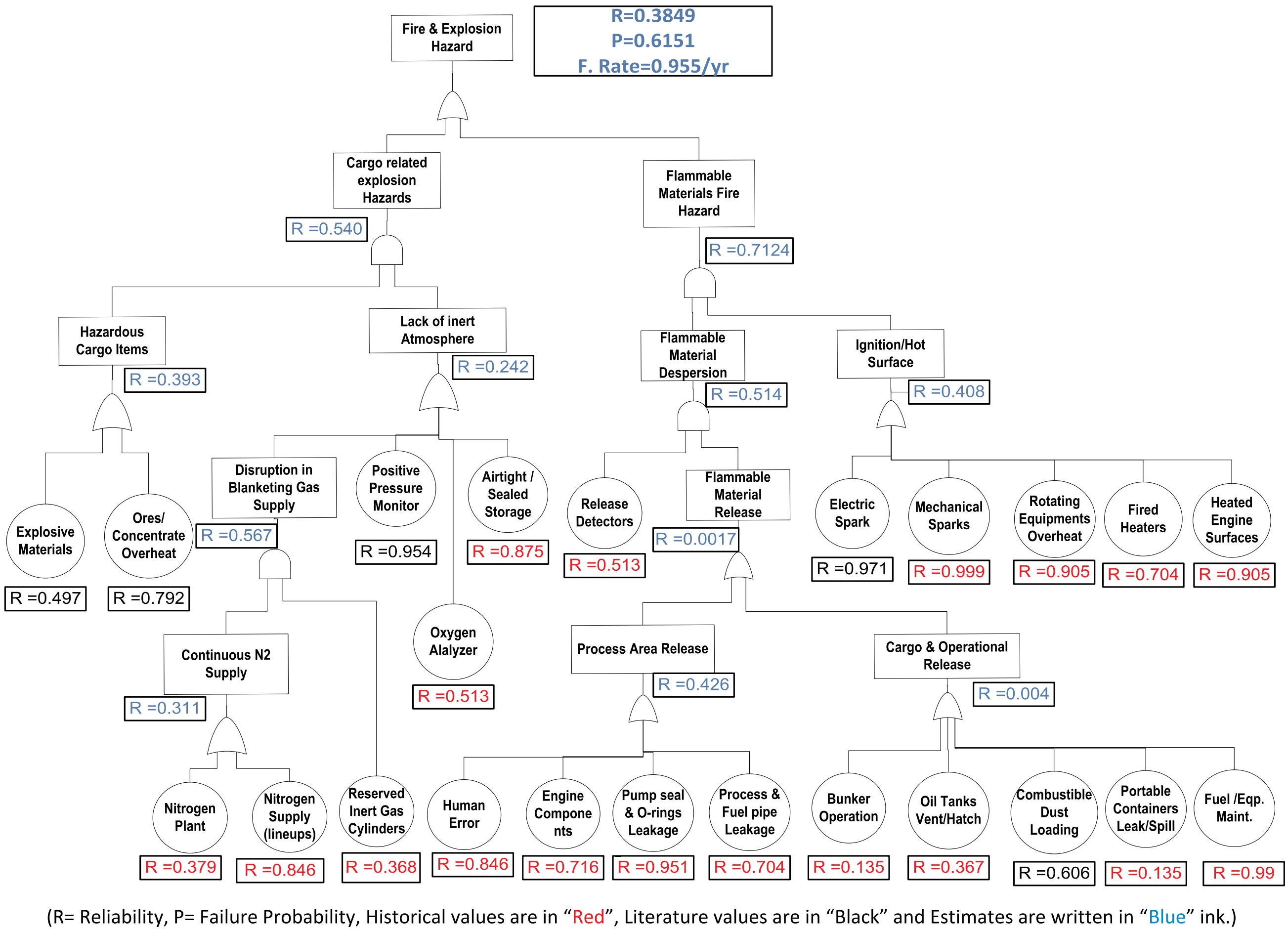


**Fig. 10.** Fault tree analysis of fire & explosion hazard scenario for the case study vessel.

The estimated likelihood of consequences for all four scenarios is available in Table 6. The following section presents further discussions on the results.

