European Maritime Safety Agency
Ref. Ares(2024)8081549 - 14/11/2024

Reliability and safety analysis

STUDY INVESTIGATING THE SAFETY OF HYDROGEN AS FUEL ON SHIPS BY DNV

EMSA/OP/21/2023

Date: 2024-11-05

About this study:

This report was commissioned by the European Maritime Safety Agency (EMSA) under service contract 2024/EMSA/OP/21/2023.

Authors:

Hans Jørgen Johnsrud (DNV), Rakel Skaret-Thoresen (DNV), Linda Sigrid Hammer (DNV) and Marius Leisner (DNV).

Recommended citation:

European Maritime Safety Agency (2024), *Reliability and safety analysis*, EMSA, Lisbon

Legal notice:

Neither the European Maritime Safety Agency (EMSA) nor any third party acting on behalf of the Agency is responsible for the use that may be made of the information contained in this report.

Copyright notice[1]:

This report and any associated materials are available online at www.emsa.europa.eu

[1] The copyright of EMSA is compatible with the CC BY 4.0 license.

Abstract

This report is developed as a part of the project “EMSA study investigating the safety of hydrogen as fuel on ships”. The overall objective of the project is to carry out a structured set of safety assessments and reliability analyses, delivering a Guidance document addressing ships using hydrogen as fuel. The purpose is to support regulators and the industry navigating towards a safe and harmonised deployment of hydrogen as fuel which could demonstrate an important step towards decarbonisation of the sector.

This report presents a comprehensive examination of three topics: Firstly, the reliability of various equipment to be used in hydrogen-fuelled ships is presented and potential failure modes are identified. Secondly, the performance and reliability of selected safety-critical systems within generic hydrogen fuel system configurations are explored. The fault trees on safety-critical systems are vital in providing the success and failure probabilities in the event tree for the risk calculation model. Thirdly, the safety analysis is used to develop a framework for a generic risk model for hydrogen-fuelled ships.

By systematically analysing these three areas, this report aims to provide valuable insights and recommendations for improving the reliability and safety of hydrogen technologies. The findings will contribute to the broader goal of delivering a guidance document addressing ships using hydrogen as fuel.

Executive summary

This report is developed as a part of the project “EMSA study investigating the safety of hydrogen as fuel on ships”. The project's overall objective is to carry out a structured set of safety assessments and reliability analyses, delivering a Guidance document addressing ships using hydrogen as fuel. The purpose is to support regulators and the industry navigating towards a safe and harmonised deployment of hydrogen as fuel which could demonstrate an important step towards decarbonisation of the sector. This report is the result of the second part of the study.

The International Maritime Organization (IMO) updated its greenhouse gas (GHG) strategy in 2023 with a goal of achieving net-zero emissions by 2050. Together with new EU regulations, this will be critical for decarbonising international shipping. Energy efficiency measures can lower GHG emissions from ships, but they will not bring the industry to net-zero emissions by 2050 without a change to zero-GHG fuels and potentially other technologies.

Most potential zero-carbon fuels, such as hydrogen, have properties posing different safety challenges from those of conventional fuel oils. This requires the development of IMO regulations and classification rules for safe design and use onboard ships in parallel with the technological progress needed for their uptake. It is important to take a systematic approach to ensure that the upcoming regulatory framework addresses all hazards associated with using hydrogen as fuel on ships.

This project uses the IMO goal-based approach outlined in IMOs “Generic guidelines for the development of goal-based standards” (MSC.1/Circ.1394/Rev.2 , 2019), and draws upon comprehensive risk assessment and reliability analysis.

What we did

This report presents a comprehensive examination of three topics: the reliability of hydrogen equipment, the reliability of safety-critical systems, and safety analysis of hydrogen ships.

The use of realistic failure data is an essential component of any quantitative risk analysis. However, collecting such data is a challenging task that raises several questions regarding the suitability of the data, the assumptions underlying it, and the uncertainties associated with it. We have investigated the reliability of selected equipment for hydrogen-fuelled ships, assessing the suitability of various databases containing failure data. The identification of the most relevant equipment for the reliability analysis is based on designs currently being conceptualized in the maritime industry. By relying on a range of data sources, this study presents a comprehensive picture of the reliability of equipment to be used in hydrogen-fuelled ships.

The reliability analyses of safety-critical systems build on the equipment-level analysis to explore the performance and reliability of selected safety-critical systems within generic hydrogen fuel system configurations. These configurations will be subjected to comprehensive risk analysis in the next deliverables of this study. Therefore, it is crucial to establish a foundation and provide insights for hazard identification and risk analysis work. The analyses not only support risk analysis but also demonstrate a methodology for assessing the performance of safety-critical systems and functions in general, thereby enhancing our ability to ensure safety and reliability for all hydrogen systems across various configurations.

The goal of our safety analysis in the last part of the report has been to develop a framework for a generic risk model (the model) for hydrogen-fuelled ships. The basis for the model is the descriptions of generic hydrogen safety hazards, threats, and risks outlined in EMSA's 2024 report, "Mapping Safety Risks for Hydrogen-Fuelled Ships". Findings from the reliability analysis of hydrogen equipment and safety-critical systems are also crucial inputs to the model.

By systematically analysing these three areas, this report aims to provide valuable insights and recommendations for improving the reliability and safety of hydrogen technologies. The findings will contribute to the broader goal of delivering a guidance document addressing ships using hydrogen as fuel.

What we found

Reliability analysis of hydrogen equipment

Leak frequencies have always been a major source of uncertainty in risk analysis (DNV, 2008). At present, the lack of hydrogen specific failure data, and uncertainties considering the suitability for ship applications, result in a high degree of uncertainty in leak frequency analysis in QRAs for hydrogen fuel system installations.

Due to the lack of experience with hydrogen-fuelled ships and consequently also of an industry-specific leak database for maritime, we have found using the generic HCRD and/or HyRAM+ databases the best alternative when establishing leak frequencies for hydrogen-fuelled ships.

The rationale for selecting HCRD is based on its extensive and high-quality dataset, its widespread use in QRAs, and its consideration of various parameters, including equipment operation in offshore environments. The reason for choosing HyRAM+ is that this toolkit forms the basis for carrying out quantitative risk assessments and modelling the consequences for hydrogen infrastructure and transportation systems. Although the leak data in HyRAM+ come from various industries and have limited hydrogen-specific information, it is currently the only dataset designed specifically for hydrogen applications. It's also worth noting that HyRAM+ is a research software that is actively being developed, so the models and data may change over time.

Although the HCRD and the HyRAM+ databases are considered to be most applicable and has highest quality, they do not account for maritime-specific factors. Additional uncertainty arises from the differences in the properties and behaviour of hydrogen compared to the mediums on which the Oil & Gas databases are based. Hydrogen is prone to leaking due to its low density and small molecular size. It's not clear how much these characteristics, in combination with the specific environmental conditions onboard a ship, will impact the reliability of data sources in accurately predicting leak frequencies. Furthermore, hydrogen installations generally have smaller equipment dimensions compared to industrial plants and offshore installations. Inspection, certification regimes, and maintenance intervals also play a significant role in the frequency of leaks in process equipment and can differ between Oil & Gas/process industry installations and ships.

For safety and control equipment, it's important to address uncertainty on a case-by-case basis in quantitative risk analysis. The data collected from the oil and gas sector is based on an industry with a requirement for demonstrating Safety Integrity Level (SIL), which is not a requirement in maritime. Hardware and software from reputable manufacturers, who also supply SIL-certified components to the oil and gas sector, are likely to be of higher standard and have less uncertainty. There is no clear and obvious preference for failure-on-demand probabilities of safety and control equipment; instead, multiple sources have been referenced. The failure data from the PDS Handbook, OREDA, CCPS Guideline, and NPRD have all been reviewed and cited in this study.

We note the following important issues for further development of the hydrogen Guidance document:

- According to the HCRD and HyRAM+ databases, heat exchangers, compressors, pumps, and filters exhibit higher leak rates compared to other individual components. Consequently, regulations concerning the arrangement of spaces where such components may be used must account for this.

- The leakage probability within a system depends on the leakage probability for each component and the number of components, e.g., system designs with numerous flanged connections and valves have a higher leak potential than a fully welded piping system.

- According to the PSD, NPRD and other databases: non-return valve/check valves, excess flow valves and actuated ESD valves (gate type) show higher failure rates compared to other individual safety and control components. Therefore, it might be necessary to incorporate other/additional protection layers.

Reliability analysis of safety-critical systems

To effectively evaluate the performance of safety-critical systems, it is essential to consider them within their specific context. This involves outlining some fundamental design assumptions. The two primary parameters that define the ship's arrangement and consequently influence the risk level for hydrogen-fuelled ships are:

- **Storage condition** of fuel onboard: Liquefied hydrogen (LH2) or compressed hydrogen gas (H2).
- **Storage location** of fuel onboard: On deck (unconfined area) or below deck in a confined space.

The analysis is performed for two different fuel containment systems and storage locations, in addition to one bunkering configuration:

- **Case 1: Compressed hydrogen storage on deck – Leak detection and fuel supply shutdown system**

  One challenge with storing compressed hydrogen on deck is the difficulty in arranging hydrogen piping with secondary enclosures due to the large number of pipes and the small dimensions. For portable tanks, there is the additional complication of non-permanent connections, which must be operated at every refuelling operation. A single-walled hydrogen system on deck will rely on leakage detection located in open air to identify and stop a hydrogen leak. In Case 1, we investigate this design feature to understand better how leakage detection's reliability affects the vessel's overall safety.

  Our findings indicate that hydrogen installations on open decks have a challenge with managing leakages within a timeframe sufficient to prevent a critical cloud build-up. Consequently, hydrogen regulations should account for this by requiring additional safety features.

- **Case 2: Liquid hydrogen storage below deck – Inert Gas System**

  In our first project delivery (EMSA, 2024), we found that dilution ventilation may not be an effective way to reduce the impact of significant hydrogen releases in enclosed spaces. Case 2 examines an alternative to a ventilated TCS, which involves maintaining a constantly inerted atmosphere inside the TCS to prevent ignition, fire, and explosion. The analysis focuses on the likelihood of having a sufficiently inert atmosphere in the TCS on demand. We also discuss other challenges associated with using inerting as a key safety measure.

  The findings indicate that the strategy of inerting spaces to prevent ignition has several challenges, including always keeping the space sufficiently inerted, preventing access for inspection and maintenance, effects of low temperature, and safely purging a hydrogen leakage without entering into the flammable range of the hydrogen atmosphere.

- **Case 3: Bunkering of liquefied hydrogen – Safe hydrogen bunkering**

  To mitigate risks related to re-fuelling, a bunkering location on an unrestricted open deck provides the best boundary conditions to bunker hydrogen safely. In Case 3, we look at the bunkering of liquefied hydrogen on a vessel where the general arrangement prevents having the bunkering manifold on the open deck. We examine the consequences of a potential leak in a semi-enclosed bunkering station, similar to those used for LNG-fuelled ships. The intention is not to quantify reliability as in the previous two cases but instead to discuss important challenges and lessons learned from recent studies.

  We found that in cases where vessel geometries do not allow for an open bunkering station, it becomes more challenging to manage the risks associated with fuel transfer. It is reasonable to assume that a hydrogen leak can quickly create an explosive atmosphere in the bunkering station, and the possibility of ignition cannot be ruled out.

Safety analysis of hydrogen-fuelled ships

The goal of our safety analysis in the last part of the report has been to develop a framework for a generic risk model (the model) for hydrogen-fuelled ships. The basis for the model is the descriptions of generic hydrogen safety hazards, threats, and risks outlined in EMSA's 2024 report, "Mapping Safety Risks for Hydrogen-Fuelled Ships". Findings from the reliability analysis of hydrogen equipment and safety-critical systems are also crucial inputs to the model.

The model not only contributes to risk quantification but also visualizes potential consequence outcomes following an initiating event, thereby enhancing our understanding of major accident risks in complex scenarios. Highlighting the potential consequences of hydrogen releases underscores the importance of stopping the event as early as possible in the chain of events, ideally by preventing any release in the first place.

As with any quantitative risk model, it is important to note that the framework developed in this study is a model representation and not a 100% accurate depiction of real-world scenarios. While it provides valuable insights and helps understand potential risks, it cannot capture every variable and nuance of actual events. It is a useful tool for risk assessment and decision-making, acknowledging the inherent uncertainties and limitations.

The aim of the model is to create a generic event tree for risk analysis that can be applied to all hydrogen loss of containment events. The model is generic and valid for both liquid, gaseous and two-phase hydrogen releases, whether they occur in enclosed spaces or on open deck.

While numerous event trees exist for loss of containment from the oil and gas industry considering hydrocarbon release, hydrogen used as fuel in shipping is a new application. QRAs need to be developed from scratch and capture new hazards and effects that are not always modelled in traditional QRAs.

We found that the greatest uncertainty in the risk model lies in the leak frequency data and ignition probability. This also aligns with a DNV study of Hydrogen Risk Assessment methods from 2008, which also pointed out uncertainties related to probabilities for failure of safety systems.

These uncertainties stem from a limited availability of databases specifically focused on hydrogen equipment failures. Additionally, hydrogen ignition models are still under development. The ignition probabilities greatly affect the estimated risk level, resulting in significant uncertainty when using ignition probabilities for hydrogen. Studies have also identified a knowledge gap regarding the exact ignition mechanisms for hydrogen releases.

Furthermore, there is high uncertainty as to whether the gas detector system can react fast enough to prevent a critical gas cloud from occurring. If leaks are in the range of 0.1 kg/s, an explosive atmosphere can be generated within a few seconds. Conventional point gas detectors are not fast enough, and the reliability of acoustic detectors is uncertain due to the potential for ultrasonic noise interference.

As with any quantitative risk analysis, there will be uncertainty associated with the final risk level calculated using this model framework. However, the method offers a structured approach to understanding risks, enabling decision-makers to make informed choices even with uncertain data. Additionally, the modelling can identify the most significant risk drivers and quantify the risk-reducing effects, aiding in selecting effective preventive and mitigating measures.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ALARP	As Low As Reasonably Practicable
CCPS	Center for Chemical Process Safety
CDP	Composite Data Products
CH2	Compressed hydrogen gas
CHS	Center for Hydrogen Safety
CPU	Central Processing Unit
DD	Dangerous detected
DOE	US Department of Energy
DU	Dangerous undetected
E/E/PE (system)	Electrical/Electronic/Programmable Electronic System
EMSA	The European Maritime Safety Agency
ESD	Emergency Shutdown
ETA	Event Tree Analysis
EUC	Equipment Under Control
FMECA	Failure Mode Effect and Criticality Analysis
FPR	Fuel Preparation Room
FSHS	Fuel Storage Hold Space
FTA	Fault Tree Analysis
GF	General failure
GHG	Greenhouse gas
H2	Gaseous hydrogen
H2LL	H2 Lessons Learned
HAZID	Hazard Identification
HAZOP	Hazard and Operability
HCRD	Hydrocarbon Release Database
HSE	The UKs Health & Safety Executive
HFT	Hardware Fault Tolerance
HyRAM	Hydrogen Risk Assessment Models
IGF Code	The International Code of Safety for Ships using Gases or other Low-flashpoint Fuels
IMO	The International Maritime Organization
IPL	Independent Protection Layer
IRT	IPL response time
KHK	The High Pressure Gas Safety Institute of Japan
LAC	Limiting Air Concentration
LEL	Lower Explosive Limit
LH2	Liquefied hydrogen

LOC	Limiting Oxygen Concentration
OPA	Layer of Protection Analysis
MLA	Marine Loading Arm
MRT	Mean repair time
MTF	Maritime Technologies Forum
MTBF	Mean Time Between Failures
MTR	Mean repair time
MTTR	Mean time to restoration
NPRD	Nonelectronic Parts Reliability Data
NPRDS	Nuclear Plant Reliability Data System
NREL	National Renewable Energy Lab
OREDA	Offshore and Onshore Reliability Data
P&ID	Process and Instrumentation Diagram
PE	Programmable electronic system
PERD	Process Equipment Reliability Database
PFD	Probability of Dangerous Failure on Demand
PFD_{avg}	Average Probability of dangerous Failure on Demand
PFH	Probability of Failure per Hour
PHA	Process Hazard Analysis
PLC	Programmable Logic Controller
PLOFAM	Process leak for offshore installations frequency assessment model
PLT	Process lag time
PR	Pressure Relief
PST	Process safety time
QCDC	Quick Connect/Disconnect Coupling
QRA	Quantitative Risk Analysis
RBD	Reliability Block Diagram
RIVM	National Institute for Health and the Environment in the Netherlands
RRF	Risk Reduction Factor
SIF	Safety-Instrumented-Function
SIL	Safety Integrity Level
SIS	Safety-Instrumented-System
SD	Safe detected
SSL	Ship-shore-link
SU	Safe undetected
TCS	Tank Connection Space
TPRD	Thermal Pressure Relief Device
UPS	Uninterruptible power supply

List of general terms

Term	Description
Critical failure	Failure of an equipment unit that causes an immediate cessation of the ability to perform a required function. A critical failure results in an unscheduled repair (ISO 14224:2016).
Electrical/electronic/ programmable electronic system (E/E/PE system)	System for control, protection or monitoring based on one or more electrical/electronic programmable electronic (E/E/PE) devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices (IEC 61508:2010).
Element	Part of a subsystem comprising a single component or any group of components that performs one or more element safety functions (IEC 62061:2021).
Equipment under control (EUC)	Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities (IEC 61508:2010, 2010).
Failure	Termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required (IEC 61508:2010, 2010).
Failure mode	One of the possible states of a faulty item, for a given required function (IEC 60050-191:1990). See chapter 2.1.3 for definitions of different failure modes.
Fault tolerance	The ability of a functional unit to continue to perform a required function in the presence of faults or errors (ISO/IEC 2382-14:1997).
Functional safety	Part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures (IEC 61508:2010, 2010).
Hazard	A potential source of harm (ISO/IEC Guide 51:1999).
Hazardous event	Event that may result in harm (IEC 61508:2010, 2010).
Mean time to restoration (MTTR) and Mean repair time (MTR)	MTTR encompasses: - the time to detect the failure (a); and, - the time spent before starting the repair (b); and, - the effective time to repair (c); and, - the time before the component is put back into operation (d) MRT encompasses the times (b), (c) and (d) of the times for MTTR (IEC 61508:2010).
Mode of operation	The way in which a safety function operates, which may be either: – low demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or – high demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or – continuous mode:
Probability of dangerous failure on demand (PFD)	Safety unavailability (IEC 60050-191:1990) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system harm (IEC 61508:2010).
Probability of dangerous failure on demand – average (PFD_{avg})	Mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system (IEC 61508:2010).
Process safety time	Period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed

Term	Description
	in the EUC to prevent the hazardous event occurring (IEC 61508:2010).
Programmable electronic system (PE system)	System for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highway (IEC 61508:2010).
Redundancy	Redundancy means having two or more items, such that if one item fails, the system can continue to function by using the other item(s). This design principle is also referred to as fault tolerance. Main categories are: Active redundancy and standby redundancy, but also hardware and software redundancy (Rausand, 2014).
Risk	Combination of the probability of occurrence of harm and the severity of that harm (ISO/IEC Guide 51:1999).
Risk Reduction Factor (RRF)	RRF quantifies the effectiveness of a safety system in reducing risk. It is calculated as the inverse of the PFD_{avg}: $$RRF = \frac{1}{PFD_{AVG}}$$ This relationship means that a lower PFD results in a higher RRF, signifying greater risk reduction. Using the same example above, if a safety system has a PFD of 0.01, its RRF would be 100, meaning it reduces the risk by a factor of 100 (Rausand, 2014).
Safety	Freedom from unacceptable risk (ISO/IEC Guide 51:1999).
Safety function	Function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event (IEC 61508:2010).
Safety integrity	Probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time (IEC 61508:2010).
Safety-Instrumented-Function (SIF)	Safety function to be implemented by a safety instrumented system (SIS)
Safety-Instrumented-System (SIS)	The equivalent to E/E/PE safety-related systems, as per IEC 61508. Instrumented system used to implement one or more SIFs (IEC 61511:2016). The main elements of a SIS are input elements, logic solver, and final elements.
Safety integrity level (SIL)	Discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest (IEC 61508:2010).
Safety-related system	Designated system that both: – implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and – is intended to achieve, on its own or with other E/E/PE safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions (IEC 61508:2010).
Subsystem	Entity of the top-level architectural design of a safety-related system where a dangerous failure of the subsystem results in dangerous failure of a safety function (IEC 61508:2010).
Tolerable risk	Risk which is accepted in a given context based on the current values of society (ISO/IEC Guide 51:1999).
Voting (K-out-of-N systems)	The reliability analysis of a system often concerns analyzing K-out-of-N systems. A K-out-of-N safety system is operational only when K, or more, out of N units work, e.g., a pressure transmitter subsystem/group with 2oo3 voting is functioning when at least two of the three transmitters are able to detect and transmit a signal when the pressure goes beyond the acceptable limits (Rausand, 2014).

1. Introduction

DNV has been awarded the “EMSA study investigating the safety of hydrogen as fuel on ships”. The project's overall objective is to conduct a structured set of safety assessments and reliability analyses, delivering a Guidance document addressing ships using hydrogen as fuel. The purpose is to support regulators and the industry navigating towards a safe and harmonised deployment of hydrogen as fuel which could demonstrate an important step towards decarbonisation of the sector.

The objective of this study is to carry out a reliability and safety analysis of the main equipment components and selected safety-related systems for hydrogen-fuelled ships. In this report, the identification of the most relevant and safety critical equipment/systems for a hydrogen-fuelled ship, for which a safety and reliability analysis is performed, builds on designs currently under conceptualisation in the maritime industry, DNV’s experience with such systems and consultations with external experts.

The International Maritime Organization (IMO) updated its greenhouse gas (GHG) strategy in 2023, with the goal of achieving net-zero emissions by 2050. Together with new EU regulations, this will be critical drivers for decarbonizing international shipping. Energy efficiency measures can lower GHG emissions from ships but will not bring the industry to net-zero emissions by 2050 without a change also to zero-GHG fuels and potentially other technologies.

Most potential zero-carbon fuels, such as hydrogen, come with safety challenges that are different from conventional fuel oils. This requires the development of IMO regulations and classification rules for safe design and use onboard ships in parallel with the technological progress needed for their uptake.

To ensure that all hazards related to the use of hydrogen as fuel on ships are covered in the regulatory framework under development, it is necessary to use a systematic approach, such as the IMO “Generic guidelines for the development of goal-based standards” (MSC.1/Circ.1394/Rev.2 , 2019), and to build on extensive risk assessment and reliability analysis.

This project will deliver a series of studies, and this report is the second study. The results from the first study were presented in the EMSA report titled “Mapping safety risks for hydrogen-fuelled ships” (EMSA, 2024) which characterised hydrogen safety hazards, system threats, and risks. It also drew up a preliminary Guidance for controlling and mitigation of these risks.

The results of this study on reliability and safety analysis will serve as critical input for subsequent studies on Hazard Identification, Risk Analysis, and Risk Assessment.

This report presents a comprehensive examination of three topics:

- Reliability of hydrogen equipment,
- Reliability of safety-critical systems, and
- Safety analysis of hydrogen-fuelled ships

The topics are interlinked, and the relation between them is illustrated in Figure 1-1.

The first part of the study (Chapter 3) focuses on the reliability analysis of hydrogen equipment. This section presents the reliability of various equipment to be used in hydrogen-fueled ships and identifies potential failure modes. The failure data of mechanical and rotating equipment is used as input for the leak frequencies in the safety analysis, while the failure data on safety and control equipment is used to provide the basic events failure rates and probability of failure-on-demand for the fault trees on safety-critical systems (Chapter 4).

The fault trees on safety-critical systems are vital in providing the success and failure probabilities in the event tree for the risk calculation model (Chapter 5). While the reliability analysis (Chapter 4) provides input to the risk model, it also serves to demonstrate a method for addressing the functionality/effectiveness, response time, robustness and reliability/availability of safety-critical systems.

By systematically analysing these three areas, this report aims to provide valuable insights and recommendations for improving the reliability and safety of hydrogen technologies. The findings will contribute to the broader goal of delivering a guidance document addressing ships using hydrogen as fuel.

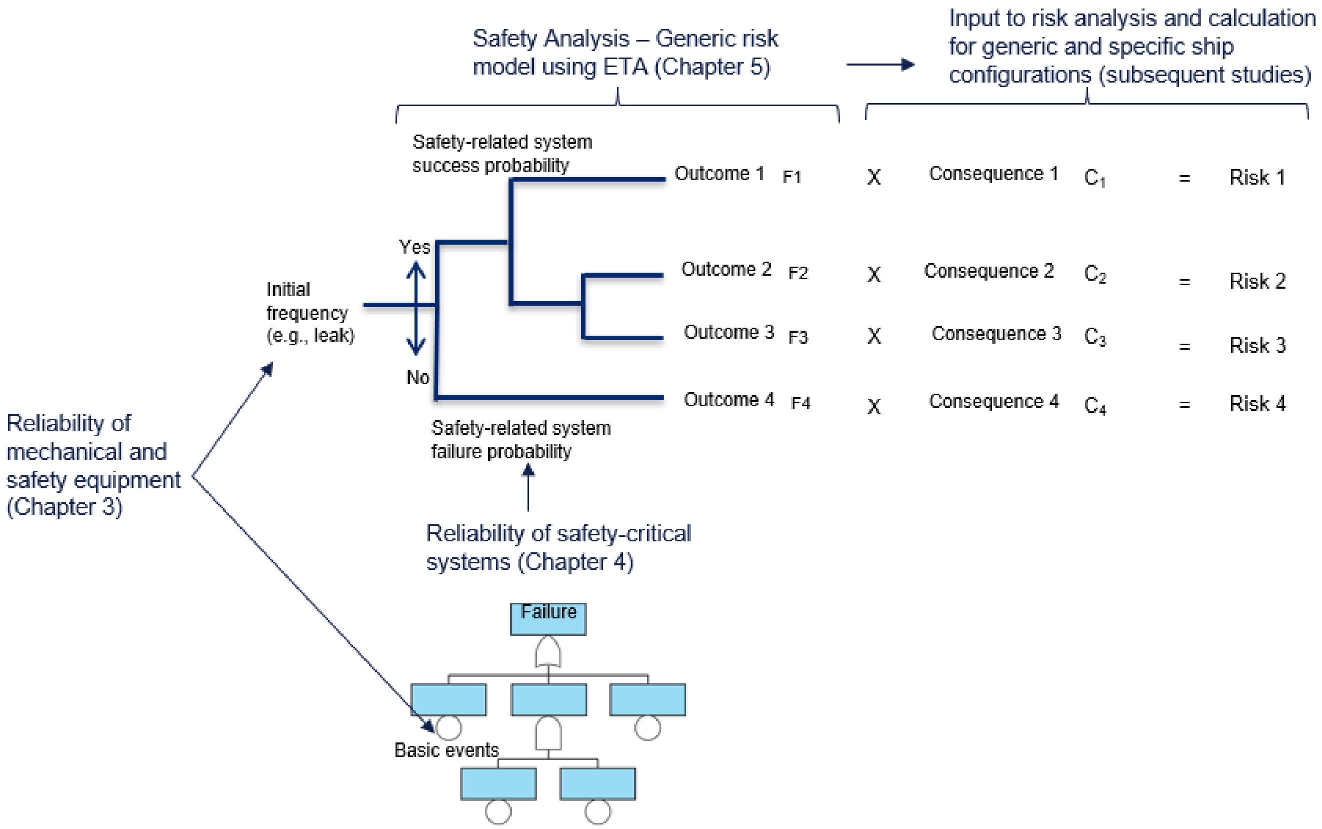

Safety Analysis – Generic risk model using ETA (Chapter 5)
Input to risk analysis and calculation for generic and specific ship configurations (subsequent studies)
Safety-related system success probability
Outcome 1 F1 X Consequence 1 C_1 = Risk 1
Yes
Initial frequency (e.g., leak)
Outcome 2 F2 X Consequence 2 C_2 = Risk 2
Outcome 3 F3 X Consequence 3 C_3 = Risk 3
No
Outcome 4 F4 X Consequence 4 C_4 = Risk 4
Safety-related system failure probability
Reliability of mechanical and safety equipment (Chapter 3)
Reliability of safety-critical systems (Chapter 4)
Failure
Basic events

Figure 1-1 Visualisation of the framework of this study on reliability and safety analysis (Source: DNV).

