Journal of
Marine Science and Engineering

MDPI

Article

Model-Based Safety Analysis and Design Enhancement of a Marine LNG Fuel Feeding System

Konstantinos Milioulis †, Victor Bolbot † and Gerasimos Theotokatos *

Maritime Safety Research Centre, Department of Naval Architecture, Ocean and Marine Engineering, University of Strathclyde, Glasgow G4 0LZ, UK; konstantinos.milioulis.2017@uni.strath.ac.uk (K.M.); victor.bolbot@strath.ac.uk (V.B.)
* Correspondence: gerasimos.theotokatos@strath.ac.uk
† These two authors have equally contributed to this study.

Abstract: Recent regulatory requirements for shipping emissions control have led to the adoption of Liquefied Natural Gas (LNG) as a marine fuel and the design of LNG-fuelled vessels. Considering the potential safety implications due to system failure/unavailability, this study aims at the safety analysis of a low-pressure LNG fuel feeding system using a novel model-based methodology. The proposed methodology is based on the functional system modelling, leading to the failure diagrams development, and combines the use of Failure Modes, Effects, and Criticality Analysis (FMECA) and Fault Tree Analysis (FTA), which are performed in MADe™ and PTC Windchill software environments. The FMECA results are employed to identify the investigated system critical components and failures as well as specifying the top events for the subsequently performed FTA, which evaluates the top events failure rates. The system critical components identification leads to the system design modification targeting reduced safety metrics. This study results demonstrate that the evaporator, pressure build-up unit, sensors, and cryogenic valve assemblies are the most critical components of the investigated system, whilst the enhanced system design exhibits a failure rate reduced by 69% in comparison to the baseline system. This study reveals the advantages of the developed methodology along with some limitations of the employed tools and contributes to the quantitative safety analysis and design of ship complex systems.

Keywords: model-based safety analysis: liquefied natural gas low-pressure fuel feed system; failure modes; effects and criticality analysis**;** fault tree analysis; dynamic fault tree analysis

Citation: Milioulis, K.; Bolbot, V.; Theotokatos, G. Model-Based Safety Analysis and Design Enhancement of a Marine LNG Fuel Feeding System. *J. Mar. Sci. Eng.* **2021**, *9*, 69. https://doi.org/10.3390/jmse9010069

Received: 9 December 2020
Accepted: 7 January 2021
Published: 11 January 2021

1. Introduction

1.1. Background

Liquified Natural Gas (LNG) has become an attractive and cost-effective solution that reduces a ship's environmental footprint, ensuring compliance with existing and forthcoming legislation [1]. The LNG feasibility and comparative assessment to other alternative fuels and after-treatment technologies were demonstrated by various studies [1–5]. Ships that use LNG as their primary fuel vary both in type and size. Recent engine developments allowed for the use of dual-fuel engines of both the low- and high-pressure types [6]. More than 500 vessels fuelled by LNG have been in operation by 2020, which is mostly attributed to the lower natural gas prices in comparison to past and the global sulphur cap imposed in the same year [7].

LNG has been transported by LNG carriers since the 1960s, demonstrating an excellent safety record with only minor incidents being reported [6,7] compared to other industries [8]. According to [9], in total, 182 incidents had been reported for LNG carriers without involving major accidents due to LNG issues. The design and operation principles of the storage and feeding systems for LNG-fuelled ships are similar to the ones for the LNG carriers. LNG must be stored in temperature lower than −140 °C in pressurised tanks. However, the LNG use introduces new risks due to the low temperature, the implications from potential leakages, and the feeding system components failures. Thus, hazardous scenarios must be thoroughly investigated during the vessel design phase to ensure its safe design and operation [7]. The basic rules set out by the International Code of safety for ships using Gas and other low flashpoint Fuel (IGF code) can be used to control hazardous scenarios, but they are prescriptive to a certain extent. They ensure the safe operation of only specific system designs and layouts, leaving room for improvement in certain areas of system safety. Moreover, the technology is still relatively new, and there is a limited number of studies regarding the general safety and reliability analyses of LNG fuel feeding systems.

1.2. Literature Review

Several studies focussed on the risk estimation of leakages from LNG systems. Chu and Chang [10] investigated different natural gas leakage scenarios for an LNG-fuelled ship and conducted a fire risk assessment based on the identified leakages type and frequency. Fu et al. [11], aiming at the system safety enhancement, proposed a framework for a quantitative risk assessment, which included the identification of various hazards, their frequency estimation, the identified accidents consequence analysis. Lee et al. [12] studied the fire risk estimation comparing two types of fuel systems for LNG-fuelled vessels in several failure scenarios. The authors proceeded to a consequence analysis using Computational Fluid Dynamics (CFD) simulations, identifying the weaknesses of the investigated systems and introducing mitigating measures.

Other safety analyses dealt with the system operational enhancement. Nwaoha et al. [13] addressed the safety enhancement of an LNG carrier containment systems during bunkering. A risk formula was developed taking into account several failure factors and employed to optimise the maintenance of the LNG containment and transfer arms systems. Lv et al. [14] analysed the risks of the LNG-powered vessels passing through narrow locks considering the traffic density area, identifying safety limitations in the ship's operation.

Several studies focussed on introducing new components to increase the LNG fuel system safety and efficiency. Seo et al. [15] proposed a "boosting system" to control the LNG tank pressure for providing a continuous and stable natural gas supply to the ship engines without the use of cryogenic pumps. Park et al. [16] studied the design and use of multi-purpose compressors proposing a configuration that manages the generated boil-off gas safely.

To address the lack of accurate reliability data at the initial design stage of complex systems, Goo et al. [17] proposed a methodology integrating the system axiomatic design with Failure Mode, Effects, and Criticality Analysis (FMECA). Martins and Schleder [18] assessed the reliability of a regasification system of a floating, storage, regasification unit (FSRU) by employing Bayesian Networks, revealing the most critical components and proposing mitigating actions to improve the overall system safety.

Several studies reported safety analyses for variousi ship systems. Niculita et al. [19] estimated the reliability, availability, and maintainability metrics of a fuel-feeding system for an oil tanker propulsion engine and investigated the system design improvement by employing a model-based approach combined with conventional safety analysis methods in MADe™. Banks et al. [2] employed the Failure Modes and Effects Analysis (FMEA) to develop diagnostic systems for failure prevention for a marine diesel engine. Lazakis et al. [20] employed the combination of FMEA and Fault Tree Analysis (FTA) to develop algorithms for the predictive maintenance of a ship's main engine. Cicek et al. [21] also used FMEA to identify potential failures of a ship's engine fuel oil feeding system, supporting the development of a risk-based preventive maintenance plan.

Based on the preceding literature review, the following research gaps were identified: (a) only a limited number of research studies addressed the safety analysis and design enhancement of LNG fuel systems; (b) studies investigating the low-pressure LNG fuel feed systems, which are widely used by ferries and cruise ships, have not been reported; and (c) model-based approaches have not been employed for safety analysis of LNG fuel systems. Therefore, this study aims at developing a novel methodology for the safety analysis and design enhancement of a low-pressure LNG fuel feeding system based on Model-Based Safety Analysis (MBSA) tools.

The novel elements of the present study include the following: (a) the novel methodology based on model-based safety tools; (b) the safety analysis of a low-pressure LNG fuel feeding system; (c) the identification of critical components for the low-pressure LNG fuel feeding system using model-based FMECA; (d) the comparative assessment of alternative LNG fuel feeding system configurations using model-based Fault Tree Analysis; (e) the LNG fuel feeding system design enhancement for preventing failures.

The remainder of this study is structured as follows. In Section 2, the developed methodology and its rationale are described. Section 3 delineates the case study details and the required input parameters. The results of the developed methodology are presented and discussed in Section 4. In Section 5, the main findings are summarised, and the conclusions of the study are presented.

2. Materials and Methods

2.1. Methods and Tools

This study employs the MADe™ (PHM Technology: Melbourne, Australia) software [22], which is an advanced model-based engineering tool that supports the safety and criticality analyses of complex systems. The main advantage of MADe™ is the effective development of the system functional model that allows for the investigation of the system failure propagation, thus supporting the identification of the system critical components and their failure end-effects. Another advantage of MADe includes its functionality to generate or update the safety analysis results based on the investigated system model much faster compared with the use of traditional methods [22], thus rendering the safety analysis of modern complex systems more effective [23]. Furthermore, MADe™ incorporates the automated implementation of the traditional FMECA and Fault Tree Analysis (FTA). An additional advantage of MADe™ is the availability of a library with the various component failure modes, which also supports more rigorous safety analysis.

FMECA and FTA are well-established safety methods, which have been used for the systems safety analysis and assurance extensively [24]. FMECA is an inductive method, where each component failure impact on the system safety is independently evaluated [25]. FMECA results in the identification of the critical physical failures and the evaluation of all the components failure modes. FMECA results facilitate the identification of top events, which can be used as input for the development of Fault Tress [26]. However, the FMECA disadvantage is that only single-point failures are captured [27]. For analysing multiple failures simultaneously, FMECA needs to be combined with FTA (or Dynamic Fault Tree Analysis (DFTA)) [27,28].

According to [25], the following steps are recommended for the system design enhancement: system functional model development, criticality assessment based on what-if analysis, Fault Trees development, system design enhancement based on developed Fault Trees, and generation of the FMECA table. However, the FMECA results are not used for the system safety enhancement but facilitate the detailed reporting for the whole safety analysis. MADe™ is not a purely Fault Tree tool; hence, it is not best suited for editing certain aspects of Fault Trees or Dynamic Fault Trees, which are critical for the systems safety analylysis. Furthermore, it is necessary to refine the Fault Tree generated by MADe™ to account for redundant components. Thus, MADe™ does not adequately support the quantitative safety analysis of complex systems, and thus, the use of PTC Windchill (PTC: Boston, MA, USA) is employed to facilitate the quantitative DFTA in the present study (overcoming this limitation of MADe).

2.2. Methodology Description

A novel model-based methodology for safety analysis of ship systems based on the MADe™ and PTC Windchill is proposed in this study. The steps and interconnections of this methodology are presented in Figure 1. In Step 1, the available information required for the safety analysis of the investigated system, including the information for the components failure modes and reliability data, is gathered. Step 2 includes the system functional model development in MADe™ based on the information acquired in Step 2. Step 3 deals with the functional model enrichment using the component failure modes (identified in Step 1). When required, additional component failure modes, mechanisms, and causes are added directly from MADe™ libraries. In Step 4, FMECA is implemented in MADe™ supported by what-if analysis based on the functional model (developed in Steps 2 and 3). FMECA is subsequently used to analyse and rank the system failures. Step 5 focusses on design enhancement and modification by using the FMECA results. Step 6 includes the development of Dynamic Fault Trees (or Fault Trees) for the quantification of the identified top events failure rates. The qualitative FT is initially developed in MADe™, and subsequently, the refined FTs are modelled in PTC Windchill [29]; the latter is used for the quantitative FTA. The Fault Trees developed for both the baseline and the enhanced system designs results (failure rates of the selected top events) are comparatively assessed to verify the associated safety enhancement.