## 4. Discussion

This case study is the preliminary step of methodical risk management applications in the marine industry. Despite scarce data, it is still possible to perform reliability estimation from available information on the operational database. Although there were no observed accidents in the case study vessel, the likelihood information helps to foresee the vulnerable systems. Results obtained from this methodology are comparable to the actual scenarios. It is to emphasize that the actual scenarios used for validation are the reported incidents related to subsystem failures (e.g. blackouts, main engine slowdown/failure). These scenarios and related data were not considered as failures in the model development steps.

The hazard scenario models are validated comparing the sub-system reliability with the corresponding actual scenario. Table 7 lists the comparison with specific observations. From the comparison, it is evident that the estimated results are comparable to the observed failures. In the results, subsystem failure incidents reported are not necessarily system failures; it was any component failure or event which had the potential to affect the performance of the subsystem. For example, although there were no fire/explosion incidents reported, potential fire/explosion hazards (e.g., material spill, ignition hazard) are reported. The electrical power trip is not frequently reported in the near-miss database considering smooth change-over between power generation units are normal. From crew-members' feedback, in some cases, our estimation yields more acceptable results than the near miss reports.

Table 7 compares estimated and observed failure information on the more likely accidents. The main propulsion engine of the case study vessel consists of mostly mechanical components, where the breakdown/malfunction frequency is the highest which is 6.96/yr. However, the innovative design of the main engine offers each cylinder as a single unit which adds multiple levels of redundancies over the critical speed. According to the results, the electrical power generation related events are likely to occur more frequently. However, in the case study due to a high level of redundancies (2 standby generators, one emergency generator and DC power), except few reported momentary blackouts no major blackouts were observed.

Nonetheless, the power failure may lead to failure of other systems. Although the severity of consequences is higher in the rest of the scenarios, the results are acceptable considering different component in the system. Provided redundancies and preventive barriers are added in the analysis to achieve more competent results.

This work could be further improved by:

- Integrating vessel's critical component monitoring with risk assessment.
- Implementing data updating algorithm; this will keep the failure data updated and thus assist in assessing real-time risk.
- Using probabilistic tools, e.g., Bayesian statistics to adopt dynamic risk assessments framework.
- Considering advance approaches of data and model uncertainty, for example, Bayesian approach, Fuzzy set theory and evidence theory.
- Incorporating monetary values for consequences and thus evaluating financial risk and developing a risk management matrix based on acceptable risk criteria.
- Developing risk-based decision-making criteria for maintenance