2. Methodology

This chapter outlines the methodology employed in this study, providing a framework for understanding the terms, definitions, and quantification methods used. The methodology is divided into two main sections: *Terms and definitions* and *analysis methods*.

Chapter 2.1 introduces the essential terms and definitions based on the principles from functional safety that form the foundation of the study, including safety-critical systems (chapter 2.1.1), layers of protection (chapter 2.1.2), and reliability measures (chapter 2.1.4). In addition, chapter 2.1.3 will define various failure-related concepts such as faults, failures, failure rates, and failure modes.

Chapter 2.2 focuses on the analysis methods used to calculate reliability of safety-critical systems and risk. It includes a detailed examination of fault tree analysis (chapter 2.2.1) for reliability analysis and event tree analysis (chapter 2.2.2) for risk calculation methodology, integrating the previous analyses to provide a comprehensive risk assessment framework.

2.1 Terms and definitions

2.1.1 Safety-critical systems

A safety system is deemed safety-critical based on the potential consequences of its failure. If a failure could lead to outcomes considered unacceptable, for instance loss of life or serious injury to people, significant damage to equipment or property and environmental harm, the safety system is classified as safety critical.

Safety-critical systems comprise all necessary components, including hardware, software, and human elements, to carry out one or more safety functions. Assessing the reliability of these systems is paramount to ensure their safe and effective operation of the hydrogen fuel system. This study is focusing on the reliability and performance of some selected safety-critical systems where the main output is towards rule development processes.

There are several standards that provide guidelines and best practices for designing, implementing, and maintaining safety-critical systems. They help ensure that systems meet the required safety integrity levels and perform reliably under all operating conditions. One of the most widely recognized standards is IEC 61508:2010, which provides a framework for the safe functioning of electrical, electronic, and programmable electronic safety-related systems (E/E/PE systems). This standard is complemented by sector-specific standards, such as IEC 61511:2016 for the process industry. There are no maritime performance standards for safety-critical systems, but the most relatable standards for fuel systems are the IEC 61511:2016 for the process industry sector, the IEC 62061:2021 Safety of machinery - Functional safety of safety-related control systems, and well as the ISO 13849:2015, Safety of machinery — Safety-related parts of control systems.

The reliability analysis will refer to terminology from the above-mentioned functional safety standards, mainly IEC 61508:2010 and EIC 61511:2016, to introduce concepts such as reliability of safety-critical systems, failure-on-demand probability, as well as safety performance and specification.

The output from the reliability analysis also serves as input to Quantitative Risk Analysis (QRA). Functional safety and QRA are both crucial components in ensuring the safety of systems, but they serve different purposes. While functional safety ensures that active safety systems (safety-instrumented systems, e.g. sensor – logic unit and final element) perform their intended functions correctly and reliably throughout their lifecycle, QRA is more about evaluating the overall risk picture for the whole ship or facility.

2.1.2 Safety barriers and layers of protection

For hydrogen fuel systems, we emphasize the integration of multiple safety barriers or protection layers. The term safety barrier is partly overlapping with our understanding of safety-critical systems. This includes both proactive (prevention) and reactive (mitigation) barriers, as well as active and passive barriers. Note that passive safety systems are not subject of functional safety, as defined in the EIC 61508:2010 and EIC 61511:2016 standards, as these standards focus on active safety systems ("safety instrumented systems").

The concept of safety barriers was introduced in the previous EMSA report ("Mapping safety risks for hydrogen-fuelled ships"), where potential threats were listed on the left side of the bowtie diagram and potential consequences on the right. Functional requirements were proposed as preventive and mitigative barrier functions.

The concept of protection layers was also introduced, illustrating the sequence in which they are activated. This aligns with the safety principles outlined in the IGF Code[2] regulations for natural gas fuel, which include the sequence of double barriers, leak detection, isolation, and segregation, among others. A generic sequence of activation that is often applied in process industries are (Rausand, 2014):

1. Process design (by using inherently safe design principles).
2. Control, using basic control functions, alarms, and operator responses to keep the system in normal (steady) state.
3. Prevention, using Safety-Instrumented Systems (SISs) and safety critical alarms to act upon deviations from normal state and thereby prevent an undesired event from occurring.
4. Mitigation, using SISs or functions implemented by other technologies, to mitigate the consequences of the undesired event. Examples include the protection that is provided by pressure relief valves.
5. Physical protection, using permanent (and more robust) safety barriers to enhance the mitigation.
6. Fire and gas detection and extinguishing, as a third strategy to mitigate the consequences of an accident, in relation to explosive gases.
7. Emergency response, using various means to limit the severity of the accident.

This sequence is also applicable to maritime applications, with some exceptions. On a ship, events can escalate so quickly that basic control functions may not respond in time. The first protection layer to address such events is often the inherently safe measures, e.g. double barriers, and the automatic safety systems, thus providing minimal to no credit to operator monitoring tasks. The IGF Code also clearly states that operational methods or procedures should never be used as a substitute for design measures. This analysis will therefore focus on the safety systems, more precisely safety that relies on active and passive systems.

2.1.3 Failure definitions

Before addressing the method of reliability calculations in chapter 2.1.4, this chapter gives a brief introduction to faults, failures, failure rates and failure modes, which are essential inputs to the calculation.

Failure and failure modes are the two most important concepts in any reliability analysis of a technical system. A failure occurs when an item is no longer able to perform one or more of its required functions and is defined as the termination of the ability of an item to perform its required function (IEV 191-05-22). Failure is therefore the event that takes place when a required function is terminated.

Note that the terms "fault" and "failure" are often used interchangeably, but they have distinct meanings in engineering and reliability contexts. *Failures* are often the result of one or more faults that were not detected or corrected in time. Thus, a *fault* is a defect or flaw in a system or component that may or may not lead to a failure. A

[2] The International Code of Safety for Ships using Gases or other Low-flashpoint Fuels (IGF Code).

failure mode describes a fault by telling how we can observe the inability of the item to perform a required function according to the functional requirements. A practical example for a mechanical equipment leakage is provided below:

- Cause: During the installation of a piping system, a pipe joint had poor welding quality.
- Fault: A small crack develops in the weld of the pipe joint.
- Failure Mechanism: Over time, cyclic stress from fluctuations in the pipe causes the crack to grow.
- Failure Mode: The pipe joint eventually fails by leaking.
- Failure: The leak results in a loss of containment, potentially causing a hazardous situation.

Another example for a safety and control system is provided below:

- Cause: A gas detector in the hydrogen fuel system is wrongly calibrated during maintenance.
- Fault: The detector provides inaccurate gas concentration readings.
- Failure Mechanism: Fault is not detected during operation (dangerous undetected) and the control system relies on these incorrect readings to monitor hydrogen levels.
- Failure Mode: If a leak occurs, the system fails to detect the hydrogen leak (detection failure) because the gas detector does not trigger an alarm.
- Failure: The undetected hydrogen leak leads to an accumulation of hydrogen gas, potentially resulting in an explosive hazard.

Very simplified, it can be said that the failure rate λ is the frequency of the occurrence of failures:

$$\lambda = \frac{Mean\ number\ of\ failures\ in\ a\ time\ interval\ of\ lenght\ t}{t}$$

Failure causes and failure mechanisms are essential for understanding why failures occur and how they can be avoided in the future. As seen from the example above, a failure cause is the circumstances during design, manufacturing, installation, or use that have led to a failure, while a failure mechanism is the physical, chemical, or other processes that have led to a failure (IEV 191-05-22).

For mechanical equipment we are considering all types of failures that could lead to loss of containment, e.g. leakage or rupture. These failure modes are typically classified in data sources as either general failures or leakage.

For safety- and control-related equipment and systems, failures can be classified as:

- **Dangerous (D) failure:** A failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that (IEC 61508:2010):
  a. prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or
  b. decreases the probability that the safety function operates correctly when required

- **Safe (S) failure:** Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that (IEC 61508:2010):
  a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or
  b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

- **Detected:** A failure that is detected by automatic diagnostic testing, internal in the item, or connected to a logic solver.

- **Undetected:** A failure that is not detected (not diagnosed) by automatic diagnostic testing, internal in the item, or connected to a logic solver. Undetected failures are usually revealed in proof tests, or if a demand should occur.

The following categories, as illustrated in Figure 2-1, of hardware failure or faults can therefore be distinguished (Rausand, 2014):

- **Dangerous undetected failures (λ_{DU}):** DU failures are preventing activation on demand and are revealed only by proof-testing or when a demand occurs, or overhaul. DU failures are sometimes called dormant or hidden failures. The DU failures are of vital importance when calculating the reliability of safety functions as they are a main contributor to safety function unavailability.

- **Dangerous detected failures (λ_{DD}):** DD failures are detected a short time after they occur, by automatic diagnostic testing. The average period of unavailability due to a DD failure is called the mean time to restoration (MTTR).

- **Safe undetected failures (λ_{SU}):** Non-dangerous failures that are not detected by automatic self-testing.

- **Safe detected failures(λ_{SD}):** Non-dangerous failures that are detected by automatic self-testing. In some configurations, early detection of failures may prevent an actual spurious trip of the system.

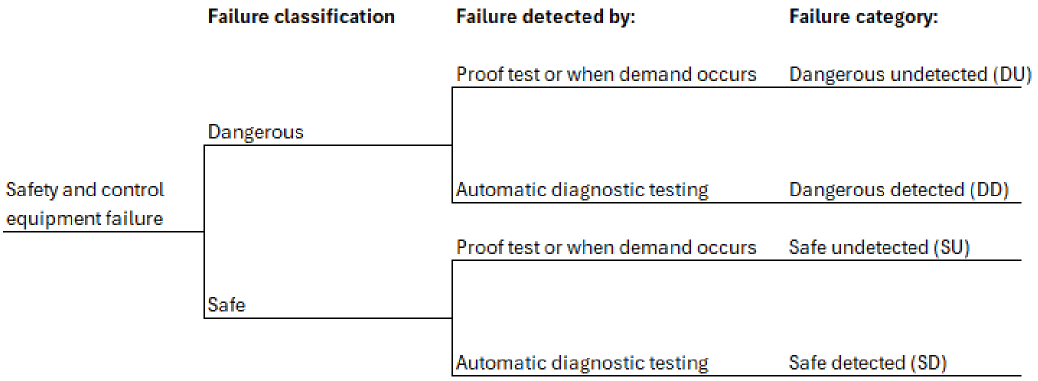

Failure classification
Failure detected by:
Failure category:
Proof test or when demand occurs
Dangerous undetected (DU)
Dangerous
Safety and control equipment failure
Automatic diagnostic testing
Dangerous detected (DD)
Proof test or when demand occurs
Safe undetected (SU)
Safe
Automatic diagnostic testing
Safe detected (SD)

Figure 2-1 Illustration of failure categories (Source: DNV).

2.1.4 Reliability and performance measure

Reliability in this study is measured using the Probability of Failure on Demand (PFD) and represents the likelihood that the safety and control equipment or the safety-critical system will fail to perform its required function when needed. IEC 61508 defines the probability of (dangerous) failure on demand (PFD) as safety unavailability of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the Equipment under control (EUC) (IEC 61508:2010).

The PFD of a safety-critical system is calculated by combining the PFD contributions of all single equipment and their voting, including both independent failures and common cause failures. In the analysis, we use the average probability of failure on demand – PFD_{avg} expressed as a value between 0 and 1, where a lower PFD_{avg} indicates higher reliability.

To calculate the PFD, the dangerous undetected failures (λ_{DU}) are used because these failures represent the most significant risk to the system's safety. This means a system could be in a failed state without any indication, posing a significant safety risk. λ_{DU} are based on random hardware failures only. Random hardware failures are failures resulting from the natural degradation mechanisms of the component, while systematic failures are typically failures that can be related to a particular cause other than natural degradation, e.g. errors made during specification, design, operation and maintenance phases of the lifecycle (Offshore Norge, 2001).

Typical examples of failure on demand of some safety and control equipment are exemplified below:

- Tank valve: Valve fails to close upon signal in case of automatic shutdown.
- Gas detection: Gas logic does not receive a signal equivalent to the upper alarm limit.
- Pressure Relief Valve (PRV): The valve fails to open at the set pressure.

Some examples of failures that are not considered relevant (more relevant for availability analysis) are:

- Shutdown (trip) of an item, where no physical failure condition of the item is revealed, with no further consequences other than process shutdown.
- Vibration and deformation that does not lead to any breakage or leakage (e.g., indent damages).
- Non-critical failures related to some degradation.

To conduct ETA and FTA analyses, it is essential to have failure data for the safety and control equipment in the form of PFD. However, the data available in the databases is typically presented as “Probability of Failing per Hour” (PFH). Therefore, we need to convert PFH data into PFD for safety and control equipment.

To calculate the PFD$_{avg}$ for the safety and control equipment, the equation below has been used with the proof test interval τ = 1 year (8760 hours) and assumed 1oo1 voting:

$$PFT_{avg}^{(1oo1)} = \frac{\lambda_{DU}\ \ \tau}{2}$$

For example, a PFD$_{avg}$ of 0.01 means there is a 1% chance that the system will fail on demand.

Achieving a low PFD involves rigorous testing, maintenance, and design improvements to ensure that the safety system performs reliably when required. However, it is not only about the system’s ability to perform tasks, such as shutting down process flows, but also about performing these tasks within a specified response time.

The categories of safety performance, as outlined by (Rausand, 2014), can be applied to evaluate additional reliability and safety aspects. The performance categories for the safety systems addressed in this study are:

- **Functionality/effectiveness.** This criterion concerns how effectively the safety barrier can reduce the risk related to a specific demand, and also the safety barrier's ability to handle different situations and variants of the demand.

- **Response time.** To reduce the risk, the safety barrier must often be activated quickly. Sometimes, a maximal response time is specified as part of the functional requirements.

- **Robustness.** The safety barrier must sometimes function in hazardous situations where it is exposed to external stresses. It is therefore important that the safety barrier is robust and not vulnerable to these stresses. This criterion is sometimes referred to as survivability.

- **Reliability/availability.** An active safety barrier can never be completely reliable and available. The reliability and availability are therefore important performance measures. Redundancy and fault tolerance may also be addressed in this category.

These categories are interlinked, making it challenging to differentiate between aspects such as fault tolerance, reliability, and robustness in practice. Therefore, this analysis does not have distinct chapters for each category; instead, all categories are addressed collectively. The intention is to highlight that the performance of safety systems encompasses many factors, all of which should be considered when assessing and evaluating their performance. This analysis focuses on the potential for major accidents. Therefore, failure modes related to false shutdowns or spurious trips are not included in this analysis.

2.2 Quantification methods

The selection of quantification methods in this study is based on the ISO guidelines 12489:2013. These guidelines provide an overview of the reliability modelling and calculation approaches, including guidelines to select them when the level of difficulty and complexity increases. The rationale for selecting fault tree analysis for reliability analysis and event tree analysis for safety analysis (QRA model) in this study is based on these guidelines. Another consideration is that while Markov models and Petri nets are well-suited for presenting results to reliability engineers, this study aims to reach a broader group of stakeholders. Therefore, the goal is to avoid making the models overly complex.

Fault and event trees are primarily used as tools to assist in the process of risk analysis and, more particularly, to provide a basis for quantified risk assessment. An introduction to fault tree analysis is provided in chapter 2.2.1 and event tree analysis in chapter 2.2.2.

2.2.1 Fault tree analysis

The Fault Tree Analysis (FTA) methodology has been applied in the reliability analysis, as detailed in IEC/ISO 31010:2009 - Risk Assessment Techniques and IEC 61025:2006 - Fault Tree Analysis.

The objectives of applying Fault Tree Analysis (FTA) are one or more of the following (IEC 61025:2006):

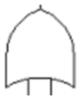
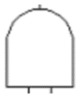
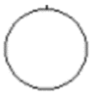
1. Estimating the frequency of occurrence of an incident.
2. Estimating the failure on demand probability of equipment and safety systems.
3. Determination of the combinations of equipment failures, operating conditions, environmental conditions, and human errors that contribute to the incident.
4. Identification of remedial measures for improving reliability or safety and determining their impact.

In this study, the scope of the FTA will cover the reliability of safety-critical equipment (point 2), more specifically, the reliability of safety-critical systems that protect the hydrogen fuel system.

FTA is a systematic and deductive process that resolves undesired top events into their immediate and basic causes. The fault tree visually represents the event relationships and uses logic gates to qualify them.

The gate and event symbols in Table 2-1 are used in the fault trees. Basic event is used for modelling the component failure modes. OR and AND gates are used for modelling the relationship between the basic events and the associated gates, and between the gates and the top event. Common cause failures are also modelled in the fault trees. The fault tree models are established using the software Reliability Workbench. A simple example of a fault tree, with the top event being the failure of safety function on demand, is shown in Figure 2-2

Table 2-1 Gate and event symbols in FTA.

Symbol	Name	Causal relation
	OR gate	Output event occurs if any one of the input events occurs
	AND gate	Output event occurs if all input events occur
	BASIC event	Basic event for which failure and repair data is available

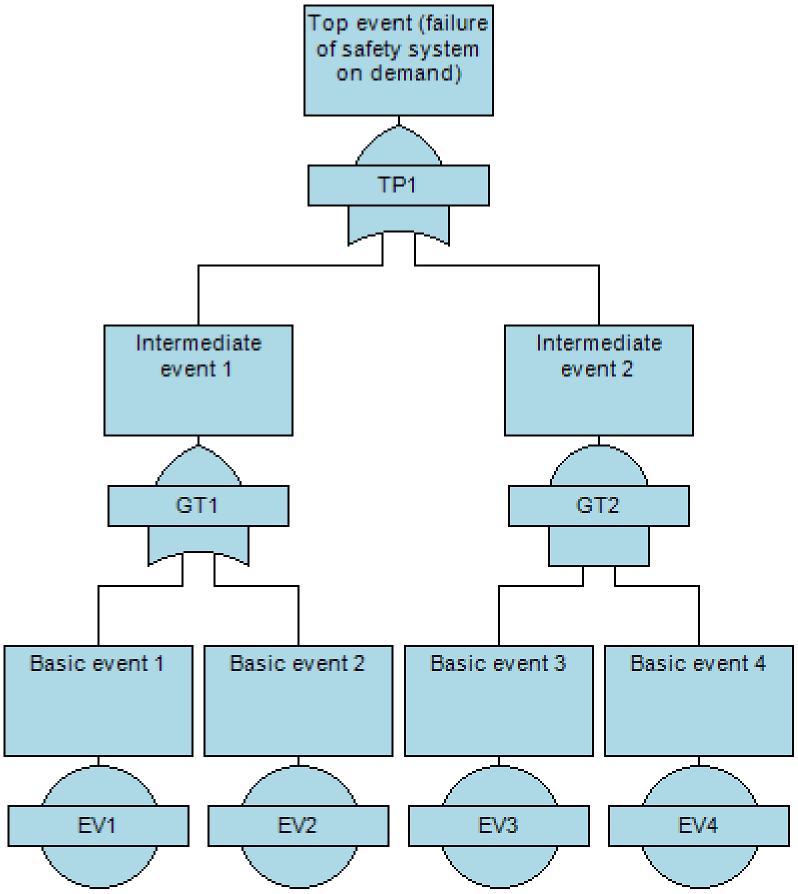


Figure 2-2 Simple example of fault tree analyses (Source: DNV).

2.2.2 Event tree analysis

The Event Tree Analysis (ETA) methodology, as detailed in IEC/ISO 31010:2009 - Risk assessment techniques and IEC 62502:2010 - Analysis techniques for dependability - Event tree analysis, has been applied in the safety analysis. ETA is a commonly used method for the analysis of hazardous events. The method is inductive, employing forward logic, as explained in the following sections.

An event tree is a graphical logic model that identifies and quantifies possible outcomes following an initiating event. The event sequences are usually characterized in terms of (IEC 62502:2010):

- **Functions:** The fulfilment (or not) of functions as mitigating factors;
- **Systems:** The intervention (or not) of systems as mitigating factors which are supposed to take action for preventing the progression of the initiating event into an accident or in the case of failure of the mitigating factors, the mitigation of the accident itself;
- **Phenomena:** The occurrence or non-occurrence of physical phenomena.

Figure 2-3 presents a simple graphical representation of an event tree, focusing exclusively on mitigative factors. The event tree begins with the initiating event, which is the starting point. In the oil & gas industry, various terms may be used to describe these events, such as undesired event, demand, process upset, or process deviation. Each subsequent event in the tree is dependent on the occurrence of its precursor event. The outcomes of these precursor events are typically binary (e.g., success or failure, yes or no), but they can also involve multiple outcomes (e.g., 100%, 20%, or 0% closure of a control valve).

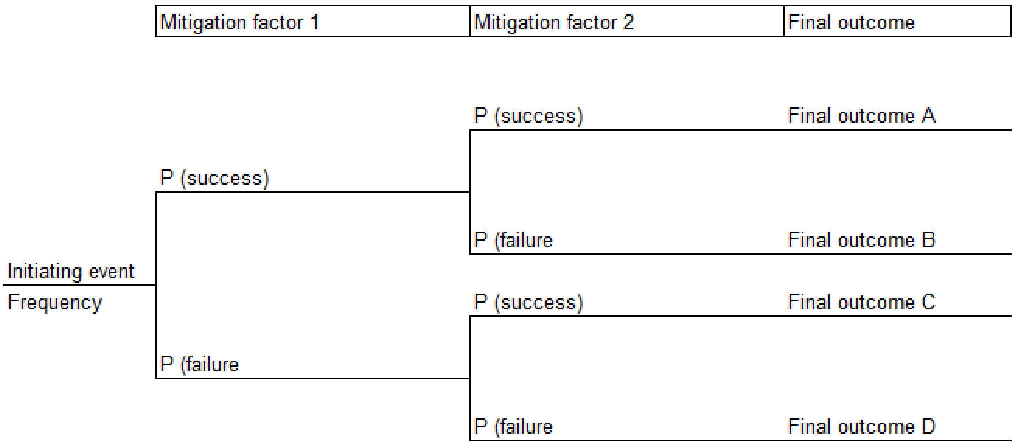


Figure 2-3 Graphical representation of an event tree (Source: DNV).

The ETA outcomes are determined by each branch's endpoint, commonly referred to as the outcome frequency. To calculate this, the frequency of the initiating event is multiplied by the probabilities associated with each branch, yielding the overall frequency of each scenario.

Finally, the event tree analysis results can be used as input for risk quantification. This involves multiplying the outcome frequency of each scenario by the severity of its consequences.

3. Reliability analysis of hydrogen equipment

Realistic failure data is an essential component of any quantitative risk analysis. However, collecting such data is a challenging task that raises several questions regarding the suitability of the data, the assumptions underlying it, and the uncertainties associated with it. This analysis investigates the reliability of selected equipment for hydrogen-fuelled ships, including an assessment of the suitability of various databases containing failure data. The identification of the most relevant equipment for the reliability analysis is based on designs currently being conceptualized in the maritime industry. By relying on a range of data sources, this study aims to present a comprehensive picture of the reliability of equipment used in hydrogen-fuelled ships.

3.1 Failure data sources

This chapter presents relevant data sources containing reliable data for equipment and reviews selected data sources to be applied in this study. Many data sources contain reliability data for equipment and components. Since this study focuses on using hydrogen as a fuel for ships, the ideal database should encompass hydrogen installations in relevant maritime environments, preferably on a ship. Obviously, such databases do not exist. The lack of data is mainly due to the fact that the use of hydrogen as fuel for transportation is relatively new and the infrastructure technologies are under development and currently mainly applied in demonstration projects. The experience data available for hydrogen installations is therefore scarce (DNV, 2008).

As recommended in the previous EMSA report on “Mapping safety risks for hydrogen-fuelled ships” (EMSA, 2024), basic failure data must either rely on historical data from general onshore and offshore process industry equipment or apply failure rates for hydrogen-specific operating experience. Maritime-specific factors must be accounted for when deriving failure data for quantitative analysis.

3.1.1 Data sources containing reliability data for equipment

There is limited availability of databases specifically focused on hydrogen equipment failures. Most QRAs for hydrogen facilities have utilized published values from other non-hydrogen sources (Sandia, 2009). Due to this limitation, a broad range of databases has therefore been reviewed in this study. The uncertainties related to the suitability of the failure data are addressed. This list of data sources is provided below (in alphabetic order):

- Center for Chemical Process Safety (CCPS): Guidelines for initiating events and independent protection layers in layer of protection analysis
- Center for Chemical Process Safety (CCPS): Process Equipment Reliability Database (PERD)
- Center for Hydrogen Safety (CHS) Data collection tool
- “Dutch Purple book” by the National Institute for Health and the Environment in the Netherlands (RIVM)
- ESReDA Handbook on Quality of Reliability Data published by DNV
- Hydrocarbon Release Database (HCRD) compiled by UK HSE
- Hydrogen Incident and Accident Database (HIAD), the H2 Lessons Learned (H2LL) database and the High Pressure Gas Safety Institute of Japan (KHK) incident database.
- HyRAM+ by Sandia (Hydrogen Plus Other Alternative Fuels Risk Assessment Models)
- Nonelectronic Parts Reliability Data (NPRD)
- NPRDS (Nuclear Plant Reliability Data System)

- National Renewable Energy Lab's (NREL) Composite Data Products (CDPs)
- Offshore and Onshore Reliability Data (OREDA)
- PDS[3] data handbook by SINTEF Research (2021 edition)
- Process leak for offshore installations frequency assessment model (PLOFAM)
- Red Book published by TNO, Dutch R&D organization
- SAFEN database (Joint Industry Project)

While the data from the databases provides a broad view of equipment reliability, it is important to acknowledge that some manufacturers may present higher reliability figures based on their own internal statistics. The scope of this study does not extend to verifying or challenging these manufacturer-provided reliability statistics. Instead, the focus remains on analyzing data from independent and diverse sources.

3.1.2 Suitability of data sources

This chapter provides some general considerations on the suitability of existing data sources for application on hydrogen-fuelled ships:

- **Marine and ship environment:** One significant uncertainty to consider when using failure data to quantify risks associated with using hydrogen as fuel on ships pertains to the environmental conditions represented therein. Components of hydrogen-related systems onboard ships are subjected to unique loads due to the maritime environment, such as sea atmosphere/spray, green sea, thermal cycling, dynamic loads, vibrations, and inclinations. General onshore equipment failure data are based on systems operating under different conditions, and thus, these maritime-specific effects are not accounted for in the databases (EMSA, 2024). Historical leak data from the offshore industry are more similar to what could be expected on a ship; encompassing leak causes linked to a marine environment.

- **Properties of hydrogen:** Hydrogen is prone to leaks, primarily because hydrogen is the smallest molecule. Thus, uncertainty arises from the differences in the properties and behaviour of hydrogen compared to the media on which the databases are based, and how these differences would influence the leak probability and failure on demand probability of safety-critical equipment.

- **Inspection, certification and maintenance**: Inspection, certification regime and maintenance intervals play an important role in how often leaks occur in process equipment, and can be different for Oil & Gas and process industry installations compared to ships.

- **Piping dimensions and operating pressure:** Hydrocarbon-containing equipment in the offshore industry is generally of larger dimension than hydrogen-containing equipment in, for example, hydrogen fuel systems or hydrogen refuelling stations. Also, operating pressures may be much lower in hydrocarbon process equipment compared to equipment in hydrogen installations (DNV, 2008).

Due to the uncertainties in considering suitability, all use of statistical failure data should be carefully evaluated before being applied in any quantitative analysis. It is crucial that the analyst thoroughly understands the failure data, including its origin, to achieve representative results in QRAs.

One possible approach to address these maritime-specific effects is to adjust the failure data using correction factors. However, due to the limited operational experience with marine hydrogen applications, accurately quantifying or estimating these factors is challenging. Thus, a common practice in quantitative risk analysis for hydrogen-fuelled ships is to apply generic leak frequencies and perform uncertainty analyses to demonstrate how

[3] PDS is a Norwegian acronym for reliability of safety instrumented systems.

variations in leak frequency might affect the overall risk level (EMSA, 2024). The variations may arise from specific operational conditions, maritime factors, and the unique characteristics of each fuel system installation.