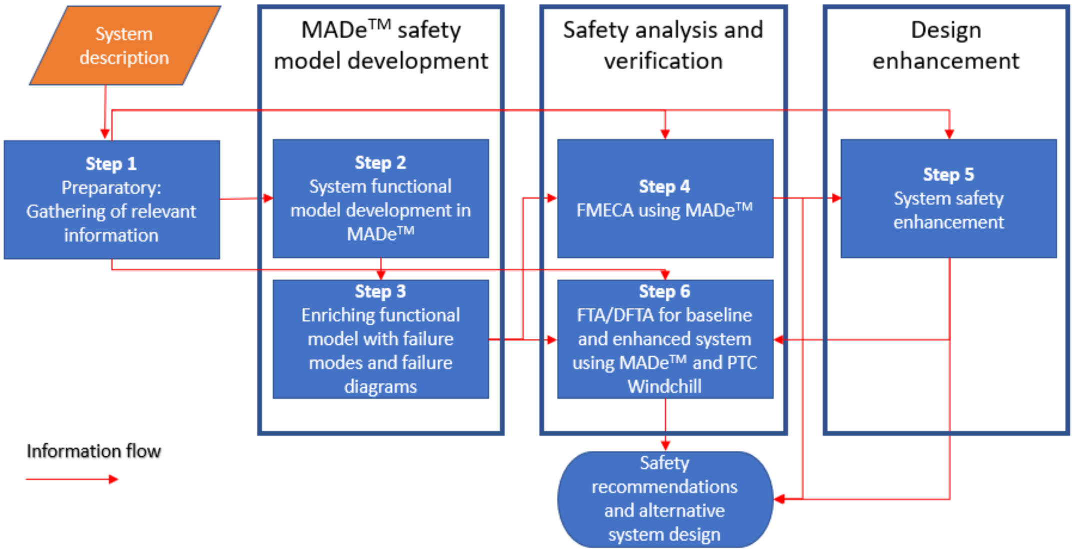

System description
MADe™ safety model development
Safety analysis and verification
Design enhancement
Step 1 Preparatory: Gathering of relevant information
Step 2 System functional model development in MADe™
Step 3 Enriching functional model with failure modes and failure diagrams
Step 4 FMECA using MADe™
Step 6 FTA/DFTA for baseline and enhanced system using MADe™ and PTC Windchill
Step 5 System safety enhancement
Safety recommendations and alternative system design
Information flow

Figure 1. Methodology flowchart.

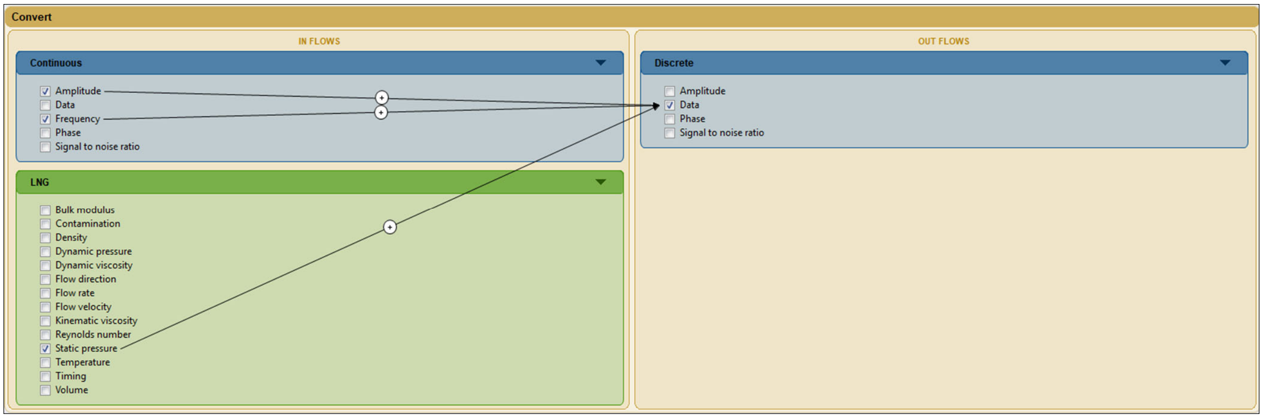
The novel elements of the presented methodology compared to the proposed approach for the systems safety analysis by using MADe™ [25,22,30] are the following: (a) the FMECA table is generated and used prior to the FTA; (b) the FMECA results are used for the system safety enhancement instead of the qualitative Fault Tree developed by MADe™; (c) both the MADe™ and PTC Windchill are employed; (d) quantitative analysis based on FTA and Dynamic FTA is used to verify the safety enhancement of the proposed system design alternatives.

2.3. Step 1—Preparatory Work

Based on the system description, typical failure modes for the system components are identified directly through the MADe™ libraries by exploiting a standardised failure concepts taxonomy. Further study of the pertinent literature is performed to determine more unusual failure modes expected for the investigated LNG system components, mainly due to their operation at low temperature. Some additional failure modes along with their respective failure rates are identified from the OREDA database [31] and pertinent publications on system safety or reliability [26,27]. This information is used in Step 3 to enrich the functional model (developed in Step 2) with failure modes and causes. The reliability data are used for the FMECA and FTA/DFTA in Steps 4 and 6, respectively.

2.4. Step 2—System Functional Modelling

The system functional modelling is based on the Fuzzy Cognitive Mapping (FCM) techniques [25]. First, the system is decomposed into its subsystems and components. Then, the subsystems and their components' functional models are developed by using the MADe™ software interface. Subsequently, the subsystems and components are interconnected using MADe™ built-in functions, which describe the operation of the system. Inflows and outflows are assigned to each function based on the functionality of the respective subsystem/component. A causal relationship is also defined for each inflow and outflow, which can take a positive or negative value depending on the individual functionality and its effect on the system operating parameters. For instance, the causal relationship between the inlet LNG flow and outlet natural gas flow of the pressure build-up unit (PBU) is positive, as the LNG mass flow entering the PBU is equal to the natural gas mass outflow. In this case, increasing the LNG mass flow rate will increase the natural gas mass flow rate. Each causal connection has a direction and a polarity. The direction of each connection represents the direction of the LNG flow. The polarity indicates whether the relationship between the connected parameters is positive or negative, i.e., directly or inversely proportional. An example of the LNG tank pressure sensor component functionality with its respective inflows and outflows is provided in Figure 2.



Convert

IN FLOWS

Continuous

☑ Amplitude
□ Data
☑ Frequency
□ Phase
□ Signal to noise ratio

LNG

□ Bulk modulus
□ Contamination
□ Density
□ Dynamic pressure
□ Dynamic viscosity
□ Flow direction
□ Flow rate
□ Flow velocity
□ Kinematic viscosity
□ Reynolds number
☑ Static pressure
□ Temperature
□ Timing
□ Volume

OUT FLOWS

Discrete

□ Amplitude
☑ Data
□ Phase
□ Signal to noise ratio

Figure 2. Liquefied Natural Gas (LNG) tank pressure sensor component functionality.

It is worth mentioning that some components may have more than one function, as their operation is described by several types of flows; this can also be modelled in MADe™. The system functional modelling is enriched in Step 3 and is used for FMECA and FTA/DFTA in Steps 4 and 6.

2.5. Step 3—Enriching the Functional Model with Failure Modes and Failure Diagrams

Following the development of the system functional model, Step 3 focusses on the definition of the failure modes for each system component, which will consequently lead to the generation of the component failure diagrams. A failure mode describes how a specific item fails to fulfil its assigned functionality [27]. To complete this step, the sources identified in the preparatory step (Step 1) (e.g., OREDA handbook, previous studies) are used. However, the majority of the failure modes can be identified by using the standardised failure concepts taxonomy system provided by MADe™. Based on these failure modes, failure diagrams are developed for each modelled system component. A typical failure diagram of the LNG tank pressure sensor is depicted in Figure 3.

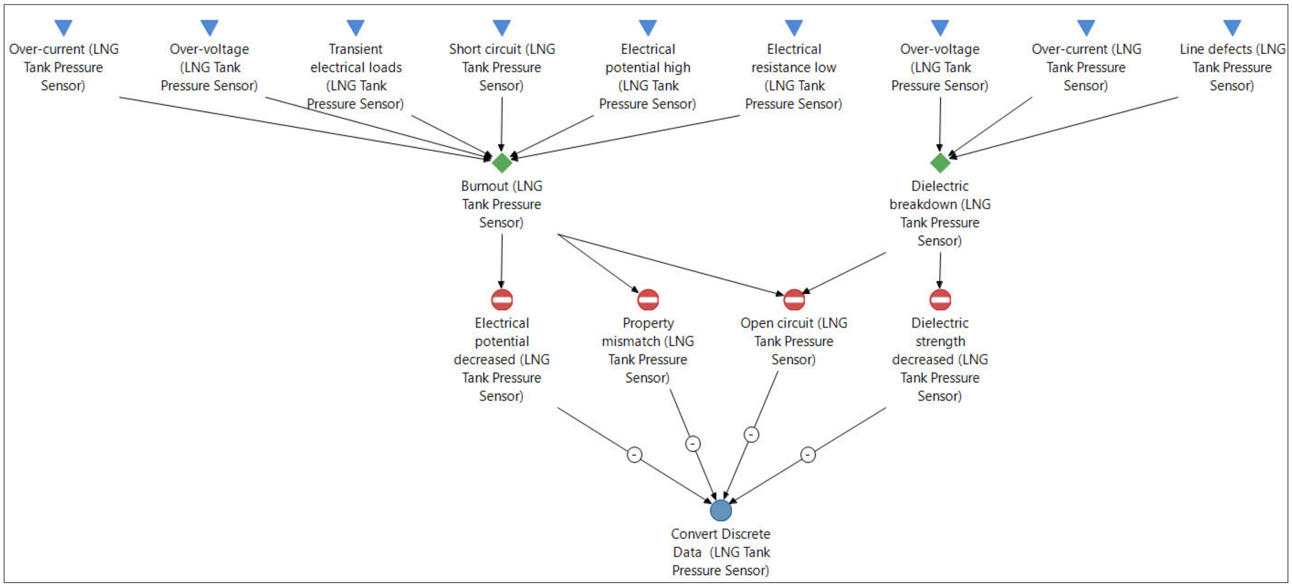

Over-current (LNG Tank Pressure Sensor)
Over-voltage (LNG Tank Pressure Sensor)
Transient electrical loads (LNG Tank Pressure Sensor)
Short circuit (LNG Tank Pressure Sensor)
Electrical potential high (LNG Tank Pressure Sensor)
Electrical resistance low (LNG Tank Pressure Sensor)
Over-voltage (LNG Tank Pressure Sensor)
Over-current (LNG Tank Pressure Sensor)
Line defects (LNG Tank Pressure Sensor)
Burnout (LNG Tank Pressure Sensor)
Dielectric breakdown (LNG Tank Pressure Sensor)
Electrical potential decreased (LNG Tank Pressure Sensor)
Property mismatch (LNG Tank Pressure Sensor)
Open circuit (LNG Tank Pressure Sensor)
Dielectric strength decreased (LNG Tank Pressure Sensor)
-
-
-
-
Convert Discrete Data (LNG Tank Pressure Sensor)

Figure 3. LNG tank pressure sensor failure diagram.