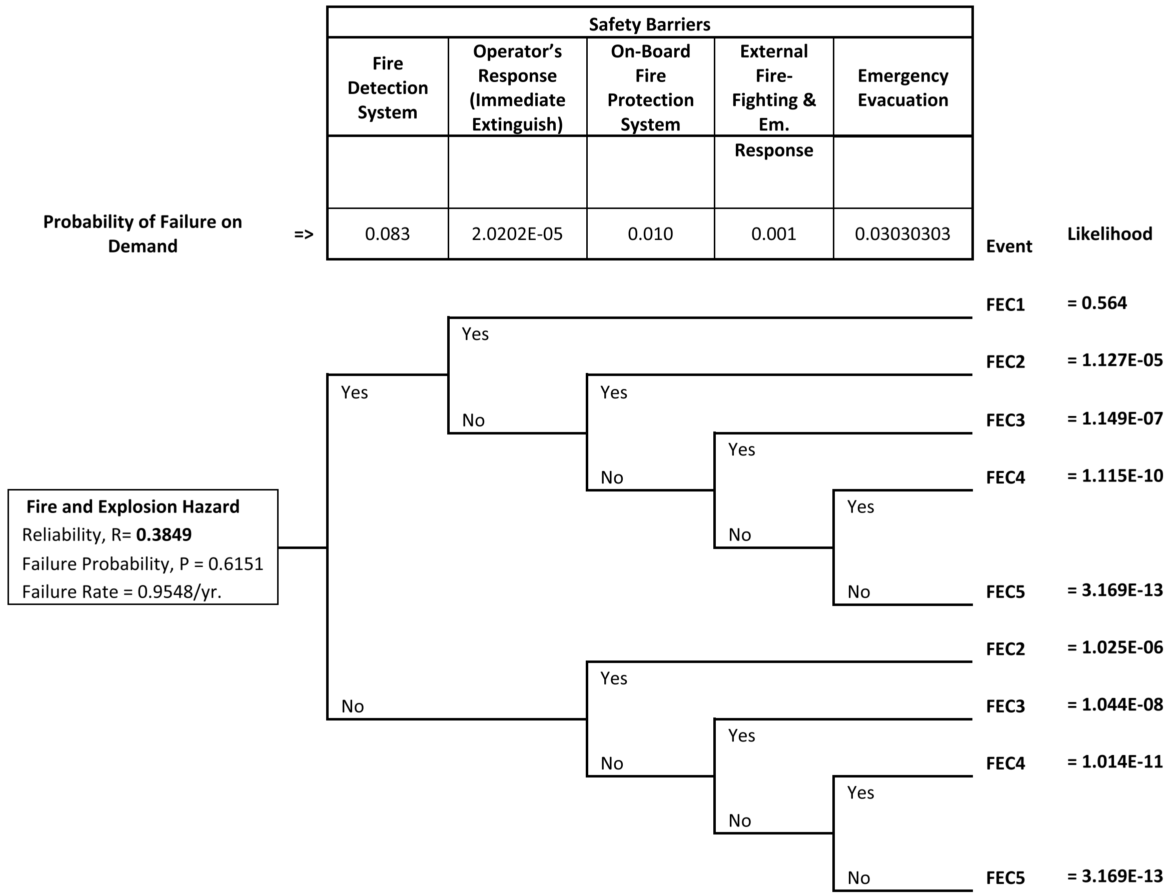

**Fig. 11.** Event tree analysis of potential fire and explosion hazard.

**Table 5**
Marine vessel subsystem reliabilities estimated from historical data.

| Sub-system | Hazard | Reliability | Failure Frequency |
|---|---|---|---|
| Deck and cargo | Fire and explosion hazard | 0.3849 | 0.95/year |
| Propulsion system | Propulsion failure | 0.0009 | 6.96/year |
| Power generation | Electrical power trip | 0.0031 | 5.78/year |
| Steering, stability and navigation | Maneuverability and navigation failure | 0.0276 | 3.59/year |

scheduling, voyage planning, personnel skill improvements, inventory and emergency planning and so on.

## 5. Conclusions

This work presents a practical and easy to implement risk assessment methodology as it uses an existing database. The bow-tie model is easy to comprehend and visualize. The developed models are comparable to actual scenarios. The results from risk assessment models match well with real-life observations. The preventive barriers are identified based on experience and design criteria. Therefore, some of the assigned probabilities are from literature. Extensive modelling and testing could provide more accurate failure probabilities.

This work is a significant step forward to establish a systematic and practical risk assessment framework for marine vessels. The framework could serve as a useful tool to manage vessel safety considering quantitative risk, which will help effective utilization of resources through prioritization and avoidance of unwanted events. This work could further be improved by considering uncertainty in the data and also by considering the detailed financial impact of the failure.