3.1.3 Review of selected data sources

This study has evaluated a wide range of data sources to identify the reliability data that are considered to be most applicable and have the highest quality. It, therefore, can be used to reasonably represent the reliability of equipment to be used in hydrogen-fuelled ships. However, maritime-specific factors must be accounted for when deriving failure data for quantitative analysis. A descriptive summary of the selected databases is provided in Appendix A.

Leak frequency data

The preferred sources for leak frequency data are HCRD and HyRAM+. The quality of the HCRD offshore dataset is exceptionally high, especially when compared to previous onshore frequencies. This is further supported by earlier studies conducted by DNV in 2006 and 2008, in co-operation with the offshore operators, which concluded that HCRD was the best quality dataset, and apparently suitable for use in onshore as well as offshore QRA (DNV, 2006) (DNV, 2008). However, it should be noted in the use of the data, results tend to indicate a higher risk than what is experienced by the industry in the North Sea. Therefore, in the early 2000s, two of the major operators commissioned DNV to develop modified HCRD frequencies (DNV, 2006). It is these values that are applied in this study.

The perhaps most well-known source for hydrogen leak frequencies is the “Hydrogen Plus Other Alternative Fuels Risk Assessment Models” (HyRAM+), provided by Sandia National Laboratories. The HyRAM+ dataset is unique as it is the only dataset that contains hydrogen-specific data. The default values for compressed hydrogen in HyRAM+ are based on generic system leak frequencies and data from compressed hydrogen systems documented in a Sandia technical report from 2009 (Sandia, 2009) and updated in the Sandia technical reports (Sandia, 2012) and (Sandia, 2020). For liquid hydrogen, leak frequencies were determined using gaseous hydrogen and liquefied natural gas data as outlined by (D. M. Brooks, 2021). However, as stated in the first Sandia report from 2009, most of the failure data are derived from various industries, such as chemical processing, nuclear power, and oil and gas. Only a small portion of this data is specific to hydrogen (Sandia, 2021). Consequently, the HyRAM+ data combines general industry data and limited hydrogen-specific failure data.

In addition, this study has applied data from NPRD for equipment missing from these two sources mentioned above.

Failure-on-demand data

There is no clear and obvious preference for failure-on-demand probabilities of safety and control equipment, such as gas detectors, temperature sensors and pressure relief valves. Instead, several sources have been referenced. These preferred sources for failure-on-demand data are:

- PDS
- OREDA
- NPRD
- CCPS

3.2 Failure data for equipment

This chapter presents the failure data associated with various types of equipment for hydrogen-fuelled ships. Understanding the failure rates and mechanisms is crucial for any risk analysis. The chapter starts with introducing the equipment taxonomy before presenting the results for rotating and mechanical equipment, electronic equipment and safety and control equipment. Finally, the chapter concludes with an analysis of the findings and offers recommendations for the use of failure data.

3.2.1 Equipment taxonomy

The taxonomy is a systematic classification of items into generic groups based on factors possibly common to several of the items (location, use, equipment subdivision, etc.). The taxonomy classification is based on ISO 14224 (Collection and exchange of reliability and maintenance data for equipment) and is presented by the hierarchy as shown in Figure 3-1 (ISO 14224:2016).

Levels 1 to 5 represent a high-level categorization of industries and plant applications regardless of the equipment units (see level 6) involved. Levels 6 to 9 are related to the equipment unit (inventory), with the subdivision in lower indenture levels corresponding to a parent-child relationship. For equipment selection to be included in the failure data collection for this analysis, taxonomy levels 6 through 9 will be used, as defined by ISO 14224. Examples of equipment units within class 6 include heat exchangers, pumps, compressors, and piping. Lower levels 7 and 8 encompass items such as gas detectors, valves, filters, and couplings. Equipment classified as parts (level 9) is limited to seals and gaskets in this study, excluding other minor parts such as bolts and nuts. The analysis does not distinguish between these equipment levels.

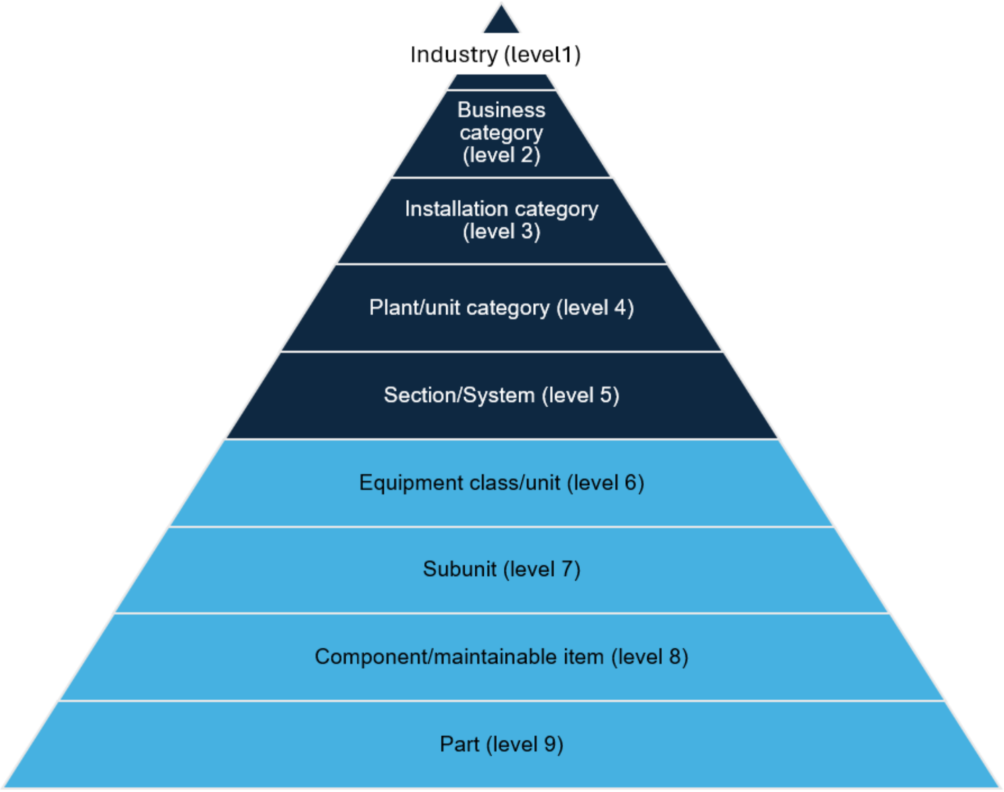

Industry (level1)
Business category (level 2)
Installation category (level 3)
Plant/unit category (level 4)
Section/System (level 5)
Equipment class/unit (level 6)
Subunit (level 7)
Component/maintainable item (level 8)
Part (level 9)

Figure 3-1 Equipment taxonomy hierarchy based on ISO 14224 (Source: DNV).

The reliability analysis will be performed on the generic equipment presented in Table 3-1. The list is created by subject matter experts based on available information on current hydrogen-fuelled ship concepts. It includes four types of equipment: Rotating equipment, mechanical equipment, electrical equipment, and safety and control equipment. It should be noted that the list consists of the most relevant equipment for a hydrogen fuel system but does not necessarily cover all components that could be included in these systems.

Table 3-1 Equipment types included in the failure data analysis

Rotating equipment	Mechanical equipment	Electrical equipment	Safety and Control
- Blowers and fans - Compressors - Electric generators - Pumps	- Filters and strainers - Heat exchangers - Pressure vessels - Pipes - Valves (manual) - Valves (remote) - Instruments and fittings - Seals/gaskets - Connections (flanges and joints) - Cylinders - Hoses	- Switchgear - Uninterruptible power supply (UPS) - Wiring	- Control logic units - Fire detectors - Gas detectors - Pressure and temperature sensors - Telecommunications - Excess flow valves - Flow restriction valves (orifice) - Non-return valves - Pressure Relief Valves (PRV) - ESD Valves (actuator) - Fire water pump - Solenoid valve/pilot valve

Table 3-2 introduce the information that is provided in the reliability analysis.

Table 3-2 Equipment information.

Column	Description
Equipment	Generic name of the equipment.
Failure mode	For *rotating equipment* and *mechanical equipment*, the relevant failure modes are: - General failure - Leakage For *electronical equipment,* the relevant failure mode is general failure. For *safety and control equipment*, the relevant failure modes are: - Dangerous undetected failures - Fail to function on demand - Critical failures When comparing failure rates across different sources, it's crucial to consider the varying presentations of data between databases. For instance, the desired failure mode for safety and control equipment is λ_{DU} (dangerous undetected), but not all databases provide this specific data, leading to the use of more general data in some cases. The failure modes presented in the three sources differ as follows: the PDS Data Handbook provides λ_{DU} (dangerous undetected), OREDA typically offers "failure on demand," and NPRD includes all types of failures. For the other equipment types, the failure mode "leakage" is applied whenever relevant. If not, a general failure mode is applied instead.

Column	Description
Database	Relevant databases that contain failure data on the equipment.
Component name as from source	Specific name of the equipment, as found from the database. This is included to enable the retrieval of information from the specific database if needed. Different databases present the names in various formats, therefor the names are displayed differently.
Failure rate	- The failure rate is presented as failures per equipment item year. - For the failure mode "leakage" the failure rate is given for different hole diameters. From the database - HyRAM+ failure data is given for five release sizes relative to the pipe flow area: 0.01%, 0.1%, 1%, 10% and 100%. Latest HyRAM Version is 5.1. - From HCRD the frequencies are given for the two-hole sizes >= 1 mm diameter and >= 50 mm diameter. - Values from NPRD are given per 1.0E06 hours and converted to per year.
For Safety and control equipment the PFD_{aug} is also presented.	The PFD_{avg} is calculated based on the failure rate value as described in Chapter 2.1.4.

3.2.2 Rotating and mechanical equipment

The following tables present the failure data for the equipment within the generic equipment groups:

- Rotating equipment in Table 3-3
- Mechanical equipment in Table 3-4

These data primarily serve to present equipment that may leak. Exceptions include some rotating equipment where general failure is also considered relevant. For instance, for a pump, both leakage and general failure/malfunction (e.g., pump stop) are considered relevant.

As stated in chapter 3.1.3, the preferred sources for leak frequency data are HCRD and HyRAM+. In addition, this study has applied data from NPRD for equipment missing from the two mentioned sources.

Note that HCRD values are modified frequencies, as explained in chapter 3.1.3.

Table 3-3 Failure data for rotating equipment.

Equipment	Failure mode	Database	Component name (as from source)	Failure rate (/year)
Blowers and fans	General failure	NPRD	Fan, ventilating	4.38E-02
Compressors	Leakage	HCRD	Centrifugal compressor	>= 1 mm DIA: 2.0E-03 >= 50 mm DIA: 6.0E-03
			Reciprocating compressor	>= 1 mm DIA: 2.7E-02 >= 50 mm DIA: 1.1E-05
		HyRAM+	Compressors	0.01%: 1.8E-01 0.1%: 1.9E-02 1%: 5.8E-03 10%: 1.4E-04 100%: 1.2E-05
Electrical generators	General failure	NPRD	Generator, electronic	3.5E-02

Equipment	Failure mode	Database	Component name (as from source)	Failure rate (/year)
Pumps	General failure	NPRD	Pumps, summary	1.58E-02
	Leakage	HCRD	Centrifugal pumps	>= 1 mm DIA: 1.8E-03 >= 50 mm DIA: 2.4E-05
			Reciprocating pumps	>= 1 mm DIA: 3.9E-03 >= 50 mm DIA: 5.2E-04

Table 3-4 Failure data for mechanical equipment.

Equipment	Failure mode	Database	Component name as from source	Failure rate (/year)
Filters and stainers	Leakage	HCRD	Filter	>= 1 mm DIA: 8.9E-04 >= 50 mm DIA: 6.4E-06
		HyRAM+	Filters	0.01%: 5.3E-03 0.1%: 5.0E-03 1%: 4.8E-03 10%: 4.6E-03 100%: 4.4E-03
Heat exchangers	Leakage	HCRD	Heat exchanger (h/c in shell)	>= 1 mm DIA: 1.4E-03 >= 50 mm DIA: 1.3E-04
			Heat exchanger (h/c in tube)	>= 1 mm DIA: 1.0E-03 >= 50 mm DIA: 4.9E-05
			Heat exchanger (plate)	>= 1 mm DIA: 6.0E-03 >= 50 mm DIA: 3.6E-04
			Heat exchanger (air cooled)	>= 1 mm DIA: 1.2E-03 >= 50 mm DIA: 6.9E-05
Pressure vessels	Leakage	HCRD	Process vessel	>= 1 mm DIA: 5.0E-04 >= 50 mm DIA: 1.1E-04
Pipes	Leakage	HCRD	Steel pipes (2'') – 1 m length	>= 1 mm DIA: 5.7E-05 >= 50 mm DIA: 0.0E+00
			Steel pipes (6'') – 1 m length	>= 1 mm DIA: 2.0E-05 >= 50 mm DIA: 7.7E-08
		HyRAM+	Pipes	0.01%: 6.7E-06 0.1%: 3.5E-06 1%: 9.3E-07 10%: 4.6E-07 100%: 1.5E-07
Valves	Leakage	HCRD	Manual valves (2'')	>= 1 mm DIA: 1.4E-05 >= 50 mm DIA: 0.0E+00
			Manual valves (6'')	>= 1 mm DIA: 4.8E-05 >= 50 mm DIA: 4.9E-07
			Actuated valves (6'')	>= 1 mm DIA: 2.6E-04 >= 50 mm DIA: 1.9E-06
		HyRAM+	Valves	0.01%: 5.6E-03 0.1%: 6.7E-04 1%: 6.0E-05

Equipment	Failure mode	Database	Component name as from source	Failure rate (/year)
				10%: 3.2E-05 100%: 6.1E-06
Instruments and fittings	Leakage	HCRD	Instrument (0.5")	>= 1 mm DIA: 2.3E-04 >= 50 mm DIA: 0.0E+00
		HyRAM+	Instruments	0.01%: 6.2E-04 0.1%: 2.0E-04 1%: 1.1E-04 10%: 1.0E-04 100%: 3.7E-05
Seales/gaskets	General failure (leakage)	NPRD	Gasket and seal set	4.09E-01
			Gasket, Summary	1,22E-01
Connections	Leakage	HyRAM+	Flanges	0.01%: 2.0E-02 0.1%: 2.2E-03 1%: 2.4E-04 10%: 2.6E-05 100%: 2.9E-06
			Joints	0.01%: 6.9E-05 0.1%: 2.4E-06 1%: 6.6E-06 10%: 5.6E-06 100%: 4.9E-06
		HCRD	Flanged joints (2")	>= 1 mm DIA: 2.3E-05 >= 50 mm DIA: 0.0E+00
			Flanged joints (6'')	>= 1 mm DIA: 4.3E-05 >= 50 mm DIA: 3.6E-07
			Flanged joints (12'')	>= 1 mm DIA: 1,2E-04 >= 50 mm DIA: 1,1E-06
Cylinders	Leakage	HyRAM+	Cylinders	0.01%: 1.1E-07 0.1%: 9.6E-07 1%: 6.6E-07 10%: 3.8E-07 100%: 2.1-08
Hose	Leakage	HyRAM+	Hoses	0.01%: 1.1E-03 0.1%: 1.9E-04 1%: 1.7E-04 10%: 1.5E-04 100%: 7.3E-05

It is not straightforward to compare the statistics from HCRD and HyRAM+. This is because the HyRAM+ failure data is given for five release sizes relative to the pipe flow area: 0.01%, 0.1%, 1%, 10% and 100%, while data from HCRD are given for the two-hole sizes >= 1 mm diameter and >= 50 mm diameter.

DNV has previously analyzed several commonly used leak frequency databases and compared them to hydrogen incident data. Comparison of HyRAM+ leak frequency, which is area-dependent against diameter-dependent exposure data in HCRD, demonstrates larger variations in leak frequency output for larger hole sizes, which is mostly due to the lack of diameter-dependence in HyRAM+. The variation, however, reduces towards smaller hole sizes, which could either be due to the under-reporting of small leaks in HCRD or overestimating in HyRAM+ due to a combination of hole-size dependent models with the selection of hydrogen-specific data. Currently, over 90% of all leaks in HyRAM+ relate to very small and small categories. To better compare the HCRD and HyRAM+ data sources, graphs showing the frequency of leaks versus hole diameter were developed for the following components: reciprocating compressors, filters, pipes, pumps, actuated valves, manual valves, joints, and hoses. The full results of the comparison are provided in Appendix B.

Since it is challenging to directly compare the leak frequencies of HCRD and HyRAM+, graphs have been created to show which equipment is most prone to leaks within each database separately. As shown in Figure 3-2, the equipment most prone to leaks, according to the HCRD, are pumps, heat exchangers and filters. Compressors, especially the reciprocating type, have a significantly higher leak rate - more than nine times that of pumps. This data was, therefore, not depicted in the figure; otherwise, other equipment data would not be possible to see. Note that the values visualized in this figure are taken as the average of the 'above 10 mm and 50 mm' diameter of equipment, and steel pipe values are per meter.

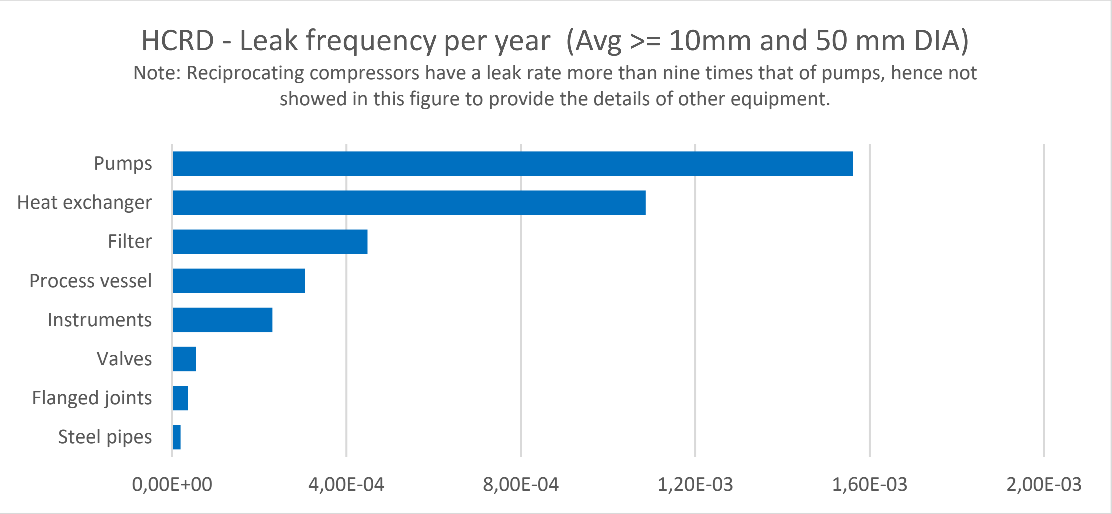


Figure 3-2 Leak frequencies per year from HCRD (Source: DNV).

As shown in Figure 3-3, the equipment most prone to leaks, according to the HyRAM+, are filters and flanges. The HyRAM+ database does not include data on compressors, pumps, and heat exchangers.

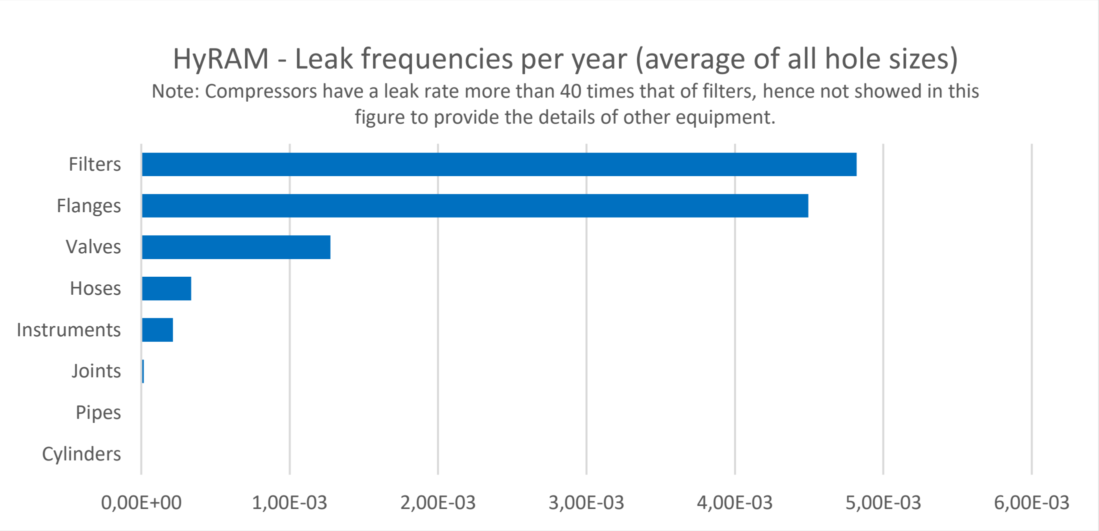


Figure 3-3 Leak frequencies per year from HyRAM+ (Source: DNV).

It is important to note that these figures list the leak rates per equipment type. While there may be a limited number of compressors, heat exchangers, pumps, and filters in a ship's hydrogen fuel system, some conceptual designs have numerous flanged connections and valves. Therefore, when estimating where a leak is most likely to occur, the quantity of each type of equipment must also be considered.

3.2.3 Electronical equipment

Table 3-5 presents the failure data for the equipment within the 'electrical equipment' group. This analysis is limited to switchgear, uninterruptible power supply (UPS) and wiring.

Table 3-5 Failure data for electrical equipment.

Equipment	Failure mode	Database	Component name (as from source)	Failure rate (1/year)
Switchgear	General failure	NPRD	Switchgear (Summary)	3.57E-01
Uninterruptible power supply (UPS)	General failure	NPRD	Uninterruptible Power Supply (summary)	1.23E-01
Wiring	General failure	NPRD	Wire, Electrical (summary)	7.91E-03

3.2.4 Safety and control equipment

As highlighted in the previous EMSA report (EMSA, 2024), it is prudent to assume the possibility of hydrogen leaks in fuel systems. Therefore, implementing effective monitoring and mitigation barriers is crucial to managing any potential loss of containment scenarios. Table 3-6 presents the failure data for the safety and control equipment. Note that the PDS failure rates are given as *Rate of dangerous undetected failures* and the OREDA failure rates are given as *Mean failure rate,* while the CCPS Guideline gives PFD_{avg} directly. The assumed proof test interval for each equipment for calculation of the $\mathrm{PFD}_{\mathrm{avg}}$ is 1 year (8760 hours).

Safety and control equipment failure data have been gathered and compared from the following sources:

- PDS Handbook
- OREDA
- CCPS Guideline
- NPRD

Table 3-6 Failure data for safety and control equipment.

Equipment	Failure mode	Database	Component name as from source	Failure rate (per 10^6 h)	PFD$_{avg}$
Control logic units	Dangerous undetected failures	PDS Data handbook	Analog input - Standard industrial PLC	0.7	3.07E-03
			CPU – logic solver (1oo1) - Standard industrial PLC	3.5	1.53E-02
			CPU – logic solver (1oo1) - Programmable safety	0.3	1.31E-03
			Digital output - Standard industrial PLC	0.7	3.07E-03
	Fail to function on demand	OREDA	CLU – Control logic units	5.22	2.29E-02
Fire detectors	Dangerous undetected failures	PDS Data handbook	Smoke detectors	0.16	7.01E-04
			Heat detector	0.37	1.62E-03
			Flame detector	0.35	1.53E-03
	Critical failures	OREDA	Fire and gas detectors, flame, (using infrared technology)	6.48	2.84E-02
Gas detectors	Dangerous undetected failures	PDS Data handbook	Electrochemical detector	1.7	7.45E-04
			Line gas detector	0.44	1.93E-03
			Aspirated IR point gas detector system	2.9	1.27E-02
			IR point gas detector	0.25	1.09E-02
			Catalytic point gas detector	1.5	6.57E-03
	Fail to function on demand	OREDA	Fire and gas detection, hydrocarbon gas, IR	0.95	4.16E-03
			Fire and gas detection, hydrocarbon gas, Catalytic	7.60	3.33E-02
Pressure and temperature sensors	Dangerous undetected failures	PDS Data handbook	Pressure transmitter	0.48	2.10E-03
			Temperature transmitter	0.10	4.38E-04
			Level transmitter	1.90	8.32E-03
			Flow transmitter	1.4	6.13E-03
	Fail to function on demand	OREDA	Input devices, pressure	0.51	2.89E-02
	All failure modes	OREDA	Input devices, temperature	3.63	1.59E-02
	General failure	NPRD	Sensor, temperature	0.42	1.84E-03
Telecommunications	Dangerous undetected failures	PDS Data handbook	PA loudspeaker	0.2	8.76E-04
	General failure	NPRD	Telephone system (summary)	8.32	3.64E-02

Equipment	Failure mode	Database	Component name as from source	Failure rate (per 10^6 h)	PFD$_{avg}$
Excess flow valves	General failure	CCPS Guideline	Excess flow valve	-	1.00E-01
Flow restrictions valves (orifice)	All failure modes	OREDA	Valves, multiple-orifice, flare, vent and blow-down	4.23	1.85E-02
	General failure	NPRD	Flow control valve	2.33	1.02E-02
	General failure	CCPS Guideline	Restrictive flow orifice	-	1.00E-02
Non-return valve/ check valve	General failure	CCPS Guideline	Check valve	-	1.00E-01
Pressure Relief Valves (PRV)	Dangerous undetected failures	PDS Data handbook	Pressure relief valve –PSV	1.90	8.32E-03
	Fails to open on demand	OREDA	Valves, relief	0.44	1.93E-03
	General failure	NPRD	Valve, Pressure relief	2.11	9.26E-03
Solenoid/ pilot valves	Fails to change position upon signal	PDS	Solenoid/Pilot Valves	0.3	1.31E-03
ESD valves (actuator)	Fails to close on demand	OREDA	Valves, ESD	1.30	5.69E-03
	General failure	NPRD	Valve, butterfly, summary	4.25	1.86E-02
			Valve, ball, summary	2.36	1.03E-02
			Valve, gate, summary	16.39	7.18E-02
			Valve, plug, summary	4.74	2.08E-02
Fire water pump	Dangerous undetected failures	PDS Data handbook	Fire water pump system (complete) – diesel electric	25	1.1E-01
			Fire water pump system (complete) – diesel hydraulic	21	9.20E-02
			Fire water pump system (complete) – diesel mechanical	14	6.13E-02
	Fail to start on demand	OREDA	Pumps, centrifugal, water fire fighting	3.66	1.6E-02

The average failure on-demand probabilities in Table 3-6 are ranked from highest to lowest in Figure 3-4.