Failure diagrams show how failures can occur based on the physics of the specific failure mode. Failure diagrams also graphically represent and map out the series of mechanisms, causes, and faults, which ultimately lead to the failure of the component functionality. The available MADe™ failure propagation diagrams for standard components can be used, but user-specific failure propagation diagrams can be also developed. Following the definition of faults' failure modes, the failure diagrams (showing the mechanisms and causes) are automatically generated in MADe™. Failure diagrams will be used at a later stage in combination with the system functional model (developed in Step 2) to develop a failure propagation table, which is employed to reveal the components failure effects on the system (Step 4) and supports the development of Fault Trees (Step 6).

2.6. *Step 4—Failure Modes, Effects, and Criticality Analysis*

In this study, FMECA is implemented with the support of MADe™. Based on the developed functional model and failure diagrams, a failure injection process is conducted. According to this, a specific failure mode is assigned for each component (e.g., low natural gas temperature at the evaporator outlet), and subsequently, a step table is generated based on the developed functional model, which determines the propagation of the respective failures throughout the system. MADe™ allows the user to simulate one or many functional failures that can occur in the system. By providing specific user input, initial FMECA tables are generated in MADe™. The investigated system failures detection methods (required for ranking the identified failure modes as described in the following paragraph) are manually added to the FMECA table.

The Risk Priority Number (RPN) method is employed to rank the components failure modes [32]. The RPN ranking is associated to the following advantages: (a) it is well documented, which allows for its effective implementation; (b) its systematic and systemic nature is suitable for swift decision making on the system design alteration [33]. Since this study does not account for the system cost, the use of more sophisticated safety methods, such as the Total Efficient Risk Priority Number (TERPN) or the Global Safety Improve Risk Assessment (G-SIRA) [32–34], is not expected to provide additional advantages.

RPN is used to rank the different failure scenarios [17] and is estimated based on the likelihood of occurrence (O), the severity (S), and the detectability (D) of each failure, according to [26]. The occurrence rankings (O) are derived from the respective component failure rates (taken from Step 1). The severity ranking (S) describes the impact of a failure mode on the system operation. The severity of each failure mode (S) is defined based on the results from the failure propagation in MADe™, depicting the failure's impact on the system's safe operation. The detectability ranking (D) describes the ability of the system through sensors (for monitoring) and the control of various system components, to detect and self-mitigate possible failures and faults. The detectability is identified based on the availability and characteristics of the sensors and diagnostic systems installed in the investigated system. A typical FMECA example (without including the respectice criticality metrics) for the system evaporator is provided in Table 1. The FMECA results are used in Step 5 for system safety enhancement.

Table 1. Failure Modes, Effects, and Criticality Analysis (FMECA) typical structure (example of the LNG evaporator).

Component	**Function**	**Failure Mode**		**Causes of Failure**	
		Functional Failure	**Fault**	**Mechanism**	**Cause**
Evaporator	Converts LNG to natural gas at the desired temperature	Low natural gas temperature	Ice outgrowths	Ice formation	Low temperature

2.7. Step 5—System Safety Enhancement

Design improvements are proposed for all the identified critical components of the investigated system. The system safety enhancement can be achieved by altering each one of the RPN contributing elements. The failure occurrence likelihood (O) can be reduced by considering the use of superior materials for the system components, the control of the failure causes and mechanisms, as well as by the implementation of more frequent inspections and maintenance tasks. The severity of each failure (S) can be reduced by adding redundant components and by interconnecting various components. The detectability (D) can be improved by installing additional sensors and employing diagnostic systems.

2.8. Step 6—Fault Tree and Dynamic Fault Tree Analysis

A Fault Tree (FT) uses the logical connections, which are graphically represented to describe intermediate or basic events connected by "OR" gates and "AND" gates, all leading to the top event. The top event is usually an undesired effect on the investigated system or a failure, and the FTA reveals the failure propagation that ultimately causes the top event occurrence. The derived FT can be used for the estimation of the top event failure rate via a series of mathematical equations considering the basic event failure rates through the gates leading to the top event [35]. The calculation of the top event failure rate through an FT is considered as a safety-related importance measure, which can represent the investigated system safety [26]. In the case of Dynamic Fault Trees (DFT), additional dynamic gates are used, such as Priority-AND (PAND), spare, Sequence Enforcing (SEQ) or Functional Dependency (FDEP) [36]. The DFTs are able to consider the temporal system effects, which can emerge in an LNG feeding system with redundant standby components [36].

In the proposed methodology, the Fault Trees developed automatically by MADe™ are used as a reference. As it is not possible to implement a detailed quantitative analysis in MADe™, these Fault Trees (or the corresponding Dynamic Fault Trees) are first refined to account for the system redundant and standby components as well as common cause failures [3,18,37,38]. Subsequently, these refined Fault Trees are modelled in PTC Windchill and employed for the estimation the top events failure rates.

3. Case Study Description

3.1. System Description

The baseline system considered in this study is a low-pressure LNG fuel feeding system, the layout of which is developed based on the information reported in [39] and [40]. This system is the most commonly used system type in LNG-fuelled vessels currently in operation and is expected to be used in future designs [41]. The function of the LNG fuel system is to transform the stored LNG into a gaseous form and heat it up so that the gaseous fuel complies with the ship dual-fuel engine(s) manufacturer requirements. The system supplies the natural gas to the ship engine(s) using a pressure difference between the LNG tank and the dual-fuel engine manifold, thus not requiring cryogenic pumps, at the desired temperature of 20 °C and pressure of approximately 5 bar [39]. The system layout is presented in Figure 4, whilst the list of system components and their description is provided in Table 2.

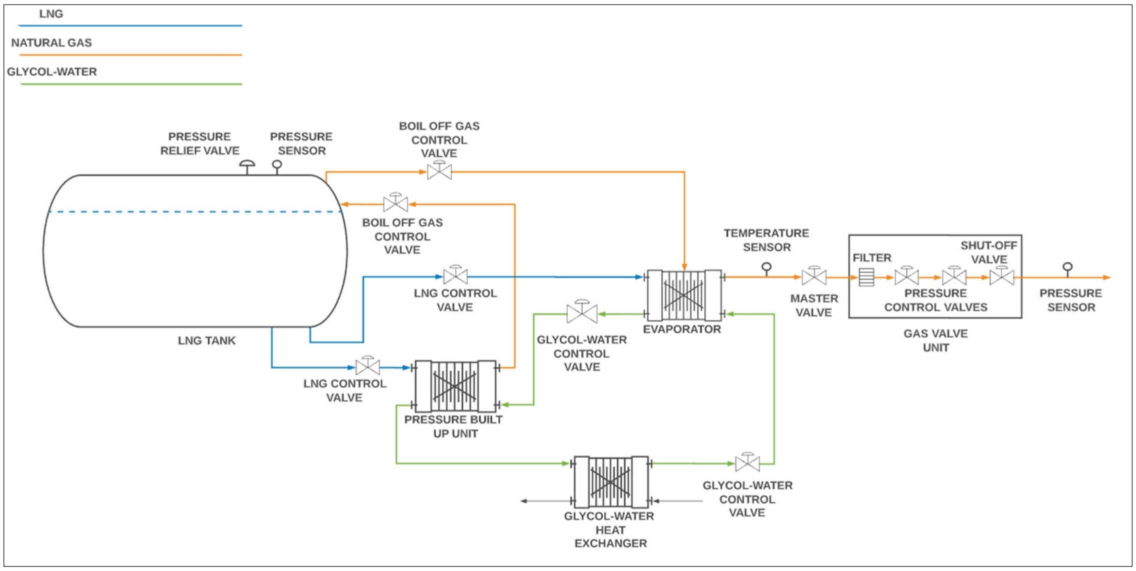


Figure 4. Low-pressure LNG fuel feeding system (adapted from [39]).

Table 2. LNG feeding system components description.

N°	Component	Description
1	LNG tank type “C”	The IMO type C tank is cylindrical by design and is a suitable solution for small-scale LNG storage. It can handle the increased pressure from boil-off gas (BOG) accumulation up to 9 bar rendering the need for BOG venting unnecessary [39].
2	Pressure build-up unit (PBU)	The pressure build-up unit (PBU) maintains a high pressure inside the tank by evaporating LNG. The PBU is utilised to maintain a steady flow of natural gas when the tank pressure drops. It consists of a heat exchanger (that employs a glycol-water solution as heating medium), insulated pipes, and regulating valves,; it is connected to the tank pressure monitoring system [39].
3	Evaporator	It is a heat exchanger that utilises a glycol-water solution as heating medium to evaporate the LNG and heat up the produced gas. The evaporator is designed so that it can deliver the gas to the engine at the required temperature of 20 °C. The evaporator also receives boil-off gas from the LNG tank, which is then heated to the desired temperature. It must be noted that the additional boil-off gas serves as a supplementary function and is not sufficient by itself to cover the requred engine fuel flow.
4	Glycol-water heat exchanger	It receives the cold glycol-water from the evaporator and PBU and heats it using warm engine cooling water to send it back and repeat the process.
5,6,7,8,9	Control valves (Boil-off gas control valve, LNG control	All the system valve assemblies include a valve control unit, a valve actuator, and a valve body. They are used to regulate the flow of the relevant medium.

	valve, glycol water control valve)	
10,11	Pressure and temperature sensors	The pressure and temperature sensors are used to monitor the relevant operating parameters. Their measurement is used to detect abnormalities in the system and to control the position (opening) of control valves. The temperature measurement is used to control the flow of glycol-water that enters the evaporator. The pressure measurement at the LNG tank is fed via a control signal to the PBU valve assembly, which maintains the high pressure inside the tank. One additional pressure sensor is placed after the GVU for regulating the natural gas pressure according to the engine(s) manufacturer requirements.
12	Natural gas filter	Cleans the natural gas from impurities before it enters the engine(s).
13	Pressure relief valve	A pressure relief valve is used to expand the pressure in the LNG tank if it exceeds the maximum allowed pressure.
14	Glycol-water	Glycol-water solution is a chemical mixture highly resistant to low temperature conditions and a reliable anti-freezer [40]
15	Gas valve unit (GVU)	It is a safety feature required by the classification societies and consists of a natural gas filter, and a series of pressure control, ventilating, and shut-off valves. It is included within a stainless steel enclosure, which is insulated and inerted for fire prevention, and it is located in a designated area outside the engine room. In this study, it is not considered as an assemply of separate components; instead, it includes the combined functionality of a natural gas valve assembly, shut-off valve, and natural gas valve filter.

3.2. Analysis Input

The failure rates that have been used in this analysis along with their sources are provided in Table 3. For the new redundant components that are added to the enhanced system design, a periodic inspection is assumed to take place every 168 h, which is in line with maintenance practices for other components.

Table 3. Component failure rates adopted from published historical data.

No.	Components	Estimated Range of Failure Rates Per Year
1	LNG tank minor failure [42]	10^{-7}
2	Pressure build-up unit (PBU) [31]	10^{-4}
3	Evaporator/Reheater [31]	10^{-4}
4	Glycol-water heat exchanger [31]	10^{-5}
5	Valve actuators [31]	10^{-6}
6	Valve control units [31]	10^{-6}
7	Valve body [31]	10^{-6}
8	Shut-off valve [31]	10^{-6}
9	LNG valve assembly [43]	10^{-3}–10^{-4}
10	Pressure sensor [44]	10^{-6}
11	Temperature sensor [44]	10^{-6}
12	Natural gas filter [18]	10^{-7}

3.3. Analysis Scope and Assumptions

Considering that the LNG feeding system is rather complex, it was necessary to limit the scope of the safety analysis by considering the following assumptions:

- The operation of the LNG fuel system is assessed in terms of its ability to supply natural gas at a constant temperature and pressure.
- Interactions with humans (undertaking the system operation and maintenance) are out of the scope of this study.
- The potential software and hardware failure modes for the system controllers are excluded from this analysis.
- System decomposition reaches to the subsystems and components level. The components parts failure modes are considered at the respective component level.