**Table 6**
Case study results from bow-tie analysis.

| Event | Consequences | Likelihood |
|---|---|---|
| a) Fire and explosion hazard scenario | | |
| **Event** | **Consequences** | **Likelihood** |
| FEC1 | Minor fire incident (near miss) | 0.5639 |
| FEC2 | Controlled fire incident (mishap) | 1.23E-05 |
| FEC3 | Fire/explosion (incident) | 1.25E-07 |
| FEC4 | Major explosion/fire (accident) | 1.22E-10 |
| FEC5 | Catastrophic explosion/fire (Catastrophe) | 6.34E-13 |
| b) Propulsion loss scenario | | |
| **Event** | **Consequences** | **Likelihood** |
| MEC0 | Engine changeover (safe) | N/A |
| MEC1 | Slowdown/propulsion loss (near miss) | 0.979177 |
| MEC2 | Rescue with assistance (mishap) | 9.79E-03 |
| MEC3 | Stranded (incident) | 9.79E-07 |
| MEC4 | Collision/grounding (accident) | 9.89E-05 |
| C) Electrical power trip scenario | | |
| **Event** | **Consequences** | **Likelihood** |
| EGC1 | Brief blackout/changeover (near miss) | 0.9966 |
| EGC2 | Momentary blackout (mishap) | 4.02E-03 |
| EGC3 | Partial blackout (incident) | 2.29E-03 |
| EGC4 | Total blackout (accident) | 2.43E-04 |
| d) Maneuverability and navigation failure scenario | | |
| **Event** | **Consequences** | **Likelihood** |
| MNC1 | Safe operation | 0.9617 |
| MNC2 | Brief loss of propulsion (near miss) | 9.72E-04 |
| MNC3 | Chance of being stranded (mishap) | 1.06E-06 |
| MNC4 | Lost steering for a short time (incident) | 9.71E-03 |
| MNC5 | Chance of grounding/drift (incident | 9.62E-03 |
| MNC6 | Chance of collision/capsize (accident) | 9.82E-06 |

**Table 7**
Comparison of estimated failure frequencies and actual scenario.

| Hazard/domain | Failure frequency (estimated) | Observed failure frequency (actual) | Observations |
|---|---|---|---|
| Fire and explosion hazard | 0.95/year | 2.66/yr. | No reported Fire Incidents, mostly material spill or near misses |
| Propulsion failure | 6.96/year | 6.3/yr. | M/E shut or in slowed down for maintenance (No major accidents reported) |
| Electrical power trip | 5.78/year | 1.09/yr. | Generator changeovers not reported in the reports. |
| Maneuverability and navigation failure | 3.59/year | 3.76/yr. | Mostly steering and navigation related near miss events (No accidents) |

## Acknowledgments

Authors thankfully acknowledge the financial support provided by the Natural Sciences and Engineering Research Council of Canada (NSERC) and Canship Ugland Ltd. for supporting this research by participating through the Engage program. Authors are thankful for the Canada Research Chair Program (Tier I) for the support to enable this study.

Authors are thankful to learned reviewers for their valuable feedback which helped to improve this manuscript.

## Supplementary materials

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.ress.2019.01.002.

## Appendix

*Appendix 1. Historical reliability data*

Tables A.1, A.2 and A.3

**Table A.1**
. Propulsion failure scenario reliability data.

| Event No. | Event title | Reliability |
|---|---|---|
| ME01 | Bottled air pressure | 0.943 |
| ME02 | Startup compressor | 0.700 |
| ME03 | Power outage/blackout | 0.003 |
| ME04 | Start-up hydraulics | 0.135 |
| ME05 | Service air compressor | 0.368 |
| ME06 | M/E trip signal | 0.497 |
| ME07 | M/E exhaust sensor | 0.867 |
| ME08 | Wiring(short circuit) | 0.990 |
| ME10 | L/O pump | 0.923 |
| ME11 | Pneumatic L/O supply | 0.787 |
| ME11 | L/O purifiers | 0.377 |
| ME12 | L/O line | 0.998 |
| ME13 | Fuel booster pump | 0.840 |
| ME14 | F/O supply | 0.598 |
| ME15 | F/O injectors | 0.526 |
| ME16 | F/O purifier | 0.001 |
| ME17 | F/O quality & temperature | 0.600 |
| ME18 | Cooler | 0.018 |
| ME19 | CW flow system | 0.368 |
| ME20 | M/E blower | 0.513 |
| ME21 | M/E turbochargers | 0.867 |
| ME22 | Air compressors | 0.607 |
| ME23 | Control air supply | 0.791 |
| ME24 | CCU/ACU control | 0.630 |
| ME25 | FIVA & speed governor | 0.751 |
| ME26 | ECU & hydraulic control system | 0.827 |
| ME27 | Coupling | 0.983 |
| ME28 | Stern tube & gearbox | 0.591 |
| ME29 | Lubrication | 0.651 |
| ME30 | M/E bearings | 0.925 |
| ME31 | Cylinder liner | 0.888 |
| ME32 | Cylinder mechanics | 0.651 |
| ME33 | Exhaust valves | 0.867 |
| ME34 | External factors | 0.999 |
| ME35 | Human (error) factors | 0.999 |