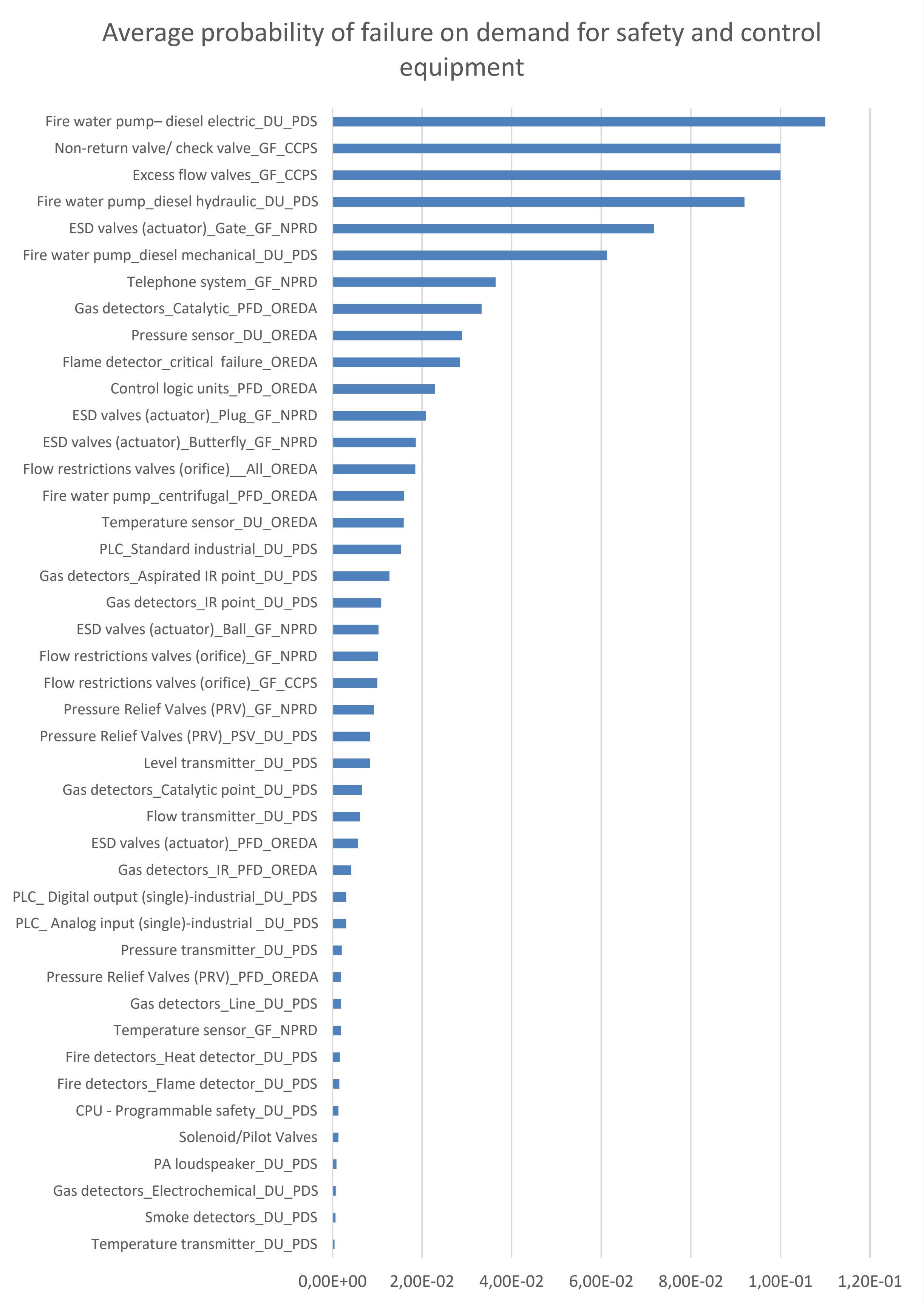


Figure 3-4 Average probability of failure on demand for safety and control equipment (Source: DNV).

The safety and control equipment that are more likely to fail on demand are:

- Fire water pumps
- Non-return valves/check valves
- Excess flow valves
- Actuated ESD valves (gate type)

Note that fire water pumps may have shorter test intervals, resulting in a lower failure-on-demand probability. However, independent third-party tests for ship applications are typically conducted annually.

Note the following abbreviations:

- GF: General Failure
- DU: Dangerous Undetected failure
- PFD: Failure on demand

There is also a notable spread of values for similar types of equipment. One example is catalytic gas detectors, where OREDA gives 3.33E-02, while PDS gives 6.57E-03, which is one order of magnitude lower. When different database sources provide varying failure rates, this can have various reasons, such as different data collection methods, industry and environmental differences, and different data record set sizes and time periods. When selecting failure rates from otherwise similar data sources, it is generally advisable to choose a conservative approach by selecting the highest failure rates.

3.3 Conclusion and recommendations

It's important to differentiate between databases that provide leak frequencies for components (such as flanges, instruments, and valves) and those that offer failure-on-demand probabilities for safety and control equipment (like gas detectors and fire water pumps). Certain equipment, like pressure relief valves, may have both types of data, as they can fail to open and be prone to leaks.

Due to the lack of experience with hydrogen-fuelled ships and consequently also of an industry-specific leak database for maritime, we consider the generic HCRD and/or HyRAM+ databases as the best alternative when establishing leak frequencies for hydrogen-fuelled ships.

The rationale for selecting HCRD is based on its extensive and high-quality dataset, widespread use in QRAs, and consideration of various parameters, including equipment operation in offshore environments. The reason for choosing HyRAM+ is that this toolkit forms the basis for carrying out quantitative risk assessments and modelling the consequences for hydrogen infrastructure and transportation systems. Although the leak data in HyRAM+ come from various industries and have limited hydrogen-specific information, it is currently the only dataset designed specifically for hydrogen applications. It's also worth noting that HyRAM+ is a regularly updated research software, so the models and data may change over time.

Although the HCRD and the HyRAM+ databases are considered the most applicable and have the highest quality, they do not account for maritime-specific factors. Additional uncertainty arises from the differences in the properties and behaviour of hydrogen compared to the mediums on which the Oil & Gas databases are based. Hydrogen is prone to leaking due to its low density and small molecular size. It's not clear how much these characteristics, in combination with the specific environmental conditions onboard a ship, will impact the reliability of data sources in accurately predicting leak frequencies. Furthermore, hydrogen installations generally have smaller equipment dimensions compared to industrial plants and offshore installations. Inspection, certification regimes, and maintenance intervals also significantly affect the frequency of leaks in process equipment and can differ between Oil & Gas/process industry installations and ships.

Leak frequencies have always been a major source of uncertainty in risk analysis (DNV, 2008). The lack of hydrogen-specific failure data and uncertainties considering the suitability for ship applications result in a high degree of uncertainty in leak frequency analysis in QRAs for hydrogen fuel system installations.

To compensate for this, a common practice in quantitative risk analysis for hydrogen-fuelled ships is to apply generic leak frequencies (such as HCRD and HyRAM+) and perform uncertainty analyses to demonstrate, e.g., how an increased leak frequency might affect the overall risk level. The adjustment may arise from specific operational conditions, maritime factors, and the unique characteristics of each fuel system installation. Regardless of the chosen leak database, the key factor is to consider uncertainty.

For safety and control equipment, it's important to address uncertainty on a case-by-case basis in quantitative risk analysis. The data collected from the oil and gas sector is based on an industry that requires demonstrating a Safety Integrity Level (SIL), which is not required in maritime. Hardware and software from reputable manufacturers supplying SIL-certified components to the oil and gas sector are likely to be of higher standard and have less uncertainty. There is no clear and obvious preference for failure-on-demand probabilities of safety and control equipment; instead, multiple sources have been referenced. The failure data from the PDS Handbook, OREDA, CCPS Guideline, and NPRD have all been reviewed and cited in this study.

We note the following important issues for further development of the hydrogen Guidance document:

- According to the HCRD and HyRAM+ databases, heat exchangers, compressors, pumps, and filters exhibit higher leak rates compared to other individual components. Consequently, regulations concerning the arrangement of spaces where such components may be used must account for this.

- The system's leakage probability depends on each component's leakage probability and the number of components; e.g., system designs with numerous flanged connections and valves have a higher leak potential than a fully welded piping system.

- According to the PSD, NPRD, and other databases, non-return valve/check valves, excess flow valves, and actuated ESD valves (gate type) show higher failure rates than other individual safety and control components. Therefore, it might be necessary to incorporate other/additional protection layers.

4. Reliability analysis of safety-critical systems

This analysis builds on the equipment-level analysis in Chapter 3 to explore the performance and reliability of selected safety-critical systems within generic hydrogen fuel system configurations. These configurations will be subjected to comprehensive risk analysis in the next deliverables of this study. Therefore, it is crucial to establish a foundation and provide insights for hazard identification and risk analysis work.

This analysis not only supports risk analysis but also demonstrates a methodology for assessing the performance of safety-critical systems and functions in general, thereby enhancing our ability to ensure safety and reliability for all hydrogen systems across various configurations.

It must be emphasized that the reliability cases analysed in the following chapters consider leakage scenarios, including full-bore ruptures. Other types of loss of containment, such as releases due to grounding, collision, and foundering, are not included.

4.1 Selection of generic ship configurations and safety-critical systems

To effectively evaluate the performance of safety-critical systems, it is essential to consider them within their specific context. This involves outlining some fundamental design assumptions. The two primary parameters that define the ship’s arrangement and consequently influence the risk level for hydrogen-fuelled ships are:

- **Storage condition** of fuel onboard: Liquefied hydrogen (LH2) or compressed hydrogen gas (H2).
- **Storage location** of fuel onboard: On deck (unconfined area) or below deck in a confined space.

For hazard identification and risk analysis in the subsequent deliverables of this study, Process and Instrumentation Diagrams (P&IDs) or high-level process flow diagrams may be applied to visualise relevant onboard system configurations for both LH2 and CH2 storage. However, for this report, we will keep the descriptions and visualisations to a minimum to provide enough context to understand the issues of the selected safety-critical systems. The descriptions are based on current concepts being proposed by designers and manufacturers today. In that respect, it is worth noting that these designs do not represent the final solutions but rather reflect the developments in the industry.

The analysis is performed for two different fuel containment systems and storage locations, in addition to one bunkering configuration:

- **Case 1: Compressed hydrogen storage on deck – Leak detection and fuel supply shutdown system**

  Many projects investigating the use of hydrogen as a fuel are looking at storing hydrogen in pressurized tanks with gas pressures typically around 350 bar. The tanks can either be fixed to the deck for refuelling from bunkering facilities on shore, or they can be portable tanks that can be lifted off the vessel and refilled at suitable facilities. One challenge with these solutions is the difficulty in arranging hydrogen piping with secondary enclosures due to the large number of pipes and the small dimensions. For portable tanks, there is the additional complication of non-permanent connections, which must be operated at every refuelling operation. As a result, the possibility of having reliable leakage detection enabling rapid shut-down, which is a feature of the double-walled piping design, is reduced. A single-walled hydrogen system on deck will rely on leakage detection located in open air to identify and stop a hydrogen leak. In Case 1, we want to investigate this design feature to better understand how the reliability of leakage detection affects the overall safety of the vessel.

- **Case 2: Liquid hydrogen storage below deck – Inert Gas System**

  In our first project delivery (EMSA, 2024), we found that dilution ventilation may not be an effective way to reduce the impact of significant hydrogen releases in enclosed spaces. When storing liquefied hydrogen below deck the issue of having hydrogen leak sources in enclosed spaces (e.g., TCS) is difficult to avoid. Case 2 examines an alternative to a ventilated TCS, which involves maintaining a constantly inerted atmosphere inside the TCS to prevent ignition, fire, and explosion. The analysis focuses on the likelihood of having a sufficiently inert atmosphere in the TCS on demand. We also discuss other challenges associated with using inerting as a key safety measure.

- **Case 3: Bunkering of liquefied hydrogen – Safe hydrogen bunkering**

  The hydrogen re-fuelling process introduces additional risks, mainly related to leakages. To mitigate these risks, a bunkering location on an unrestricted open deck provides the best boundary conditions to bunker hydrogen safely. In Case 3, we look at the bunkering of liquefied hydrogen on a vessel where the general arrangement prevents having the bunkering manifold on open deck. We examine consequences of a potential leak in a semi-enclosed bunkering station, similar to those used for LNG-fuelled ships. These bunkering stations typically have hatches on the ship's side open during bunkering to allow for the connection of the bunkering hose or Marine Loading Arm (MLA) to the connection point onboard. Risks considered in this case may also apply to open bunkering stations. The intention is not to quantify reliability as in the previous two cases but instead to discuss important challenges and lessons learned from recent studies. This assessment will only focus on the ship systems, excluding the bunkering hose and onshore bunkering facility from its scope.

4.2 Case 1: Compressed hydrogen storage on deck – Leak detection and fuel supply shutdown system

The compressed hydrogen storage on deck configuration is based on various concepts featuring swappable lift-on/lift-off hydrogen containers with composite material cylinders (hereinafter referred to as tanks) designed to carry compressed hydrogen gas at pressures around 350-380 bar. For this configuration, the leak detection and fuel supply shutdown system has been selected for reliability analysis.

4.2.1 Fuel system description

A concept illustration of the hydrogen fuel system is provided in Figure 4-1. The tanks (cylinders) are arranged either vertically or horizontally within the container, with all portable containers positioned on the open deck. It is worth noting that this analysis could also be relevant for fixed tank storage of compressed hydrogen, given the similarity in safety concepts.

For the purposes of this analysis, it is assumed that single-walled piping from the tanks is equipped with a remotely activated tank valve for each cylinder. For some concepts, this is not the case, and the shutdown valve is assigned to a group or section of tanks. Consequently, if a leak occurs upstream of the tank valve, the entire volume of all tanks connected to that section will be released. We have assumed that the piping from the tanks is connected to a common manifold valve before hydrogen is fed to the fuel preparation system

The design safety philosophy is to quickly detect any gas leaks, automatically isolate the leakage, and dilute the escaped gas with natural ventilation. However, the dilution process may be hampered by potential obstructions, such as the hydrogen containers themselves, the compartment structure around the containers, bulwarks, funnels, and other bulkheads designed to separate the hydrogen area from the cargo operation area. For high-momentum jets with a release rate above a certain size, the gas will be driven by its momentum, and not by buoyancy, and the cloud can therefore build up at all locations before it moves upwards (MarHySafe, 2021). Thus, the debate often centres on whether the storage area can be considered fully open or semi-enclosed, with the latter being more susceptible to the dangers of gas concentration build-up. This analysis, therefore, considers a gas leak in a semi-enclosed area.

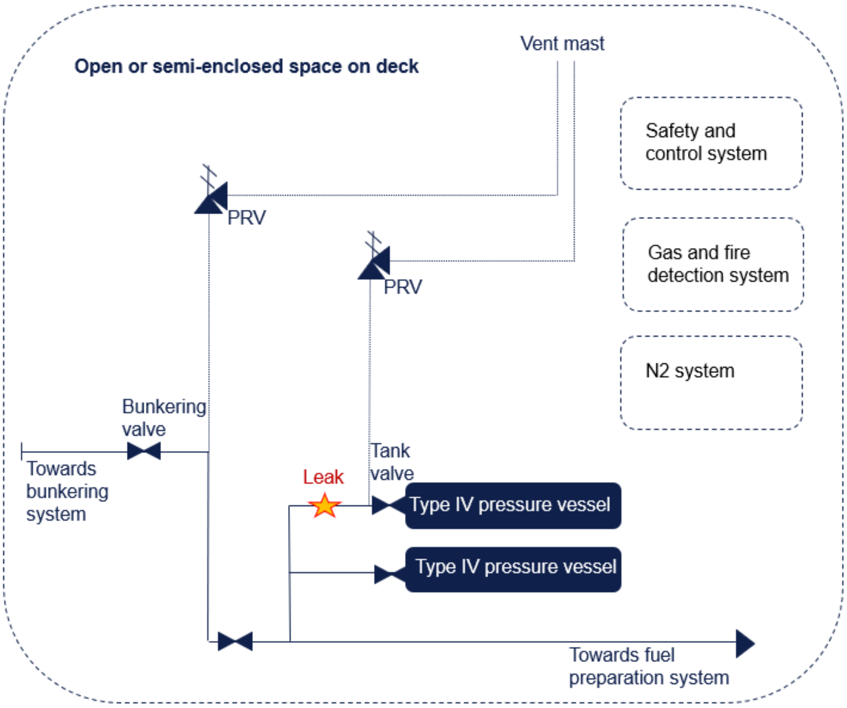


Figure 4-1 Illustration of the concept for compressed hydrogen storage on deck (Source: DNV).

4.2.2 Safety system description

The hydrogen leak detection and automatic shutdown function has been selected for reliability analysis. The principle of the safety function is based on the leak detection and automatic shutdown function applied to LNG-fuelled ships. In the event of a gas leak, the IGF Code require that the safety system shall be arranged to automatically close down the fuel supply system in a way that will isolate the gas supply from the leak.

The safety of compressed hydrogen fuel systems on open deck relies heavily on the successful dilution of gas by natural ventilation upon leaks, but also on the system shutdown function. The success of this safety philosophy requires that leaks in the piping downstream of the tank valves are stopped immediately. This will require rapid gas detection and subsequent closing of isolation valves to stop the release of hydrogen.

The detection and shut-down safety function utilizes three subsystems:

- **Sensor subsystem –** Gas detectors detect a potentially hazardous event and produce an electrical signal that is sent to the logic solver.
- **Logic solver subsystem** - detects the electrical signal exceeding a given threshold and sends a signal to the final element subsystem.
- **Final element subsystem** - performs the safety function by closing the tank valve(s). The gas supply from each individual tank (cylinder) is remotely controlled by a pneumatically actuated tank valve, acting as the final element subsystem to shut down flow in case of emergency (leak).

The three subsystems act together to detect the deviation (i.e., demand) and bring the fuel system into a safe state. In brief, the safety function shall detect, react, and avert. The system is illustrated in Figure 4-2.

The final elements (tank valves) are designed according to the de-energize-to-trip principle, where it is energized during normal operation and removal of the energy will cause a trip action. This principle is also a basis for the fail-safe principle.

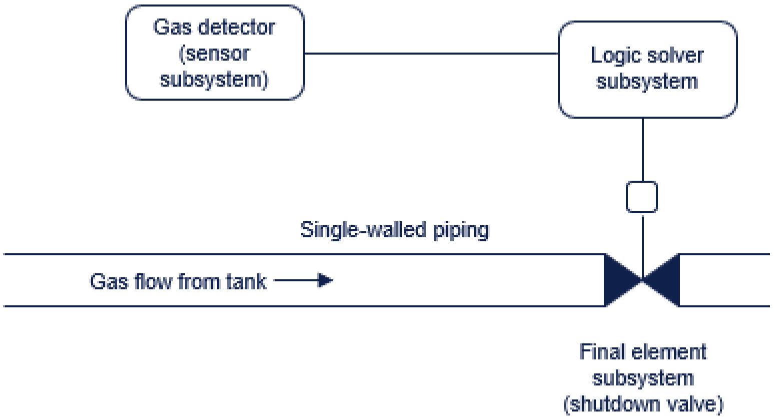

Gas detector (sensor subsystem)
Logic solver subsystem
Single-walled piping
Gas flow from tank
Final element subsystem (shutdown valve)

Figure 4-2 Illustration of the safety function of detecting leaks and stopping flow (Source: DNV).

Gas detector subsystem

The IGF Code does not specify an exact number of gas detectors to be installed. Instead, it mandates that the number of detectors in each space should be determined based on the size, layout, and ventilation of the area. However, it does define the number of detectors required to initiate a shutdown of the fuel system in case of a hazardous event. For instance, an automatic shutdown of the tank valve must occur when gas is detected by two detectors in the Tank Connection Space (TCS) or the Fuel Preparation Room (FPR) at 40% LEL[4]. Gas detection by one detector at 20% LEL should trigger an alarm. This balances the need for early detection versus the risk of spurious shutdowns. Depending on the system arrangement, it may also be necessary to close other valves in the system to isolate a leakage.

There are no specific requirements for gas detection for open deck solutions, as these are based on hazard and risk evaluations, including gas dispersion analysis. For Case 1, concerning the automatic shutdown function on a semi-enclosed deck, we have applied the 2oo2 (two out of two) voting logic to the detector subsystem as a theoretical example. This approach is similar to the requirement for two detectors in the TCS or FPR. When the logic solver subsystem receives signals from both sensors, it processes these signals and initiates the decision to close the tank valve(s).

The latest development in the industry is to consider applying acoustic gas detectors to open and semi-enclosed spaces on deck. The argument for selecting acoustic leak detectors is that if a smaller leak occurs in a location with good ventilation, it may not be detected by a point gas detector. For both indoor and outdoor releases, the response from traditional point detectors is based on the gas coming directly in contact with the sensor element, while acoustic leak detectors respond to the sound of leakage and do not need to wait for a gas concentration to accumulate and form a potentially explosive cloud before they can detect the leak (MSA, 2021). For these systems, reference to LEL is therefore irrelevant.

The uncertainty relates to the system’s ability to detect leakages. It is claimed that the sensors are unaffected by environmental conditions like wind, leak dilution, background noises and the direction of the leak, which would imply that they have high detection reliability and robustness. However, there is ongoing research into how the system may be affected by intermittent ultrasonic noise and noise interference. There is also a lack of experience in the integration of acoustic leak detection into existing conventional gas detection for ship applications.

[4] Alternatively, one self-monitoring detector.

Logic solver subsystem

This unit detects if the electrical signal exceeds a given threshold and sends a signal to the final elements. Logic solvers in this context is the Programmable Electronic Controllers (PLCs). No redundancy is assumed for the logic solver subsystem in this case.

Shutdown of the tank valve

The gas supply from each tank is remotely controlled by a pneumatically actuated valve, such as a ball valve or gate valve. These pneumatic valves are typically of fail-to-close type, meaning they will close if the instrument air supply is lost. This fail-safe function is normally achieved using a spring return arrangement. During normal operation, the valve remains open by applying instrument air pressure to the actuator, which compresses the spring. Thus, the valve is considered normally energized. When the pressure is released, the valve closes due to the spring force, adhering to the de-energize-to-trip principle.

The instrument air supply is managed by solenoid valves, which are electrically operated and can quickly open or close to control the flow of instrument air. These solenoid valves receive electrical signals from the PLC to either allow or cut off the air supply to the actuator of the shutdown valve. Depending on the system arrangement, it may also be necessary to close other valves in the fuel system. Solenoid valves are also referred to as pilot valves.

4.2.3 Reliability analysis

The top event of the fault tree in this analysis is the failure of the safety function to bring the system to a safe state, i.e. failure to function on demand. Two types of failed states are considered: “No shutdown” and “delayed shutdown”, thereby concentrating on the likelihood of major failures only. The reason is also to simplify the structure of the fault tree, as it would be far too complex to take all single AND- and OR-gate structures that might lead to some level of safety system malfunction, e.g. leaking shutoff valve in closed position. Additionally, human factors are excluded from the fault tree analysis. Consequently, no credit is given to the continuous surveillance of alarms by the crew, as it is assumed that a critical gas cloud would form long before the crew could detect the issue and initiate a manual shutdown.

The logic and data of the fault tree are shown in Figure 4.3. The top event - *failure of the function on demand (TP1)* – occurs if either the *no shutdown (GT1)* occurs, or the *delayed shutdown (EV1)* occurs.

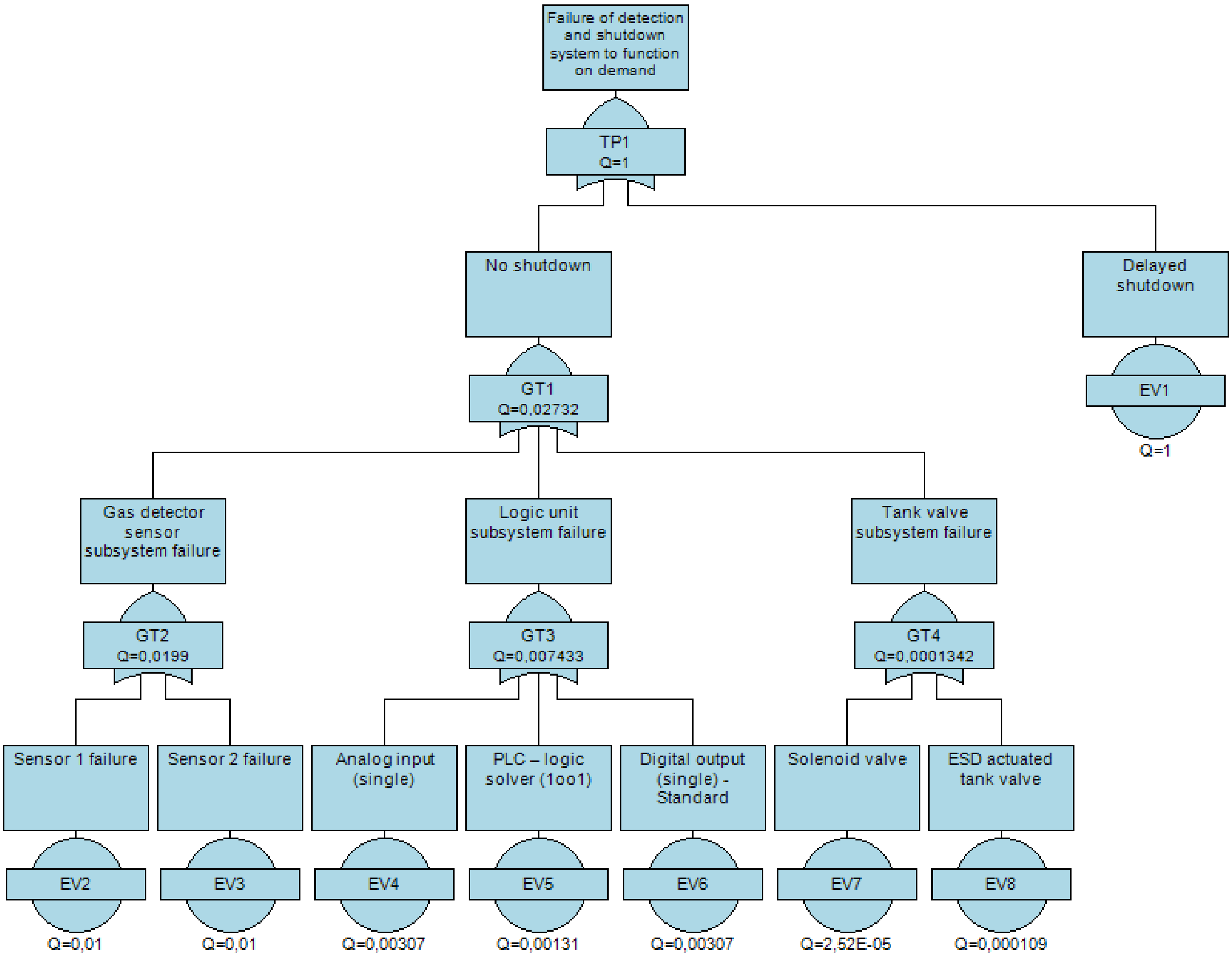


Figure 4-3 Fault tree for safety function - detection and shutdown (Source: DNV).

Delayed shutdown (EV1)

Starting with the *delayed shutdown (EV1)*, it is the response time of the gas sensors subsystem and the tank valve subsystem which is of primary concern. This is because the logic solver subsystems are designed for real-time control and have fast, deterministic response times. They are optimized to respond quickly to input signals and make control decisions in milliseconds or even microseconds.

Process safety time of fire and explosion scenarios

When evaluating the response time, it is important to confirm that the functions can successfully complete their action and that the process can return to a safe operating condition within the process safety time (PST). As defined in Guidelines for Safe and Reliable Instrumented Protective Systems (CCPS 2007b), the PST is "The time period between a failure occurring in the process or its control system and the occurrence of the hazardous event. " (CCPS, 2015). The PST represents an overall scenario timeline, and the safety function should step in along this. timeline and take action. To ensure that the Individual Protection Layers (IPL) will perform its intended function, two important time-based parameters can be considered: The IPL response time (IRT) and the process lag time (PLT).

- The IRT is the time for a given IPL to detect an out-of-limit condition and complete the actions intended to achieve a safe state (but does not include the time of full recovery to the safe state).

- Once the safety function has successfully responded, the PLT represents how much time it will take for the process to achieve or maintain a safe state (i.e. closing time of tank valves).

Failing to bring the fuel system to a safe state within the PST can ultimately lead to the consequence of concern. Of concern for this fuel system is the two major consequences: Jet fires and explosions, which are addressed separately:

- **PST for explosions:** The cloud build-up time for hydrogen leaks is extremely short compared to other gases. A ‘critical cloud’, that can cause significant damage and harm to the ship and its systems if ignited, can form within seconds. Recent studies by DNV indicate that this can occur in just **5 seconds** with leaks in the range of 0.1 kg/s (DNV, 2019) (DNV, 2023). This rapid build-up is due to hydrogen’s low density and rapid expansion upon release. Additionally, the release speed of hydrogen is faster than other gases. Therefore, the required time for detection and shutdown (IRT and PLT) is very critical for preventing explosions. Assuming that the IRT and PLT is within PST, there is the additional unavoidable discharge of hydrogen inventory in the pipes.

- **PST for jet fire and ruptures:** A jet fire is a type of fire that occurs when a flammable gas or liquid is released under pressure from a small opening, such as a pipe or vessel, and ignites. Jet fires may cause escalation or domino effects to other hydrogen systems, e.g. due to rupture, but may also lead to damage to essential safety components or lead to structural failure of load-bearing construction elements due to direct flame impingement. The ship structure around the hydrogen systems is assumed to be fitted with fire insulation. The hydrogen systems are considered to be the weak points, such as tanks, piping, and safety systems. According to (ISO 19881:2018), cylinders are subjected to a fire test, which requires that the cylinder must not rupture until the pressure is released through a Thermal Pressure Relief Device (TPRD). However, these rupture scenarios due to jet fire are likely to be measured in minutes, not seconds. The same applies to piping, which, being unprotected, can be exposed to fire. Pipe rupture is assumed if the fire duration and intensity exceed a certain threshold. However, this too is measured in minutes, not seconds.