- The following worst-case scenarios were considered: (a) disruption of the natural gas supply and (b) shut down (stop) of the LNG fuel system. The severity ranking (S) of these scenarions was set to eight (8).
- Due to the lack of relevant data, the occurrence likelihood is considered the same for all the failure modes of each system component.
- The RPN threshold of 100 is employed to describe a safe system conditions in line with [32]. The systems components exhibiting the highest RPN values are flagged as critical.
- Pressure relief valves are excluded from this analysis, as they are not considered to influence the natural gas supply.
- Due to the lack of data for the LNG valve assemblies, the failure rates were not derived considering each valve component. Instead, one failure rate was assigned to all LNG valve components (actuator, body, control unit).

4. Results and Discussion

4.1. Step 1—Preparatory Work

The identified failure modes for the system components are provided in Table 4. The OREDA database [31], MADe™ [22], and MIL-HDBK-338B [26] were used to identify these failure modes. Most faults are referring to the degradation of the physical components caused by the low or fluctuating operating temperature or corrosion. However, for some components, failure can be caused by a combination of environmental conditions and inappropriate design, such as heat penetration to the LNG tank or by short-circuits for sensors. This information is used in Step 4 for the functional model enrichment.

Table 4. Failure modes of system components.

No.	Components	Failure Modes		
		Faults	Mechanisms	Causes
1	LNG tank	High boil-off gas evaporation rate	-	Heat penetration into the fuel tank
2	Pressure build-up unit	Fractured	Brittle fracture	Low temperature
		Ice outgrowths	Ice formation	Low temperature
		Shrunk	Thermal contraction	Low temperature
		Corroded	Corrosive fatigue	Temperature fluctuations
		Surface cracks	Corrosive fatigue	Temperature fluctuations
3	Evaporator	Fractured	Brittle fracture	Low temperature
		Ice outgrowths	Ice formation	Low temperature
		Shrunk	Thermal contraction	Low temperature
		Corroded	Corrosive fatigue	Temperature fluctuations
		Surface cracks	Corrosive fatigue	Temperature fluctuations
4	Glycol–water heat exchanger	Fractured	Thermal fatigue	Temperature fluctuations
		Corroded	Corrosive attack	Corrosive contaminant
		Perforated	Corrosive attack	Corrosive contaminant
		Shrunk	Thermal contraction	Low temperature
		Expanded	Thermal expansion	Temperature difference
5	Valve actuator	Open circuit	Tensile fracture	Transient mechanical load
		Fractured	Brittle fracture	Low temperature
		Seized	Abrasive wear	Insufficient lubricant
6	Valve control unit	Short circuit	Thermal degradation	High temperature
		Open circuit	Tensile fracture	Transient mechanical load
7	Valve body	Fractured	Brittle fracture	High mechanical load
		Blocked	Silting	Contaminated input flow
8	LNG valve actuator	Ice outgrowths	Ice formation	Low temperature
		Open circuit	Tensile fracture	Transient mechanical load
		Fractured	Brittle fracture	Low temperature
9	LNG valve control unit	Short circuit	Thermal degradation	High temperature
		Open circuit	Tensile fracture	Transient mechanical load
10	LNG valve body	Frozen	Ice formation	Low temperature
		Fractured	Brittle fracture	High mechanical load

11	Sensors	Open circuit	Burnout	Short circuit
		Electrical potential decreased	Burnout	Short circuit
		Dielectric strength decreased	Dielectric breakdown	Line defects or over-voltage
12	Natural gas filter	Blocked	Silting	Contaminated input flow

4.2. Step 2—System Functional Modelling

Following the system description, the analysis scope definition, and the identification of the component failure modes, the functional modelling of the investigated LNG fuel system was developed in MADe™. Table 5 presents the defined functions of each system component. Figure 5 presents the functional model flowchart of the investigated LNG fuel system, as it appears in MADe™. This flowchart almost follows the system layout diagram presented in Figure 4, using the MADe™ formalism.

Table 5. Component functionality in the model.

No.	Component	Functions
1	LNG Tank	Store/Provide LNG
2	PBU	Convert LNG, Regulate Pressure
3	Evaporator	Convert LNG, Regulate Pressure
4	Glycol-Water Heat Exchanger	Regulate LNG Supply, Increase Water Flow
5	Natural Gas Valve Actuator	Convert Amplitude to Mechanical Energy
6	Natural Gas Valve Control Unit	Convert Data to Amplitude
7	Natural Gas Valve Body	Regulate the Flow
8	LNG Valve Actuator	Convert Amplitude to Mechanical Energy
9	LNG Valve Control Unit	Convert Data to Amplitude
10	LNG Valve Body	Regulate the Flow
11	Temperature and Pressure Sensors	Convert Amplitude to Data
12	Natural Gas Filter	Regulate NG Supply, Decontamination

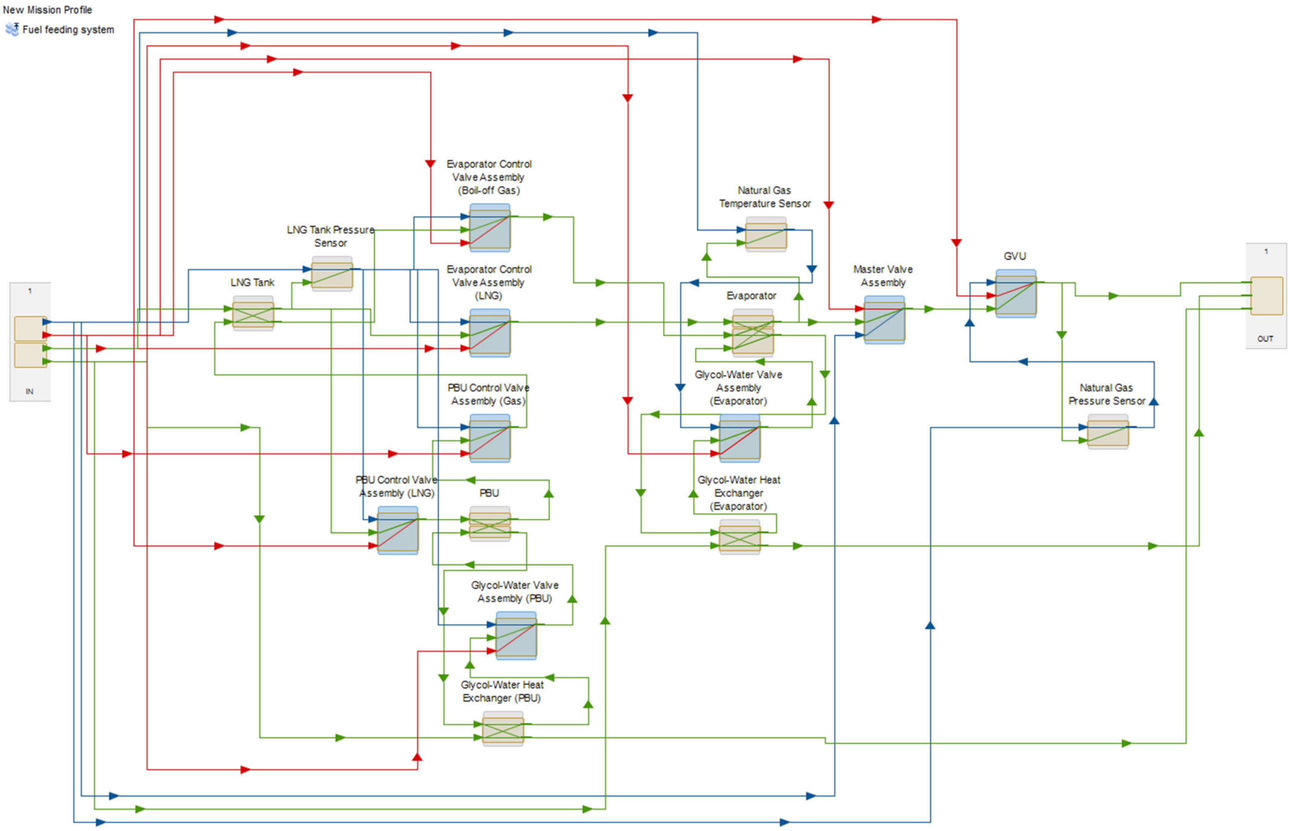

New Mission Profile
Fuel feeding system
1
IN
LNG Tank
LNG Tank Pressure Sensor
Evaporator Control Valve Assembly (Boil-off Gas)
Evaporator Control Valve Assembly (LNG)
PBU Control Valve Assembly (Gas)
PBU Control Valve Assembly (LNG)
PBU
Glycol-Water Valve Assembly (PBU)
Glycol-Water Heat Exchanger (PBU)
Natural Gas Temperature Sensor
Evaporator
Glycol-Water Valve Assembly (Evaporator)
Glycol-Water Heat Exchanger (Evaporator)
Master Valve Assembly
GVU
Natural Gas Pressure Sensor
1
OUT

Figure 5. LNG fuel system functional model in MADe™.

4.3. Step 3—Enriching the Functional Model with Failure Modes and Failure Diagrams

This study focusses on the system's functionality to supply a steady flow of natural gas at the required pressure and temperature range. The consequences of each failure mode will have a negative end-effect at the pressure and temperature of natural gas.

Based on the identified information in Step 1, the failure modes and failure diagrams are built for the investigated system components. As the produced amount of information is vast, only some indicative results are provided herein. The failure diagram of the LNG tank pressure sensor is presented in Figure 6. A combination of nine types of causes will lead to two different mechanisms (burnout and dielectric breakdown), which will then lead to three separate faults (open circuit, electrical potential decreased, and dielectric strength decreased). These faults will result in the deterioration of the tank pressure sensor signal quality (providing an erroneous output or no output at all), which will negatively affect the performance of the LNG valve assemblies that are controlled using this sensor signal.