**Table A.2**
Electrical power generation system reliabilities.

| Event No. | Event title | Reliability |
|---|---|---|
| EG01 | Main bus | 0.002 |
| EG02 | (Short circuit) grounding | 0.819 |
| EG03 | Control panel | 0.522 |
| EG04 | Peripherical trip device | 0.819 |
| EG05 | Load controller | 0.497 |
| EG06 | Voltage regulator | 0.990 |
| EG07 | Rotor/stator | 0.512 |
| EG08 | Mechanical | 0.990 |
| EG09 | Coupling | 0.983 |
| EG10 | Gearbox | 1.000 |
| EG11 | Air compressors | 0.607 |
| EG12 | Governor & overspeed trip | 0.607 |
| EG13 | D/G control system | 0.572 |
| EG14 | Control air supply | 0.791 |
| EG15 | L/O pump | 0.923 |
| EG16 | G/E L/O purifiers | 0.223 |
| EG17 | L/O filter | 0.779 |
| EG18 | F/O injection pumps | 0.659 |
| EG19 | D/G fuel system | 0.792 |
| EG20 | F/O purifier | 0.001 |
| EG21 & EG22 | Cooling system | 0.368 |
| EG23 | D/G blower | 0.513 |
| EG24 | D/G turbochargers | 0.755 |
| EG25 | Cylinder mechanics | 0.941 |
| EG26 | Misc. mechanical | 0.741 |
| EG27 | Human (error) factors | 0.961 |
| EG28 | External factors | 1.000 |
| EG29 | F/O quality & temperature | 0.600 |

**Table A.3**
Maneuverability and navigation sub-system reliability data.

| Event No. | Event title | Reliability |
|---|---|---|
| MN01 | Power outage/blackout | 0.0031 |
| MN02 | Transformer | 0.9999 |
| MN03 | Electronic control unit | 0.5718 |
| MN04 | UPS battery | 0.9891 |
| MN05 | Gearbox | 0.8111 |
| MN06 | Rudder movement | 0.9990 |
| MN07 | Autopilot | 0.6065 |
| MN08 | Changeover switch | 0.9096 |
| MN09 | Hydraulic level | 0.9999 |
| MN10 | Hydraulic pressure | 0.9999 |
| MN11 | Hydraulic oil level | 0.9999 |
| MN12 | Hydraulic oil (leakage) | 0.5488 |
| MN13 | Hydraulic pump | 0.7919 |
| MN14 | Gangway | 0.6065 |
| MN15 | Winch motor | 0.8975 |
| MN16 | Winch drum | 0.6703 |
| MN17 | Loose/torn mooring cable | 0.9990 |
| MN18 | Electronics communication | 0.3679 |
| MN19 | Draft and speed sensor | 0.6065 |
| MN20 | DGPS and navigation | 0.6065 |
| MN21 | Mast and deck watch | 0.9999 |
| MN22 | Bridge window and navigator | 0.9716 |
| MN23 | Pilot and anchorage | 0.3679 |
| MN24 | Gyro sensor | 0.6065 |
| MN25 | Ballast vent | 0.7165 |
| MN26 | Line-up (wrong valve) | 0.7165 |
| MN27 | Ballast pump | 0.9306 |
| MN28 | Level measurement | 0.1889 |
| MN29 | Ingress (blockage) | 0.5134 |
| MN30 | Sea ice factor | 0.6065 |
| MN31 | Frozen lines | 0.9048 |
| MN32 | External factors | 0.9999 |

## References

[1] Corbett JJ, Winebrake J. The impacts of globalisation on international maritime transport activity: past trends and future perspectives. OECD/ITF Glob. Forum Transp. Environ. a Glob. World. Guadalajara, Mexico: Energy Environmental Research Associates, the US; 2008. p. 31.
[2] SOLAS. International Convention for the Safety of Life at Sea (SOLAS). 1974 http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx; 1974 (accessed September 22, 2017).
[3] IMO. Guidelines for ships operating in polar waters. 2010.