Performance assessment of gas detectors

Conventional point gas detectors are not fast enough to prevent a critical cloud (to avoid explosion), as the gas must first accumulate and travel from the leak point to the detector. It must also take into account the time it takes for the gas detector to reach 90% or 50% of the correct reading when a gas concentration is injected into the sensor head (Petro-Online, 2010).

Acoustic detectors may detect leaks in time. Unlike conventional gas detectors that raise alarms at a certain percentage of the Lower Explosive Limit (LEL), acoustic detectors are set to detect specific mass flow rates (leak rates). The time for ultrasonic sound to travel from the leak spot to the detector is typically measured in microseconds (Petro-Online, 2010). However, there are several factors that can hinder an effective response time, according to guidance documents developed by the UK HSE:

- **Short timescale, intermittent ultrasonic noise.** Such interference can be eliminated by setting a time delay to ensure that only continuous noise will cause an alarm (HSE, 2024). This delay would be measured in seconds.

- **Continuous ultrasonic noise interference** can arise from general noise level onboard a ship (e.g. fans, machinery, vibrations, etc.) or leaks in instrument air systems etc. Mapping of sound and adjustment of the setting on the detector may allow the background interference to be "backed off", and the detector will then respond only to noise whose sound power level is above the background level. However, this is sensitive to and depending on the successful process of mapping ultrasonic sound, which is used to characterise the area before installation (HSE, 2024).

- **Additional modes of failure and deterioration** of acoustic leak detectors (typical characteristics), listed in other research report by the UK HSE (HSE, 2017) are: Wrong location/placement of detector due to incorrect mapping or wrong set up (e.g. too much attenuation), drift in detector response and aging and stress.

In addition, the philosophy of integration of acoustic leak detection into existing conventional gas detection systems, alarm and trip systems for maritime or ship applications is not clear, and no experience exists at present.

Conclusion - Process safety time vs. gas detector performance

There is high uncertainty as to whether the gas detector system can prevent a critical gas cloud and explosion from occurring. This is because an explosion can occur within a few seconds if there are leaks in the range of 0.1 kg/s. Conventional point gas detectors are not fast enough, and there is uncertainty regarding acoustic detectors due to the potential for ultrasonic noise interference. Given this high uncertainty, this analysis conservatively assumes that preventing the rapid build-up of a critical gas cloud is unlikely. The delayed shutdown event is, therefore, assumed to have a PFD_{avg} of 1.0. This is the only basic event that is quantified using expert judgment. However, it is only valid for a release of a certain leak rate, typically 0.1 kg/s and above. For smaller leak rates, the PFD will be lower, but it is not estimated in this analysis.

The response time for the safety function to prevent significant consequences from jet fires are more likely, either by gas detection or flame/heat detection. This is because the jet fire consequences may develop over minutes (making time for the safety function to act), while an explosion can occur within a few seconds.

Consequently, since the top event – *failure of the safety system to function on demand (TP1)* – can result from either a complete shutdown failure or a delayed shutdown, the top event probability is also considered to be 1.0. This means that an enhanced safety function or additional protection layers are necessary.

No shutdown (GT1)

While calculating the top event probability is straightforward, it is also interesting to find the failure probability for the *no shutdown failure (GT1).* This event occurs if either of the following basic events occurs (OR-gate):

- **Sensor failure (GT2):** Gas detectors fail to detect abnormal conditions.
- **Logic solver failure (GT3):** Logic solvers fail to process sensor data correctly.
- **Valve actuation failure (GT4):** Shutdown valves fail to actuate.

We have applied the 2oo2 (two out of two) voting logic to the detector (sensor) subsystem as a practical example. There are no failure data on the acoustic gas detectors, according to the reliability analysis of equipment in chapter 3. However, there are certified Safety Integrity Level 2 (SIL-2) capable[5] acoustic gas detectors available in the market. For a SIL-2 capable safety equipment, the PFD_{avg} ranges between 10^{-2} and 10^{-3} and is therefore conservatively set at 10^{-2} (0.01) for each gas detector (EV2 and EV3).

For the logic unit subsystem failure we examine a branch that utilizes an OR-gate to represent the failure logic involving three critical elements: an analog input, a PLC, and a digital output. The OR-gate indicates that a failure in any one of these elements can lead to the overall system failure. The PFD_{avg} for the input (EV4) and output (EV6) is 3.07E-3 and 1.31E-3 for the safety PLC (EV5), as per Table 3-6. The periodical test interval assumption is τ = 8760 h (= 1 year).

The tank valves may have a shorter “test interval” since they are in regular use to close and open individual tanks for flow. In every bunkering operation the tank valves will be closed. The mean failure-to-close-on-demand rate for a single valve is 1.3E-06 per hour, using the value from OREDA in Table 3-6. One tank valve (EV16) is assumed. Assuming the tank valves are in use once every bunkering (one-week “test interval”), then the PFD_{avg} for the tank valve (EV8) has been calculated using equation 1 with the proof test interval τ = 1 week (168 hours), to be 1.09E-04:

$$PFD_{avg}^{(1001)} tank\ valve = \frac{\lambda_{DU}\ \tau}{2} = \frac{1.3E^{-06}\ x\ 168}{2} = 1.09\ x\ 10^{-04}$$

[5] Note: Equipment and components are suitable for use within a given SIL environment but are not individually SIL rated.

For the solenoid valve (EV7), which controls the instrument air flow, a failure-to-function-on-demand rate of 0.3E-06 per hour is applied based on the PDS data handbook. Furthermore, assuming proof test interval τ = 1 week (168 hours, this gives a PFDavg of 2.52E-05:

$$PFD_{avg}^{(1001)} solenoid\ valve = \frac{\lambda_{DU}\ \ \tau}{2} = \frac{0.3E^{-06}\ x\ 168}{2} = 2.52\ x\ 10^{-05}$$

From Figure 4-3, it can be seen that the gas detector subsystem has the highest failure probability compared to the logic unit and shutdown valve subsystems. This is mainly due to:

- Lack of redundancy, with assumed 2oo2 of sensor configuration according to the current industry practice for gas fuelled ships. If we assume 2oo3 voting for the sensors, the relibility and availability will be improved.
- Only automatically actuated system shutdowns are considered, e.g. an alarm being triggered due to gas detection at one sensor is excluded from the fault tree analysis since human actions are then required to initiate shutdown.

4.2.4 Conclusion and recommendations

The results indicate that an enhanced safety function or other independent prevention and/or mitigation protection layers are necessary to avoid explosions in the event of leakage from the single-walled piping downstream of the tank valve for a compressed hydrogen storage tank on open deck. For prevention measures, it is advisable to eliminate all potential leak sources by using welded connections and to avoid storage in congested and semi-enclosed areas as far as possible. The critical challenge in reducing leak sources lies in the weldability of small gas pipes, which requires further assessment. Prevention layers are always preferable to mitigation layers. Therefore, if increasing the piping size makes it more robust and weldable, this may outweigh the risks and consequences of having more inventory in the pipes.

The mitigation protection layers need to consider that the cloud build-up time for hydrogen leaks is extremely short compared to other gases. A ‘critical cloud’ that can cause significant damage and harm to the ship and its systems if ignited, can form within seconds. Recent studies by DNV indicate that this can occur in just 5 seconds with leaks in the range of 0.1 kg/s (DNV, 2019) (DNV, 2023). Acoustic detectors are often proposed for compressed hydrogen storage configurations on open and semi-enclosed decks. However, there are several factors that can hinder an effective response time, such as intermittent ultrasonic noise and noise interference.

A more in-depth analysis of acoustic detectors for use in compressed hydrogen storage configurations on both open and semi-enclosed decks should be considered. Additionally, other protection layers should be evaluated to prevent the build-up of a critical gas cloud. Restrictive flow orifice (hereafter referred to as orifice) and excess flow valves are two safety devices that could add an additional protection layer.

Orifices are primarily used for measuring and controlling the flow rate of fluids (both liquids and gases) in pipes. In the context of preventing a critical gas cloud, they can also be employed to limit flow rates to a specified maximum based on the potential pressure drop across the orifice. Orifices come in various designs, each offering specific advantages for different applications and flow characteristics. With no moving parts, orifices are considered reliable. This design ensures that the leak rate is limited to a certain rate upon loss of containment. The critical challenge is to determine this limiting leak rate. Additionally, the feasibility of such devices should be evaluated, as they may impact the efficiency of tank filling operations. The generic PFD_{avg} of orifices suggested for use in Layer of Protection Analysis (LOPA) is 0.01 (CCPS, 2015).

Excess flow valves are an alternative to orifice flow restriction; these are mechanical devices designed to stop the flow of a fluid when a predetermined flow rate is reached. They are mitigative protection layers often installed in a storage tank outlet or pipe to ensure that the flow from an accidental pipe failure downstream of the valve will be stopped, thereby reducing the probability of a catastrophic loss of tank contents. However, their limitation is that they are primarily intended to prevent loss of containment in the event of a full pipe rupture. Excess flow valves are not effective in cases where the flow rate is not high enough to close the excess flow valve (CCPS, 2015). It was also the consensus of the CCPS guidelines on "Initiating events and independent protection layers in layer of protection analysis" from 2015 that the principle of operation and design of an excess flow valve is similar to that of a check valve. The generic PFD of excess flow valves suggested for use in LOPA was 0.1, indicating a low reliability. However, it was noted that a thorough analysis may justify a PFD of 0.01 for some systems (CCPS, 2015).

To summarise, we conclude that hydrogen installations on open decks have a challenge with managing leakages within a timeframe sufficient to prevent a critical cloud build-up. Consequently, hydrogen regulations should account for this by requiring additional safety features. Issues to consider include:

1. Potential leak sources should be minimised as far as possible by avoiding detachable connections and leak-prone piping components. One challenge is that pipe dimensions used in smaller compressed hydrogen installations can be difficult to weld.

2. The fuel containment system, pressure relief system, and deck layout should be arranged to prevent discharged hydrogen from accumulating in confined and congested areas.

3. Traditional gas detectors which rely on contact with leaked hydrogen to detect leakages will likely have too long response time to prevent critical cloud build-up. Acoustic gas detectors are untried in ship applications, and testing and trials must be carried out to gain confidence in their reliability.

4. The use of strategically mounted excess flow valves and restrictive orifices can be used to limit leakages. Orifices will not stop a leak, and excess flow valves require a significant increase in flow rate to close. Additionally, the current default PDF value indicates low reliability of excess flow valves.

5. Applying double barriers for compressed hydrogen piping systems would ease detection, ease prevention of ignition and ease prevention of ignitable hydrogen concentration in confined/semi-enclosed spaces as hydrogen released within the double barrier can be vented to a safe location.

4.3 Case 2: Liquefied hydrogen storage below deck – Inert atmosphere function

The below-deck configuration for storing liquefied hydrogen is based on various concepts, featuring an IMO Type C fuel tank with a Tank Connection Space (TCS) located within a Fuel Storage Hold Space (FSHS). The configuration is based on the requirements in the IGF Code for LNG-fuelled ships with the addition of an inerted atmosphere in the TCS to account for the higher ignition risk of hydrogen. The overall safety integrity of the TCS has been addressed, including a reliability analysis of the inert gas system.

4.3.1 Fuel system description

A concept illustration of the hydrogen fuel system is provided in Figure 4-4. The liquefied hydrogen storage below deck is based on a concept with a TCS enclosing all tank connections, which is gas-tight and fully welded to the tank.

The previous EMSA report (EMSA, 2024) concluded that dilution ventilation is unsuitable as a mitigation strategy for more significant hydrogen releases in enclosed spaces. This conclusion is based on (MarHySafe, 2021) where ventilation as a possible risk mitigation measure for hydrogen installations has been discussed and analysed. CFD analyses of hydrogen releases in enclosed spaces indicate that a typical maritime room (80 m^3) can only withstand a leak of up to 220 g of hydrogen for a short-duration gas leak, assuming ignition occurs. While ventilation can serve as a safety barrier to prevent small leakages from creating an ignitable hydrogen atmosphere, it cannot prevent potential ignition and jet fire. Therefore, for significant hydrogen releases in enclosed spaces, forced ventilation should not be considered a reliable safety barrier. This case analyses one alternative to a ventilated TCS, which could be to operate with a constantly inerted atmosphere inside the TCS to eliminate the possibility of ignition and consequently fire and explosion. Single-walled piping inside the TCS is assumed apart from the LH2 piping, where vacuum insulation will be a prerequisite. A minimum of flanged connections with subsequent liquid leak potential into TCS is assumed, typically at the vaporizer. The TCS is assumed to be accessed through an airlock arrangement.

The fuel tank is filled through the bunkering system with a top spray line and a bottom filling line. The fuel is supplied via the bottom connection in the tank to a vaporiser towards consumers. Supply pressure is managed through a pressure build-up vaporizer supplying warm hydrogen gas to the ullage space of the tank. There will be a heating medium for the closed-loop heat exchanger systems in the TCS.

Additional assumptions for this case are:

- A mechanical ventilation system to enable safe entry into the TCS is provided.
- A pressure relief system with sufficient capacity is arranged to prevent damage due to pressure rise from rapidly evaporating liquid hydrogen.

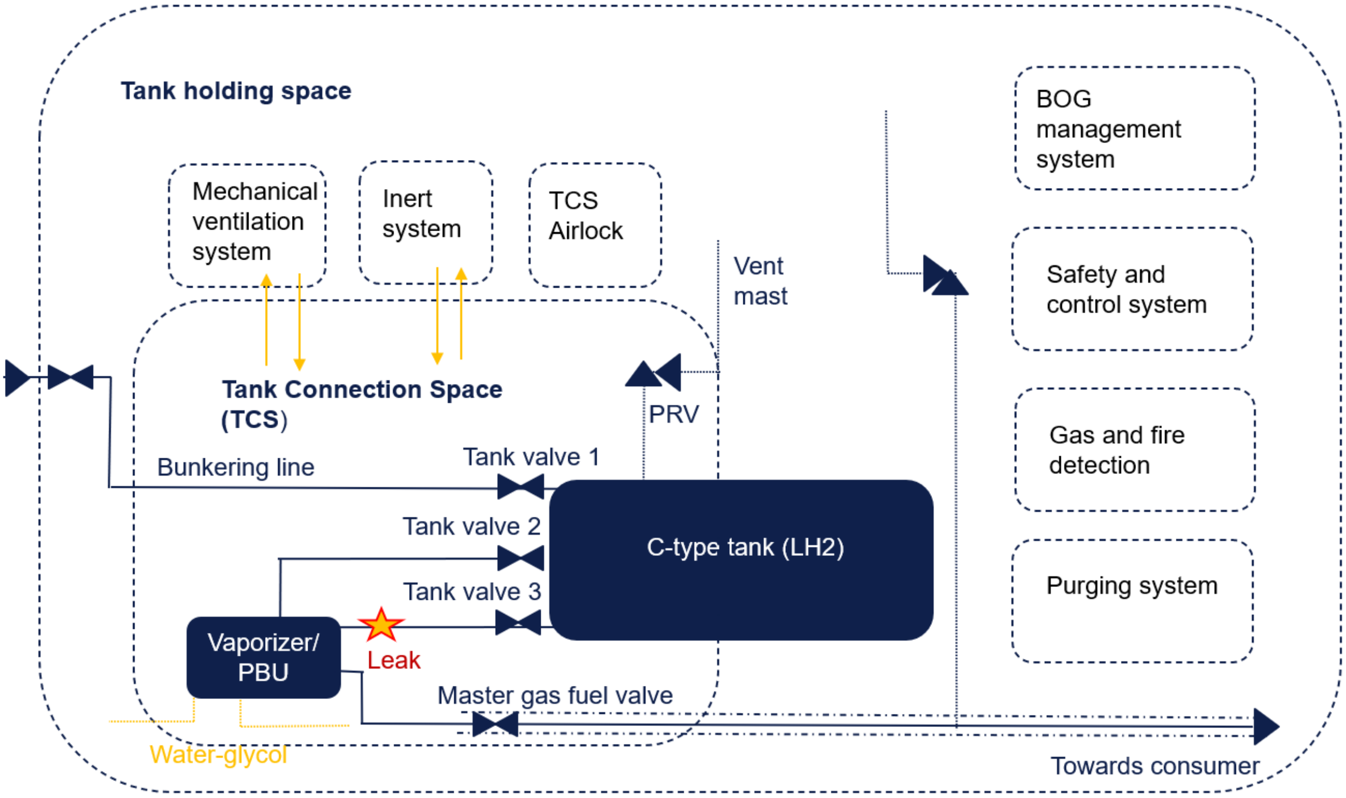


Figure 4-4 Illustration of the concept for liquefied hydrogen stored below deck (Source: DNV).

4.3.2 Safety system description

The function of the TCS is to safely contain any system leaks within a limited space and thereby ensure that the rest of the ship, persons on board, and the environment are not endangered. The potential dangers that could compromise the TCS function in a liquid leakage scenario are:

- **Flammable effects:** When released into an environment with ambient temperature and pressure, liquefied hydrogen will rapidly vaporize, creating a flammable atmosphere. This can lead to potential hazards such as jet fires, explosions (deflagrations), and/or detonations. In the context of inerted TCS concepts, a flammable atmosphere can only form if the hydrogen-air-inert mixture exceeds the Limiting Oxygen Concentration (LOC). The LOC is the minimum oxygen concentration in a hydrogen-air-inert mixture below which ignition cannot occur. It can be calculated from the oxygen concentration in air using the formula LOC = 0,209 of Limiting Air Concentration (LAC) (HySafe, 2006).

- **Overpressure effects:** The pressure inside the space will increase if liquefied hydrogen is spilt and vaporised within the TCS. Depending on the dimensioning of the pressure relief and the vaporisation rate, the pressure increase may be sufficient to damage the structure.

- **Cryogenic effects:** LH2 is stored at temperatures that will cause embrittlement if normal ship steel is exposed to leakage and temperatures below acceptable limits. Embrittlement is a phenomenon that results in a significant reduction in material tensile strength, ductility and fracture toughness. However, there are also other potential dangers that follow liquefied hydrogen spills:

    - **Loss of safety functions:** The TCS contain equipment and systems that are required for the safety of the ship. It is important to ensure that they remain operational after the event.

    - **Condensing and solidifying:** All gases (except for helium) will be condensed and solidified in contact with cryogenically stored hydrogen. If air or other gases enter an LH2 system, the solidified gases can create restrictions in the piping system, interfere with the normal operation of valves and damage valve seats (EMSA, 2024). A leakage of LH2 can cool down the space below the condensation temperature of nitrogen in seconds, as demonstrated at DNV’s Spadeadam facility in the UK (FFI, 2021).

    - **Cryo-pumping:** In a process known as cryo-pumping the reduction in volume of condensing gases may create a vacuum that can draw in yet even more gas. Large quantities of condensed or solidified materials can accumulate if the leak persists for long periods of time. At some point, should the system be warmed for maintenance, these solidified materials will vaporise, possibly resulting in high pressures or forming explosive mixtures. These other gases might also carry heat into the liquid hydrogen and cause enhanced evaporation losses or “unexpected” pressure rises (EMSA, 2024).

This case covers the prevention of flammable effects. Prior to allowing hydrogen to be supplied towards the consumers, the TCS must be ready for operation. This implies that the space must be purged with inert gas to an oxygen level where ignition of hydrogen is not possible. The TCS in this case is assumed to be a closed system with a constant slight overpressure of inert gas to prevent air ingress into the TCS. As shown in Figure 4-5, we are then in the lower left corner of the diagram (green point in the figure), for instance, a point defined by 1 % oxygen and 99 % inert gas (e.g., nitrogen). In case of air intrusion into the TCS and a hydrogen leak should occur, we would be in the flammable region, e.g. 10 % hydrogen, 10 % oxygen and 80 % inert gas (blue point in the figure).

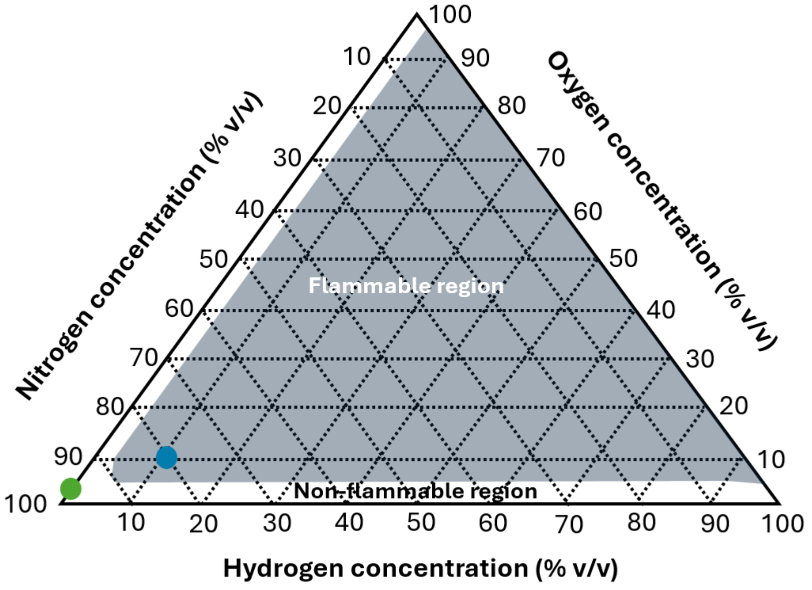


Figure 4-5 Flammability limits at a pressure of 101.3 kPa and a temperature of 25ºC (Source: DNV).

4.3.3 Reliability analysis

The inert gas system is a safety-critical system. If there is an oxygen concentration level above the LOC in the TCS, which is undetected (dangerous undetected failure), and a leak occurs, the consequences can be severe due to high ignition probability and subsequent fire and explosion effects. The safety system should ensure that there is always an inert atmosphere in the space during operations. The reliability analysis considers the top event of *Undetected oxygen concentration > LOC.* The logic and data of the fault tree are shown in Figure 4-6 and described below. The top event occurs only if both gates *O2 introduced into TCS (GT1)* and the *O2 sensor system (EV1)* fails. Both these two events are considered to be dangerous undetected events. If there is an undetected oxygen concentration higher than LOC, then the inert safety function is unavailable and cannot prevent an ignition in case of a leak, resulting in fire/explosion in TCS.

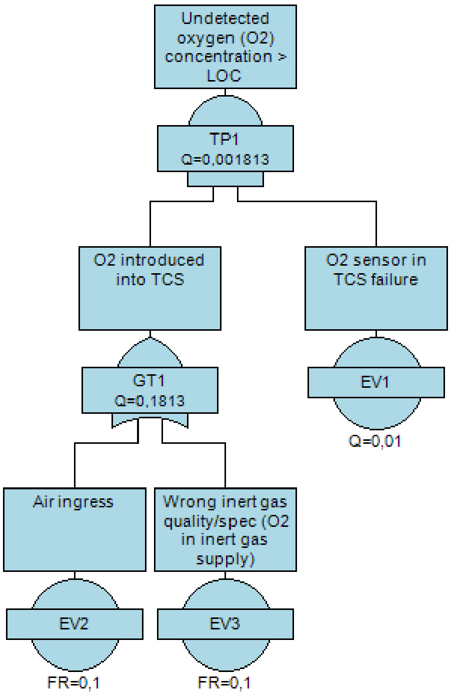


Figure 4-6 Fault tree for Oxygen concentration > LOC (Source: DNV).

O2 introduced into TCS (GT1) can occur if either *Air ingress (EV1)* or *Wrong inert gas quality/spec (O2 in inert gas supply) (EV2* occurs.

Air ingress (EV2) can occur if there are leak paths and there is a loss of overpressure. These two are not independent events because when there is a leak, a subsequent reduction in pressure inside TCS will occur. If there is no pressure monitoring system, the final event will be oxygen ingress into TCS. Positive pressure inside the TCS is preventing air from entering. Air leaks could result from openings such as the inert gas inlet, ventilation ducts, cable penetrations, cracks, and pressure relief outlets. Additionally, defective hatch gaskets or doors in the airlock access arrangement could also cause air leaks. There are no known specific failure rates for such leaks. It is conservatively applied a failure rate of 0.1 per year in lack of specific data.

The wrong inert gas quality/spec (O2 in inert gas supply) (EV3) could occur if the oxygen content in the produced inert gas is too high. Similar to EV2, it is conservatively applied a failure rate of 0.1 per year in lack of specific data.

For O2 sensor in TCS failure (EV1) it is assumed a PFDavg of 1.0E-2, in line with a SIL-2 capable sensor.

The failure-on-demand probability of the top event then becomes 1.81E-03, i.e. fail in every 552 demands. The reliability can be improved by redundancy in O2 gas detection, redundant inert gas supply, pressure monitoring of TCS, and enhanced integrity of structure and equipment to avoid leak paths for air.

4.3.4 Conclusion and recommendations

This quantitative exercise has only considered the likelihood of having a sufficiently inert atmosphere in a TCS when leakage occurs. Other complications with using inerted spaces as a means to prevent ignition are discussed in the following.

The limiting oxygen concentration (LOC) is defined as the limiting concentration of oxygen below which combustion is not possible, independent of the fuel concentration. When purging procedures are developed and used, it is important to be aware that hydrogen systems (LOC 5%) require more thorough purging than hydrocarbons, which have LOCs in the 11-15% range. The same issue applies if an inert gas is used as a safety barrier to prevent ignition in secondary enclosures or spaces. A hydrogen atmosphere is also more sensitive to air entering than methane due to a high upper flammable limit (UFL). Having hydrogen concentrations above the UFL in an inerted space is still very dangerous. If the concentrations are lowered by introducing fresh air, the atmosphere in the space will enter the flammable/explosive range.

An inert atmosphere will prevent access for inspection and maintenance. If the TCS is gas-freed for entrance, the primary safeguard that prevents an explosion would be removed without the possibility to gas-free the hydrogen system. Also, removing the possibility of close-up inspection and maintenance could have an unfavourable effect on the reliability of essential safety functions.

To maintain an inert atmosphere in the TCS, ventilation arrangements must be closed off to prevent the inert gas from escaping. This implies that the protected space is vulnerable to pressure increases due to leaks. A pressure relief system with sufficient capacity would have to be arranged to prevent damage due to pressure rise from rapidly evaporating LH2 or expanding CH2. The isolated ventilation system would pose a risk to the inerted atmosphere as a potential air supply source.

Since hydrogen can ignite with less oxygen than natural gas (5% vs 12%), a hydrogen installation would have stricter requirements for inert gas quality than what is commonly provided for hydrocarbons.

A leakage of LH2 can rapidly cool down the atmosphere in a tank connection space below the condensation temperature of nitrogen, as demonstrated at DNV's Spadeadam facility in the UK (FFI, 2021). It is not clear how this will affect the flammability of the TCS atmosphere.

After a leak event where the safety barriers have functioned as intended, the tank connection space will contain hydrogen and inert gas, which need to be vented safely to open air. This process will also have a risk of unintentionally introducing oxygen to the TCS with a corresponding risk of explosion.

4.4 Case 3: Bunkering of liquefied hydrogen

This case analyses the bunkering of liquefied hydrogen. The proposed preventive and mitigation measures for hydrogen bunkering were introduced in the EMSA report “Mapping safety risks for hydrogen-fuelled ships” (EMSA, 2024). We found that a ship bunkering station should be arranged to reduce the consequences of an ignition event as far as possible. This implies preferably locating the bunkering station on the open deck. In case it is not possible to have the bunkering station on the open deck, it would need to be located in an enclosed or semi-enclosed space.

In this case, we examine a potential leak in a semi-enclosed bunkering station, similar to those used for LNG applications. These bunkering stations typically have hatches on the ship's side open during bunkering to allow for the connection of the bunkering hose or Marine Loading Arm (MLA) to the connection point onboard. The risks considered in this case may also apply to open bunkering stations.

Case 3 is assessed qualitatively, addressing important challenges and lessons learned from recent studies. The Maritime Technologies Forum (MTF) conducted a DNV-led study on "Guidelines for the development of liquefied hydrogen bunkering systems and procedures" (MTF, 2024). The report, submitted to the IMO by Japan, Norway, Singapore, and the United Kingdom, addresses technological progress, regulatory gaps, risks, and technical solutions related to liquefied hydrogen bunkering. The study gathered information from ongoing developments in ISO and the experiences of vessels like the Norwegian liquefied hydrogen-fuelled ferry Hydra and the liquid hydrogen carrier Suiso Frontier operating between Japan and Australia.