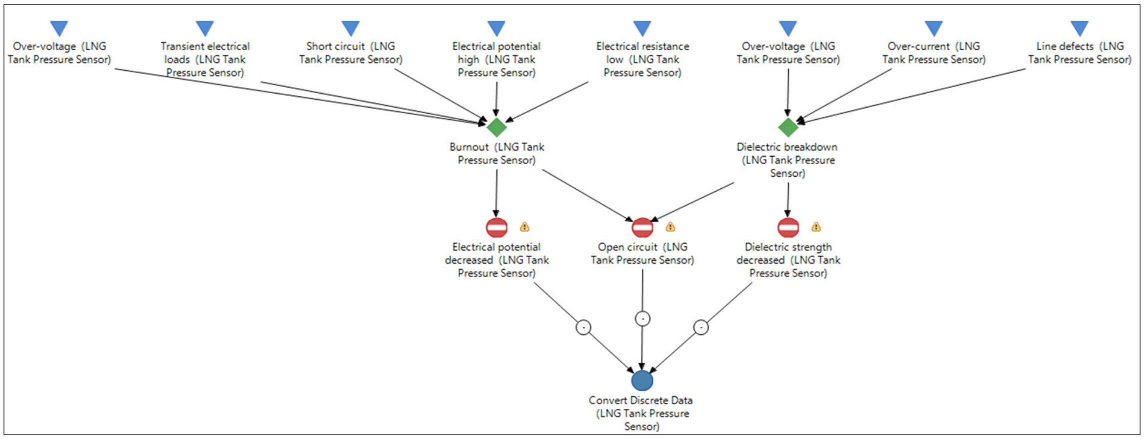

Over-voltage (LNG Tank Pressure Sensor)
Transient electrical loads (LNG Tank Pressure Sensor)
Short circuit (LNG Tank Pressure Sensor)
Electrical potential high (LNG Tank Pressure Sensor)
Electrical resistance low (LNG Tank Pressure Sensor)
Over-voltage (LNG Tank Pressure Sensor)
Over-current (LNG Tank Pressure Sensor)
Line defects (LNG Tank Pressure Sensor)
Burnout (LNG Tank Pressure Sensor)
Dielectric breakdown (LNG Tank Pressure Sensor)
Electrical potential decreased (LNG Tank Pressure Sensor)
Open circuit (LNG Tank Pressure Sensor)
Dielectric strength decreased (LNG Tank Pressure Sensor)
Convert Discrete Data (LNG Tank Pressure Sensor)

Figure 6. LNG tank pressure sensor failure diagram.

4.4. Step 4—FMECA and Safety Enhancement Based on MADe™

Following the LNG fuel feeding system modelling, the failure propagation of each component must be first investigated. Once the undesired failure is injected, the propagation of this failure within the LNG fuel system and its impact on to the system components are automatically generated in MADe™ in the form of numbered steps. In total, 13 functional failures were injected in the system, which are presented in Table 6.

Table 6. Functional failures injection affecting the supply of natural gas.

No.	Component	Flow Property	Functional Failure Response
1	LNG tank	Pressure	Low and High
2	Pressure build-up unit	Pressure	Low
3	Evaporator	Pressure and Temperature	Low
4	Glycol-water heat exchanger	Pressure and Temperature	Low
5	Valve actuators	Mechanical energy	Low
6	Valve control units	Amplitude	Low
7	Valve bodies	Pressure	Low
8	Pressure sensors	Data	Low and High
9	Temperature sensor	Data	Low and High
10	Natural gas filter	Pressure	Low

The generated FMECA table is presented in Table 7. The occurrence values (O) were derived based on the respective component failure rates. The detectability values (D) were derived taking into account the system layout, the accessibility of each component, and the relevant sensors, according to the guidelines provided in [28].

Table 7. FMECA table as generated from MADe indicating the Risk Priority Number (RPN) of each system component failure mode (O: Occurrence; S: Severity; D: Detectability).

No	Component	Function	Failure Mode	Causes of failure			Failure end effect	Detection method	Criticality			
			Functional Failure	**Fault**	**Mechanism**	**Cause**			**O**	**S**	**D**	**RPN**
1	LNG tank	Stores the LNG	Overpressure	High boil-off gas evaporation rate	-	Heat penetration into the fuel tank	To vent the excessive boil-off gas	LNG pressure sensor	**3**	**4**	**1**	**12**
2	Pressure build-up unit	Maintains the pressure inside the LNG tank	Disrupted natural gas supply to the LNG tank	Fractured Ice outgrowths Shrunk Corroded Surface cracks	Brittle fracture Ice formation Thermal contraction Corrosive fatigue Corrosive fatigue	Low temperature Low temperature Low temperature Temperature fluctuations Temperature fluctuations	To stop the entire system	LNG pressure sensor	**4**	**8**	**4**	**128**
3	Evaporator	Converts LNG to natural gas at the desired temperature	Low natural gas temperature	Fractured Ice outgrowths Shrunk Corroded Surface cracks	Brittle fracture Ice formation Thermal contraction Corrosive fatigue Corrosive fatigue	Low temperature Low temperature Low temperature Temperature fluctuations Temperature fluctuations	To stop the entire system	Temperature sensor	**4**	**8**	**4**	**128**
4	Glycol-water heat exchanger	Increases the temperature of the natural gas	Low natural gas temperature & pressure	Fractured Corroded Perforated Shrunk	Thermal fatigue Corrosive attack Corrosive attack Thermal contraction	Temperature fluctuations Corrosive contaminant Corrosive contaminant Low temperature	To stop the entire system	Temperature & Pressure sensors	**3**	**8**	**3**	**72**

				Expanded	Thermal expansion	Temperature difference						
5	Natural gas valve assembly	Regulates the flow of natural gas via control signal	Controller malfunction	Short circuit	Thermal degradation	High temperature	To stop the entire system	Natural gas temperature sensor	**2**	**8**	**3**	**48**
				Open circuit	Tensile fracture	Transient mechanical load						
			Actuator malfunction	Open circuit	Tensile fracture	Transient mechanical load						
			Valve body malfunction	Seized	Abrasive wear	Insufficient lubricant						
				Fractured	Brittle fracture	High mechanical load						
				Blocked	Silting	Contaminated input flow						
6	Glycol-water valve assembly	Regulates the flow of glycol-water via control signal	Controller malfunction	Short circuit	Thermal degradation	High temperature	To stop the entire system	Natural gas temperature sensor	**2**	**8**	**3**	**48**
				Open circuit	Tensile fracture	Transient mechanical load						
			Actuator malfunction	Open circuit	Tensile fracture	Transient mechanical load						
				Fractured	Brittle fracture	Low temperature						
			Valve body malfunction	Seized	Abrasive wear	Insufficient lubricant						
				Fractured	Brittle fracture	High mechanical load						
				Blocked	Silting	Contaminated input flow						
7	Shut-off valve	Blocks the flow of natural gas via control signal	Controller malfunction	Short circuit	Thermal degradation	High temperature	Failure to stop the supply of natural gas to the engine	Human perception, Natural gas pressure sensor	**2**	**10**	**2**	**40**
				Open circuit	Tensile fracture	Transient mechanical load						

			Valve body malfunction	Seized Fractured Corroded	Abrasive wear Brittle fracture Corrosive fatigue	Insufficient lubricant High mechanical load Insufficient lubricant						
8	LNG valve assembly	Regulates the flow of LNG via control signal	Controller malfunction	Short circuit Open circuit	Thermal degradation Tensile fracture	High temperature Transient mechanical load	To stop the entire system	LNG pressure sensor	**5**	**8**	**3**	**120**
			Actuator malfunction	Ice outgrowths Open circuit Fractured	Ice formation Tensile fracture Brittle fracture	Low temperature Transient mechanical load Low temperature						
			Valve body malfunction	Frozen Fractured	Ice formation Brittle fracture	Low temperature High mechanical load						
9	Pressure sensor	Measures the pressure inside the LNG tank	Faulty measurement	Open circuit Electrical potential decreased Dielectric strength decreased	Burnout Burnout Dielectric breakdown	Short circuit Short circuit Line defects or Over voltage	To stop the entire system	Incomplete engine combustion	**2**	**8**	**8**	**128**
10	Temperature sensor	Measures the temperature of the natural gas coming from the evaporator	Faulty measurement	Open circuit Electrical potential decreased Dielectric strength decreased	Burnout Burnout Dielectric breakdown	Short circuit Short circuit Line defects or Over voltage	To stop the entire system	Incomplete engine combustion	**2**	**8**	**8**	**128**
11	Natural gas filter	Cleans natural gas from impurities	Natural gas filter blocked	Blocked	Silting	Contaminated input flow	Natural gas flow pressure drop	Pressure sensor, regular maintenance	**1**	**4**	**2**	**8**

The severity (S) for most scenarios was set to 8 as stated in Section 3.3, since their failure leads to the natural gas unavailability. The investigated LNG fuel feeding system baseline configuration does not have any redundant components, which means that a component failure will most likely result in the fuel system operation disruption, thus jeopardising its safety. Therefore, the severity values for the component failures, which will cause the system stopping, will be high. However, the shut-off valve severity was set to 10, as the uncontrolled provision of natural gas can eventually lead to leakage and potential fire in the engine room. For the LNG tank overpressure, it is considered that it will lead to the release of natural gas in the environment. Natural gas primarily consists of methane, which is a gas with high global warming potential and potential for ignition. However, since the amount of stored gas and potential release is small, the tank is located outside the machinery space on deck, and since it is lighter than air, we can assume the effect to be small. The occurrence (O) of the glycol–water and the natural gas valve components (actuators, bodies, control units) were considered to be the same due to their identical failure rates.

The derived PRN values for the system main components are presented in Figure 7. As it can be observed, the RPN values for several components exceed the set RPN threshold (100), above which the failure scenarios are not considered safe. Based on these results, the following components are identified as critical: the evaporator, the PBU, the temperature and pressure sensors, as well as the LNG valve assembly. For the evaporator and the PBU, the combination of a moderate failure rates (O) and a high severity resulted in their high criticality. The pressure and temperature sensors are also found critical due to the high severity of their failure and the high difficulty of the detection of these failures. A sensor erroneous measurement/signal can only be detected through the installation of redundant sensors or by using model-based observers for monitoring the system components. Lastly, the LNG valves, which include all the cryogenic system valves, are found to be critical due to their high failure rate (attributed to the very low LNG temperatures [45]) and high failure severity.

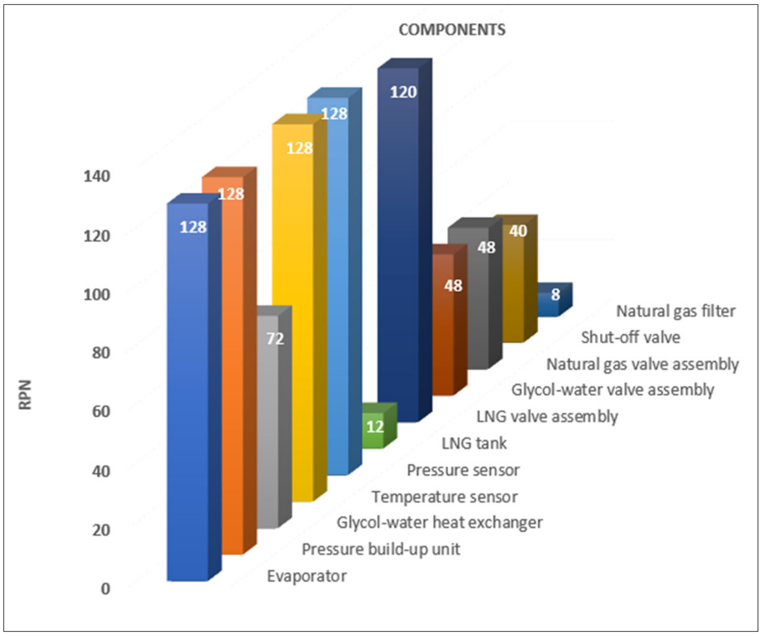


Figure 7. LNG fuel system component RPN values.

4.5. Step 5—System Safety Enhancement

The main weakness of the investigated system baseline configuration is the absence of redundant components, which can result in several single-point failures. To enhance the system safety, the system configuration needs to include fault-tolerant techniques allowing for the system operation in the presence of failures. The primary goal of the system designer is to divert the propagation of failures so that the system continues to operate despite failures. The modified system still must be able to detect, diagnose, and recover from the faults. Increasing the system redudancy can mitigate the failure of the the system components [26].