[4] Canada Shipping Act. Canada shipping act 2001 (c. 26). Ministries of Transport, Fisheries and Oceans; 2001.
[5] Blanco-Bazán A. Specific regulations for shipping and environmental protection in the Arctic: the work of the international maritime organization. Int J Mar Coast Law 2009;24:381–6. https://doi.org/10.1163/157180809X421734.
[6] Jensen O. Arctic shipping guidelines: towards a legal regime for navigation safety and environmental protection? Polar Rec POLAR REC 2008;44:107–14. https://doi.org/10.1017/S0032247407007127.
[7] Ellis B., Brigham L.. Arctic Marine Shipping Assessment 2009 Report. Protection of the Arctic Marine Environment Working Group; 2009.
[8] Kum S, Sahin B. A root cause analysis for Arctic Marine accidents from 1993 to 2011. Saf Sci 2015;74:206–20. https://doi.org/10.1016/j.ssci.2014.12.010.
[9] STCW. STCW 95 : international convention on standards of Training, Certification, and watchkeeping for Seafarers, 1978. London, England: International Maritime Organization; 1995.
[10] Smith DJ. Reliability, maintainability and Risk : practical methods for engineers including reliability centred maintenance and safety-related systems. 8th ed Saint Louis: Elsevier Science; 2011.
[11] Rausand M, Vatn J. Reliability centred maintenance. Springer Ser. Reliab. Eng.; 2008. https://doi.org/10.1007/978-1-84800-011-7_4.
[12] Nowlan FS, Heap HF. Reliability centered maintenance. Reliab Eng Syst Saf 1978;60:1–16. https://doi.org/10.1201/9781420031843.ch6.
[13] Smith AM. Reliability-centered maintenance. New York: McGraw-Hill; 1993.
[14] Moubray J. Reliability-centred maintenance. New York: Industrial Press; 1997.
[15] Li W. Reliability-centered maintenance. Risk Assess. Power syst. Hoboken, NJ, USA: John Wiley & Sons, Inc.; 2005. p. 211–27. https://doi.org/10.1002/0471707724.ch10.
[16] Spouge J. A guide to quantitative risk assessment for offshore installations. CMPT; 1999. Place of publication not identified.
[17] CCPS. Guidelines for chemical process quantitative risk analysis. Center for Chemical Process Safety/ American Institute of Chemical Engineers; 2000.
[18] Mokashi AJ, Wang J, Vermar AK. A study of reliability-centred maintenance in maritime operations. Mar Policy 2002. https://doi.org/10.1016/S0308-597X(02)00014-3.
[19] Choi I.-H., Chang D.. Reliability and availability assessment of seabed storage tanks using fault tree analysis 2016. doi:10.1016/j.oceaneng.2016.04.021.
[20] Moore NA, Perakis AN. Development of a diesel engine reliability database (DEREL) for the U.S. Coast Guard. Mar Technol SNAME News Summer 1999;36.
[21] Hovey DJ, Farmer EJ. Pipeline accident, failure probability determined from historical data. Oil Gas J 1993;91.
[22] Baalisampang T, Abbassi R, Garaniya V, Khan F, Dadashzadeh M. Review and analysis of fire and explosion accidents in maritime transportation. Ocean Eng 2018;158:350–66. https://doi.org/10.1016/j.oceaneng.2018.04.022.
[23] Li S, Meng Q, Qu X. An overview of maritime waterway quantitative risk assessment models. Risk Anal 2012;32:496–512. https://doi.org/10.1111/j.1539-6924.2011.01697.x.
[24] Yao Y, Meng C, Wang C, Jin S. Preventive maintenance policies for equipment under condition monitoring based on two types of failure rate. J Fail Anal Prev 2016;16:1–10. https://doi.org/10.1007/s11668-016-0111-4.
[25] Afenyo M, Khan F, Veitch B, Yang M. Arctic shipping accident scenario analysis using Bayesian Network approach. Ocean Eng 2017. https://doi.org/10.1016/j.oceaneng.2017.02.002.