The key observations from this study, which will be further elaborated in this analysis, are:

- Experience gained from bunkering arrangements for LNG cannot be re-used directly
- The bunkering process will be more complex
- Need for more insulated components
- Need for vessel-specific procedures for bunkering and maybe more automated operations
- Enhanced crew training and certification
- Updated Safety Management Systems to include additional safety aspects of hydrogen

4.4.1 Bunkering arrangement description

A concept illustration of the liquefied hydrogen bunkering arrangement is provided in Figure 4-7. The bunkering system for the receiving ship is assumed to be similar to the liquefied hydrogen system described in Case 2, except for the bunkering connection point. In addition, the following assumptions for arrangement, incl. control and safety functions, are made for the bunkering station and interface with the bunkering supplier:

- Semi-enclosed bunkering station located on the side of the ship
- The LH2 is led from the bunkering station to the IMO type C tank(s) via a vacuum-insulated double-walled piping system to prevent air condensation.
- Dry Quick Connect/Disconnect Couplings (Dry QCDC), allowing easy connection/disconnection without the use of manual intensive operation (such as tightening bolts), whilst including self-containing stop valves at the female and male ends to avoid spillage of hose and receiving line content that may possibly be contained in the lines
- One bunkering line and one vapour return line (if used)
- Interface with inert gas supply system
- Leak (low temperature), gas and flame detection system, incl. alarms and automatically operated isolation valves.
- Control and monitoring system, incl. tank level alarm and monitoring systems
- A ship-shore-link (SSL) or equivalent means for ESD communication between the receiving ship and supplier
- Pressure relief lines (routed to vent mast)
- Drip tray
- Communication system

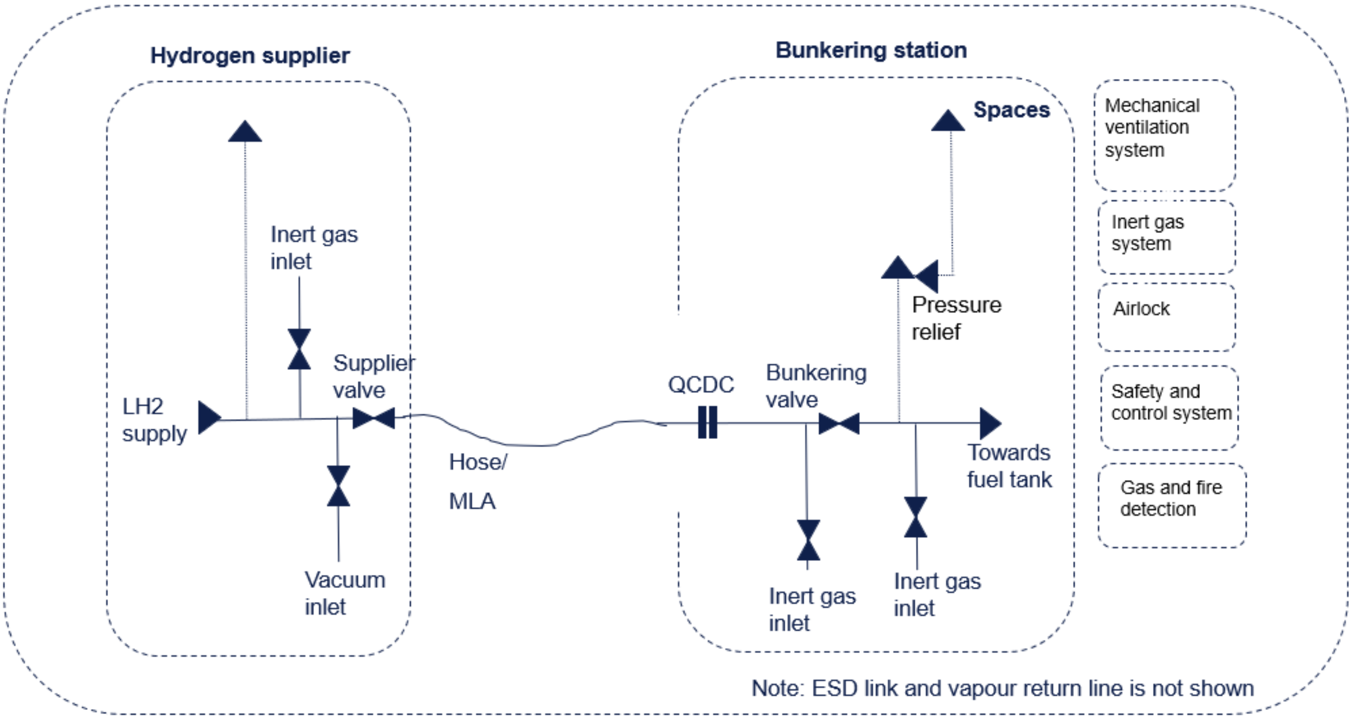


Figure 4-7 Illustration of the concept for liquefied hydrogen bunkering (Source: DNV).

Other essential non-ship systems, equipment and arrangements that influence the risk picture, but are typically not covered by regulations or rules applicable to hydrogen-fuelled ships are:

- Bunkering hose (cryogenic, vacuum insulated flexible) or use of Marine Loading Arm (MLA). Flexible hoses may also be supported by an MLA.
- Emergency Release System (ERS), in case of ship drift-away incidents. The general functionality of ERS includes a break-away coupling or Emergency Release Coupling (ERC) and emergency shutdown function. If powered (remote actuated), this system is referred to as Powered Emergency Release Coupling (PERC). This is located at one end of the transfer system, either the receiving ship end or the bunker supplier end, The coupling gives way before excessive pull causes the hose to break or other damage.
- Safety zones

Depending on the depressurizing, gas freeing and purging concept, the following systems may be implemented, either by bunkering supplier or receiving ship:

- Vacuum interface (if used, vacuum followed by inert gas injection)
- Expansion tank (for collecting liquid after depressurizing the process line after bunkering)

4.4.2 Reliability analysis

This case will explore the potential flammable effects, including fire and explosion. The release of liquid hydrogen in the bunkering station can occur due to leakages in pipes, pipe connections, valves, instruments, and the QCDC coupling and bunkering hose. Leaks in pipes can be managed by using double-walled vacuum-insulated piping systems, and connections can be welded to minimize the potential for leaks. However, for the coupling, there is no secondary barrier. There have been incidents of leakage from QCDCs during LNG bunkering operations for 6” and 8” nominal diameter bunkering hoses. The root cause of the failures is not fully clear but can be due to excessive hose movement and lack of hose support ((SGMF, 2019). Other generic causes may be improper connections, damaged gaskets, or general hardware failure. A failing QCDC can lead to the release of liquid hydrogen into the bunkering station, and ship designers need to consider how to manage such a spill scenario.

In LNG applications, mechanical ventilation is a well-established safety barrier for semi-enclosed bunkering stations. However, due to the rapid cloud build-up after both gaseous and liquefied spills, normal ventilation rates as used for LNG are not sufficient to dilute hydrogen gas:

- In the MarHySafe project, a scenario calculation by DNV demonstrated that in the event of a continuous gaseous leak at a rate of 10 g/s in an enclosed room with an air exchange rate of once every 36 seconds (100 air changes/hr), it could be conservatively assumed that the majority of the hydrogen will contribute to the formation of an explosive cloud. Over time, a steady-state cloud size will be established, typically within 1 to 3 minutes, depending on the ventilation and leak rates (MarHySafe, 2021).

- Gexcon conducted a study analysing various leak scenarios, including one involving a downward-directed gaseous hydrogen leak with a hole size of 0.5mm^2 for 30 seconds in a ventilated compressor room, which is equivalent in size to a 20-foot container. The study assumed there were five air intakes on the side and extract ventilation on the roof with a flow rate of 1,000 m^3/h and a vent area of 0.09 m^2. The results showed that, even with 10x the original ventilation rate (10,000m^3/h), the gas will fill the entire enclosure within seconds, and a maximum cloud size is developed after only 10 seconds. Increasing the ventilation from 5x to 10x the original ventilation rate would only reduce the flammable volume from around 15 m^3 to 13 m^3. While the 10x ventilation rate would use approx. 40 s to reduce the flammable volume (m^3) to zero, the original rate would use more than 80 s (Gexcon, 2022).

The main parameters that govern the explosion risk in an enclosure are the mass of hydrogen that can leak (kg), the ventilation rate (ACH, 1/h), and the enclosure volume (m3). The use of a risk-based approach should consider all scenarios with increasing hole sizes up to full-bore rupture. Based on this, the bunkering station layout, size and ventilation rate could be optimized. However, as demonstrated in the above studies, there is a significant challenge in diluting the hydrogen cloud to concentrations below which no damaging overpressures from the explosion are expected.

Since there is an opening for the bunkering hose or the MLA, inerted bunkering station is not an option. The bunkering station size and geometry is also something that should be considered. A small room can be beneficial with respect to explosion overpressure potential. However, a small room can also develop a critical cloud with less gas than a large room, meaning that small rooms may need to change air at a greater rate than a large room (provided the same mass of gas is leaked) (MarHySafe, 2021).

4.4.3 Conclusion and recommendations

To summarise, the process of transferring fuel introduces additional leakage hazards and system threats, which must be carefully managed to ensure safe bunkering. If the bunkering station is situated on an open deck without significant congestion or any semi-enclosed spaces nearby, natural dilution can help disperse any leakages. An open environment will also reduce the impact of an ignited gas cloud.

In cases where vessel geometries do not allow for an open bunkering station, it becomes more challenging to manage the risks associated with fuel transfer. It is reasonable to assume that a hydrogen leak can quickly create an explosive atmosphere in the bunkering station, and the possibility of ignition cannot be ruled out.

Consequently, hydrogen regulations should account for this by requiring additional safety features. Issues to consider include:

- Bunkering stations should be located on the unobstructed open deck, if feasible, based on the ship's design.

- All leak sources related to the bunkering system onboard must be safeguarded by secondary enclosures designed to contain leaks and direct them to a secure location. This would leave the bunkering connection as the high-risk leakage point.

- In cases where semi-enclosed bunkering station arrangements are required due to the ship's design, it is important to minimize the volume of the bunkering station that could potentially experience large leaks. One way to do this is by separating the area of the bunker manifold connection point from the rest of the bunkering station. The separation should aim to ensure that this part of the bunkering station can withstand the effects of an ignited leak.

5. Safety analysis of hydrogen-fuelled ships

The goal of the safety analysis has been to develop a *framework* for a *generic risk model* (the model) for hydrogen-fuelled ships. The basis for the model is the descriptions of generic hydrogen safety hazards, threats, and risks outlined in EMSA's 2024 report, "Mapping Safety Risks for Hydrogen-Fuelled Ships". Findings from the reliability analysis of hydrogen equipment (Chapter 3) and safety-critical systems (Chapter 4) are also crucial inputs to the model.

The model not only contributes to risk quantification but also visualizes potential consequence outcomes following an initiating event, thereby enhancing our understanding of major accident risks in complex scenarios. Highlighting the potential consequences of hydrogen releases underscores the importance of stopping the event as early as possible in the chain of events, ideally by preventing any release in the first place.

As with any quantitative risk model, it is important to note that the framework developed in this study is a model representation and not a 100% accurate depiction of real-world scenarios. While it provides valuable insights and helps understand potential risks, it cannot capture every variable and nuance of actual events. It is a useful tool for risk assessment and decision-making, acknowledging the inherent uncertainties and limitations.

5.1 Establishing context

The aim of the model is to create a generic event tree for consequence- and risk analysis that can be applied to all hydrogen loss of containment events, as outlined in chapter 5.3. The model is generic and valid for both liquid, gaseous and two-phase hydrogen releases, whether they occur in enclosed spaces or on open deck.

The model is based on event tree methodology, which follows the logical sequence of potential outcomes as a result of an initiating event. This method explicitly looks at all outcomes that can occur due to the actions of preventive and mitigative safety barriers. The methodology was generally explained in Chapter 2.2.2. This approach is particularly valuable in assessing safety and reliability in complex systems, such as those involving hydrogen-related processes.

While there exist numerous event trees for loss of containment from the oil and gas industry considering hydrocarbon release, hydrogen maritime applications are new. The QRA therefore needs to be developed from scratch and capture new hazards and effects that are not always modelled in traditional QRAs.

5.2 Event tree structure

In Figure 5-1, the event tree illustrates how different branches represent the progression of events following an initial event. Each branch’s probability and the frequency of the initiating event are crucial in determining the overall risk and impact of potential scenarios. The gates that constitute the event tree, listed below, are described in the subsequent chapters:

- Initiating event frequency
- Immediate ignition probability
- Detection and shutdown probabilities
- Delayed ignition probability
- Flame front acceleration (flash fire, deflagration and/or detonation)
- Escalation probability

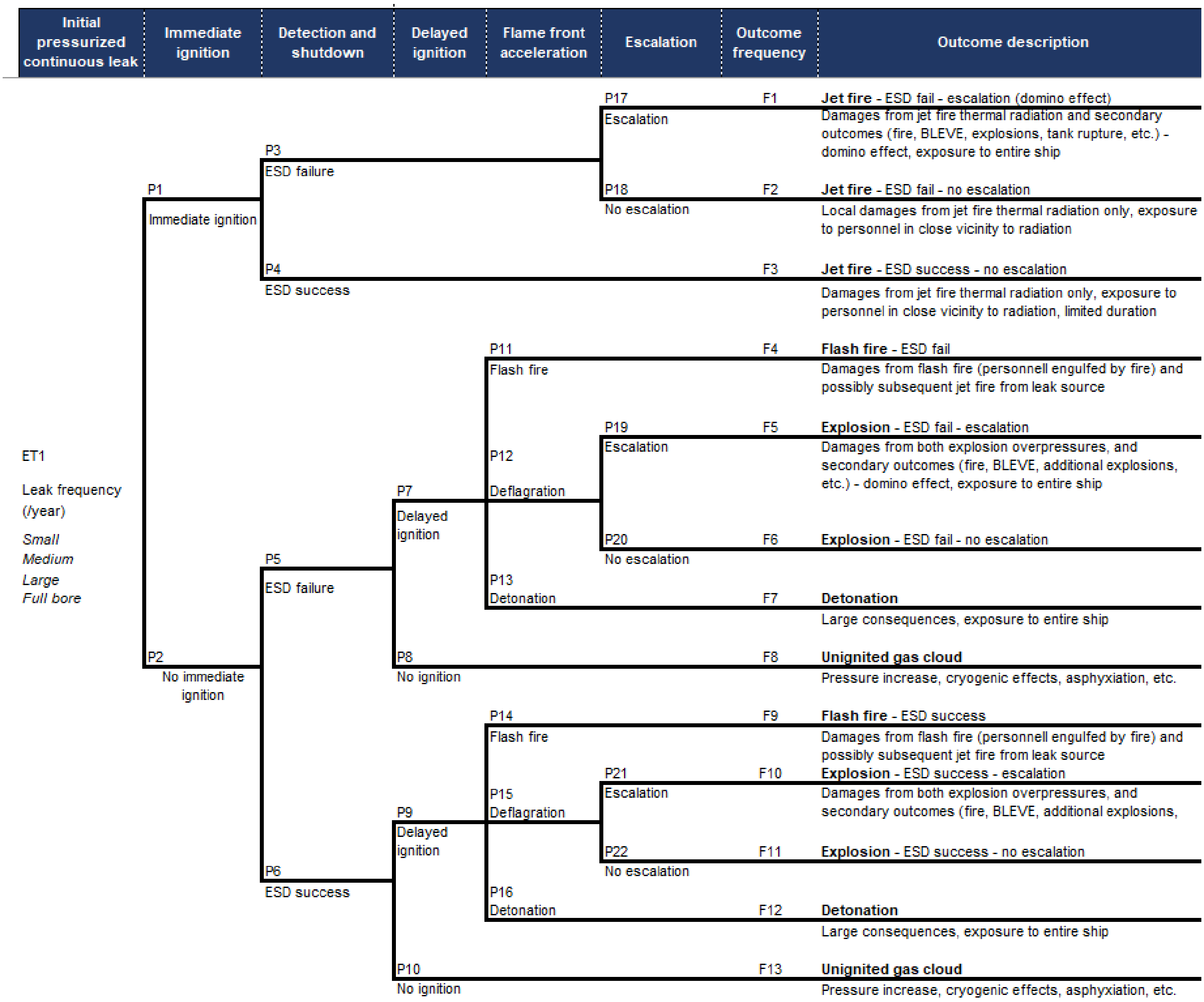

Initial pressurized continuous leak
Immediate ignition
Detection and shutdown
Delayed ignition
Flame front acceleration
Escalation
Outcome frequency
Outcome description
ET1
Leak frequency (/year)
Small
Medium
Large
Full bore
P1 Immediate ignition
P2 No immediate ignition
P3 ESD failure
P4 ESD success
P5 ESD failure
P6 ESD success
P7 Delayed ignition
P8 No ignition
P9 Delayed ignition
P10 No ignition
P11 Flash fire
P12 Deflagration
P13 Detonation
P14 Flash fire
P15 Deflagration
P16 Detonation
P17 Escalation
P18 No escalation
P19 Escalation
P20 No escalation
P21 Escalation
P22 No escalation
F1 Jet fire - ESD fail - escalation (domino effect)
Damages from jet fire thermal radiation and secondary outcomes (fire, BLEVE, explosions, tank rupture, etc.) - domino effect, exposure to entire ship
F2 Jet fire - ESD fail - no escalation
Local damages from jet fire thermal radiation only, exposure to personnel in close vicinity to radiation
F3 Jet fire - ESD success - no escalation
Damages from jet fire thermal radiation only, exposure to personnel in close vicinity to radiation, limited duration
F4 Flash fire - ESD fail
Damages from flash fire (personnell engulfed by fire) and possibly subsequent jet fire from leak source
F5 Explosion - ESD fail - escalation
Damages from both explosion overpressures, and secondary outcomes (fire, BLEVE, additional explosions, etc.) - domino effect, exposure to entire ship
F6 Explosion - ESD fail - no escalation
F7 Detonation
Large consequences, exposure to entire ship
F8 Unignited gas cloud
Pressure increase, cryogenic effects, asphyxiation, etc.
F9 Flash fire - ESD success
Damages from flash fire (personnell engulfed by fire) and possibly subsequent jet fire from leak source
F10 Explosion - ESD success - escalation
Damages from both explosion overpressures, and secondary outcomes (fire, BLEVE, additional explosions,
F11 Explosion - ESD success - no escalation
F12 Detonation
Large consequences, exposure to entire ship
F13 Unignited gas cloud
Pressure increase, cryogenic effects, asphyxiation, etc.

Figure 5-1 The generic event tree analysis model (Source: DNV).

Specific quantitative analyses and failure data are required to quantify the values in the event tree. This includes failure data required to quantify the leak frequencies (ET1), as well as the failure-on-demand probabilities of gas detection and shutdown (P3-P6). Ignition probabilities (P1, P7 and P9) must be established based on historical data, ignition models and/or expert judgement. Additional quantitative analysis, such as CFD and explosion risk analysis, are required to quantify the likelihood and extent of flammable effects (P11-P16), including possible secondary effects considering escalation (P19-P22).

5.3 Initiating event frequency

QRAs often define Loss of Containment events (LOCs) as the initiating events that may lead to an outflow of hydrogen. Note that several other names may be used in the industry for these initiating events, among which are undesired events, accidental events, process upsets or deviations. The events are expressed as frequencies, i.e. as the expected number of occurrences per unit of time, such as events per year.

5.3.1 Loss of containment categories

The initiating events can broadly be grouped in the categories listed below. The categories are based on the standard categorization of the Dutch Guideline for quantitative risk assessment (‘the Purple Book’).

- **Leakage LOCs** encompass all failures related to process leakages, typically caused by welding failures, brittle fractures, stress and vibrations, improper installation or maintenance, material defects, and similar factors. These events do not require other circumstances (such as overpressure) to result in a release. It is important to note that this category includes all types of leakages, ranging from minor leaks to full-bore ruptures of pipes and pressure vessels. In some standards, these events are also referred to as generic LOCs.

- **External-impact LOCs** are typically caused by mechanical impacts, such as collision, allision, grounding, dropped objects, swinging loads, etc. An important consideration is the placement of the hydrogen fuel system, including the storage tank(s) and associated equipment.

- **Specific LOCs** can be part of the LOCs mentioned above or be modelled separately, but often, they can be based on the same methodology as the leak and external impact LOCs. This could include loading and unloading loss of containment, external or internal fire from non-hydrogen events, etc.

This model focuses on failures categorized as Leakage LOCs, which have been identified as a primary risk contributor in previous quantitative risk assessments for hydrogen-fuelled ships (DNV, 2023). While the focus is on leakage LOCs, it is important to mention that the risk of external-impact LOCs and other specific incidents such as damage from external fire should also be assessed using relevant statistics for the specific ship type. Depending on the ship design and placement of fuel tanks, external-impact LOCs and specific LOCs can also be major risk drivers. The IMO document SLF 55/INF.7 (Revision of the damage stability regulations for ro-ro passenger ships) provides valuable background for assessing collision and grounding damage for ships, which can be applied for estimating the probability of fuel tank damage in the event of a collision causing water ingress to the ship.

5.3.2 Leak characteristics

Leaks can occur as either continuous leaks or instantaneous releases. Instantaneous releases may result from rupture of the piping, e.g. due to fatigue cracks or thermal fatigue. Continuous leaks can be categorized as either full-pressure or zero-pressure leaks. The logic of the event tree can be applied on all these scenarios. However, this analysis focuses on continuous pressurized leaks, which have been identified as the primary risk contributors in previous quantitative risk assessments for hydrogen-fuelled ships. Pressurized leaks are also the most relevant for hydrogen fuel systems. Additionally, approximately 95% of all registered leaks in the HCRD database are pressurized leaks.

5.3.3 Leak frequency data

Leak frequency refers to the likelihood of a leak occurring in a specific piece of equipment over a given period. The frequency can be derived from failure data and/or detailed fault tree analysis. This study will apply the failure data for relevant hydrogen equipment found from the analysis in chapter 3. To calculate the total leak frequency, the parts count method can be applied by counting the number of specific equipment parts within a system. Each type of equipment (e.g., valves, pumps, flanges) has an associated leak frequency based on the failure data. The following steps should be applied to derive the overall leak frequency for a system or ship:

- Identify and count equipment types: This includes counting type, number and size of process equipment, operating pressure, and which phase of the inventory is being released.

- Apply leak frequencies: Multiply the number of each equipment type or category by its specific leak frequency from historical data.

- Sum the frequencies: Add up the leak frequencies for all equipment types to get the total leak frequency for the system or ship.

The assessment of equipment parts count is primarily derived from detailed P&IDs for each specific system on the ship. However, it can also be based on higher-level process flow diagrams, though this approach involves making assumptions and introduces greater uncertainty.

In a risk-based approach, all possible leak sizes should be considered and associated with a frequency. To reflect the various release events, a minimum of five process leak scenario categories are typically defined. Each release scenario category is represented by the size of the leak (percentage of the cross-sectional area). The relative area is then converted to hole size representative of the process segment. These hole size distributions per segment will be used to establish release rates categories.

The alternative is to use release rate ranges. A study by DNV concluded that use of release rate ranges as opposed to hole size ranges does not introduce additional inaccuracies into the calculation process (DNV, 2014). This is particularly relevant for CFD based studies, where it can be efficient to set up the model based on release rate categories, as CFD scenarios based in release rate can represent leaks from multiple segments in the same space/area.

The release rate of hydrogen can decay rapidly, with the initial release rate occurring only momentarily when the leak starts. Despite this, the initial release rate is often used in QRA to simplify modelling the hydrogen cloud build-up, ignoring transient effects. Properly accounting for rapid decay requires modelling leaks as transient. The 2014-study by DNV also concluded that there is no reason to assume that adopting an “initial release rate”-approach results in a decrease in accuracy of the analysis, and that using it can often reduce the amount of computational effort involved. This is especially true when the consequence analysis includes expensive techniques such as CFD where it is not cost effective to model numerous scenarios (DNV, 2014).

Note that for piping and valves with a secondary enclosure, a reduction factor of 10 may be applied to the leak frequency. While the simultaneous failure of both barriers is highly improbable, common cause failures related to manufacturing, assembly, or maintenance may still occur. Therefore, these potential failures should be considered until the failure modes associated with the loss of containment in hydrogen systems are thoroughly studied.

After the establishment of frequencies and the release hole sizes or rates, the immediate ignition probabilities per release category can be found (see chapter 5.4).

The uncertainties for leak frequency data were discussed in 3.3.

5.4 Immediate ignition probability

A distinction is made between two types of ignitions: Immediate and delayed. The first gate in the event tree “Immediate ignition probability – P1” determines whether the released hydrogen ignites immediately. This is chosen as the initial gate because it will most likely occur before the detection and shutdown safety system will be able to react, i.e.: detect, then send and process signal, and finally close valves to isolate and stop flow.

Immediate ignition is ignition resulting from a mechanism that is related to the cause of the loss of containment. Immediate ignition occurs before a combustible cloud has formed, and will therefore not generate an explosion, only a jet fire (F1-F3 in event tree).

The following sections discuss ignition mechanisms, data and ignition models.

5.4.1 Accident data and ignition mechanisms

There are data supporting that immediate ignition of hydrogen leaks is common. A review of postulated mechanisms in spontaneous ignition of hydrogen leaks, (Astbury and Hawksworth, 2007) refer to data from the Major Hazard Incident Database Service (MHIDAS) finding that for 81 incidents involving hydrogen a delay between release and ignition was reported in only 4 releases. It was assumed that the other 77 events ignited immediately. In another review of hydrogen ignition mechanisms, (Molkov, 2012) refers to the same study on hydrogen incidents and comes to the same conclusions as (Astbury and Hawksworth, 2007); there is a knowledge gap on the exact ignition mechanisms for release of hydrogen. Mechanisms that have been considered by Astbury and Hawksworth are: The reverse Joule-Thomson effect, electrostatic charge generation, diffusion ignition and sudden adiabatic compression, and hot surface ignition.

Although the data indicate a high portion of immediate ignition compared to delayed ignition, immediate ignition is not guaranteed. Experts suggest that immediate ignition is not as common as perceived. They point to accidents where hydrogen leaks did not ignite immediately, for instance; the hydrogen pipeline incident in Binnenmaas in 2007, the incident in Santa Clara, California in 2019, and the Kjørbo incident in Norway in 2019. DNV have carried out free jet H2 release experiments at over 1kg/s without any spontaneous ignition (MarHySafe, 2021). This supports the arguments that while hydrogen is highly flammable and have a high ignition likelihood, the conditions required for immediate ignition are not always met.

As claimed in the review by Astbury and Hawksworth, the postulated ignition mechanisms in the literature does not account for all the reported ignitions and non-ignitions of hydrogen releases, and the investigations, where no apparent ignition source was present, have often been too superficial. The review further conclude that further work is required to establish the conditions under which hydrogen release ignite, particularly with respect to electrostatic phenomena (Astbury and Hawksworth, 2007).

These findings emphasize the role of ignition mechanisms, environmental factors, and the presence of ignition sources. Another factor, often overlooked, is whether the release impacts other surfaces, known as impingement. Leaks that are likely to impinge on a surface may justify applying a relatively high ignition probability for instantaneous ignitions. This is because the impact on surfaces can create conditions that enhance the likelihood of ignition, such as increased turbulence, heat generation, etc.

5.4.2 Ignition models

There are available models and tabulated values to quantify the immediate ignition probability of hydrogen leaks. However, as highlighted in (EMSA, 2024), the greatest uncertainties in risk models often lie in the leak frequency and ignition probability estimations. This is primarily due to the limited research available on hydrogen releases compared to hydrocarbons. Consequently, there are divergences in expert opinions, which arise from varying interpretations of theoretical models, field and laboratory experiments, and real-world observations (accidents).

The previous EMSA report provided a brief background on the ignition probability models. The below sections provide some more details into these ignition models.