Based on the criticality analysis results, the following changes to the LNG fuel system baseline configuration are proposed to enhance its safety: (a) addition of by-pass cryogenic valves; (b) addition of temperature and pressure sensors to ensure accurate readings and diagnosis of potential system failures; (c) addition of heat exchanger/reheater and associated components; and (d) addition of a heating system inside the LNG tank. The resultant enhanced LNG fuel feeding system layout is presented in Figure 8, where the proposed design changes are displayed in red color.

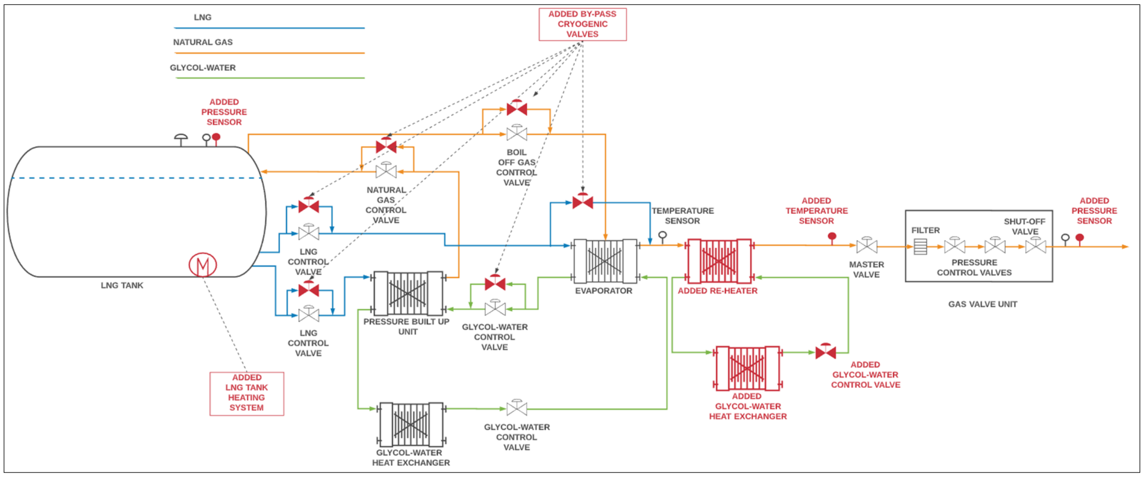


Figure 8. Modified LNG fuel feeding system to accommodate the proposed changes towards safety enhancement.

The added by-pass cryogenic valves include the following: (a) valves that operate at very low temperatures for both LNG control valves that regulate the flow to the evaporator and a PBU; (b) the boil-off gas control valve upstream of the evaporator; (c) the natural gas control valve downstream from the PBU; and (d) the glycol-water control valve downstream the evaporator.

An additional pressure sensor was added to the LNG tank so that the control can always receive appropriate tank pressure signal. A temperature sensor was also added downstream of the re-heater to ensure that the potential failures of the evaporator and the re-heater are detected. An additional pressure sensor at the end of the fuel line will ensure redundancy on the gas supply presure signal.

For addressing the evaporator criticality, a solution must be found, which besides the added redundancy also decreases the individual components thermal loading and therefore reduces the occurrence and severity of failures. After reviewing the pertinent literature on regasification systems [18,46], where multiple levels of evaporators and re-heaters were proposed to work in parallel to evaporate the LNG and heat up the produced natural gas, a re-heating system after the evaporator was added in the modified system configuration. The evaporator and the re-heater operate together with a reduced thermal load, decreasing the possibility of failures and at the same time increasing the system redundancy. The re-heating components include (a) the natural gas re-heater; (b) an additional glycol-water heat exchanger; and (c) an additional glycol-water control valve.

To mitigate a potential PBU failure, a heating system was added inside the LNG tank, as proposed in [15], where different types of LNG fuel feeding systems were compared.

This component operates in case of a PBU failure, using the glycol-water mixture to increase the LNG evaporation rate, thus maintaining the required LNG tank pressure.

4.6. Step 6—FT and DFT Analysis

The DFTA is employed in this study to validate the results from the FMECA and ensure that the proposed system changes indeed lead to enhanced safety. FTA was carried out for the baseline and the modified system configurations with the following top events: (a) natural gas temperature drop at the engine inlet; (b) natural gas pressure drop at the engine inlet; and (c) fuel feeding system shut down. Hence, six FTs/DFTs are developed in total. The failure rates presented in Table 3 are used as input in the performed FTA.

The FT for the top event (c) (fuel system shutdown) for the baseline system configuration, modelled in PTC Windchill [29], is presented in Figure 9. The other two top events (a and b) are intermediate events to this Fault Tree and their top events are included at the second level of the FT in Figure 9. The top events (a) and (b) include, in a lower hierarchy level, the failure of the glycol–water heat exchanger. However, as the latter is a common failure in the Fault Tree of the top event (c), it is propagated to the level below the top event. To simplify the presented FT, the subsystems were included (blue triangles in Figure 9) that include all the relevant basic events resulting in the LNG tank pressure drop and natural gas flow disruption, respectively.

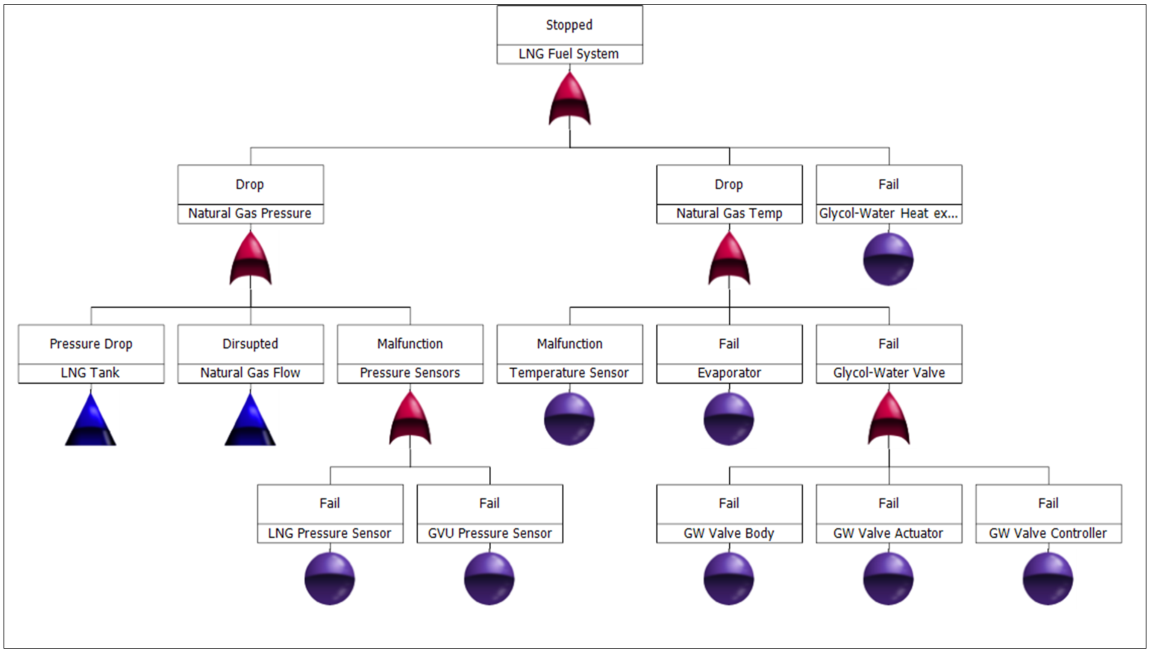


Figure 9. Baseline system configuration Fault Tree developed in PTC Windchill for the top event (c) (fuel system shut down).

The Fault Tree for the top event (c) for the modified system configuration, modelled in PTC Windchill [29], is presented in Figure 10. Similarly, with the previous Fault Tree, the considered top events (a) and (b) are intermediate events in the Fault Tree (c). The PAND gate is used for representing the failure of the heating subsystem, where the evaporator first fails, followed by the re-heater system failure. The FTs were refined to a certain extent to increase the results consistency by eliminating identical basic events occurring simultaneously. More details for these Fault Trees are provided in Appendix A.

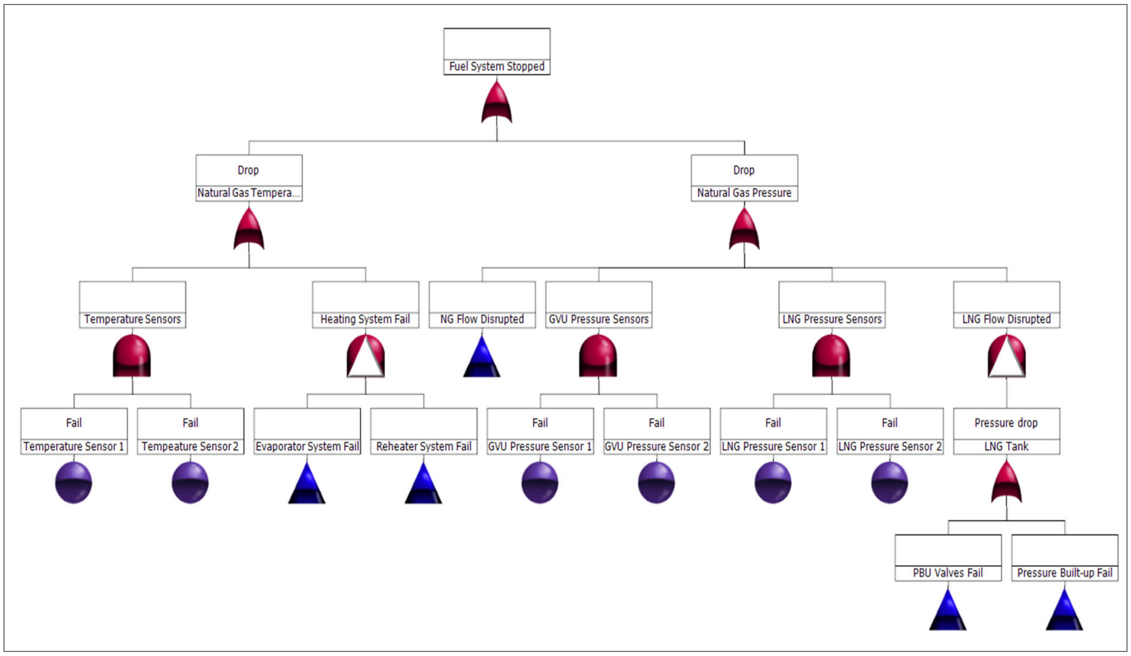


Figure 10. Modified LNG fuel system configuration Fault Tree developed in PTC Windchill.

The estimated failure rates for the baseline and the modified LNG fuel system configurations are provided in Figure 11 and Table 8. As expected, due to the added components and sensors, the results yielded a significant reduction in the failure rates for each top event. The most important top event is the "Fuel System Shut down", which represents the overall system failure.