[26] Brandsæter A, Hoffmann P. Marine shipping quantitative risk analysis. Oslo, Norway: ENBRIDGE Northern Gateway Project; 2010.
[27] Chai T, Weng J, De-qi X. Development of a quantitative risk assessment model for ship collisions in fairways. Saf Sci 2017;91:71–83. https://doi.org/10.1016/j.ssci.2016.07.018.
[28] Goerlandt F, Montewka J. A framework for risk analysis of maritime transportation systems: a case study for oil spill from tankers in a ship-ship collision. Saf Sci 2015;76:42–66. https://doi.org/10.1016/j.ssci.2015.02.009.
[29] Goerlandt F, Goite H, Valdez Banda OA, Höglund A, Ahonen-Rainio P, Lensu M. An analysis of wintertime navigational accidents in the Northern Baltic Sea. Saf Sci 2017;92:66–84. https://doi.org/10.1016/j.ssci.2016.09.011.
[30] Baksh AA, Abbassi R, Garaniya V, Khan F. Marine transportation risk assessment using Bayesian Network: application to Arctic waters. Ocean Eng 2018;159:422–36. https://doi.org/10.1016/j.oceaneng.2018.04.024.
[31] Zhang M, Zhang D, Goerlandt F, Yan X, Kujala P. Use of HFACS and fault tree model for collision risk factors analysis of icebreaker assistance in ice-covered waters. Saf Sci 2018;111:128–43. https://doi.org/10.1016/j.ssci.2018.07.002.
[32] Fu S, Yan X, Zhang D, Zhang M. Risk influencing factors analysis of Arctic maritime transportation systems: a Chinese perspective. Marit Policy Manag 2018;45:439–55. https://doi.org/10.1080/03088839.2018.1448477.
[33] Fu S, Zhang D, Montewka J, Zio E, Yan X. A quantitative approach for risk assessment of a ship stuck in ice in Arctic waters. Saf Sci 2018;107:145–54. https://doi.org/10.1016/j.ssci.2017.07.001.
[34] Valdez Banda OA, Goerlandt F, Kuzmin V, Kujala P, Montewka J. Risk management model of winter navigation operations. Mar Pollut Bull 2016;108:242–62. https://doi.org/10.1016/j.marpolbul.2016.03.071.
[35] Valdez Banda OA, Goerlandt F, Montewka J, Kujala P. A risk analysis of winter navigation in Finnish sea areas. Accid Anal Prev 2015;79:100–16. https://doi.org/10.1016/j.aap.2015.03.024.
[36] Goerlandt F, Montewka J. Maritime transportation risk analysis: review and analysis in light of some foundational issues. Reliab Eng Syst Saf 2015;138:115–34. https://doi.org/10.1016/j.ress.2015.01.025.
[37] Rathnayaka S, Khan F, Amyotte P. SHIPP methodology: predictive accident modeling approach. Part II. validation with case study. Process Saf Environ Prot 2011;89:75–88http://dx.doi.org/10.1016/j.psep.2010.12.002.
[38] Clarification of the risk concept - Petroleum Safety Authority Norway n.d. http://www.ptil.no/risk-and-risk-management/clarification-of-the-risk-concept-article11908-897.html (accessed December 25, 2018).
[39] ISO 31000. Risk management – Guidelines n.d. https://www.iso.org/standard/65694.html; 2018 accessed December 25, 2018.
[40] ISO 31000. Risk management – Principles and guidelines n.d https://www.iso.org/standard/43170.html; 2009 accessed December 25, 2018.
[41] Moosemiller M. Avoiding pitfalls in assembling an equipment failure rate database for risk assessments. J. Hazard. Mater. 2006. https://doi.org/10.1016/j.jhazmat.2005.07.064.
[42] Cadwallader LC, Eide SA. Component failure rate data sources for probabilistic safety and reliability. Process Saf Prog 2010. https://doi.org/10.1002/prs.10372.
[43] SINTEF Industrial Management. OREDA : offshore reliability data handbook. Høvik, Norway: Norske Veritas; 2002.
[44] Mannan S, Lees FP. Lee's loss prevention in the process industries : hazard identification, assessment, and control. Elsevier; 2012. p. 2757–95.