HyRAM+: The ignition model in the HyRAM+ toolkit is unique because it is specifically intended for hydrogen (SANDIA, 2021). The default HyRAM+ hydrogen ignition probabilities are a function of hydrogen release rate and are given in Table 5-1. The values are taken from (Tchouvelev, 2008), which were adapted for hydrogen from values suggested in the study by A.W. Cox, F.P. Lees, and M.L. Ang (A.W. Cox, 2003).

The immediate and delayed ignition probabilities are independent, and each is relative to a hydrogen release. The delayed ignition probability is not conditional upon the immediate ignition not occurring. Therefore, the total probability of hydrogen ignition is the sum of the immediate and delayed ignition probabilities (SANDIA, 2021). In this model, 2/3 of the total ignition probability is immediate ignition and 1/3 delayed ignition. A limitation with HyRAM+ is that the ignition probability is in step functions and has no refining of leaks above 6.25 kg/s, meaning that all leaks above this value have the same total ignition probability of 35 %. A review by the Norwegian Directorate for Civil Protection (DSB) acknowledge that the ignition probability for hydrogen can be significantly higher than what the HyRAM+ model states (DSB, 2021).

Table 5-1 HyRam+ ignition probabilities (Sandia, 2023).

H2 Release Rate (kg/s)	P(Immediate Ignition)	P(Delayed Ignition)
<0.125	0.008	0.004
0.125-6.25	0.053	0.027
>6.25	0.230	0.120

HYEX: The HYEX ignition model is based on the HyRAM+ model for small leak rates, while it is improved by being made continuous as a function of leak rate and takes into account that large leaks may have a significantly higher ignition probability than the HyRAM/"DNV model" suggests (DSB, 2021). This model is expressed as:

$$Ignition\ probability = Minimum(1.0; 0.55 \times Leak\ rate^{0.87}; 0.267 \times Leak\ rate^{0.52}),$$

The equation above represents the total ignition probability. The distribution between instantaneous ignition and delayed ignition is 2/3 instantaneous ignition and 1/3 delayed ignition. When using this model, all leaks over 12.5 kg/s will have a total ignition probability of 1.0 (DSB, 2021).

The HYEX model was originally set up for unobstructed jet leaks, but it is also recommended for use in the event of tank rupture and liquid hydrogen leakage. However, there are arguments both for and against adjusting this ratio, due to factors such as lower emission torque and lower temperature for liquid leaks, but also the slower dilution in air and heavy gas behaviour (DSB, 2021).

Considering that indoor leaks can cause accumulation of gas and thus increased (or reduced) gas cloud volume, it is proposed for leaks that can fill the entire room to concentrations above 8% to adjust delayed ignition probability in the following way (DSB, 2021):

$$Delayed\ enclosed\ ignition\ probability = Minimum(1.0 - P(early\ ignition); 0.018\ x\ Room\ volume^{0.35})$$

EIHP2: As Part of the EIHP2 project (European Integrated Hydrogen Project Phase 2) a set of ignition probabilities for use on hydrogen refuelling stations was developed. The probabilities were assessed based on several literature sources and experiments (EIHP2, 2003).

Dutch "Purple Book": Model described in Guidelines for Quantitative Risk Assessment "Purple Book" Part 1 Establishments. The Dutch "Purple Book" method separates between direct ignition and delayed ignition. For the direct ignition probability, the method separates between low reactive gases such as ethane and propane and "average to high" reactive gases such as acetylene and benzene. It is not stated which category hydrogen falls into, but it is likely that it falls in the "average to high" reactive gas category. Table 5-2 presents the values for immediate ignition from high reactive gases.

Table 5-2 Dutch "Purple Book" ignition probabilities (RIVM, 2005).

Continuous release Rate (kg/s)	Gas, average/high reactive, P immediate ignition
<10 kg/s	0.2
10-100 kg/s	0.5
>100kg/s	0.7

5.4.3 Immediate ignition summary

The ignition properties make hydrogen easier to ignite compared with natural gas. It can therefore be expected that more of the hydrogen leaks will ignite than the natural gas leaks. The hydrogen ignition models are under development, meaning that there is still a high uncertainty associated with using ignition probabilities for hydrogen. Therefore, conservative values should be applied in quantitative risk analysis (MarHySafe, 2021).

As seen from the brief presentation of the ignition models, none of them assumes a probability of 100%. Malkov (2012) noted that while the non-ignition events are being reported as zero in databases, such as MHIDAS, it is worth acknowledging that these are major accident event databases and releases of hydrogen which have simply dispersed and did not involve any flammable effects, are not recorded.

The split between immediate and delayed ignition in the HyRAM+ and HYEX models assumes 2/3 of the ignition is immediate and 1/3 is delayed; this is adopted from the hydrocarbon ignition probability approach. Due to the rapid cloud development from hydrogen jet leaks, and the uncertainty related to ignition of hydrogen releases, a 50-50% split could be considered a conservative approach when modelling ignition in QRAs.

As highlighted in EMSA's 2024 report, according to (ISO, 2015) and (NASA, 1997), regulators are advised to assume an ignition source is present even when acceptable standards for certified electrical equipment are followed. This implies that ignition of hydrogen in a release scenario should be assumed.

5.5 Detection and shutdown probabilities

The detection and shut-down safety function utilizes three subsystems, meaning that the failure-on-demand probability must be considered for each of the elements:

- **Sensor subsystem –** Gas detectors, detects a potential hazardous event and produces an electrical signal that is sent to the logic solver.
- **Logic solver subsystem** - detects the electrical signal exceeding a given threshold and sends a signal to the final element subsystem.
- **Final element subsystem** - performs the safety function by closing valves to stop the flow and isolate the leaking section.

To be able to establish the detection and shutdown probability, the process safety time (PST), introduced in chapter 4.2.3 must be estimated. The PST is the time period between a failure occurring in the process or its control system and the occurrence of the hazardous event. The safety system must detect and complete the actions intended to achieve a safe state, before any hazardous consequences occur (e.g. ignition, cryogenic damage, etc.). Thus, both the release characteristics, the geometry and space/environmental conditions, as well as technologies for sensor, logic solver and closing valves, incl. any redundancy must be considered. Also, if sensors, logic solvers and final elements have incorporated redundant architectures (e.g., 1oo2, 2oo3 voting configurations), this must be captured in the analysis.

Considering the mentioned points, the probabilities for failure-on-demand must be considered case-by-case for each QRA scenario. This was demonstrated in Case 1 and Case 2 of this report where the probability of successful gas detection and shutdown in a fuel concept with compressed hydrogen gas was analysed in chapter 4.2, while the detection in an inerted space for liquefied hydrogen fuel system was analysed in chapter 4.3.

It is noted that the default successful detection and isolation probability in HyRAM+ is 0.9. However, it is also stated that this value can vary significantly based on a particular system setup, and so the analyst needs to carefully consider the particulars of the system being assessed and decide if this default value is appropriate (Sandia, 2023).

Some considerations to be made when establishing failure probability for each of the subsystems are provided in the following sections.

Sensor subsystem

According to ISO 15916, the probability of successful sensor subsystem relies on the sensors; accuracy, reliability, cross sensitivity, maintainability, calibration, zero drift, detection limits (high and low), response time, recovering or non-recovering in time, active or passive techniques with and without energy supply, and compatibility with the system (ISO/TR 15916:2015). General performance requirements of detectors for flammable gases are found in IEC 60079-29-1:2016.

A variety of technologies are available to detect hydrogen gas (ISO 26142:2010). The sensors range from conventional (point, line, etc.) to relatively new technologies, such as acoustic gas detectors. Measuring principles and limitations of common gas detection technologies, not limited to hydrogen, are defined in IEC 60079-29-2:2015. However, some sensor technologies may not be suitable for hydrogen. A report titled ‘Overview of Hydrogen Safety Sensors and Requirements’ is provided by the U.S. Department of Energy (DOE) and the National Renewable Energy Laboratory (NREL), authored by W.J. Buttner, M.B. Post, R. Burgess, and C. Rivkin (2011). The report is recognizing that the availability of safety sensors is critical for the successful utilization of hydrogen and includes a generalized ranking of various sensor technologies to selected performance metrics. The DOE has also published a list of target specifications for hydrogen safety sensors, which includes a response time less than 1 second (DOE, 2017).

Acoustic leak detection was discussed in Case 1 in chapter 4.2.3. This is a relatively new technology which are often applied in a location with good ventilation and good dilution, where gas leaks may not be detected by a point gas detector due to the low concentration.

It may also be that conventional gas detection methods are used together with acoustic gas detectors to increase the probability of successful detection. The inherent reliability of the equipment, subject to calibration, robustness, reach, etc. is of utmost significance. The ISO 26142 standard state that a reliability analysis shall be conducted on the hydrogen detection apparatus in accordance with a recognised international standard.

For conventional gas detectors, the element of placement is crucial, considering the distance to the release source, ventilation condition and the geometry of the area. For acoustic detectors, as discussed in 4.2.2, the uncertainty relates to the system’s ability to detect leakages. It is claimed that the sensors are unaffected by environmental conditions like wind, leak dilution, background noises and the direction of the leak, which would imply that they have high detection reliability and robustness. However, there is ongoing research into how the system may be affected by intermittent ultrasonic noise and noise interference. There is also a lack of experience in the integration of acoustic leak detection into existing conventional gas detection for ship applications.

Note that the ISO 26142 standard provides requirements for stationary (refuelling stations on shore) hydrogen detection apparatus, covering both performance requirements and test methods.

Logic solver subsystem

The logic solver subsystem’s primary role is to process inputs from sensors and determine the appropriate response to maintain or achieve a safe state. It acts as the logic unit of a safety-instrumented-system, executing pre-programmed safety logic to mitigate risks.

Final element subsystem - Isolation and shutdown

The hydrogen flow from a tank is shutdown by isolation valves when a leak is detected. The released hydrogen volume will depend on the release rate, the closing time of the valves and the hydrogen volume within the isolated segment. The isolation of a hydrogen volume is essential to minimize the amount of gas that can leak. The hydrogen volume represents the amount of gas that can lead to an explosion or a fire. The mass of gas released can be used as a design criterion to prevent critical explosions. Unsuccessful shutdown (failure on demand) may lead to a significant gas cloud, with potentially high consequences. Isolation should be initiated automatically for hydrogen systems. A manual shutdown can be unreliable and can lead to a large gas cloud before a shutdown is performed (MarHySafe, 2021).

5.6 Delayed ignition probability

Delayed ignition within this context is any ignition not being immediate. Delayed ignitions are related to ignitions due to exposed ignition sources, such as hot surfaces, sparks or other ignition sources. Delayed ignitions can result in explosions, detonations and flash fires and can ignite residual jet fires. A delayed ignition of a jet leak can therefore result in both an explosion and a subsequent jet fire from the same leak source.

Hydrogen ignition models were presented and discussed in chapter 5.4.2, also including delayed ignition probabilities.

5.7 Flame front acceleration

Hydrogen, due to its high energy content and wide flammability range, poses significant risks when leaked and ignited. The behaviour of an ignited hydrogen leak is modelled as three primary outcomes in the event tree: explosion, detonation, and flash fire. Understanding these outcomes begins with the concept of flame front acceleration (or burning velocity).

Flame front acceleration refers to the increase in the speed of the flame front as it propagates through a combustible mixture. This phenomenon is influenced by various factors, including the concentration of hydrogen, the presence of obstacles and confinement, and the initial turbulence of the mixture.

5.7.1 Explosion

When hydrogen and an oxidizer (air) are allowed to form a mixture within the flammability limits prior to ignition (premixed mixture), after ignition, the following chemical reaction (combustion) may propagate through the combustible region. The resulting combustion process releases heat. The resulting expansion of the products, if fast enough, can cause a pressure wave to propagate from the source (ISO/TR 15916:2015).

The process where a flame propagates *subsonically* into regions of unburnt mixtures is known as a deflagration. In semi-enclosed and enclosed spaces, the confinement traps the expanding reaction products, creating a bulk flow that pushes the flame front faster into the unburnt mixture. This process can speed up the flame to hundreds of meters per second, causing significant overpressures, reaching several hundred kPa (ISO/TR 15916:2015). The high flame acceleration in congested areas also means that there is greater difficulty in venting the explosion fast enough and it can give high explosion pressures even in small clouds.

Under suitable fluid dynamic conditions, a deflagration wave can accelerate to near the speed of sound and can even transition to a detonation wave (known as a deflagration to detonation transition, or DDT (ISO/TR 15916:2015).

Explosions can cause harm in several ways, to be considered in QRAs:

- Pressure effects: The rapid expansion of gases creates a high-pressure wave that can cause injuries or fatalities to people nearby and structural damage.
- Flying debris (projectiles): The force of the explosion can propel fragments of the exploded material and surrounding objects at high speeds, turning them into dangerous projectiles. This debris can cause injuries or fatalities and further damage structures.

- Escalation: Explosions can cause secondary explosions if they encounter flammable materials, due to the heat and fire of explosions, and the damage that occur due to the explosion pressure.

Consequence analyses models for explosion risk are available in two main categories: the 3D Computational Fluid Dynamics (CFD) model; and the 1D phenomenological models, including simplified 'rule-of-thumb' calculations. While phenomenological models and simplified rule-of-thumb calculations are used to get a rough first-estimate and quick overview, the CFD models offers more precise calculations, and is the preferred tool when local geometrical and gas dynamic effects need to be accounted for (MarHySafe, 2021).

The MarHySafe Handbook for hydrogen-fuelled ships provides a methodology for quantifying explosion risk (chapter 8.2.2 and Appendix C). Also note that a validation of tools for modelling the flammable effects of hydrogen was presented in the EMSA report (2024), "Mapping safety risks for hydrogen-fuelled ships".

5.7.2 Detonation

While a deflagration wave is a *subsonic* process where the pressure change across the flame is negligible, a detonation is a *supersonic* process, which has very significant pressure rise across the front (10 times or more). A detonation is a self-sustaining explosion process with a leading shock of 20 bar that compresses the gas to a point of autoignition. The subsequent combustion provides the energy to maintain the shockwave. Detonability varies from fuel to fuel, and detonations would not occur in any realistic situation with natural gas but are entirely credible for hydrogen (DNV, 2022).

Detonation limits are the range of composition within which detonations have been observed in laboratory and field experiments. Detonation limits are a strong function of mixture composition, initial pressure and temperature but are usually considered to be narrower than the flammability limits. In addition, detonability is much more strongly dependent on the ignition source, confinement, and the physical size of the environment than flammability limits. The ability to initiate and propagate a detonation requires a set of critical conditions to be satisfied, and despite extensive research into the subject, the limits are empirical in nature (EMSA, 2024).

5.7.3 Flash Fire

A flash fire is a rapid, but relatively short-lived, combustion event that occurs when the flame front accelerates through a flammable mixture without generating significant overpressure. This is mostly relevant for open environments, with no obstacles in the path of the cloud. In an open environment with no confinement, the flame will propagate with laminar or "smooth flow" at a burning velocity into the unburnt mixture in the order of 2 m/s to 3 m/s (which is about 10 times faster than for hydrocarbon flames) (ISO/TR 15916:2015).

The combustion process generates high temperatures, which can cause severe burns and ignite other flammable materials. In QRAs, it is normal to assume that flash fire can harm people inside the cloud only. Flash fires are particularly hazardous to personnel, as the rapid spread of flames can result in severe injuries or fatalities.

5.8 Escalation probability

When we talk about escalation, we refer to the potential for initial hydrogen fires or explosions to cause damage to other hydrogen equipment and systems, which in turn can lead to more flammable material being released and cause catastrophic rupture. This chain of event is often referred to as a domino effect, were the worst-case situation gets out of control.

Ships do not have the same access to external emergency units as onshore facilities, and to some extent offshore facilities with standby vessels. An additional consideration for ships is that there is limited physical separation distance available to protect from explosion loads and heat from jet fires. Implementing effective mitigation strategies onboard is therefore crucial in ensuring that the risks associated with hydrogen initial- and potential escalation of events, can be managed.

The impact by either *initial* fire/explosions and/or *escalation* fire/explosion/catastrophic rupture may lead to consequences in terms of:

- Direct impact (injuries or fatalities)
- Impairment of muster stations, means of rescue and life saving devices
- Loss of ship safety functions
- Loss of power and manoeuvrability
- Loss of ship stability, water ingress

For fuel concepts involving compressed hydrogen storage, one of the primary concerns is the potential for a fire or explosion from an initial event to impact one or multiple cylinders or piping sections, which can then escalate to other cylinders or pipes. In the case of liquefied hydrogen storage systems, incidents within the TCS can affect the fuel storage tank, the insulation of piping can also be damaged. For LH2 tanks, the design case for pressure relief is typically loss of vacuum insulation. This will result in a rapid heating and boiloff.

By understanding the factors that influence the escalation probability, robust analysis techniques and methodologies can be applied in QRAs to evaluate potential risks and develop effective mitigation strategies.

The following chapters will discuss more on how initial hydrogen fire/explosion can escalate to other hydrogen equipment and systems, thereby worsen the situation.

5.8.1 Escalation caused by jet fire

Jet fire occurs when a flammable gas or liquid is released under pressure from a small opening, such as a pipe or vessel, and ignites. The resulting flame is typically long and narrow, resembling a jet, and can be extremely intense and focused. Larger hydrogen jet fires have similar properties as natural gas jet fires, though the hydrogen jet fires do have higher flame temperatures. For smaller fires, the flames are near invisible, and a lower fraction of heat is radiated from the fire than would be the case with natural gas (MarHySafe, 2021).

In compressed hydrogen storage systems, hydrogen cylinders or sections of cylinders may be affected by fire, either cause by hydrogen initial events, or by other fire sources. The hydrogen cylinders are usually safeguarded by Thermal Pressure Relief Device (TPRD). The TPRD is activated in case of fire and temperature typically exceeding 110ºC. In case a TPRD is triggered, the entire relevant cylinder/section is vented off avoiding pressure build up inside the cylinder. Venting rate and duration to cylinder/section is depressurized must be evaluated. Values may be taken from testing performed by the manufacturer and compared to the results of the fire analysis in the QRA considering fire duration, heat flux and distance. The following should be considered:

- It should be assumed that the cylinders can break/rupture if an accidental fire dose is larger than the fire dose that it is exposed to in the test (dose criterion).

- An exceedance of the dose criterion can also occur due to a less hot fire and a longer duration than the TPRD release time. However, in this case, the rupture may cause less damage since the pressure can already be reduced sufficiently.

- Failure of the TPRD may cause overheating of the cylinders and may result in its catastrophic failure, releasing the flammable gas and the large amount of stored mechanical energy. Note that fire exposure of cylinders may also cause smaller leaks caused by heat transfer from fire through the composite wrap to melt the polymer liner, although the focus in QRAs are primarily on the catastrophic rupture scenario. Thus, the reliability of the TPRD system (sensor, logic/mechanic unit and actuator), as well as the location of temperature sensors should be carefully considered. If fire is not located close enough to activate the TPRD, hydrogen remains in the cylinder.

- Any structural element than can reduce the heat flux from an impinging jet fire on a cylinder must be considered in the analysis, as this can reduce the risk of over-pressurization.

Studies carried out at the Southwest Research Institute demonstrated that the catastrophic rupture of the tank can occur. The test was done for tank type IV at operating pressure of 350 barg and total hydrogen mass of 1.64 kg. In the test the pressure relief device was removed, meaning that controlled venting was prevented. The failure time, after fire initiation (i.e., fire resistance) was measured as 6 min and 27 s (SWRI, 2002).

Piping, both containing gaseous and liquefied hydrogen, can also be exposed to a fire and a time to rupture can be assumed.

Both NFPA-2 and the European Industrial Gases Association (EIGA) include prescribed safety distances for jet fire based on non-marine applications. In the MarHySafe study it was considered that NFPA-2 may provide relevant input despite being based on onshore hydrogen applications (MarHySafe, 2021).

5.8.2 Escalation caused by explosion

Estimating hydrogen explosion risk is a key element in hydrogen risk analyses. Similar to jet fires, hydrogen explosions can cause significant damage to storage tanks, piping, and safety instrumented systems. The threshold criteria for causing a chain of events due to explosion is overpressure. It is already established that hydrogen generates higher pressures in an explosion compared to other fuels.

Typical considerations to be made for explosion potential and possible escalation effects are:

- How much force or momentum can the boss neck of the cylinders and piping withstand?
- At what overpressure will the deck, bulkheads and other essential ship structure collapse, and what will the subsequent events be?
- When will windows shatter and turn into high-velocity projectiles, causing potentially severe injuries or fatalities?

The overpressure criteria applied in the QRA for human vulnerability relates to injury to the body due to the pressure change. However, it should also be noted that fatalities may also be caused by:

- Injury as a result of fragments or debris produced by the overpressure impacting on the body.
- Injury as a result of the body being thrown by the explosion wind/blast and impacting on stationary objects or structures.

Escalation may also be considered for detonation events. However, in quantitative analysis, the damages from detonations are often so severe that they constitute an escalation event in themselves, or the resulting damages are comparable.

5.9 Discussion and uncertainty

It is found that the greatest uncertainty in the risk model lies in the leak frequency data and ignition probability. This also aligns with a DNV study of Hydrogen Risk Assessment methods from 2008. In that study, it was concluded that the greatest uncertainty in QRAs for hydrogen installations are (DNV, 2008):

- Leak frequencies
- Probabilities for failure of safety systems, including probabilities for human failure when operating equipment or safety systems (incl. containment, shutdown and isolation of process segments, gas detection and ignition source control)
- Ignition probabilities

This is because there is a limited availability of databases specifically focused on hydrogen equipment failures. Additionally, hydrogen ignition models are still under development. The ignition probabilities greatly affect the estimated risk level, resulting in significant uncertainty when using ignition probabilities for hydrogen. Studies have also identified a knowledge gap regarding the exact ignition mechanisms for hydrogen releases.

Furthermore, there is high uncertainty as to whether the gas detector system can react fast enough to prevent a critical gas cloud from occurring. This was assessed in chapter 4.2 and 4.3. If leaks are in the range of 0.1 kg/s, an explosive atmosphere can be generated within a few seconds. Conventional point gas detectors are not fast enough, and the reliability of acoustic detectors is uncertain due to the potential for ultrasonic noise interference.

As with any quantitative risk analysis, there will be uncertainty associated with the final risk level calculated using this model framework. However, the method offers a structured approach to understanding risks, enabling decision-makers to make informed choices even with uncertain data. Additionally, the modelling can identify the most significant risk drivers and quantify the risk-reducing effects, aiding in the selection of effective preventive and mitigating measures.

6. References

A.W. Cox, F. L. (2003). Classification of Hazardous Locations. Institution of Chemical Engineers.

Astbury and Hawksworth. (2007). Spontaneous ignition of hydrogen leaks: A review of postulated mechanisms. Harpur Hill, Buxton, SK17 9JN UK: Health and Safety Laboratory.

Astbury, G. a. (2021). Spontaneous ignition of hydrogen leaks: A review of postulated mechanisms. Harpur Hill, Buxton, SK17 9JN UK: Health and Safety Laboratory.

Buttner, W.J., Post, M.B, Burgess, R., and Rivkin, C. (2011) An overview of hydrogen safety sensors and requirements. International Journal of Hydrogen Energy. Volume 36, Issue 3, February 2011, Pages 2462-2470.

CCPS. (2015). Center for Chemical Process Safety (CCPS): Guidelines for initiating events and independent protection layers of protection analysis. New York: Wiley.

D. M. Brooks, B. D. (2021). Development of liquid hydrogen leak frequencies using a Bayesian update process. International Conference on Hydrogen Safety.

DNV. (2006). Leak frequencies from the hydrocarbon release database. DNV Consulting.

DNV. (2008). Main report – Survey of Hydrogen Risk Assessment methods. Report no.: 2005-1621. Rev 2, January 2008.

DNV. (2014). Modelling of Accidental Hydrocarbon Releases in QRAs: Hole Size Versus Initial Release Rate Basis. IChemE SYMPOSIUM SERIES NO 159.

DNV. (2019). Vedlegg 6 - Sikkerhetsavstand for fylleanlegg for hydrogen som drivstoff til lette kjøretøy, Rapportnr.: 2018-1200, Rev. 1. Oslo, Norway: DNV GL.

DNV. (2021). Closing the safety gap in an era of transformation.

DNV. (2023). Towards Standardized Compressed Hydrogen Containers Through Maritime QRAs. Spadeadam, UK: FABIG Tech. Meeting: Fire & Blast Challenges of the Energy Transition.

DOE (2017). Department of Energy - Technical Plan — Safety, Chapter 3.8. Hydrogen Safety.

DSB. (2021). Guidelines for quantitative risk analysis of facilities handling hazardous substances. Norwegian Directorate for Civil Protection.

EMSA. (2024). Mapping safety risks for hydrogen-fuelled ships, European Maritime Safety Agency, Lisbon.

Gexcon. (2022). FLACS-CFD User Group (FLUG) Meeting: Is ventilation your trustworthy old friend when it comes to hydrogen.

HSE. (2012). Failure rate and Event data for use within Land Use Planning Risk Assessments, HSE LUP Data Dossier HID C15,.

HSE. (2017). Fixed flammable gas detector systems on offshore installations: optimisation and assessment of effectiveness. Research Report RR1123. UK Health and Safety Executive (HSE).

HSE. (2024, 09 03). Operational guidance. Hentet fra Acoustic leak detection SPC/TECH/OSD/05: https://www.hse.gov.uk/foi/internalops/hid_circs/technical_osd/spc_tech_osd_05.htm

HySafe. (2006). Biennial Report on Hydrogen Safety (Version 1.2) - Chapter V. Hydrogen Safety Barriers and Safety Measures .

IEC. (2010). FAQ – Edition 2.0: E) Key concepts". IEC 61508 – Functional Safety. International Electrotechnical Commission. Hentet fra https://web.archive.org/web/20201025025914/https://www.iec.ch/functionalsafety/faq-ed2/page5.htm

IEC 60050-191:1990. (1990). International Electrotechnical Vocabulary (IEV) - Part 191: Dependability and quality of service.

IEC 60079-29-1:2016. Explosive atmospheres - Part 29-1: Gas detectors - Performance requirements of detectors for flammable gases

IEC 60079-29-2:2015. Explosive atmospheres - Part 29-2: Gas detectors - Selection, installation, use and maintenance of detectors for flammable gases and oxygen.

IEC 61025:2006 . (2006). Fault tree analysis (FTA).

IEC 61508:2010. (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems.

IEC 61511:2016. (2016). Functional safety - Safety instrumented systems for the process industry sector.

IEC 62061:2021. (2021). Safety of machinery - Functional safety of safety-related control systems.

IEC 62502:2010. (2010). Analysis techniques for dependability - Event tree analysis (ETA). International Electrotechnical Commission.

IEV 191-05-22. (u.d.). IEC 60050 - International Electrotechnical Vocabulary.

ISO 12489. (2013). Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems.

ISO 14224:2016. (2016). Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment.

ISO 19881:2018. (2018). Gaseous hydrogen — Land vehicle fuel containers.

ISO 26142:2010. (2010). Hydrogen detection apparatus — Stationary applications.

ISO/IEC 2382-14:1997. (1997). Information technology — Vocabulary — Part 14: Reliability, maintainability and availability.

ISO/IEC Guide 51:1999. (1999). Safety aspects — Guidelines for their inclusion in standards.

ISO/TR 15916:2015. (2015). Basic considerations for the safety of hydrogen systems.

J. X Wen, e. a. (2023). Safety of cryogenic liquid hydrogen bunkering operations - The gaps between existing knowhow and industry needs. 10th International Conference On Hydrogen Safety (ICHS 2023), Sep 2023, Québec (CA), Canada, (ss. 447-460).

MarHySafe. (2021). Handbook for hydrogen-fuelled vessels. MarHySafe JDP Phase 1. DNV, 1st edition (2021- 06).

Molkov. (2012). Fundamentals of Hydrogen Safety Engineering I & II.

MSA. (2021). Why ultrasonic gas detection? Hentet fra https://hysafe.info/uploads/papers/2021/194.pdf

MSC.1/Circ.1394/Rev.2 . (2019). Generic guidelines for the development of goal-based standards. IMO.

MTF. (2024). Maritime Technologies Forum : Guidelines for the development of liquefied hydrogen bunkering systems and procedures.

NASA. (1997). Safety standar for hydrogen and hydrogn systems. Washington DC: Office of Safety and Mission Assurance.

Offshore Norge. (2001). 070 – Offshore Norge Recommended guidelines for application of IEC 61508 and IEC 61511 in the norwegian petroleum industry.