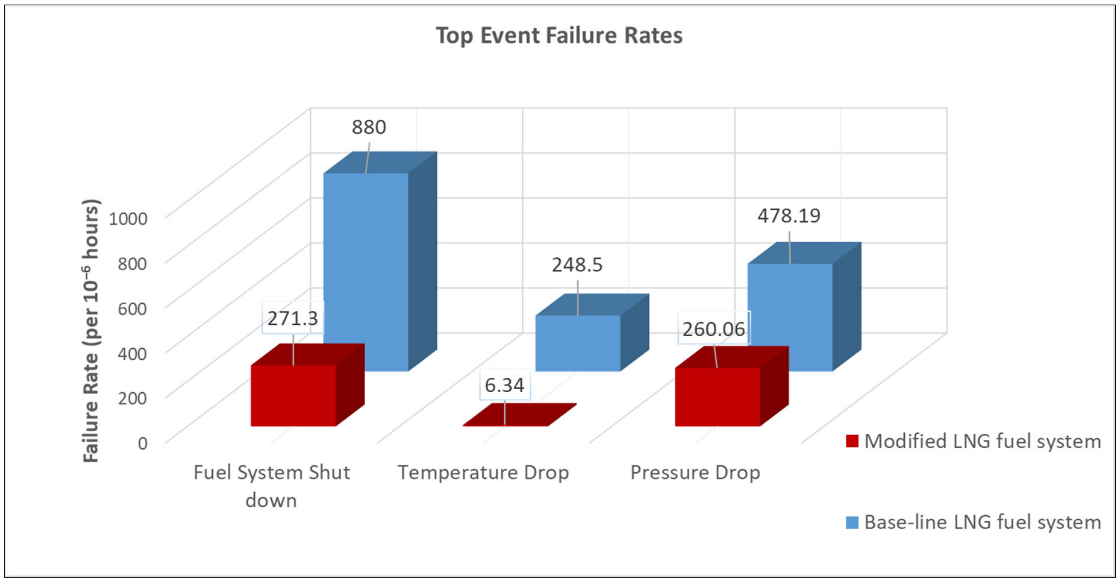


Figure 11. Derived failure rates for the baseline and modified LNG fuel system configurations.

Table 8. Enhanced LNG fuel system top event failure rates reduction.

Top Event	Reduction
Fuel System Shut Down	69%
Temperature Drop	97%
Pressure Drop	46%

4.7. Discussion on the Results and Methodology

The results in the first part of the analysis (FMECA) are aligned with the results of previous studies on LNG carriers systems [38] and shore regasification plants [18], exhibiting similar criticality metrics, using similar failure rate inputs. According to [38], the most critical components were found to be the cryogenic valve assemblies (referred to as, 'Process control valves'), followed by the boil-off gas (BOG) heater and vaporiser. According to [18], all the LNG gate valves and the cryogenic heat exchangers are the components that negatively affect the system reliability (represented as the time to failure).

The employed methodology proved to be useful and effective. The available libraries in MADe™ facilitated the application of the performed analysis. FMECA and Fault Trees were developed automatically from the relevant system models with minor adjustments. The methodology supported the system safety enhancement, and the derived system safety metrics were compared to the respective ones of the baseline system. A similar methodology with the presented could potentially be employed for safety analysis of other ship systems, such as propulsion systems and ballast treatment systems, and it can be extended for the case of other alternative fuels (e.g., hydrogen), thus providing to the system designer tools for the rendering the safety analysis during the system design process more effective.

The developed Fault Trees and the FTA implemented in MADe™ were comprehensive enough in terms of detail but lacked flexibility in terms of editing the intermediate events. In addition, they revealed limitations in calculating the system failure rate simultaneously accounting for both temperature and pressure drops. These concerns prompted the development and refinement of Fault Trees and Dynamic Fault Trees in PTC Windchill. Therefore, the complementary use of MADe™ in combination with other tools can be employed to further support the quantified safety analysis.

Finally, the control system failures (hardware and software) were not considerd in this study, which indicates that some failure scenarios were ignored [3]. Several assumptions were made regarding the distribution of failure modes. Furthermore, a cost–benefit analysis was out of the scope of in this study. However, from an industrial perspective, it is important to ensure that the system design is both safe, and cost-efficient. The OREDA database was employed to identify the system components failure rates, which are used to the RPN calculation. As OREDA is related to offshore assets systems/compnetes data, the use of such information for the case of ship systems/components is an important limitation. Nonetheless, these limitations provide directions for future research.

5. Conclusions

This study proposed a novel methodology for the ships systems quantitative model-based safety analysis, which combines the system functional modelling, the failure propagation analysis, FMECA, and FTA. This methodology was implemented for the low-pressure LNG fuel feeding system of an LNG-fuelled ship and led to the safety improvement of the investigated system.

The main findings of this study are the following:

- The system functional modelling substantially contributed to the better understanding of the system components interactions and their impact on the overall system safety.

- The FMECA led to the identification of failure modes and the RPN calculation, which resulted in the classification of the system critical components and the specification of the most critical failure events.
- The FTA allowed for the quantitative evaluation of the identified top events and the comparative assessment of the alternative system configurations employing as safety metrics the top event failure rates.
- The developed methodology effectively supported the quantitative safety analysis and the design of safe marine systems. In the design phase, emphasis must be placed on the critical system components, sensors, and control equipment.
- The most critical components (in terms of the RPN) of the investigated low-pressure LNG fuel feeding system were found to be the evaporator, the pressure build-up unit (PBU), the temperature and pressure sensors, as well as the LNG and cryogenic valve assemblies.
- The recommended modified system configuration included additional valves, a reheater assembly, an LNG tank heating system, as well as pressure and temperature sensors.
- The modified system configuration exhibited a reduction in the failure rate of the system shut down top event by 69% compared with the baseline system design.
- Particular attention must be placed on the quality of the data obtained from the pertinent literature, as it strongly influences the safety analysis results. As the LNG technology is relatively recent, data discrepancies or unavailability must be compensated by the use of reasonable and justifiable assumptions. In this respect, the results must be used with caution and need to be verified by considering the pertinent literature and experts' advice.
- The proposed methodology leads to better insights of the underlying parameters that affect the investigated system safety and can be swiftly applied to other ship systems.

Considering the immense pressure of the shipping industry to design and operate safe systems and adopt new technologies, this study provides a useful approach supporting the systems design with a focus on safety. Future studies will include the extension of the developed methodology to incorporate uncertainty and cost–benefit analyses, thus leading to a holistic design for safety approach.

Author Contributions: Conceptualization, K.M, V.B. and G.T.; methodology, K.M, V.B. and G.T.; software, K.M.; validation, V.B. and G.T.; formal analysis, V.B. and G.T..; writing—original draft preparation, K.M, V.B. and G.T.; writing—review and editing, K.M, V.B. and G.T.; visualization, K.M.; supervision, G.T.; project administration, G.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to confidentiality.

Acknowledgments: The authors greatly acknowledge the funding from DNV GL AS and RCCL for the MSRC establishment and operation. The opinions expressed herein are those of the authors and should not be construed to reflect the views of DNV GL AS, RCCL, or the acknowledged individuals and their associated organisations. The authors are grateful to PHM Technology for the provision of the academic licence of MADe™.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Employed Fault Trees and Dynamic Fault Trees structure

The Fault Trees that were developed in this study are presented in Figures A1–A3. Figure A1 shows the FT for the evaporator valves subsystem with the added by-pass cryogenic valves for the LNG fuel system modified configuration. Figure A2 presents the FT for the LNG tank pressure drop top event for the LNG fuel system baseline configuration. Finally, Figure A3 presents the FT for the top event of the disrupted natural gas flow for the LNG fuel system baseline configuration.

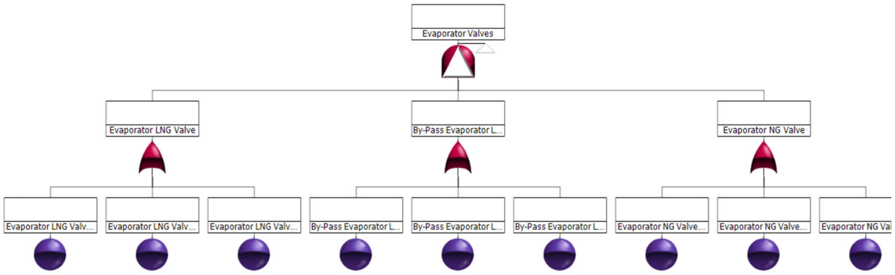


Figure A1. Fault tree for the evaporator valve subsystem developed in PTC Windchill.

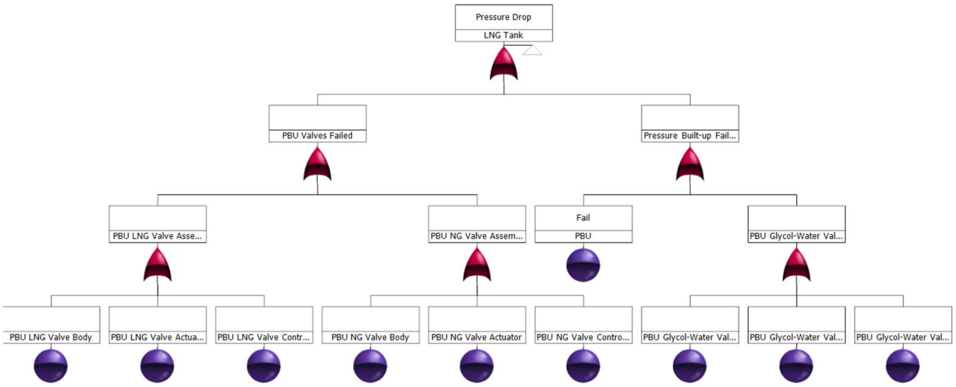


Figure A2. Fault tree for the top event of the tank pressure drop developed in PTC Windchill.

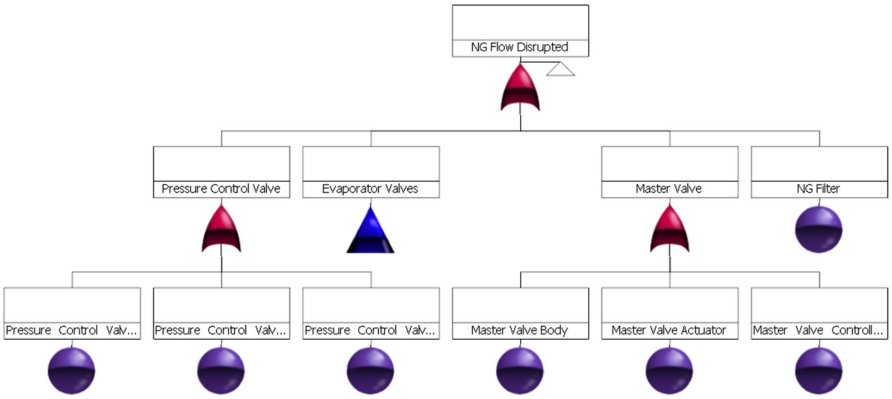


Figure A3. Fault tree for the top event of the disrupted natural gas flow developed in PTC Windchill.

Abbreviations

CFD	Computational Fluid Dynamics
CO_2	Carbon dioxide

ECA	Emission control areas
FMECA	Failure Modes, Effects, and Criticality Analysis
FTA	Fault Tree Analysis
DFTA	Dynamic Fault Tree Analysis
GA	Genetic Algorithms
HFO	Heavy Fuel Oil
IGF	International code of safety for ships using Gas and other low flashpoint Fuels
LNG	Liquefied Natural Gas
BOG	Boil-off gas
MBSA	Model-Based Safety Analysis
NOx	Nitrogen oxide
PM	Particulate matter
SOx	Sulphur oxide
PBU	Pressure build-up unit
GVU	Gas Valve Unit

References

1. Andersen, M.L.; Clausen, N.B.; Sames, P.C. Costs and benefits of LNG as ship fuel for container vessels. Available online: http://www.lngbunkering.org/sites/default/files/2013%20GL_MAN_LNG_study_web.pdf (accessed on 25 December 2018).
2. Banks, J.; Hines, J.; Lebold, M. *Failure Modes and Predictive Diagnostics Considerations for Diesel Engines;* Defense Technical Information Center: Virginia, VA, USA, 2001.
3. Bolbot, V.; Theotokatos, G.; Boulougouris, E.; Psarros, G.; Hamann, R. A Novel Method for Safety Analysis of Cyber-Physical Systems—Application to a Ship Exhaust Gas Scrubber System. *Safety* **2020**, *6*, 26.
4. Bolbot, V.; Trivyza, N.; Theotokatos, G.; Boulougouris, E.; Rentizelas, A.; Vassalos, D. Cruise ships power plant optimisation and comparative analysis. *Energy* **2020**, *196*, 117061.
5. Trivyza, N.L.; Rentizelas, A.; Theotokatos, G. A novel multi-objective decision support method for ship energy systems synthesis to enhance sustainability. *Energy Convers. Manag.* **2018**, *168*, 128–149.
6. Schlick, H. Potentials and challenges of gas and dual-fuel engines for marine application. Available online: https://www.cimac.com/cms/upload/events/cascades/cascades_2014_busan/presentations/Presentation_Session2_AVL_CASCADES_Busan_Oct2014_Harald_Schlick (accessed on 10 April 2019).
7. Pitblado, R.; Baik, J.; Hughes, G.; Ferro, C.; Shaw, S. Consequences of liquefied natural gas marine incidents. *Process Saf. Prog.* **2004**, *24*, 108–114.
8. Hamutuk, L. Appendix 4. History of Accidents in the LNG Industry. Sunrise LNG in Timor-Leste: Dreams, Realities and Challenges. Available online: <https://www.laohamutuk.org/Oil/LNG/app4.htm> (accessed on 4 January 2021).
9. IMO. FSA-Liquefied Natural Gas (LNG) Carriers Details of the Formal Safety Assessment. FORMAL SAFETY ASSESSMENT. Denmark: IMO. Available online: <http://www.safedor.org/resources/MSC_83-INF-3.pdf> (accessed on 4 January 2021).
10. Chu, B.; Chang, D. Effect of full-bore natural gas release on fire and individual risks: A case study for an LNG-Fueled ship. *J. Nat. Gas Sci. Eng.* **2016**, *37*, 237–247.
11. Fu, S.; Yan, X.; Zhang, D.; Li, C.; Zio, E. Framework for the quantitative assessment of the risk of leakage from LNG-fueled vessels by an event tree-CFD. *J. Loss Prev. Process Ind.* **2016**, *43*, 42–52.
12. Lee, S.; Seo, S.; Chang, D. Fire risk comparison of fuel gas supply systems for LNG fuelled ships. *Nat. Gas. Sci. Eng.* **2015**, *27*, 1788–1795.
13. Nwaoha, T.C.; Yang, Z.; Wang, J.; Bonsall, S. Application of genetic algorithm to risk-based maintenance operations of liquefied natural gas carrier systems. ARCHIVE Proceedings of the Institution of Mechanical Engineers Part. E Journal of Process. *Mech. Eng. 1989–1996* **2010**; *225*, 40–52.
14. Lv, P.; Zhuang, Y.; Jian, D.; Su, W. Study on lockage safety of LNG-fueled ships based on FSA. *PLoS ONE* **2017**, *12(4)*, 1–12.
15. Seo, S.; Han, S.; Lee, S.; Chang, D. A pump-free boosting system and its application to liquefied natural gas supply for large ships. *Energy* **2015**, *105*, 70–79.
16. Park, H.; Lee, S.; Jeong, J.; Chang, D. Design of the compressor-assisted LNG fuel gas supply system. *Energy* **2018**, *158*, 1017–1027.
17. Goo, B.; Lee, J.; Seo, S.; Chang, D.; Chung, H. Design of reliability critical system using axiomatic design with FMECA. *Int. J. Nav. Archit. Ocean Eng.* **2017**, *11*, 11–21.
18. Martins, M.R.; Schleder, A.M. Reliability Analysis of the Regasification System on Board of a FSRU Using Bayesian Networks, Natural Gas—Extraction to End Use, Sreenath Borra Gupta, IntechOpen. Available online: https://www.intechopen.com/books/natural-gas-extraction-to-end-use/reliability-analysis-of-the-regasification-system-on-board-of-a-fsru-using-bayesian-networks (accessed on 10 May 2020).
19. Niculita, O.; Nwora, O.; Skaf, Z. Towards Design of Prognostics and Health Management Solutions for Maritime Assets. *Procedia CIRP* **2016**, *59*, 122–132.

20. Lazakis, I.; Raptodimos, Y.; Varelas, T. Predicting ship machinery system condition through analytical reliability tools and artificial neural networks. *Ocean Eng.* **2018**, *152*, 404–415, doi:10.1016/j.oceaneng.2017.11.017.
21. Cicek, K.; Turan, H.H.; Topcu, Y.I.; Searslan, M.N. Risk-Based Preventive Maintenance Planning using Failure Mode and Effect Analysis (FMEA) for Marine Engine Systems. In Proocedings of the 2nd International Conference on Engineering System Management and Applications: Sharjah, United Arab Emirates, 2010.
22. PHM Technology. MADe-Maintenance Aware Design. Available online: https://www.phmtechnology.com (accessed on 05 October 2018).
23. Bolbot, V.; Theotokatos, G.; Bujorianu, L.; Boulougouris, E.; and Vassalos, D. Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. *Reliab. Eng. Syst. Saf.* **2019**, *182*, 179–193.
24. Thomas, J. Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis, Engineering Systems Division, Massachusetts Institute of Technology. Available online: http://sunnyday.mit.edu/JThomas-Thesis.pdf(accessed on 7 December 2020).
25. PHM Technology. MADe Training Course-Fundamentals & Application-MADe v3.7.2. Available online: https://www.phmtechnology.com/made/how-made-works/ (accessed on 20 December 2018).
26. Department of Defense, USA. MIL-HDBK-338B*:* Military handbook—Electronic reliability design handbook. Available online: https://www.navsea.navy.mil/Portals/103/Documents/NSWC_Crane/SD-18/Test%20Methods/MILHDBK338B.pdf (accessed on 7 December 2020).
27. ISO 31010. Risk management—Risk assessment techniques, International Organization for Standardization. Available online: https://www.iso.org/standard/72140.html (accessed on 10 April 2019).
28. Department of Defense, USA. MIL-STD-1629A: Military Standard—Electronic reliability design standard. Available online: http://www.barringer1.com/mil_files/MIL-STD-1629RevA (accessed on 10 April 2019).
29. PTC. Windchill PLM Software. Available online: https://www.ptc.com/en/products/plm/plm-products/windchill (accessed on 02 March 2019).
30. PHM Technology. MADe for Safety. Available online: https://www.phmtechnology.com/assets/downloads/default/MADe%20for%20Safety.pdf (accessed on 05 October 2018).
31. OREDA. OREDA Handbook, SINTEF & NTNU, 6th Edition. Available online.: https://www.sintef.no/en/projects/oreda-handbook2 (accessed on 15 February 2019).
32. Kim, K.O.; Zuo, M.J. General model for the risk priority number in failure mode and effects analysis. *Reliab. Eng. Syst. Saf.* **2018**, *169*, 321–329.
33. Bona, G.; Silvestri, A.; Forcina, A.; Petrillo, A. Total efficient risk priority number (TERPN): A new method for risk assessment. *J. Risk Res.* **2017**, *21*, 1384–1408.
34. Bona, G.; Silvestri, A.; Felice, F.; Forcina, A.; Petrillo, A. An Analytical Model to Measure the Effectiveness of Safety Management Systems: Global Safety Improve Risk Assessment (G-SIRA) Method. *J. Fail. Anal. Prev.* **2016**, *16*, 1024–1037.
35. Ruijters, E.; Stoelinga, M. Fault tree analysis A survey of the state-of-the-artin modeling, analysis, and tools. *Comput. Sci. Rev.* **2014**, *15*, 29–62.
36. Čepin, M.; Mavko, B. A dynamic fault tree. *Reliab. Eng. Syst. Saf.* **2002**, *75*, 83–91.
37. Cobo, G.A. Importance Measures, Workshop on "PSA Applications", Sofia, Bulgaria. Available online: https://inis.iaea.org/collection/NCLCollectionStore/_Public/28/059/28059559.pdf (accessed on 15 March 2019).
38. Komal, C.D.; Lee, S.Y. Fuzzy reliability analysis of dual-fuel steam turbine propulsion system in LNG carriers considering data uncertainty. *J. Nat. Gas. Sci. Eng.* **2015**, *23*, 148–164.
39. Wärtsilä, 2018. Wärtsilä 50DF Product guide. Available online: https://cdn.wartsila.com/docs/default-source/product-files/engines/df-engine/product-guide-o-e-w50df.pdf?sfvrsn=9 (accessed on 12 November 2018).
40. Theotokatos, G.; Livanos, G.A.; Dimitrellou, S.; Strantzali, E.; Pagonis, D.N.; Politis, K.; Theodoulides, A.; Peirounakis, D.; Mizithras, P. Design of LNG storage and feeding system for an open type ferry, Towards Green Marine Technology and Transport, 1st Edition.; CRC Press: Boca Raton, FL, USA, **2015**; pp. 473–481.
41. DNV-GL, 2018. LNG regulatory update: "Best fuel of the future", conference & study tour. Available online: http://www.golng.eu/files/Main/20180417/2.%20Ole%20Vidar%20Nilsen%20-%20DNV%20GL.pdf (accessed on 28 October 2018).
42. HSE. Health & Safety Executive—Failure Rate and Event Data for use within Risk Assessments. Available online: https://www.hse.gov.uk/landuseplanning/failure-rates.pdf (accessed 4 April 2019).
43. Davies, P.A.; Fort, E. LNG as a marine fuel: Likelihood of LNG releases. *Mar. Eng. Technol.* **2013**, *12*, 3–10.
44. Cadwallader, L.C. Reliability Estimates for Selected Sensors in Fusion Applications, Idaho National Engineering Laboratory, Office of Scientific and Technical Information (OSTI). Available online: https://www.researchgate.net/publication/236539403_Reliability_estimates_for_selected_sensors_in_fusion_applications (accessed on 10 February 2019).
45. Fydrych, J. & Consogno, G., A maintenance strategy for a multi-valve cryogenic distribution system. *Mater. Sci. Eng.* **2017,** *278***,** 012014.
46. Wärtsilä Oil & Gas Systems AS. Wärtsilä Gas. Systems: LNG Systems. Available online: https://cdn.wartsila.com/docs/default-source/oil-gas-documents/brochure-offshore-lng-systems.pdf (accessed on 10 April 2019).