OREDA. (2015). OREDA handbook .

Petro-Online. (2010). Fixed Gas Detectors – Total Speed Of Response. Petro-Online.

Quanterion Solutions Incorporated. (2016). Nonelectronic Parts Reliability Data.

Rausand, M. (2014). Reliability of Safet-Critical Systems: Theory and Applications. John Wiley & Sons, Incorporated.

RIVM. (2005). Guidelines for quantitative risk assessment ("The Purple Book" - CPR 18E).

Sandia. (2009). Analyses to Support Development of Risk-Informed Separation Distances for Hydrogen Codes and Standards. Sandia National Laboratories.

Sandia. (2012). Early-stage quantitative risk assessment to support development of codes and standard requirements for indoor fueling of hydrogen vehicles. Technical Report SAND2012-10150. Sandia National Laboratories.

Sandia. (2020). Final report on hydrogen plant hazards and risk analysis supporting hydrogen plant siting near nuclear power plants. Technical Report SAND2020-7946. Sandia National Laboratories.

Sandia. (2021). Hydrogen Risk Assessment Models (HyRAM) Version 3.1. Sandia National Laboratories.

Sandia. (2023). Hydrogen Plus Other Alternative Fuels - Risk Assessment Models (HyRAM+) - Version 5.1 Technical Reference Manual. Sandia National Laboratories.

SGMF. (2019). Formal Safety Notice: Recommended actions to prevent LNG leakages from dry-disconnect coupling in service on hose bunkering/transfer systems.

SINTEF. (2013). PDS Method Handbook 2013 Edition - Reliability Prediction Method for Safety Instrumented Systems. NO-7465 Trondheim, Norway: Safety Research.

SINTEF. (2021). Reliability data for safety equipment, PDS data handbook.

SWRI. (2002). Analysis of induced catastrophic failure of a 500 psig type iv hydrogen cylinder. Southwest Research Institute.

Tchouvelev, A. V. (2008). Knowledge gaps in hydrogen safety: A white paper. International Energy Agency Hydrogen Implementing Agreement Task 19.

West, M. A.-D. (2022). Critical Review and Analysis of Hydrogen Safety Data Collection Tools. International Journal of Hydrogen Energy, Volume 47, Issue 40, Pages 17845-17858.

Appendix A Summary of evaluated reliability databases

HyRAM+ by Sandia National Laboratories

HyRAM+ is developed at Sandia National Laboratories for the U.S. Department of Energy to increase access to technical data about hydrogen safety and to enable the use of that data to support development and revision of national and international codes and standards (Sandia, 2021). The HyRAM+ dataset from the Sandia report is unique as it is the only dataset that contain hydrogen specific data, although the dataset is limited and includes generic probabilities for hydrogen equipment failures for nine types of components. However, this data set is not ship specific and the frequencies are based on older leak frequency data published between 1975 and 2006.

Comparison of HyRAM+ leak frequency which is area-dependent against diameter-dependent exposure data in PLOFAM and UK HCRD demonstrates larger variations in leak frequency output for larger hole sizes, which is mostly due to the lack of diameter-dependence in HyRAM+. The variation, however, reduces towards smaller hole sizes, which could either be due to the under-reporting of small leaks in HCRD/PLOFAM or overestimating in HyRAM+ due to a combination of hole-size dependent models with the selection of hydrogen-specific data. Currently, over 90% of all leaks in HyRAM+ relate to very small and small categories.

The HyRAM+ data focuses on leaks and not the failure-on-demand probability of safety-critical equipment. Despite uncertainties with HyRAM+ application as described above, no other hydrogen-specific alternative leak record database has been established.

Considerations to be made when collecting data from HyRAM+:

- Failure rates are given as the annual frequency of random leaks for individual components.
- Failure data for five release sizes relative to the pipe flow area is given: 0.01%, 0.1%, 1%, 10% and 100%.
- The lognormal distribution is not symmetric on a linear scale and can cover multiple orders of magnitude, which can lead to unrealistically high values for the arithmetic mean. Therefore, the geometric mean (median) is used.
- The HyRAM+ data is a blend of general industry data and limited hydrogen-specific failure data.

HCRD by the UK HSE

The UK Health & Safety Executive’s (HSE) hydrocarbon leak frequency database (HCRD) (HSE, 2012) has been collecting data on all significant releases in the UK Offshore Sector since 1992. The HSE has also estimated the exposed population of equipment items and determined leak frequencies and size breakdowns for each equipment type. The quality of the HSE offshore dataset is exceptionally high, especially when compared to previous onshore frequencies. For each leak underlying the frequency values, it is possible to establish the hole diameter, the system and equipment type, the hydrocarbon type and pressure, the estimated quantity released, and many other parameters. This database has been extensively used for offshore QRAs. However, this dataset is not specific to ships or hydrogen applications.

The main issue is that when QRAs use the unmodified HSE leak frequencies, the analysis tend to indicate a higher risk than what is experienced in the industry. Therefore, there has been a desire to modify the frequencies to better align the risks with actual experience. Norwegian operators Statoil and Norsk Hydro initiated a project to develop standardized leak frequencies, commissioning DNV Consulting to undertake the work.

These modified frequencies have been used in this study. The method of obtaining the modified leak frequencies from the HCRD involves three main steps. First, grouping data for different types and sizes of equipment where there is insufficient experience to show significant differences between them. Second, fitting analytical leak frequency functions to the data to obtain a smooth variation of leak frequency with equipment and hole size. And eventually, splitting the leak frequencies into different leak scenarios to promote compatibility with different approaches to outflow modelling in the QRA (DNV, 2006).

Considerations to be made when collecting data from HCRD:

- Failure rates are expressed as frequency of full leaks per equipment item year.
- A full leak is defined as when the outflow is consistent with or greater than a leak at the operating pressure controlled by ESD and blowdown.
- The frequencies are given for two groups of hole diameter sizes, group size one >= 1 mm diameter and group size two >= 50 mm diameter.
- If a failure frequency is given as 0.0E+00, this does not mean that the frequency is zero, but that there is no data available.

PDS Data handbook by SINTEF Research

The PDS Data handbook (2021 edition) provides reliability data based on field feedback for components of safety instrumented systems, subsea and drilling equipment, and selected non-instrumented safety critical equipment (SINTEF, 2021). Considerable effort has been made to ensure that the data are credible, traceable, documented and justified, in line with requirements in the IEC 61508 and IEC 61511 standards. The most important data source for this handbook is extensive operational experience gathered from Norwegian offshore (and some onshore) oil and gas facilities during the last 10–15 years.

Considerations to be made when collecting data from PDS Data handbook:

- Failure rates are expressed as failures per million operating hours.
- The failure rate used is the λDU which is the rate of dangerous undetected failures (only revealed by a functional test or upon a planned or unplanned demand).
- PFDavg is calculated by using λDU.

OREDA

OREDA (Offshore & onshore reliability data), established in 1981 by the Norwegian Petroleum Directorate (now Petroleum Safety Authority), serves as an extensive databank of reliability data for both topside and subsea equipment used in offshore and onshore operations (OREDA, 2015). It encompasses data collection and analysis from over 18,000 equipment units, documenting 43,000 failure records and 80,000 maintenance records. Additionally, the databank includes insights from subsea fields with a cumulative operating experience exceeding 2,000 years. Various failure modes are represented for each component.

Considerations made when collecting data from OREDA:

- Failure rates are expressed as failures per million operating hours, with the mean failure rate being used.
- This database includes various failure modes, which is not consistent across all equipment.
- The specific failure mode used is specified for each case. When available, the preferred failure mode, “fail to function on demand,” is utilized.
- PFDavg is calculated by using the λ for the given failure mode.

NPRD

The Nonelectronic Parts Reliability Data (NPRD) from 2016 provides field failure rate data for a diverse range of mechanical and electromechanical parts and assemblies (Quanterion Solutions Incorporated, 2016). These parts cover ground, airborne, and naval environments. The failure rate data in this document is a cumulative compilation from the early 1970s through late 2014.

Considerations made when collecting data from NPRD:

- Failure rates are expressed as failures per million operating hours.
- Data is provided for different environments, such as airborne, ground, naval, naval sheltered, and naval submarine. Data is taken from the naval (N) environment, which represents typical fleet operations aboard a surface vessel. If naval data is unavailable, data from other environments (airborne and ground) is used.
- PFDavg is calculated by using the λ for the given failure mode.

CCPS Guideline

“Guidelines for initiating events and independent protection layers of protection analysis” is a book in a series of process safety guidelines and concept books published by the Center for Chemical Process Safety (CCPS). (CCPS, 2015).

The CCPS Guideline is only used as source for a few probabilities of failure on demand within this study. This database gives the PFD, not PFD_{avg}.

Appendix B Graphs of leak frequencies relative to hole diameter

For this comparison, a pipe size of 25 mm diameter was used as a basis to reflect different hole diameters. Note that the HCRD analysis used unmodified data from the 10-year period 2006-2015. Since this data is older, the analysis provides an indication of the differences between the sources for one equipment size, rather than precise values for all hole sizes.

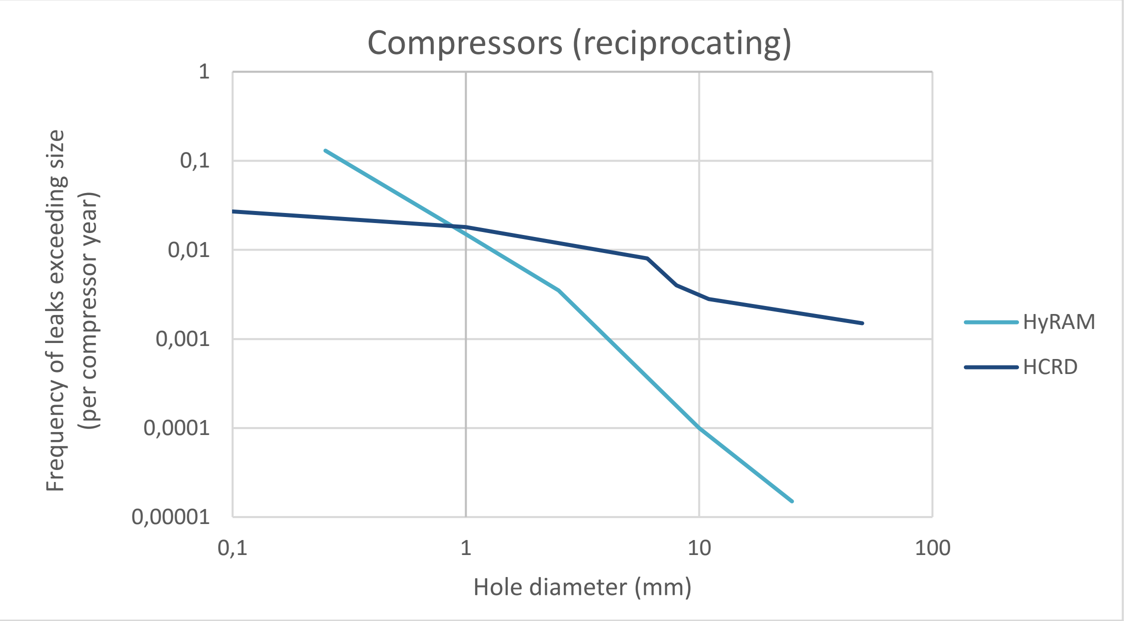


Figure 6-1 Compressor leak frequency relative to hole diameter (Source: DNV).

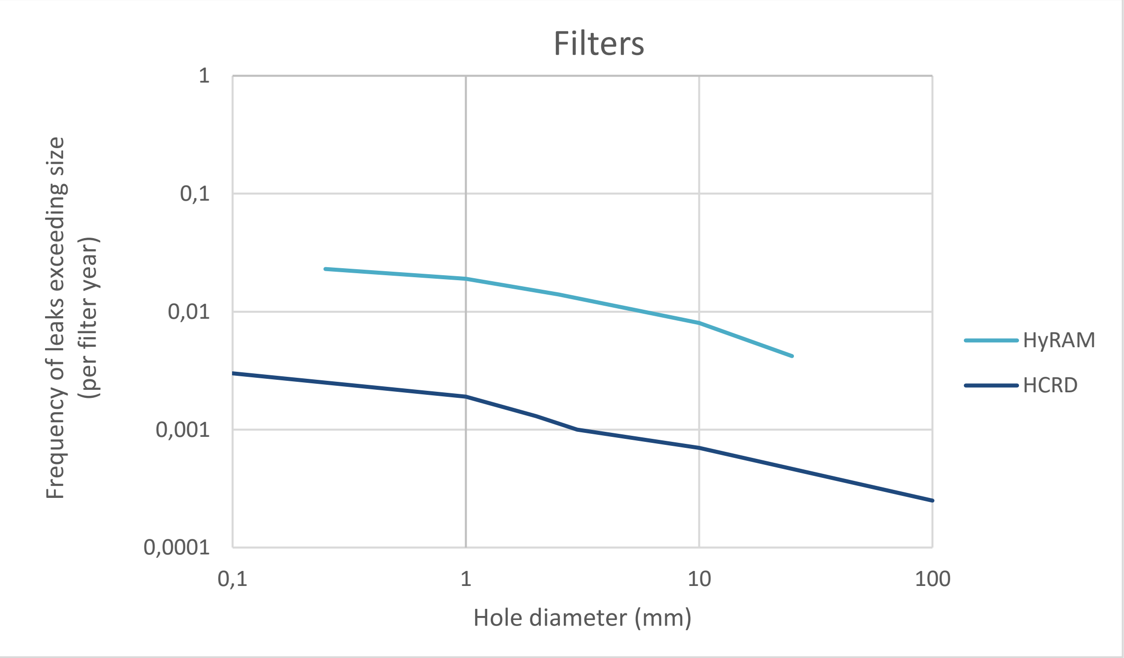


Figure 6-2 Filter leak frequency relative to hole diameter (Source: DNV).

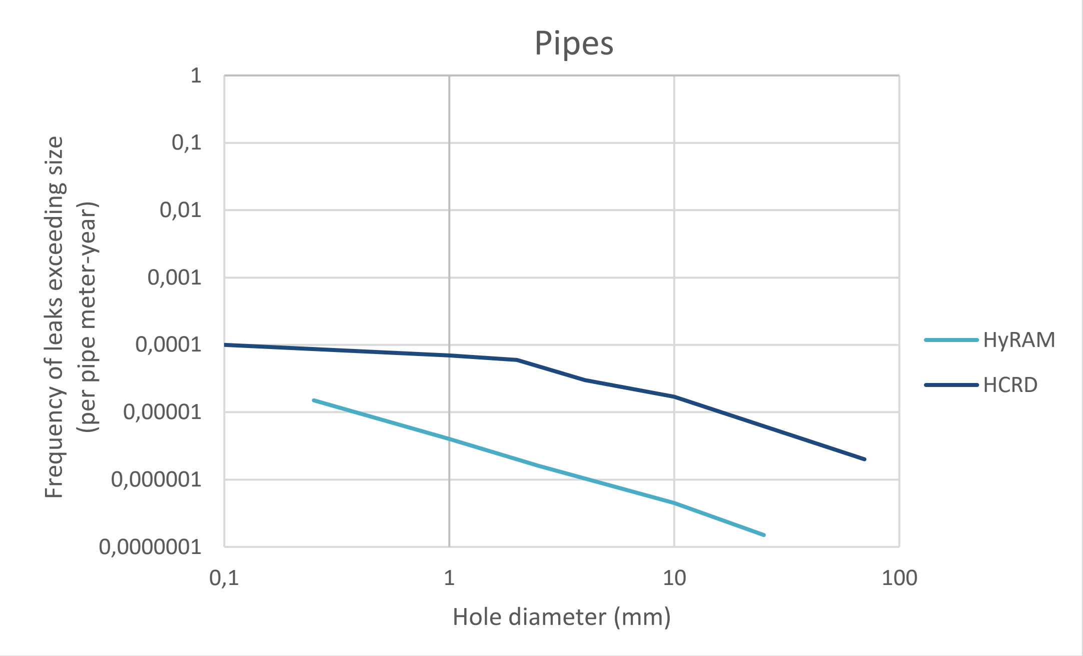


Figure 6-3 Pipe leak frequency relative to hole diameter (Source: DNV).

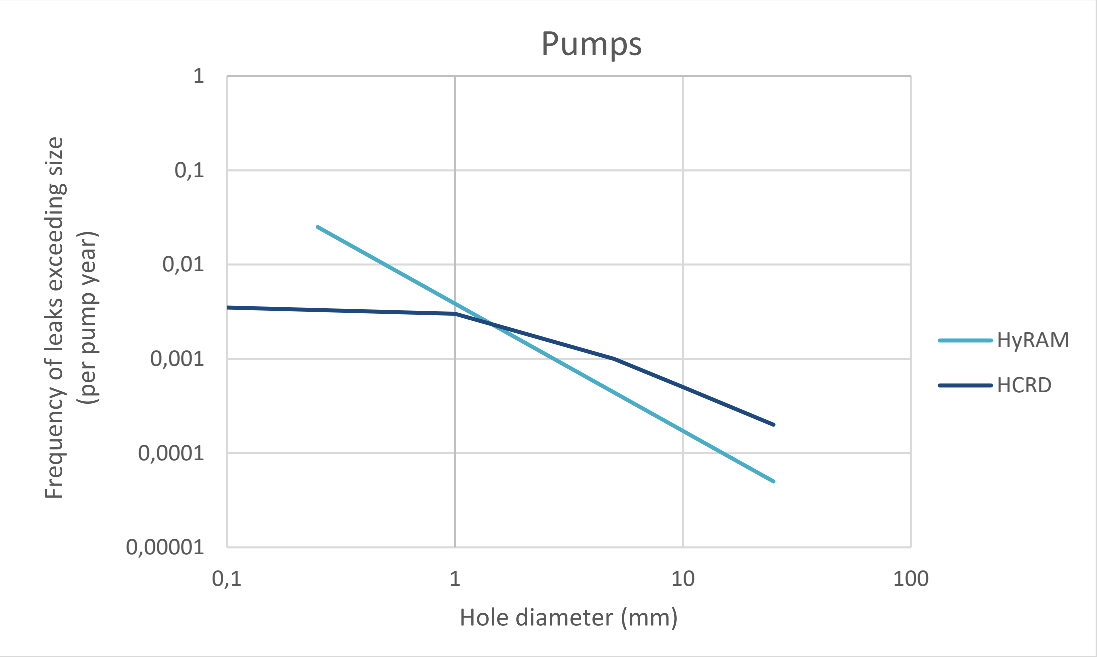


Figure 6-4 Pump leak frequency relative to hole diameter (Source: DNV).

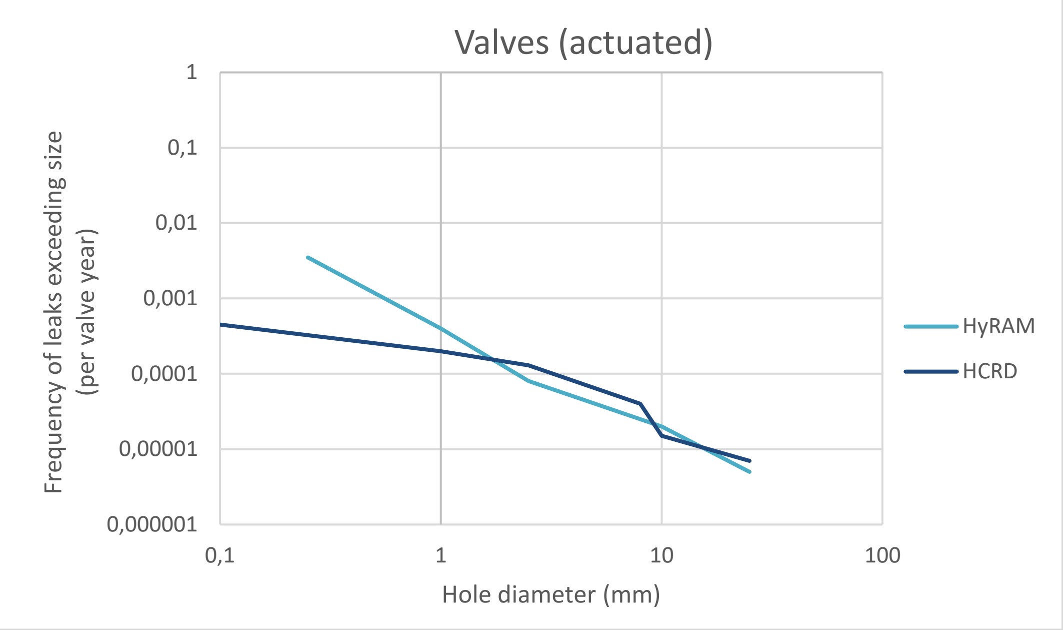


Figure 6-5 Valve (actuated) leak frequency relative to hole diameter (Source: DNV).

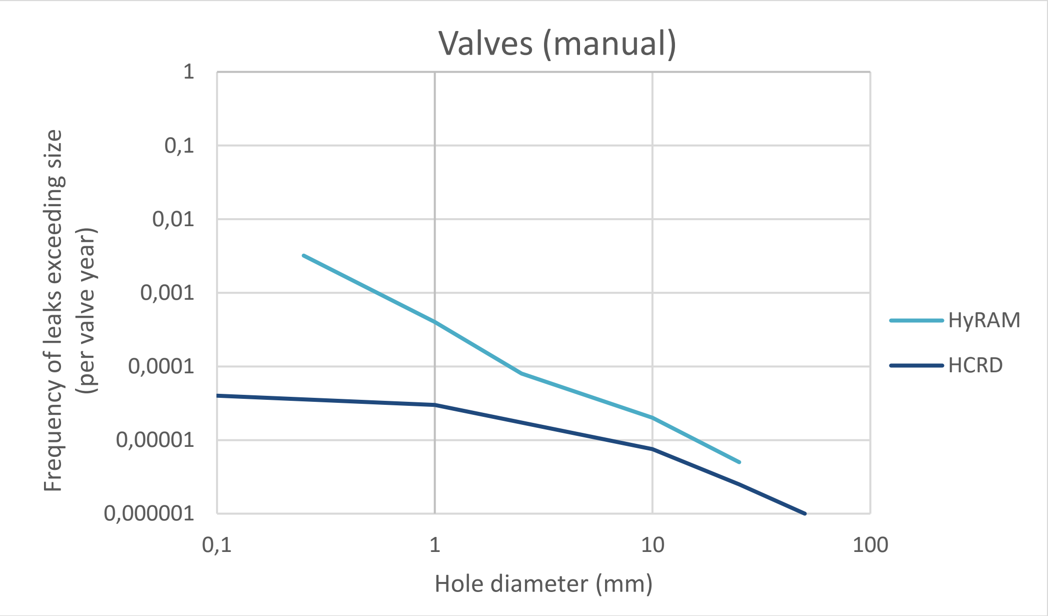


Figure 6-6 Valve (manual) leak frequency relative to hole diameter (Source: DNV)

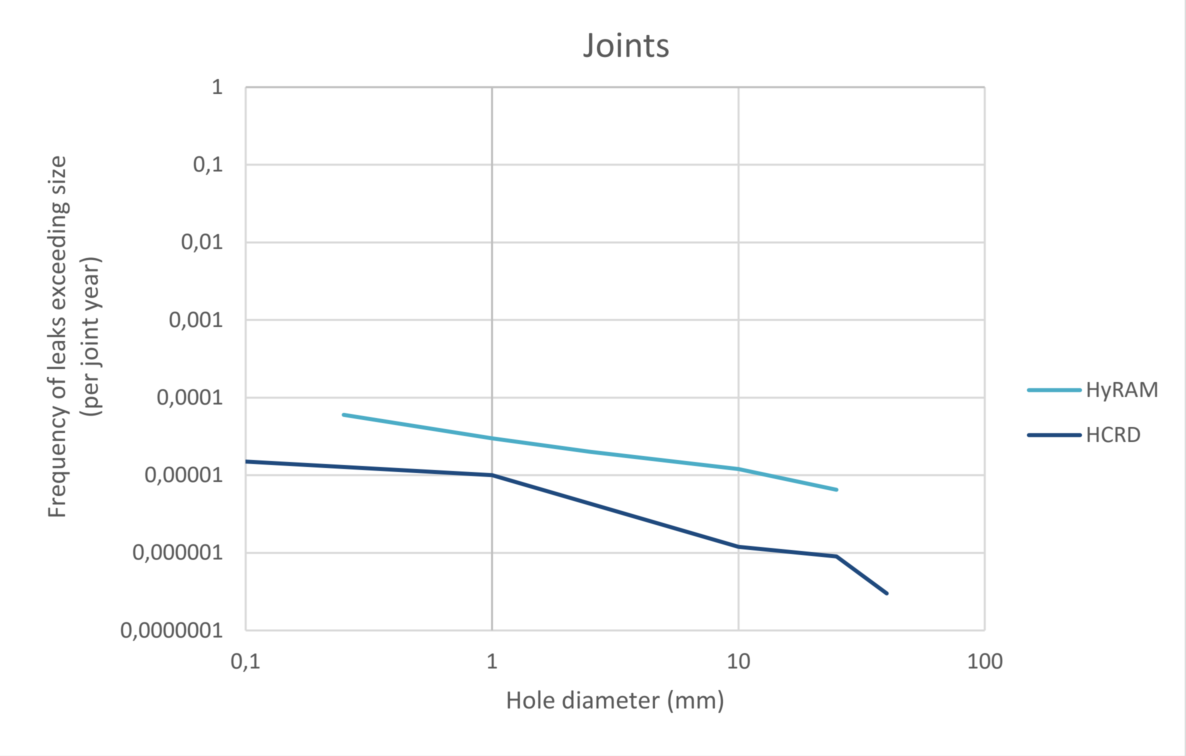


Figure 6-7 Joint leak frequency relative to hole diameter (Source: DNV).

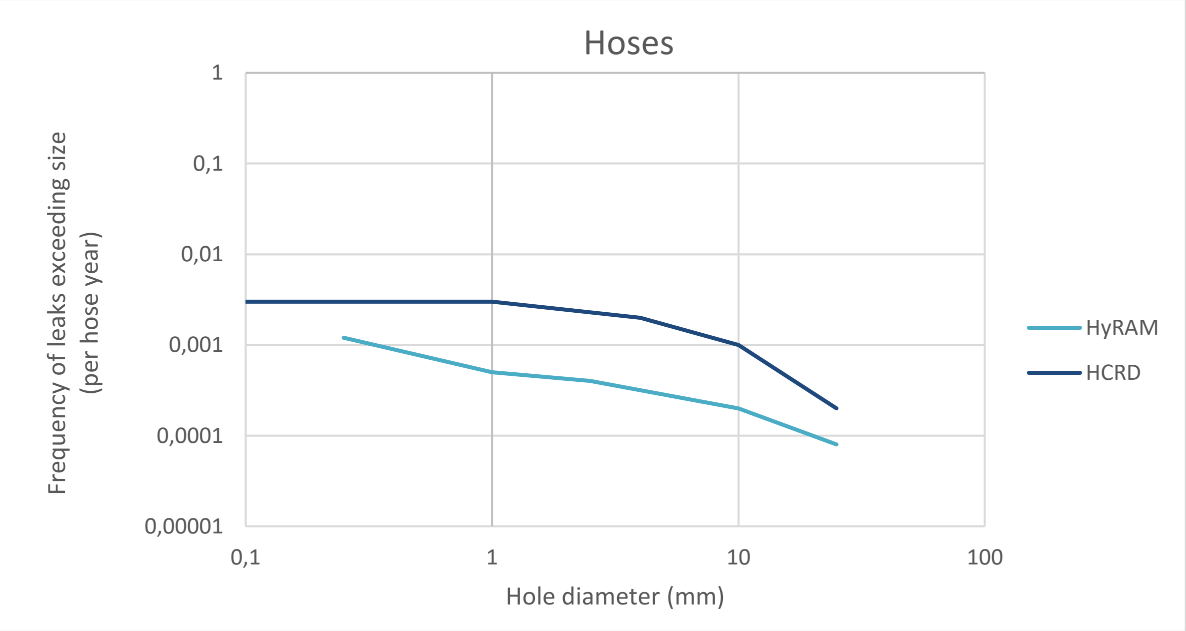


Figure 6-8 Hose leak frequency relative to hole diameter (Source: DNV).

European Maritime Safety Agency
Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu