DOCTORAL DISSERTATION

博士論文

Accident Modelling and Uncertainty Assessment in Risk and Reliability Quantifications to support New Technology System using Bayesian Approach

By

MAHESH KODOTH

(マヘシュ　コドート)

Supervisor

PROF. TADAHIRO SHIBUTANI

Graduate School of Environment and Information Sciences

Yokohama National University

YOKOHAMA – JAPAN

2020

Accident Modelling and Uncertainty Assessment in Risk and Reliability Quantifications to support New Technology System using Bayesian Approach

Research Case Studies:

- *Accident/Leak rate Modelling*
- *Accident rate uncertainty modelling*
- *QRA Parameter Verification analysis*
- *Improvement in reliability quantification*
- *Risk based Inspection Model*
- *Human Reliability Analysis*

The thesis for the Doctoral course

Submitted By:

Mr. MAHESH KODOTH

Supervised By:

Professor. TADAHIRO SHIBUTANI

September 2019

Yokohama National University

Graduate School of Environment and Information Sciences

Risk Management and Environmental Science

Safety Management Course

Shibutani Laboratory

Author Contact information:

Tel & Fax: +81-804-060-4242

E-mail: mahesh-kodoth-cd@ynu.jp

BLANK PAGE

PREFACE

This Doctoral Thesis is written in culmination of my research at Department of Risk Management and Environment Sciences, which is a part of Graduate School of Environment and Information Sciences at the Yokohama National University (YNU), Yokohama, Japan. This work has been performed during the spring of 2017 in continuation of the project thesis written in the autumn of 2019 and final submission in 2020.

This thesis is prepared in collaboration with the Strategic Innovative Program (SIP) project, financed by the Japan Institute of Science and technology (JST), coordinated by YNU and supported by Japanese Government MEXT Scholarship. The intended reader for this thesis should have practical experience in areas related to risk and operations in the oil and gas industry and/or education equivalent to Risk Analysis and Process Safety Management. In addition, certain basic knowledge on Bayesian Belief Networks is advantageous to understand the models discussed in this thesis.

The Ph.D has been a unique opportunity for contributing to fields in which I take great interest, namely technical safety and reliability, to be used in engineering plants.

Yokohama, Japan
March 2020

_____
Mahesh KrishnaKumar Kodoth

ACKNOWLEDGEMENT

I would like to thank several people for their comments, contributions and valuable assistance during the writing of this Ph.D thesis. Foremost amongst my acknowledgement I am very grateful to the almighty God, for giving me the will and ability to accomplish my goals.

Firstly, my supervisor, Professor Tadahiro Shibutani for his time, patience, positive attitude and invaluable guidance which was very vital in the execution of this work. The work could not have been completed without the fruitful discussions with him during the tenure. His presence during the Ph.D. period was extremely valuable.

Thanks go out to the Strategic Innovation Program (SIP) project team for giving me the opportunity to be a part of the Hydrogen Safety Project and engaging me in many enlightening discussions through the study programme. A special thank you to Prof. Tadahiro Shibutani, Prof. Naoya Kasai and Prof. Atsumi Miyake from Institute of Advanced Sciences (IAS), Yokohama National University, for their inputs on critical aspects of the Safety and Risk Management of Technological Systems.

I would also like to thank my other colleagues at Department of Risk Management and Information Sciences, Yokohama National University, in particular Prof. Tadahiro Shibutani and Prof. Atsumi Miyake, for giving me the opportunity to work closely with the Risk management department through 2017-2020. This experience was vital in kindling my interest in the field of risk analysis. Special mention to the faculty and students of the Risk Management and Safety study group at YNU, without whom this Ph.D. thesis would never be complete.

Finally, a heartfelt thank you to the dearest people in my life, (Mr. KrishnaKumar Kalliat, Mrs. Shylaja Kodoth, Mr. Pramod Kumar, and Mrs. Anupama Kodoth), my wife (Mrs. Gayatri Nayanar) who supported me throughout the past 3 years and especially during my study and living abroad at YNU, Japan.

SUMMARY

The overall objective of this Ph.D thesis has been to develop strategies for addressing uncertainties in the risk assessment. It addresses Accident Modelling and Improvement in Risk and Reliability Quantifications based on Probabilistic and Statistical Modelling to support New Process Technology Risk Assessment. The concept of the research aims at addressing uncertainties in risk and accident modelling by using dynamic bayesian based assessment.

Leak rate estimation, Failure frequency estimation and Risk based Inspection modelling are some of the important measures of risk and reliability quantification. Risk quantifications involve many uncertainties, and assessing probabilities to represent these uncertainties is itself a complex task utilizing a variety of information sources. At a practical level, uncertainties are driven by three important modelling issues; accident, failure probability and risk based model. The current modelling issues are related to model structuring, probability assessment, information gathering, and sensitivity analysis. The doctoral research is focused on addressing uncertainty in these areas of risk and reliability quantifications to support risk assessment.

By virtue of the new knowledge developed during the Ph.D, the decision makers are expected to gain a better insight into the pros and cons of accident analysis using statistical models, improvement areas in risk assessment, how uncertainty in risk assessment influences major accidents, the risk based inspection model, the degree and distribution of the causes of human factors in the hydrogen station unwanted releases.

The key objectives of this thesis include:

- *Propose a model for lack of data uncertainty and its treatment.*
- *Statistical interpretation of data and use of advanced frequency based models for accident and failure data analysis.*
- *Develop quantitative insights in the study to set performance standards for availability and reliability in operation and maintenance of the Hydrogen stations.*
- *Verification of risk and reliability quantifications using aging/life parameter method.*
- *Improvement in risk and reliability quantification using Bayesian update process.*
- *Propose a risk based inspection model to optimize inspection test for identified safety critical components.*
- *Propose a methodology for human error critical task assessment using bayesian networks.*

Contents

CORE CONCEPT PART I

1. INTRODUCTION

1.1 Background

Executing innovative technology-based system entails a range of potential hazards that can have a direct or indirect effect on the social lives and wellbeing (Nakayama et al., 2015). The potential of risk is much higher than conventional systems simply because failures and failure modes are not previously characterized. The risk posed by new technological systems and/or processes are not only limited to safety and social issues, but can considerably impact the environment, public confidence as well as damage to the property (Jafari et al., 2012). However, the acceptance of new technological system is crucial in order to reap benefits such as increased industrial opportunities, market growth, employment rate, etc. The positive effects of the new technological system can be seen as a reason for implementing the system, however it also induces some risks i.e. negative effects. The, undesirable, uncertain or uncontrollable event is termed as "process accident" or just "accident".

An accident modelling is an important study to understand consequences well in advance and accordingly take appropriate safety measures to prevent accident occurrence (Sakamoto et al., 2018). Accident modelling can reveal safety characteristics at the early design stage of the system before they are brought into the real world. The process accidents are more likely to occur in the energy industry if the concept of accident is not well understood. The accidents related to new technology systems (hydrogen) involving high pressure equipment's as stated by Sakamoto et al. (2016) is shown in table below.

Table 1. New technology accidents (hydrogen)

Source Name	Country/Year	Number of accidents	Database administrator
High Pressure Gas Safety Act Database (KHK)	Japan (2005–2014)	21	High Pressure Gas Safety Institute of Japan
Hydrogen Incident and Accident database (HIRD)	USA (2004–2012)	22	Pacific Northwest National Laboratory, USA

The total number of incidents and accidents in Japan from 2005 to 2014 is 21. In Japan, mainly accident occurred around a screw joint (Sakamoto et al., 2016). The total number of incidents in the USA from 2004 to 2012 is 22. The emergence of newer technologies mainly aims at extending convenience to the public. However, the hazards related to these technologies are often ignored and a single mishap often leads to dissatisfaction and unacceptance by the public and other authorities. This leads to difficulties in the implementation of such technologies thereby making it necessary to consider the public safety aspects associated with the technologies.

In a society that has grown increasingly complex with multifaceted socio-economic problems, an accident events, as the ones listed above will have undesired consequences. The harm resulting from such undesired consequences may be greater than the expected outcome or alternatively could result in domino effects. Thus, it is no longer credible to develop preventive measures for accidents as they arise. Earlier, many of the accidents were unknown, thus there was a tendency to adopt a traditional accident analysis model. Traditional accident models are unable to present a holistic picture of system/process safety and are not capable of accommodating modelling of multiple causal factors. As shown in Fig.1, traditional accident models do not necessarily detect the undesired event leading to accidents. They are more of a descriptive type rather than a predictive type model. One of the drawbacks associated with accident modelling methods is the un-adopted comprehensive quantification (i.e. no cyclic parameter updating to reduce the uncertainty). The traditional accident modelling methods lack the concept of updating parameters based on new evidence or findings. The problems associated with such approaches can be better understood from Fig.1.

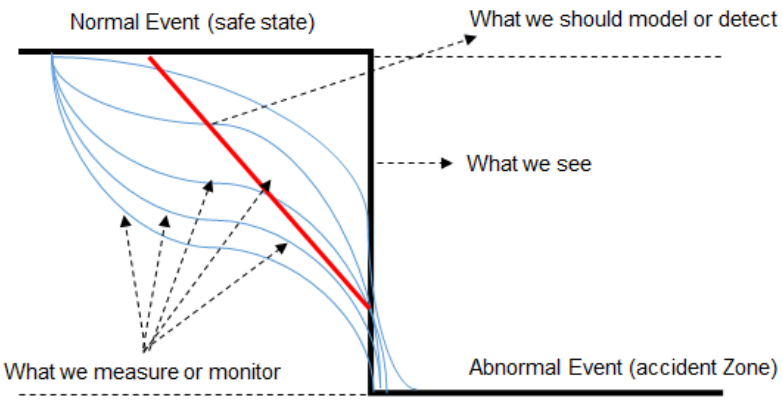


Figure 1. Accident concept from traditional approaches

One of the examples of the traditional approach is seen in gasoline-powered vehicles. Gas propulsion technology has been widely adopted in Japan over the years after being introduced in the beginning of the 20th century. The execution of such technology was accompanied by technological developments (including infrastructure such as roads) and regulatory adjustments, from which safety measures were derived (MacLean and Lave, 2003). Today, we are forecasting the rise of new hydrogen technology such as electric vehicles and fuel cell vehicles. This technology is likely to spread relatively quickly given the technical innovations and government support attached to it, not to mention the fact that the technological infrastructure (that used for gasoline-powered vehicles) is already in place. However, to ascertain the risks presented by such technology, including unexpected events such as accidents and natural disasters, we must go beyond analyzing existing vehicle propulsion technology and other relevant technologies.

In addition to understanding the accident characteristics, reliability is an important factor in the development of new technological systems. Nevertheless, several factors influence the reliability of a system, for instance, the environmental conditions, operational changes etc. The equipment must be reliable enough to safeguard the environment, and make the exploitation of the hydrogen economically feasible for a rather long period. Therefore, before an authority accepts to install a new hydrogen system, authority personnel must be convinced that the new system has a sufficiently high reliability and a prerequisite is that failures requiring hydrogen- station repair interventions must not occur. A system intervention requires often a long production downtime at a cost of several million dollars. The time to the first planned shutdown may be scheduled in five years, or even longer, and it is important that the installed system is able to survive at least this period without failure (Rahimi and Rausand, 2013).

Due to the nature of newer technologies, defining risk is vital and can influence the way we choose to live with risk in everyday life. Hydrogen energy system being easily accessible to public strengthens the requirement to understand the concept of risk. In addition to risk review, the accident characteristic should be studied to understand the trend of accident occurrence in new systems. Such study can reveal failure frequency, downtime, root causes etc. Thus, the concept of the research aims at addressing uncertainties in risk and accident modelling by using dynamic bayesian based assessment. The research

identifies issues related to new technology system such as hydrogen fuel station in the field of risk and reliability quantification. It involves assessing uncertainties in the risk and reliability field and using hydrogen energy system as a case study. Various modeling techniques and methods will be discussed to provide treatment of uncertainties. The outline of the thesis is organized such that Part I focuses on core concept on risk and reliability, accident analysis, safety classification of new technology (hydrogen) system. Part II addresses various technical safety and risk uncertainties and adopts modelling techniques to reduce the uncertainties.

The scope of the research is focused mainly on probability risk and uncertainty associated with it. It is to be noted that consequence risk is not considered in the scope of this research. Accident modelling and probability uncertainty is key issues for most of the failures involved in the process industry and especially with new technology system. The terms system, equipment, and technology are frequently used in this thesis. Technology can be defined as "the scientific study and use of applied sciences, and the application of this to practical tasks in industry" or as "application of knowledge to practical purposes" (DNV, 2011). Equipment and system therefore, denote any physical technical items, components or instruments. The thesis is structured in a way that reflects the characteristics of hydrogen fueling stations, the subject matter of the research. Hydrogen energy is already used in settings such as plants and business facilities. Therefore, the technology and system are not especially new in this aspect. Nonetheless, this research classify hydrogen energy as a technological innovation because the technology is set to be increasingly adopted in public's daily life activities such as hydrogen fueling stations and fuel cell vehicles.

1.1.1 About Research Concept and Motivation

This PhD project contributes to the scientific evaluation of the presented work by a detailed description of the model, an assessment of the content, and a description of the limitations and benefits of the model. The research aim to benefit academic risk analyst and process industry engineers who constantly perform various risk assessments on engineering system. Taking into account the practical engineering challenges, the research attempts to keep the work as simple as possible.

The concept of the research is focused on three things:

1. New technology system (or engineering system)
2. Treatment of uncertainties in risk and reliability quantification
3. Bayesian dynamic modelling

The originality of the research is the application of dynamic modelling for treatment of uncertainties in the field of risk and reliability quantification for new technology system. The bayesian technique is quite old and has been commonly used across various applications. Fundamentally though these technique often are 'black boxes' and are not easily understood by safety engineers, in applications such as accident modelling or risk and reliability field. This could be due to the complexity of the approach or lack of availability of software in the risk field. Another limitation in the 'industrial risk learning' case is that it involves collecting abundant data for statistical interpretation. You need a good reliability data to justify risk model for example. New engineering system lacks such good quality data and hence not compatible with the existing statistical modelling approach.

These limitations make it difficult or impossible to make models that work with only a small amount of data and leverage domain-specific expertise. They also adversely affect models in dangerous or legally complicated contexts such as risk or insurance. The models that yield predictions must come with confidence that allow one to assess risk. For example, it's important to know the uncertainty estimates when predicting likelihood of a hydrogen release having a high consequences.

Until recently the practical engineering challenges of implementing these systems were prohibitive, and required a large amount of specialized knowledge. Thus we introduce probabilistic dynamic modelling to risk science. Probabilistic dynamic modelling (PDM) hides the complexity of Bayesian inference, making these advanced techniques accessible to a broad audience of risk and reliability analysts. PDM allows to incorporate your domain knowledge with your observed data. It is powerful for three reasons:

- For allowing to incorporate domain knowledge
- Works well with small or scarce datasets
- It is interpretable

In the past 10 years, several researchers have introduced the concept of bayesian in the academic science, however they were conceptually applied without addressing practical challenges in the risk and reliability field. If we go beyond these limitations, we open the door to new kinds of products and analyses that is the subject of this thesis. The fundamental ideas of probabilities and distributions of results are the basic building blocks of models utilized in this paradigm. One of the impactful idea in this research has been deep learning for risk analysis. This can change the way we perceive and treat risk in the near future.

In this PhD project, it was possible to perform case studies where the method can be tested for a specific application. In this case, the results may be validated qualitatively or by expert judgments, or preferably, compare the results with outcomes from other recognized and comparable methods. The development of frameworks and methods is based on logic arguments, initial assumptions, existing methods, and knowledge to derive new relationships or insight. In such cases, the validity of the method is confirmed by comparing with other suitable methods.

In the early phase of design and operation, a new technology system is aimed on only the positive aspects of the risk such as profit, usability, social benefits etc. However, it should be understood that these are not the only benefits the technology can bring to the society. The negative aspects of the risk such as injury, leakage etc. can also bring benefits to the society over the long run by reducing production downtime, increasing safety, environmental protection and company reputation through public confidence. The process safety is a vast field with numerous areas that can be addressed to improve safety and risk. The PhD project focuses on safety and reliability engineering areas. The idea of introducing dynamic modelling in various safety and reliability engineering aspects was the key motivation in undergoing the PhD project. Therefore, we decided to address several issues that are often highlighted in several research papers however still there is insufficient data. These topics mainly contribute to uncertainty in the risk. Wide range of topics such as lack of data, accident analysis, verification of risk assessment, inspection interval, leak rate analysis etc. are covered and will be addressed using the research principles underlined in the PhD project.

1.1.2 Scope of Research

The scope of the research is focused mainly on probability risk (reliability) and uncertainty associated with it. Consequence part of the risk is not addressed in Accident modelling and probability uncertainty is key issues for most of the failures involved in the process industry and especially with new technology system. The main reason for choosing probability side of the risk is as follows:

① In case of new technology systems, probability (or frequency) is hard to estimate due to lack of statistical and failure data. Data uncertainty assessment is therefore necessary in probability estimation.

② On the other side, consequence of the new technology can be estimated through chemical and physical characteristics of the source fuel. The data uncertainty is significantly lower in case of consequence modelling.

③ Probability (or frequency) is a key parameter since most of the initial events are failures with high probability and low consequence. This is typically the case with new technology system.

④ Consequence risk is a key parameter for major accident hazard (MAH) with low probability and high consequence. This is more likely to happen in case of natural disaster.

1.2 Principles of Risk and Safety

1.2.1 The Risk Concept – Review of Risk

The definition of risk must be agreed before establishing the concept of risk. This section reviews the different definition and meaning of the concept of risk. This thesis is addressed in a very broad manner, the risk term can be interpreted in different ways depending on the individual roles, areas of effects, and academic/industry disciplines concerned. It is also considered that risk can be perceived in a different way depending on the concerned parties. For example, the risk perceived by owner can be altogether different from the way risk perceived by operator or public. This section outlines two key concepts that are essential in understanding the risk concept applied to this thesis i.e. “social risk” and “process risk.” Process risk is commonly used across process industry due to the possibility of fire and/or explosion resulting from the process failure. However, it is not common to find data on social

risk in the industry guidelines. Perhaps this could be due to the nature of risk that is considered vital across the industry.

However, due to the nature of hydrogen, safety issues on the risk of fire and explosion based on process risk are not the only thing to be considered when planning social implementation. Discussions on the social implementation of hydrogen fueling stations should be treated equally and assessed with proper care. Social risk matters to consider include user-friendliness, business continuity, and environmental impact. Such risks are fundamental matters in hydrogen energy system and they warrant careful examination. Some of the risks associated with these areas offset risks in other areas. All risks must be managed comprehensively to ensure that the stations, in addition to being reliable themselves, reliably serve the local community and society as a whole. This is why the concept of risk needs to be extended and risk should be defined as comprehensive social risk.

A general risk model is concerned with safety risks (risks to human health, property and the environment). A comprehensive social risk model is focused on process risk and social safety that explores the consequences to people's lives, social dynamics, and values. Risk is an important concept, and fields such as safety engineering have developed effective conceptual models for risk. Organizations such as the Atomic Energy Commission and Massachusetts Institute of Technology, as well as individual theorists like Herbert William Heinrich, have introduced models for quantifying the likelihood that an event will occur and the effects (the scale of the damage that would result from such an event). This approach emphasizes the negative effects of risk. Quantifying likelihood and effect is advantageous in that it enables an objective judgment. On the contrary, you cannot quantify all likelihoods and effects. Moreover, in as much as these models focus on negative effects, they are less effective for analyzing the potential positive effects alongside the negative ones. Examples of positive effects include how the technology will make life more convenient or contribute to the economy.

Most of the techniques employed in risk assessment are typically categorized based on the amount of detailed assessment. This further widens the definition of risk to qualitative risk and quantitative risk. In qualitative risk, the risk is assessed based on certain qualitative criteria without numerical

quantification. However, in quantitative risk assessment detailed quantification and modelling is involved to assess risk (Kaplan and Garrick, 1981). Most analysts would probably see the need for both quantitative methods and qualitative methods. Another important parameter that has an effect on the definition of risk is "time". It has been found that there has been a gradual change from narrow risk perspectives based on probabilities to broader non-probability based risk. This also notices a distinction between risk as a concept and how this concept is measured. The concept of risk is widening to suit various development needs of risk analysis (Thompson et al., 2005).

From the above concept of risk from different perspectives, the definitions of the risk can be broadly categorized into;

① Social risk vs Process risk

② Safety risk vs Comprehensive social risk

③ Positive effects vs Negative effects

④ Qualitative risk vs Quantitative risk

⑤ Probability risk vs Non probability (consequence) risk

There is no universal definition of risk. This thesis define risk as "the effect of uncertainty following the rules of probability". The classification of risk definition is as follows:

I. Risk=Probability of an (undesirable) event

a) Risk is the chance of loss in terms of safety or environment.

b) Risk equals the probability of a leak event.

c) Risk means the likelihood of a specific effect originating from a certain hazard occurring within a specified period or in specified circumstance.

II. Risk=Probability Uncertainty

a) Risk is measurable uncertainty, i.e., uncertainty where the distribution of the outcome in a group of instances is known either through calculation a priori for limited data or from statistics of past experience for well-known data.

The understanding of the concept of 'uncertain risk and probability' may be influenced by the interpretation of two central concepts in risk research: 'uncertainty in risk' and 'probability'. According to Walker and colleagues uncertainty is 'any deviation from the unachievable ideal of completely deterministic knowledge of the relevant system' (Walker et al., 2003). The concept is generally understood to express something uncertain, but for that uncertainty to constitute a risk, something must be known about it (Hansson 2002). Different approaches to risk and definitions (e.g. based on probabilities, expected values, uncertainty or undesirable events) have been discussed extensively in the risk literature (Althaus 2005; Aven 2010, 2012, 2014; Aven and Renn 2009; Aven et al., 2011). The uncertainty can be due to various parameters, out of which some key factors will be detailed in the study. The uncertainty of risks risk refers to both the positive and negative consequences of uncertainty.

In this PhD project, the uncertain risk described aspects were categorized in six overarching themes:

- Accident/leak rate uncertainty using statistical interpretation
- Accident rate uncertainty modelling due to lack of data
- Uncertainty about verifications aspects related to risk assessment
- Failure rate uncertainty modelling
- Sensitivity analysis on Inspection Interval based on uncertain risk types
- Ambiguity in the understanding of risk and errors caused from human judgement and actions

Safety engineers adopt the concept of risk, but within a limited scope. Consequently, businesses and public authorities have tended to employ risk treatments that focus on preventing events from reoccurring. Similarly, when safety and risk assessments are performed for technological innovations, these assessments typically focus on safety issues concerning internal parties and parties who are peripheral to the system; these assessments seldom cover risks to the public as a whole. Why is this so? One reason is that, as mentioned above, risk tends to be defined narrowly. Another reason is that technological risks (and their effects) tend to be analyzed in a reductionist manner, mostly within a technological context. On the other hand, when social scientists analyze risk, they adopt a more holistic perspective. However, their assessments tend to be general and abstract, making it hard to derive specific safety evaluations or safety measures.

1.2.2 Classification and Qualification of New Technology in terms of Safety

The solution to the amount of detailing the comprehensive risk assessment should depend on the level of newness of the technology. The newness of the technology can be classified into several systems to assist in prioritizing safety activities. For example, in terms of safety, new technology is defined as that which (i) has never been previously characterized, (ii) has extremely limited data on failures and accidents, or (iii) new or unknown failure modes. The hydrogen fueling station can be more related to the gasoline or petroleum industry due to the nature of the chemical characteristic.

In the DNV guideline (DNV, 2011), technology is classified as new when its characteristics are unknown i.e. not proven. The concept explained in DNV guidelines is generic that applies across any new technology. However, this thesis is limited to safety issues only and therefore the DNV guideline is modified to understand the implications of new technology in terms of safety and risk. Technology can be classified as new when its safety characteristics are unknown i.e. not safety proven. The safety characteristics refer to the possible failure modes of the system. Technology is said to be safety proven when it has a well-documented risk record of accomplishment or database system from the potential hazardous environment application. The record or database should list all potential or real failures that have occurred in the past with similar systems or likely to occur. Documentation of failure modes and failures can provide confidence in the system design or operation. Such documentation must provide confidence in the technology from practical operations, with respect to the ability of the technology to meet the specified requirements (DNV, 2011; IEC61508, 2010).

Safety qualification of new technology is the process of providing the evidence that the technology will operate within the tolerable risk limits with an acceptable level of confidence. New equipment or installation to be qualified for safety can be classified according to: (i) the newness of the technology and (ii) the amount of risk experience from previous applications of similar technology in the actual operational and environmental context. Based on these factors, the safety of new technology can be classified into four categories of newness:

① No new technical uncertainties: This is the least demanding category, where proven in use technology is used in a known application.

② New technical uncertainties: This category has two subcategories: a) Technology with a limited field history (i.e., partly known) that is used in a known application. b) Proven in use technology that is used in a new application for the company/user.

③ New technical challenges: This category has three subcategories: a) New or unproven technology that is used in a known application. b) Technology with a limited field history (i.e., partly known) that is used in a new application for the company/user. c) Proven technology that is used for a new application for the whole industry.

④ Demanding new technical challenges: This is the most demanding category where: a) New or unproven technology is used in a new application both for the company/user and for the in1dustry. b) Technology with limited field history that is used in a new application for the industry.

Table 2. New technology Categorization: Safety

Application Area	**Degree of safety of technology**		
	Proven in use	Limited field history	Unknown failure modes
Known	1	2	3
Limited Knowledge	2	3	4
New	3	4	4

This classification applies to the totality of the applied technology as well as to each of its parts, functions, and subsystems. It is used to highlight where care must be taken due to limited field history. Technology in category 1 is proven technology where proven methods for qualification, tests, calculations, and analysis can be used to document margins. Technology in categories 2 to 4 is defined as new technology and must be qualified according to a qualification procedure. By distinguishing between 2, 3, and 4, it is possible to focus on the areas of concern.

An equipment or installation should be qualified for safety once there is enough evidence that the new technology meets the minimum criteria. DNV defines qualification as “confirmation by examination and provision of evidence that the new technology meets the specified requirements for the intended use.” Thus, the safety qualification is a systematic process aiming to-

1. Reduce the risk and increase the probability of product success.
2. Ensure that the product is fit for purpose before being put into operation.

In order to set the criteria for the qualification of a new technology, the responsible authority or institution should serve the following purposes:

- Provide proof of fitness for the purpose of introducing the new product/technology to the market.
- The system integrator, who integrates the new technology into a larger system, needs to evaluate the effect on the total system reliability and to use it as input to the reliability assessment of a larger system.
- The end-user of the new technology must optimize the risk posed by the new technology over the benefits of the technology. The risk introduced by the new technology must be grossly disproportionate to the benefits obtained through its operation.

1.2.3 Safety Qualification of Hydrogen energy system (mainly hydrogen fueling stations)

The hydrogen-based technology should be classified under Category 3 due to limited knowledge of the application and extremely limited data on accidents/failures. The qualification of a hydrogen system implies that based on the provided evidence, whether the system is fit-for-purpose and can start its operational phase. Performance criteria for the product and/or the technologies must be specified by the developer, regulatory bodies, or by the end-user and may be related to various reliability measures based on the time-to-failure probability distribution and/or some defined margins against specified failure modes (e.g., see DNV, 2011; IEC60300, 2007). Due to the high number of tasks that needs to be verified for Qualification, it is advised to categorize qualification into 3 stages namely

① Planning Stage Qualification

② Design Stage Qualification

③ Implementation Stage Qualification

1.2.3.1 Planning Stage Qualification

In this stage, the feasibility of the implementation of a hydrogen energy system should be considered. The following points must be thoroughly reviewed and examined for the planning stage qualification of hydrogen energy system.

- List the hazards associated with hydrogen fueling stations as exhaustively as possible from multiple viewpoints. All identified hazards must be recorded in a hazard register. The hazards should be identified from the viewpoint of operators, public and initiating authorities. Ideally, the assessment should broadly examine the general trends in energy (hydrogen and other energy), the life cycle of hydrogen fueling stations, and similar themes.
- Briefly identify the potential failure modes and cause consequence pair so as to pinpoint the risks that could have major effects.
- If proceeding with the implementation would entail significant issues, the parties should consider measures to mitigate the effects of these issues. They must then verify the effectiveness of these strategies and incorporate them into the implementation schedule.
- If unsure as to what mitigation strategies to adopt or whether the measures will be effective, review whether it is advisable to proceed with the implementation in the first place.
- The risk analyst should determine the impact of the implementation of hydrogen fueling stations and the hydrogen energy system on the society once implemented and conclude whether such implementation would be appropriate.
- The risk analysts should examine all possible risks and effects to identify any abnormal scenario that could have major effects. Even small unimaginable risks should not be missed.
- Analyse in detail the risks that could have major effects on the individuals or environment.
- Analyse the risks of system failure and natural disasters. Other risks to analyse include human error and terrorist attacks.

1.2.3.2 Design Stage Qualification

Once the planning stage is finalized, the risk assessment should be refined before introducing the system. A complete risk assessment should be performed at this stage before the system is actually constructed and operated. The following points must be thoroughly reviewed and examined for the design stage qualification of the hydrogen energy system.

- Consider the risks associated with hydrogen fueling stations during normal, abnormal, and accident situations. It is also important to consider the variation in risks and social values depending on the local environments.
- Confirm all potential failure modes are identified and addressed in a satisfactory manner so that margins to failure are documented and the reliability of the product can be proven.
- In addition to preventative measures, consider mitigation measures that can help reduce the escalation of potential event that has occurred.
- Consider the likelihood that smaller risks (for which risk treatments have not been devised) will have major effects once the technology or system is diffused.
- Analyse the trade-offs with competing technologies or systems. This analysis should be conducted from an overall society perspective.

1.2.3.3 Implementation Stage Qualification

At this stage, more evidence that is new can be observed either randomly or through inspection. No matter how extensively it is executed, the hydrogen energy system will eventually be replaced by an alternative system and require disposal. While proceeding with the execution, the team should assess end-of-life treatments.

- In case of modifications or replacement, assess risks associated with the system being replaced by another system.
- Gather new evidence observed and update the model to obtain new results on risks.
- Refine (update) all the documentation associated with the safety and risk of hydrogen energy system. The documentation may include Hazard register, HAZOP, QRA, Probability estimation, etc.
- Identify any new hazard introduced to the system by means of modification or aging conditions. A proactive risk management is required in such cases to prevent any unexpected outcome.

1.2.4 Static versus Dynamic (Bayesian) approaches

Static approaches are traditional risk assessment approach that uses an initial set of data to quantitatively assess the risk and reliability of systems. The input data is obtained through several ways such as

manufacturer data, plant maintenance database, external sources such as certificates, handbooks, records, etc. Once the system is quantitatively assessed to identify and evaluate the risk, the risk is treated as a constant parameter. Static approaches can have some serious limitations. These limitations cannot overcome the current industry limitations. Some limitation of the static approach is as follows:

- Traditional methods are not suitable for "sparse" data – New technology systems and high reliability systems often have sparse data.
- No Real Prior Knowledge - Traditional reliability analysis makes no assumptions about the population prior to taking sample data.
- Highly Relying on External Sources
- Unable to capture the dynamic behaviour of the process operation
- Unable to update the quantitative results

The dynamic approach is aimed to resolve the above limitation with the adoption of Bayesian approach. Dynamic risk analysis is the ability to provide continuous acquisition, effective process and meaningful communication of risk through quantitative assessment. Dealing with data in this manner is particularly interesting in managing risk and asset integrity of engineering plants. Research in this context is faced with the dilemma that, while there have been significant developments in understanding how accidents occur, there has been no comparable development in understanding how to adequately assess and reduce risks (Bouloiz et al., 2013), considering both process and personnel side of safety (Fabiano et al., 1995). In safety and risk management area, Simon et al. (2018) has explicitly described a need for an integrated and holistic system approach to address both technical and social aspects. Advanced research trends include knowledge-based methods combined with process models, such as Petri nets, signed digraphs, and dynamic simulation.

The application of BN in the field of risk and reliability was explored by many researchers, e.g. Yeo et al. (2016). A system is safe if it is impervious and resilient to perturbations, thus the identification and assessment of relevant hazards is an essential prerequisite for system safety. Nevertheless, traditional methods for risk assessment do not take into account interactions between system components and do not adequately address human and organizational factors, thus being not appropriate for complex

systems (Leveson, 2004). Some efforts have been made to include human and organizational factors (Milazzo et al., 2010), while few works attempt to integrate organizational and human factors (HFs) in a dynamic approach. As examples based on Bayesian theory, Kalantarnia et al. (2009) proposed a method for dynamic safety management and Meel & Seider (2006) estimated the dynamic probabilities of accident sequences having different severity levels by using statistical analyses of near-miss and incidents.

In this work, a dynamic approach for addressing uncertainty in risk assessment, based on the evaluation of the state of the system under analysis, is outlined to be applied for those cases when a static assessment method is not trustable. The Bayesian networks are constructed from Fault Trees Analyses (FTA) and failure rates represent a priori probabilities. The modelling provides a set of independent nodes (root elements of FTA, i.e. critical items) and intermediate events for the top event. The network's training is performed by using historical reliability data and accident data series collected from the evidences of KHK reports.

1.3 Case Study - About Hydrogen Fueling Station in Japan

Hydrogen is receiving increasing attention as a future energy carrier in Japan. It is expected that widespread usage of hydrogen energy will result in energy savings, strengthen energy security, and reduce the environmental impact of energy consumption. One of the primary uses for hydrogen at present is in fuel cell vehicles (FCV's). FCVs were introduced into the Japanese market in 2014, and the Government of Japan is planning to have approximately 40,000 FCV's in Japan by 2020 (METI, 2016).The two main safety issues in HRS are: (i) the operating pressure of standard HRS in Japan is substantially high at 82 MPa. (ii) Inherent unsafe characteristics of hydrogen fuel can possible lead to explosion and fire: hydrogen is likely to leak because of its low density, large flammability range, and low minimum ignition energy. Meaning risks are associated with the high-pressure condition in addition to the known hazardous properties of hydrogen. Considering these scenarios, it is inevitably necessary to reduce the risk associated with possible breakdowns in HRSs.

Various projects that focused on introducing FCV and Hydrogen Refueling Station (HRS) have been implemented. One such major project is the Japan Hydrogen & Fuel Cell Demonstration Project (JHFC), which conducted FCV research activities from 2002 to 2010 (JHFC, 2017). For HRS, the "Concurrent Operation of Hydrogen Stations with Different Types of Fuel and Different Methods - The First Demonstration Study in the World" project was implemented with the objective of researching actual efficiency and any problems associated with HRS. In addition to these projects, several laws have been revised to facilitate the implementation of hydrogen energy (METI, 2015). For example, the High Pressure Gas Safety Act was revised to expand the varieties of steel used for facilities such as pipelines, lowering the safety factor for pipelines, and devise rules relevant for liquid HRS. Further, an HRS and a gas station can be installed at the same place according to the Fire Safety Act. The Building Standards Act has also been revised to enable the storage of sufficient hydrogen stock to provide hydrogen in cities. These laws enabled FCVs and HRSs to be introduced and utilized in the market.

Hydrogen refueling stations (HRSs) are a key infrastructure in the fuel supply chain for fuel cell vehicles (FCVs). Several hundreds of stations are planned until 2020 in the worldwide (IEA, 2015). Since pressurized hydrogen is used in FCVs having enough cruising distance, a large amount of pressurized hydrogen is stored at HRS. Thus, there are risks due to pressurized hydrogen at the HRS. When an accident takes place with respect to the high-pressure gas, a notification report shall be submitted to the prefectural governor or police official due to the High Pressure Gas Safety Act (KHK, 2015). Accident information such as hydrogen leakage at an HRS is available in the high-pressure gas incidents database of The High Pressure Gas Safety Institute of Japan (KHK, 2012). This database contains a compilation of high-pressure gas accidents, including the accident information for HRSs. It also provides information on which facility tends to fail and on the accident count through years. Considering the accident statistics of natural gas stations, there are concerns that HRS accidents may increase as more HRSs are implemented in the future.

It is well-known that there is a possibility of abnormal events occurring at an HRS due to increased activities and operations performed at the HRS. As HRSs store and dispense hydrogen at relatively high pressure, they are controlled by the aforementioned Act. The Act defines "accident" as follows:(i)

Explosion, (ii) Fire, (iii) Leak, (iv) Degradation, (v) Others. In legal terms, explosions, fires, spouting or leaks, rupture or damage, and loss or burglary are defined as “accidents” (Yamada et al., 2015).

1.4 Research Challenges and Questions

Based on a thorough literature review of both academic studies and published technical reports by industrial organizations and companies, overall challenges have been divided into three main categories:

I. Challenges regarding Accidental data of HRS: data evaluation, statistical modelling, challenges due to lack of data, improvements, and new developments.

II. Challenges regarding Reliability/failure rate: prediction methods, new environment, new system, using available field data, follow-up in operational phase, continuous improvement, new developments.

III. Challenges regarding human failures and inspection as a threat to reliability: identification of critical components, risk influencing factors, human error quantification, inspection estimation, and optimization.

More specifically, the following specific challenges related to the qualification and reliability assessments have been identified. The above challenges are described in more detail below.

1.4.1 Operational time-based leak/accident data analysis of HRS

One of the ways to analyse hydrogen-based accidents is to collate data from the key Institutions that are responsible to record such accidents data. For example, in Japan, the high-pressure gas institute (KHK) are responsible for recording all minor to major accidents related to LPG, gasoline or hydrogen related technology. The lessons learned from the accidents can be used as prior information to prevent the cause of accident in the future. A further statistical modelling using these data and advanced distributions can provide a better estimation of accidents. The result from the analysis can be used to make decisions improving safety measures across all the installation thereby improving public confidence in the technological systems in Japan. However, in the case of new technological systems such as hydrogen stations, lack of data or inaccurate data can result in accident rate uncertainty. Hence, an appropriate

model is required to understand accident rate uncertainty in the statistical modelling techniques. The first part of the research focuses on two aspects:

i. Leak Frequency Analysis using Bayesian and Frequentist methods (refer to case study 1)
ii. Accident rate uncertainty modelling due to lack of data (refer to case study 2)

1.4.2 Reliability improvement through dynamic modelling of a hydrogen technology system

Risk and reliability quantifications forms a key element in the risk assessment of new technological systems introduced. Reliability is an important factor in the development of hydrogen systems. But several factors influencing the reliability of an equipment, for instance, the environmental conditions will change significantly as time passes (e.g., reduced pressure, changed gas/oil ratio, more produced water, different chemical content). The system must be reliable enough to safeguard the environment, and make the exploitation of the hydrogen processes economically feasible for a rather long period. The numerical risk and reliability figures estimated from risk assessment help the stakeholders make critical decisions concerning the system/process involved. The second part of the research focuses on risk and reliability quantifications. The failure frequency estimation and consequence modelling are the two important measures of risk quantification. The estimation of failure rates provides a key input to QRA quantification. The limitations of current risk assessment/quantification approach are:

- Inability to capture the dynamic behavior of the process operation;
- Inability to update the quantitative results;
- Inability to take account of early into account;
- Significant uncertainty of quantitative estimation;
- No predictive capabilities;
- Utilization of risk assessment in early stage of the process life cycle (design stage not in operational or modification stages).

Reliability analyses and predictions should be performed from the early stages of the product development process. This ensures all necessary factors such as environmental, human factors and other possibilities are taken into account. There are several approaches for predicting reliability. Obtaining a point value for the reliability is not the single purpose of such an analysis. The analysis should help

designers to compare alternative designs, identify potential design weaknesses and give advice on how the design can be improved. Such reliability improvements may be related to physical design changes, establishing requirements and objectives for reliability testing, and so on. An important objective of reliability analysis is, therefore, to provide a decision basis that can be comprehended by design engineers (Lundteigen and Rausand, 2009).

Successful reliability prediction generally requires developing a reliability model of the system considering its structure and later assigning failure data to the model. The level of detail of the model will depend on the level of design detail available at the time. In regards to failure data, prediction of reliability using field data is the most reliable form of data requirement for any industry. However, the hydrogen system being a new technology, there is not much data available. Most of the new hydrogen systems are adapted from similar systems such as gasoline technology. Related equipment reliability information can be collated from OREDA (OREDA, 2009). However, this information cannot be used directly for new hydrogen systems, because their designs have been modified, systems are not alike and there are different environmental stresses and operations. Currently, no practical method is available that can be used to extrapolate the available reliability data from similar and known systems and come up with a failure rate prediction for new hydrogen based systems operating in a different environment. Relevant research questions to address are therefore:

- What kind of reliability modelling and calculation approaches are suitable for new systems?
- How can a more realistic reliability prediction be achieved for new technologies where no field data are available?
- What initial values can be used to predict the preliminary failure rate of new systems?
- How can new failure observations be integrated into the reliability model to predict a more real failure information on the systems?

Focusing on the above limitations and challenges, the second part of this research draws conclusions on how failure rates and failure probability can be controlled in practice. The proposed Bayesian framework (dynamic approach) addresses the above requirements by providing a periodic updating process that allows industry knowledge about failure rates to be incorporated in a prior distribution and

cyclical update of new survival data as it becomes available. The study also demonstrates that the failure rate can vary by a small to large margin based on the life parameter chosen for reliability predictions. Hence, the QRA should be verified to select correct life parameter depending on the actual usage conditions. Based on this theory the second part of the research focuses on two aspects:

i. QRA Parameter Verification analysis (refer to case study 3)
ii. Improvement in reliability quantification - dynamic approach (refer to case study 4)

1.4.3 Integrating Human Factors and Risk based Inspection into New Technology systems

The third part (last part) of the research focuses on other risk analysis limitations such as human factors and risk based inspection assessment. This is because human factors and inspection requirements have a vital role in the overall risk analysis. They form a major part of the preventive/mitigate measures. On the negative side, human factors are accounted to be the major contributor to accidents. Under such circumstances, human reliability analysis for new technological systems should be prioritized in advance. Another important assessment i.e. risk based inspection model is an important integral part of the plant maintenance which needs to be continuously monitored from safety, reliability and availability point of view. New technological system identifies the requirement to maintain the equipment and components in terms of reliability and availability aspects through preventive maintenance. Based on this theory the third part of the research focuses on two aspects:

i. Risk-based inspection (RBI) methodology to decide inspection time in relation to the risks (refer to case study 5)
ii. Human error critical task assessment on HRS (refer to case study 6)

To summarize - accident rate, failure frequency, inspection time and human error assessment are some of the important measures of risk and reliability quantification. However, there are uncertainties associated within these areas that lead to small to large uncertainties in overall risk assessment. Risk quantifications involve many uncertainties, and assessing probabilities to represent these uncertainties is itself a complex task utilizing a variety of information sources. At a practical level, uncertainties are driven by three important modelling issues i.e. accident, failure probability and human factor. The

current modelling issues are related to model structuring, probability assessment, information gathering, and sensitivity analysis. The doctoral research is focused on addressing uncertainty in these areas of risk and reliability quantifications to support risk assessment.

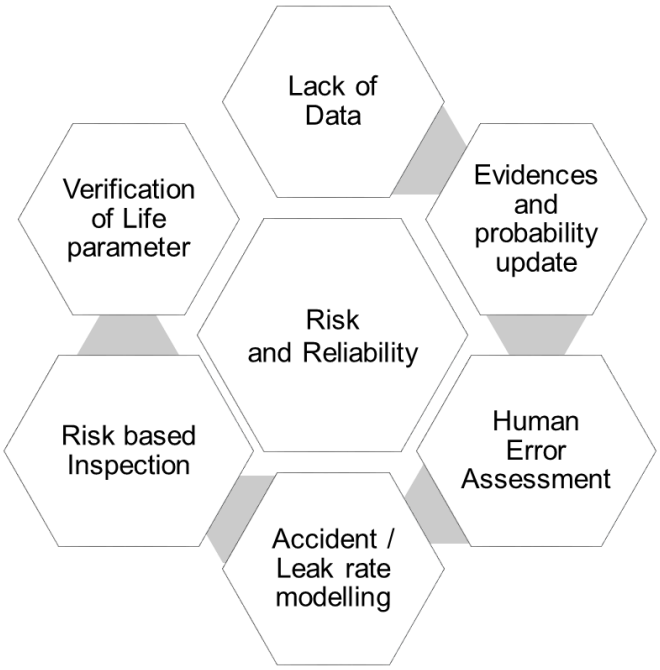


Figure 2. Uncertain risk areas for application of bayesian technique

In most of the cases, hydrogen-refueling station is selected as a base application for illustrative purpose. However, it should be noted that the theme of the research is focused on process industry (i.e. .oil and gas, power plants) and hence the work presented should be viewed from a broader sense, not just limiting to hydrogen technology/system. The research is divided into 6 main areas of research associated with the risk assessment of technological systems. All these areas are carefully selected looking at the current industry related issues faced by the process industry. Some of the current issues are already addressed in this section. The six main areas of this research are as follows:

① Accident Modelling and Inspection Interval forecast

② Accident rate data uncertainty analysis

③ Verification of appropriate life parameters in risk and reliability quantifications

④ Improvement in reliability quantification to support BS EN 61511 failure probability analysis

⑤ Risk Based Inspection Model for Hydrogen Storage Process using Bayesian Network

⑥ Human Factor Modelling using advanced probabilistic models

The above areas address uncertainties related to one or the other parts of risk assessment (QRA). Reducing or improving uncertainties in the above fields will more or less reduce uncertainties in the risk assessment thereby improving its quality and accuracy. Broadly speaking, there are uncertainties associated with several areas related to risk and reliability quantifications. These areas include Accident analysis, failure probability analysis and QRA verification. The three key areas are described in brief in the next part. This research focuses on uncertainty areas within risk assessment that needs some uncertainty modelling to improve the risk assessment process.

Table 3. Key Aspects of New Technology Risk and Reliability Case Analysis

Case Analysis			
Accident Analysis & Risk & Reliability Quantifications	Accident Analysis	Case Study 1	Accident/Leak rate estimation using statistical interpretation
		Case Study 2	Accident rate uncertainty modelling due to lack of data
			Inspection Interval forecasts based on accident estimation
	Failure Probability Analysis	Case Study 3	QRA Verification analysis (parameter verification)
		Case Study 4	Improvement in reliability quantification (dynamic approach)
	Task-based Risk analysis	Case Study 5	Risk Based Inspection Model for Hydrogen Storage Process using Bayesian Network
		Case Study 6	Human Reliability Analysis (probabilistic graphical model)

The Ph.D thesis addresses all the key aspects and suggests new analytical methods to overcome uncertainties associated with risk and reliability quantifications that mainly can be used by academic researchers, reliability analysts, design and end users in risk assessment.

1.5 Objectives

The main objective of this thesis is:

"To develop systematic approaches that contribute to uncertainties in the risk and reliability quantifications of new technology system using dynamic bayesian assessment"

In the initial phase, a general concept on risk and safety is discussed. This includes review of risk, change in risk term through recent development rends, accident analysis and safety classification of new technology system such as hydrogen energy system. In the second phase, the research focuses on risk and safety modelling methods by assessing their uncertainties. This involves identification of gaps in the existing risk and reliability quantifications and providing solutions to overcome them. The

concept of the research primarily aims at addressing uncertainties in risk and accident modelling by using dynamic bayesian based assessment.

Some fundamental studies such as review of the state of the art risk and reliability assessment related work, verification of risk assessment or QRA will be addressed to ensure that the uncertainties identified are treated during the assessment. The outcome of this thesis will help users to overcome uncertainties by taking into account all necessary parameters in the quantifications. This will allow higher confidence in the result and improve process safety related decisions made based on the results.

Based on the main objective and the research challenges, the more specific objectives are:

- Statistical interpretation of data and use of advanced frequency based models for leak data analysis.
- Propose a model for lack of accident data uncertainty and its treatment.
- Verification of risk and reliability quantifications using Aging/Life parameter method.
- Improvement in risk and reliability quantification using Bayesian update process.
- Propose a risk based inspection methodology to avoid under and over estimation of inspection times for hydrogen storage process.
- Propose a methodology to analyse liquid hydrogen leak incidents in the fueling station with respect to human factors as the root causes.

The above objectives will be individually addressed in Part II of the thesis.

Case analysis 1 proposes leak rate estimation using time based evaluation methods that utilize historical HRS accident information. In addition, leak frequency estimates from the other two methods i.e. non-parametric based and leak hole-size based were examined. In non-parametric approach, the leak frequency is estimated based on Bayesian update. Thereafter, a comparison of these three approaches were made to understand the trend of leak rate data.

Case analysis 2 discusses the accident data uncertainty has not been so well-established, partly due to low probabilities involved and partly due to the complexity of such accidents (Threadgold, 2011). For this purpose, we have introduced a study on the accident data uncertainty based on time correlation model. This article estimates the uncertainty and accident rate by time correlation model that is

fundamental to the challenge of lack of data. This new way of dealing with and interpreting accident information can be utilized to evaluate new systems such as HRS in the future.

Case analysis 3 discusses verification of appropriate parameters in failure estimation and its influence on the reliability assessment to offset the limitations associated with data scarcity and QRA uncertainty problems. The selection of the appropriate parameter in reliability assessment can be one of the possible ways to verify and validate the accuracy of QRA results. Accordingly, the objectives of this paper are as follows:

i. To estimate the failure rate based on the number of fillings and survival time of HRS.
ii. To employ a non-parametric approach to estimate cumulative failure as a function of the number of fillings.
iii. To use a parametric approach to estimate cumulative failure as a function of survival time.
iv. To compare both parameters to choose correct life parameter for reliability quantification.

Case analysis 4 draws conclusions on how failure rates and failure probability can be controlled in practice. New technology, such as hydrogen failure data has serious challenges with extremely limited failure data. One possible way is to use surrogate failure data from other settings such as commercial nuclear power plants, chemical plants, and offshore oil and natural gas platforms. This article proposes Bayesian framework that addresses the requirements by allowing industry knowledge about failure rates to be incorporated in a prior gamma distribution and periodic updating process with new survival data as it becomes available. Monte Carlo simulation is adopted which makes it practical to solve uncertainty in the failure rate estimation and update these models with many trials in seconds.

In case analysis 5, a probabilistic graphical model, based on an acceptable level of risk, is proposed to avoid under and over estimation of inspection time interval. It presents an advanced risk-based inspection (RBI) methodology to optimize inspection time in relation to the risks. Bayesian Network (BN) is applied to model the risk and the associated uncertainty.

Case analysis 6 discusses about human factor analysis in liquid hydrogen leak incident using probabilistic graphical model. It proposes a methodology in order to analyse liquid hydrogen leak

(transfer leak) incidents in the refueling station with respect to human factors as the root cause. A semi-quantitative graphical method of human factor analysis for the refueling station liquid hydrogen releases helps to prioritise the causes that need to be analyzed first and/or in the greatest level of detail, based upon the degree of anticipated risk that they pose.

1.6 Outline of the thesis

This thesis has two main parts:

- **Part I Core Concept**: Part I focuses on general concept of risk and reliability, accident analysis, safety classification of new technology (hydrogen) system. This part presents the background, the challenges and research questions, literature review as well as the objectives and the scope of this thesis, and then proceeds to a discussion of the research methodology and approach. Finally, the main results are summarized and the possible areas for future research are indicated.
- **Part II Case Analysis**: Part II is concerned about various technical safety and risk uncertainties and adopts modelling techniques to reduce the uncertainties. This part includes six case studies published or prepared during the thesis. These analysis consist of the main work and achievements.

Part I Core Concept will be presented in the form of sections addressing current problems and research review related to risk and reliability quantifications in the process industry. Part I of the thesis will comprise of 6 sections in total. Section 1 focuses on the concept of risk and accident modelling is detailed in this chapter. It provides research background, concept, motivation, objectives. Chapter 2 outlines current research areas with shortcomings (problem statement). Chapter 3 outlines literature reviews with detailing information about the research study associated with this research theme (refer to Fig.2). Chapter 4 explains the research concept, design and framework. Chapter 5 presents contributions based on the results and discussions made. Chapter 6 lists the references.

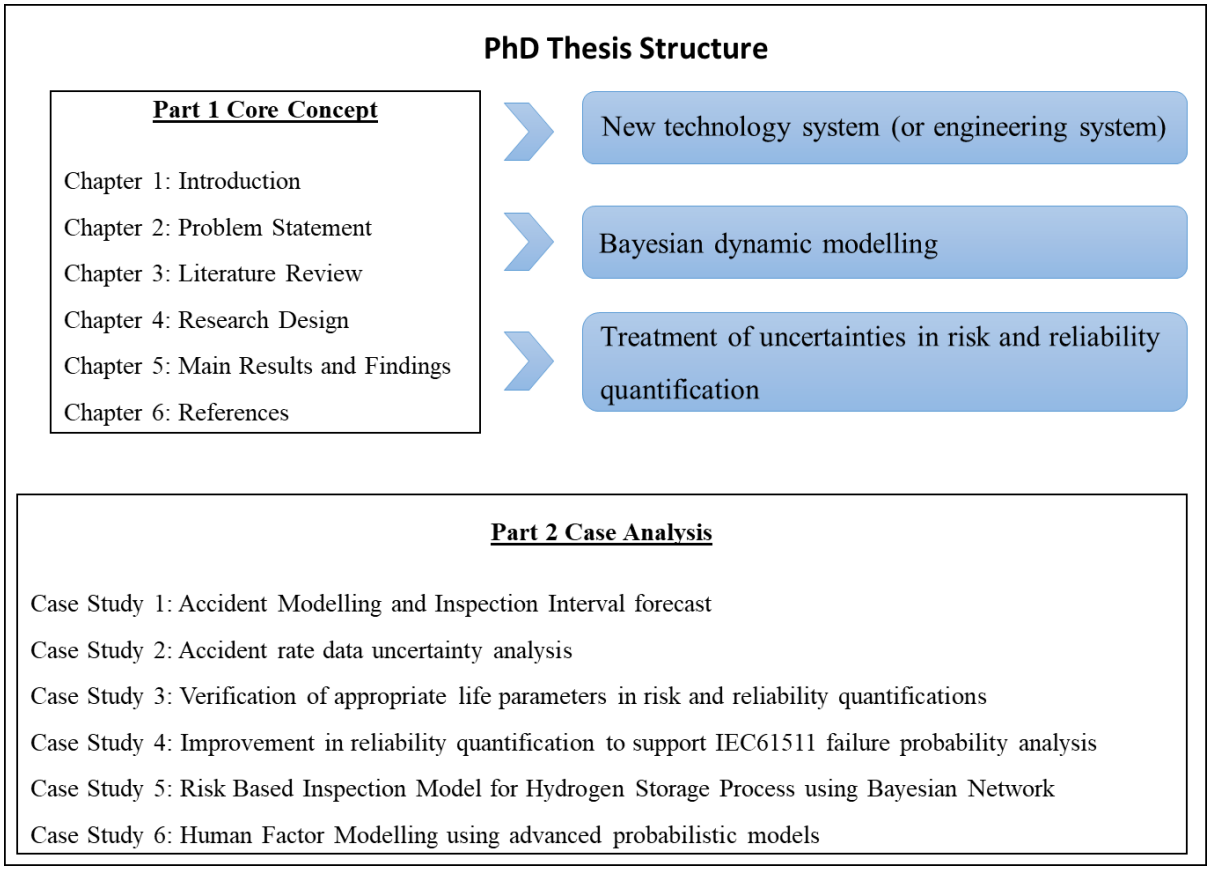


Figure 2. Structure of the thesis

Part II Case analysis consists of six case studies. Case study 1 presents leak frequency analysis for HRS using frequency-based risk evaluation methods. Case study 2 presents evaluating uncertainty in accident rate estimation at HRS using time correlation model. Case study 3 addresses verification of life parameters in risk and reliability quantifications of process hazards. Case study 4 addresses improvement in reliability quantification to support BS EN 61511 failure probability analysis. Case study 5 proposes risk based inspection model for hydrogen storage process using bayesian network. Case study 6 addresses human factor analysis for liquid hydrogen leak incident using probabilistic graphical model.

2. PROBLEM STATEMENT

The main purpose of the thesis is to address specific issues related to risk and reliability quantifications. In total, six key issues related to the existing risk quantification approach have been identified and listed down in this section. The Ph.D. thesis will be presented in the form of case analysis addressing problems related to risk and reliability quantifications in the process industry. The problems related to risk and reliability in the process sector are listed below with solutions in detail in Part II Case study 1-6.

- **Problem Statement 1:** Leak frequency Analysis and Unrevealed leak time estimation

Leak frequency analysis is a method of understanding the characteristics of risks at HRSs. However, hydrogen failure data for leak frequency is extremely limited. Additionally, the unrevealed leak time is an important function of the leak frequency. Unrevealed leak time can reveal key safety characteristics for hydrogen sensor to detect leak.

Solution: To address the above issue, a leak rate estimation using time-based evaluation methods is developed that utilize historical HRS accident information. In addition, leak frequency estimates from another two methods (non-parametric and leak-hole-size) were examined. In the non-parametric approach, the leak frequency is estimated based on a Bayesian update. The three approaches were compared to understand the trend of leak rate data. For more details on this subject, refer to Part II – Case study 1.

- **Problem Statement 2:** Accident Rate Uncertainty Evaluation due to lack of data

Collecting data about accidents in the past will provide a hint to understand the trend in the possibility of accidents occurrence by identifying its operation time. However, in new technology; accident rate estimation can have a high degree of uncertainty due to absence of major accident direct data in the late operational period. The uncertainty in the estimation is proportional to the data unavailability, which increases over long operation period due to decrease in number of stations.

Solution: To address this issue, a suitable time correlation model is adopted in the estimation to reflect lack (due to the limited operation period of HRS) or abundance of accident data. For more details on this subject, refer to Part II - Case study 2.

- **Problem Statement 3:** Verification of QRA through selection of appropriate life parameter

It is critically important to use the parameter for accurate reliability estimation. The standard "time" parameter can be non-suitable sometimes in the sense that it does not represent the actual usage conditions. This can lead to large uncertainty in the risk and reliability quantifications. This recognizes a need for collecting sufficient and improved reliability parameter for new technology systems

Solution: Selection of the appropriate parameter in reliability assessment can be one of the possible ways to offset the problem with data scarcity or QRA uncertainty problems. A non-parametric approach is established to provide verification of appropriate parameter in failure estimation and its influence on the reliability assessment. For more details on this subject, refer to Part II - Case study 3.

- **Problem Statement 4:** Failure data uncertainty in reliability quantification

The international standard for functional safety BS EN 61511 specifies the usage of credible, realistic failure rate data in failure probability analysis and requires that operational data be monitored against design data. However, in reality, these requirements have proven difficult for operators because of the lack of failure data records and a large amount of sample data required for traditional frequentist methods. Lack of failure data leads to uncertainty in risk and reliability quantifications making risk assessment decisions weak.

Solution: The proposed Bayesian framework addresses the requirements by providing a cyclical updating process that allows industry knowledge about failure rates to be incorporated in a prior distribution and cyclical updated with new data as it becomes available. Uncertainty analysis is performed on failure rate (PFD calculation) using Monte Carlo simulation. For more details on this subject, refer to Part II - Case study 4.

- **Problem Statement 5:** Risk based Inspection Model using Bayesian Network

Inspection Interval has not been addressed for hydrogen-based technology due to limited data. Adequate inspection is mandatory at regular intervals to ensure safe operations involving hazardous chemicals such as hydrogen. An appropriate inspection routine will also increase the chance of authority's approval and public acceptance which is a pre-requisite for successful implementation and operation of new technology systems such as hydrogen stations

Solution: To develop risk based inspection model by implementing a BN analysis. Risk level is calculated via BN considering the failure probabilities (Pf) and the possible consequences. The maintenance plan is determined after setting the evidence that the system operates at the lowest possible risk using BN and Influence Diagram. For more details on this subject, refer to Part II - Case study 5.

- **Problem Statement 6:** Human factor Modelling using probabilistic graphical model

The accident analysis at refueling stations shows that several factors that influence the initiating cause lead to flammable material (fuel) release. One of the evaluations recorded in the High Pressure Gas Safety Act (Japan) in terms of accident causes shows that human factor is one of the key causes for accidents in Japan. Human factors is an area which has not received as much attention as it deserves. This shows the need for a strategy to understand areas of improvement in the field of human factors to help prevent accidents.

Solution: To develop a methodology to analyse a liquid hydrogen transfer leak incident in the refueling station with respect to human factors as root causes. For more details on this subject, refer to Part II - Case study 6.

2.1 Critical points of research

- Propose a model for lack of data uncertainty and its treatment.
- Statistical interpretation of data and use advanced frequency based models for accident and failure data analysis.
- Develop quantitative insights in the study to set performance standards for availability and reliability in operation and maintenance of the Hydrogen stations.
- Verification of risk and reliability quantifications using Aging/Life parameter method.
- Improvement in risk and reliability quantification using Bayesian update process.
- Propose a risk based inspection methodology to avoid under and over estimation of inspection times for hydrogen storage process.

3. LITERATURE REVIEW

This section represents the literature survey for all the studies undertaken as a part of this research. This involves risk assessment and its uncertainties, accident analysis and various safety and risk modelling techniques implemented on the technology systems such as hydrogen stations. The overall research related papers that are referred and reviewed are described in this section.

The initial research activity involves thorough review of the literatures and developed research questions. The literature review extend across the body of journals, abstracts, references, published reports and recommended practices by industry, and within the scope of reliability qualification, hydrogen systems, and other relevant subjects. It is necessary that existing sources of evidence, especially systematic reviews, are considered carefully prior to undertaking research. Review of literature, ongoing research and development (R&D) reports, and industry practices are carried out in order to obtain enough knowledge about the state of the art both in the scientific and the practical point of view. In addition, the professional experience from my academic supervisor has contributed valuable input in the identification and solution of problems.

To begin with, in regards to hydrogen based technology, academic studies are inadequate, and the development of the existing approaches has mainly been done by institutes and industry organizations. Risk assessment of hydrogen fueling stations have been reported by several researchers, however most of the researchers focus on traditional risk analysis for hydrogen-based technology due to the ease of use and verified models available for quantification. These existing literature surveys provide a starting point for the research and support for all the further activities. In this section, firstly the concept of risk with recent development trends will be discussed, followed by the literature review associated with traditional risk assessment for hydrogen based technology and finally the treatment of uncertainties in risk assessment and dynamic modelling will be discussed.

The risk concept has many definitions in the scientific risk fields. Quite many definitions can be found in journals for e.g. Wood (1964), Crowe and Horn (1967), DFI (2007), Aven and Renn (2009) and Aven

et al. (2011), but there are many more. Against this history, we introduce a new risk concept for new technology system that adheres to the International Organization for Standardization's latest risk management standards, ISO 31000. In that it defines risk as "the effect of uncertainty". According to this meaning, risk refers to positive as well as negative effects of uncertainty. We believe that defining risk for new technology system should explore social science as well as engineering perspectives. Whereas existing conceptual limit their scope to safety and risk assessments for specific technological innovations, comprehensive social risk additionally focuses on the social implementation of the innovation, and emphasizes shared decision-making among the stakeholders (such as people, businesses, and public authorities). Under this conceptual model, risk analysis and evaluation follow the principle of living with risk. According to this principle, something that generates risk generates value too. For example, if a risk is scaled at 0, the accompanying benefit is 0 too; thus, the parties must selectively adopt a certain level of risk to gain any benefits.

The initial safety studies on hydrogen energy system can be conducted using traditional risk identification approaches. Various safety related studies such as HAZOP, FMEA, etc. have been conducted on the HRS to ensure the risk is acceptable for its use and operation. Nakayama et al. (2016) carried out the preliminary hazard identification to a hybrid gasoline-hydrogen fueling station with an on-site hydrogen production system using organic chemical hydride. Jones (1984) applied hazard and operability study (HAZOP) to liquid hydrogen fueling station. It is important to identify and select representative credible accident scenarios for further investigation (Markowski and Siuta, 2017). CEC (2004) reported the failure mode and effects analysis (FMEA) for hydrogen fueling systems to the California Energy Commission. Kikukawa et al. (2009) performed the FMEA and HAZOP to identify possible accident scenarios for liquid hydrogen fueling stations. Pasman and Rogers (2012) performed risk assessment for compressed and liquefied hydrogen transportation and tank station by means of Bayesian networks. LaChance (2009) performed QRA to determine separation distances for HRSs. Matthijsen and Kooi (2006) performed a quantitative risk assessment (QRA) of hydrogen filling stations with the generic data taken from references (Redbook, 1997). Tsunemi et al. (2017) estimated the consequence and damage caused by an organic hydride HRS numerically.

In addition to traditional methods, some advanced probabilistic models have been employed for hydrogen energy system by some researchers to quantify the risks. For example, Khalil (2018) provided a science-based framework for ensuring a safe use of hydrogen as an energy carrier and an emission-free transportation fuel. Khalil (2017) employed state-of-the-art visual flowcharting methodology is employed to develop a probabilistic model to quantify occupational risks of fire and explosion events initiated by leaks that ignite within enclosed spaces. The author demonstrated the functionality of his proposed model by a hydrogen refuelling station (HRS) case study in which gaseous hydrogen is postulated to leak from its compressor system.

Accident modelling is an important area addressed in this thesis. In the high pressure gas safety act law, explosions, fires, spouting or leak, rupture or damage, and loss or burglary are defined as "accidents" (KHK, 2015; Yamada, 2015). For example, a small leakage (i.e. leak area is 0.01 % of total flow area) at an HRS is recognized as an accident and needs to be reported. In the case of hydrogen fuel, even a small leak in a confined space can potentially lead to a catastrophic event. Most accidents at HRSs are due to hydrogen leaks. In fact, almost all accidents at HRSs reported in the database are hydrogen leaks (KHK, 2012). In this case, the accident rate can be considered to be almost equivalent to the leak rate. In this study, the "leakage or leak rate" refers to an "accident", as defined in the High Pressure Gas Safety Act. Thus, in the latter part of the thesis, it is noted that accident and leak estimation is treated as equal entity.

Hydrogen energy systems are vulnerable to devastating accidents because they deal with hazardous substances at high pressure and/or temperature. Based on the new technology system categorization, hydrogen can be characterized as complex systems where a low probability high consequence event makes it likely that an accident in a given site causes loss in neighboring facilities, leading to a sequence of accidents (Khan and Abbasi, 1998). So, the adoption of safety measures followed by a comprehensive social risk assessment is crucial to maintain the risk level within the acceptance criteria. Risk assessment methodologies such as quantitative risk analysis (QRA), probabilistic safety analysis (PSA), and optimal risk analysis (ORA) comprise different steps among which accident scenario analysis is a

common task. Accident scenario analysis includes accident sequence modelling and consequence assessment (Khan, 2001).

A review of accident scenario analysis was carried out in the initial phase of the research. Several methodologies have been used for accident scenario analysis, each of which benefits from different techniques. For example, Sklet (2006) used barrier block diagrams to investigate hydrocarbon release accidents on offshore platforms. Delvosalle et al. (2005) used the bow-tie (BT) technique in ARAMIS project to identify major and reference accident scenarios in process plants. However, it is difficult to find a single technique to completely capture different phases of an accident from the beginning to the end, and also being flexible enough to fit a variety of accidents. Nivolianitou et al. (2004) made a comparison between some selected techniques such as fault trees, event trees, and Petri nets for accident investigation, considering criteria such as event sequence, event dependency, and modelling assumptions. There are also other relevant works in the literature such as that of Khan and Abbasi (1998), and Sklet (2004), devoted to qualitative comparison among different techniques.

Minor leakages of hydrogen are the common types of accidents and incidents in the hydrogen stations. However, some have led to serious consequences such as fire (Sakamoto et al., 2016). The risks involved in two types of hydrogen fueling stations were identified using a hazard identification (HAZID) study (Nakayama et al. 2016). The leakage of hydrogen due to an accident is important for the consequence analysis. Many studies focus on the hydrogen release behavior (Tanaka et al., 2007, Kessler et al., 2014, Yamada et al., 2015). It is necessary to evaluate the maximum amount of hydrogen released from each facility to conduct the consequence analysis of the worst-case scenario for which the consequence is the highest. The risk assessment based on the maximum amount of hydrogen released was conducted (Takano et al., 2007, Tanaka et al., 2007, Kessler et al., 2014). Although the risk assessments of each component, such as pipes and accumulators, have been conducted, quantitative risk assessments considering the entire hydrogen fueling station are lacking. For example, if multiple safety measures in a hydrogen fueling station fail simultaneously, it could lead to serious accidents (Sakamoto et al., 2018).

With reference to hydrogen accidents, accident and leak modelling of HRS have been reported by several researchers. A comprehensive safety analysis of hydrogen plants in oil refineries was carried out by Mohammadfam and Zarei, (2015) to determine risks that may lead to catastrophic accidents. Some advanced probabilistic models were employed by some researchers to quantify risks caused by leaks. Khalil, (2017) employed state-of-the-art visual flowcharting methodology to develop a probabilistic model to quantify occupational risks of fire and explosion events initiated by leaks that ignite within enclosed spaces. The author demonstrated the functionality of his proposed model by a HRS case study in which gaseous hydrogen is postulated to leak from its compressor system. This Ph.D thesis proposes leak rate estimation using time-based evaluation methods that utilize historical HRS accident information. In addition, leak frequency estimates from another two methods (non-parametric and leak-hole-size) will be examined. In the non-parametric approach, the leak frequency is estimated based on a Bayesian update. The three approaches will then be compared to understand the trend of leak rate data. The quantitative insights of this study can be used to set performance standards for the availability and reliability in the operation and maintenance of HRSs.

The application of various existing techniques for accident modelling is restricted due to scarce data. The issue of scarce data is modelled using a precursor data and hierarchical Bayesian methodology (Yang et. al., 2013, Gheriani et. al., 2017). However, it is found that the accident data based on actual conditions are rare and not realistic. This could add uncertainty in the overall risk estimation. Thus, compared to the risk analysis, the accident data uncertainty has not been so well-established, partly due to low probabilities involved and partly due to the complexity of such accidents. For this purpose, we have introduced a study on the accident data uncertainty based on time correlation model (refer to case study 2). It estimates the uncertainty and accident rate by time correlation model that are fundamental to the challenge of lack of data and not been addressed in previous models. Another key characteristic is to estimate accident rate based on statistical interpretation. This methods reflects latest data from key sources and updates the model to get real time data. Accident rate estimation reveals the trend of accident occurrence in the hydrogen system which can be crucial in making critical decisions.

Apart from the accident modelling, quantification of risk numerically require use of quantitative risk assessment (QRA). The verification and validation of QRA has become a great concern to public acceptance of HRSs. The validity of QRA was reviewed by Goerlandt et al. (2016). Generic validity approaches such as benchmark tests have been proposed, but it was pointed out that an evidence-based approach is needed to support the validity of QRA results. One of the ways to justify verification is to select appropriate reliability (life) parameter in safety and reliability engineering. The life parameter should represent actual conditions of the product or equipment under analysis. This requires selection of some life parameter other than the traditional mean time to failure (MTTF) approach.

In QRA, risks are calculated from frequencies of scenarios and their consequences. Estimation of failure rates provides a key input to QRA quantification. Unfortunately, QRA methods contain a large amount of uncertainty due to the lack of field failure data. This recognizes a need for collecting sufficient and improved reliability data for new technology systems (Rademaeker et al. 2014). Casamirra et al. (2009) used the fault tree analysis (FTA) to determine the frequency of the accident scenarios based on generic failure data. However, as most of the traditional risk analysis techniques (such as Fault Tree Analysis (FTA) and Event Tree Analysis (ETA)) are static and non-updatable conventional models, they regularly fail to fully capture the variation of risks during operation (Paltrinieri and Khan, 2016). Besides, conventional techniques use only binary variables and do not represent conditional dependencies (Martins et al., 2014). Another way is to employ a Bayesian statistical approach to estimate failure rate from prior data. LaChance et al. (2009) developed a Bayesian model to estimate leak frequency of various components used in a HRS. Pörn (1996) proposed a "two-stage" update of the hierarchical Bayesian process, although the procedure format is quite different since it preceded the widespread availability of computerized Bayesian algorithms. Newer methods for treatments of hierarchical Bayes are covered by Droguett et al. (2006). Hierarchical Bayesian models may also be viewed as a special case of a Bayesian Belief Networks. Khakzad and Reniers (2015) proposed a Bayesian network (BN) methodology to estimate both on-site and off-site risks posed by major accidents in chemical plants.

Recently, in the latest 2nd edition of IEC 61511, International functional safety standard specifies use of realistic and credible failure data in failure probability analysis. Unfortunately, new technology, such as hydrogen failure data is extremely limited. One possible way is to use surrogate failure data from other settings such as commercial nuclear power plants, chemical plants, and offshore oil and natural gas platforms. The proposed Bayesian framework in this Ph.D thesis addresses the requirements by allowing industry knowledge about failure rates to be incorporated in a prior gamma distribution and periodic updating process with new survival data as it becomes available. Monte Carlo simulation is adopted which make it practical to solve uncertainty in the failure rate estimation and update these models with many trials in seconds. The result shows that the process of updating failure rate with more samples of new observations and modelling failure data uncertainty using Monte Carlo simulation can be effective in improving reliability quantifications in the existing BS EN 61511 standard.

Meanwhile, from the operation and maintenance point of view, inspection interval is one area that is of utmost importance to prevent failures and not addressed in any research papers. Effective inspection can influence major accident risk. Routine Inspection is a key means to improve and maintain the integrity of HRS. Lack of inspection or erroneous maintenance may cause a sudden or gradual deterioration into a system failure. The literature on the definition of inspection in different applications is vast. (Bhandari et al., 2015; Garg and Deshmukh, 2006) defines inspection as all the appropriate actions for retaining an item or a part of an equipment and restoring it to a given condition. A more recent type of inspection is risk-based inspection (RBI) which integrates reliability with safety and environmental issues and minimizes the probability of system failure and its consequences related to safety, economic, and environment (Khan and Haddara, 2003). As the data set using for failure rate calculations through the condition based maintenance (CBM) approaches are mostly limited, RBI have been considered as a complement of CBM through the different operational conditions (BahooToroody et al., 2019; Abaei et al., 2018). RBI can be adopted to assure the level of risk and its associated cost. The base principle of this technique is to prioritize the maintenance of the components based on the level of risk. Accordingly, based on BN, Abbassi et al. (2016) presented an RBI methodology, applied

to an offshore process facility. In order to address the above issues, an advanced RBI methodology is proposed in this Ph.D thesis to decide inspection time in relation to the risks.

In terms of accident causes, the record shows that out of 429 accidents in the year 2015, inadequate facility maintenance and management was the cause for 203 (47%) accidents, inadequate facility design and fabrication defects was the cause for 87 (20%) accidents, and 46 (11%) were caused by human factors, together contributing to 78% of the total accidents. Some studies reveal that organizational and human factors account for a considerable proportion of process accidents (Sakamoto et al., 2016; Karuiki, 2007) In addition, existing studies report that the leakage at joints in the dispenser is mainly due to human error (Sakamoto et al., 2016) With regard to leakage from flexible hose and valve, the cause of all the accidents in US is human error. For the same category, human error and natural disaster are the leading causes in Japan.

The risk associated with the refueling stations could change the perception of people towards accepting hydrogen as a fuel for fuel cell vehicles. Similarly, the process industry has faced some catastrophic incidents that are mostly attributed to human factors (Karuiki, 2007). The past study from UK HSE shows that human factors have contributed to several major accidents such as Piper Alpha, BP Texas refinery, etc. (HSE, 1999; Manca 2012). At the broadest level of categorization, 47% of the identified accidents involved human error in one form or another (Bradley, 1999). Past studies show that more importance is given to technical aspects of systems in order to reduce the possibility of release (Leva, 2015). In spite of improvement in the performance of technical systems, it has been noted that accidents are on the rise. Thus, the technology has reached to point where the improved safety can only be achieved through a better understanding of human error mechanisms (Yamada et al., 2015; Leva et al., 2015).

4. RESEARCH DESIGN

This section considers the aspects of the research design process that were applied during this research project, including the research method, and the selected research approach.

4.1 Research Approach

The research performed in this thesis is mainly on the development of new frameworks and methods for fulfilling the current risk and reliability quantification needs, and forming the basis for further research and aiming to meet the dynamic needs of the future. Many of the scientific studies in the field of reliability and safety engineering are related to the development of models, methods, and frameworks for reliability and safety analysis. As this research focuses on process industries or hydrogen system, it aims to develop new frameworks and methods meant for practical applications in this industry. The new models, frameworks, and methods have been developed based on the existing literature within qualification and reliability assessment.

In this context, verification and validation are not often possible due to a wide range of unsolved issues. From a classical point of view, the usefulness of models should be empirically verified, for example, by experiments or by collecting field data (Goerlandt et al., 2016). Empirical verification may be impossible in the reliability and safety-engineering field, where we deal with analyzing and modelling of unexpected events such as failures, accidents and catastrophes. These events occur infrequently. It is very costly and time-consuming to carry out experiments and collect data to confirm the models and modelling results. Thus, the evaluation and verification of the scientific work and the models must be done by approaches other than empirical or experimental methods.

Many of the scientific studies in the field of reliability and safety engineering are related to the development of models, methods, and frameworks for reliability and safety analysis. As this research focuses on hydrogen energy or a new technology system, it aims to develop new frameworks and methods meant for practical applications in this industry. The new models, frameworks, and methods have been developed based on the existing literature within risk and reliability assessment.

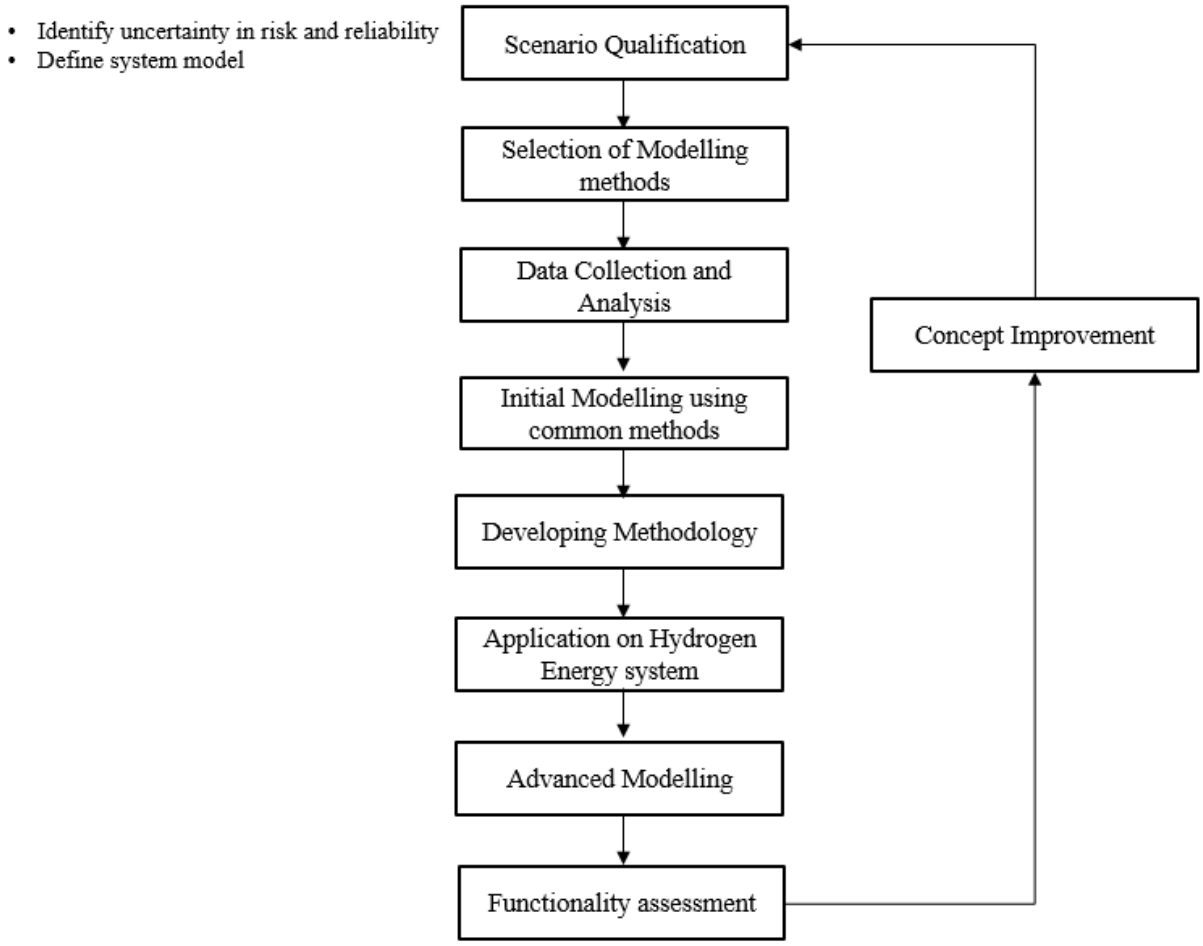


Figure 3. Research basic process flow

The research will comprise of all the steps shown in Fig.3 in the process. Firstly, the uncertainty scenario should be defined. Suitable methods must be selected to ensure that all potential risk uncertainties are identified and addressed in a satisfactory manner so that the uncertainties of failure are documented and the reliability of the product can be proven. The research makes use of some commonly applied methods such as Weibull, failure probability and fault tree analysis. A simple and creative methodology should be defined to introduce a systematic examination of the process. Once the initial statistical or probability modelling is conducted using basic methods, the final modelling uses an advanced Bayesian approach to assess the dynamic behavior of risk. The dynamic assessment of risks can reduce many problems associated with uncertainties in the risks.

The reliability prediction methods adopted in this research is classified into three categories: (1) statistical distribution methods, (2) physics-of-failure methods, and (3) top-down similarity analysis

methods based on an external failure database combined with Fault tree or Probabilistic Graphical method. The first and third category is based on statistical analysis of failure data, while the second category is based on physics-of-failure models. Case study 1 and 2 of the research will utilize statistical methods, case study 3 will be based on physics-of-failure methods, while case study 4 and 5 will utilize external failure database combined with Bayesian. In the past, Foucher et al. (2002) compare these methods and conclude that the best prediction is achieved by a combination of different methods, depending on the phase of the system's lifecycle and objectives and assumptions of the manufacturer.

4.2 Research Framework

The research framework forms the foundation of the research concept. It is very important to develop a solid framework in order to execute the proposed strategy. The modelling is divided into two main categories i.e. initial modelling and Final (advanced modelling). The initial modelling relies on input data gathered from several sources. Some data cannot be directly applied to the model and thus require some form of refinement or conversion to make it suitable for advanced analysis. Initial modelling purpose is to convert or develop data in a format suitable for advanced analysis. There are general methods adopted to perform initial modelling. As explained in previous section, the general methods used for initial modelling care categorized as (1) statistical distribution methods, (2) physics-of-failure methods, and (3) top-down similarity analysis methods based on an external failure database combined with Bayesian.

1. Statistical distribution method:

The important thing to note is that there are several problems associated with the prior data. For e.g.

- There are some months with no accident and the operation period is different for each HRS.
- Stations with different operation period i.e. uncertainty associated with data over operation period.
- Extremely limited data.

Using the prior (input) data, the accident or failure rate for each month is estimated using statistical modelling. The statistical modelling can

- Estimate accident rate for each month by the condition that the adjacent accident rate is similar to each other.

- Estimate uncertainty associated with data over operation period.

2. Physics-of-failure method:

Usually, time is a common parameter of reliability measurement. The reliability can also be measured using actual loading or plant conditions. The initial data can be available in various units of measurement and risk analysts should make a reasonable judgement on which risk metric is more realistic. This method adopts a non-time parameter to measure reliability. In this research, the number of filling parameter is used as a life parameter to measure reliability based on two conditions i.e. usage and physics of failure.

Physics of Failure:

- Main Leakage (Internal & External) is the failure mode under consideration
- Corrosion leakage is due to wear and tear
- Seal wear and tear is proportional to number of fillings

Usage:

- The number of fillings on an average is to be considered
- The public access to hydrogen station is mainly only to the dispenser. Hence, the hose connection, improper joints and supply of hydrogen fuel is the actual usage condition of the hydrogen station.

3. Top-down similarity analysis method:

Equipment's reliability prediction is well established and is often based on the parts count and operating experiences. This is particularly true in the case of oil and gas industry that has maintained failure and maintenance database from various external sources. Initial failure data for critical components are collated from industry external sources i.e. SINTEF, OREDA, etc. The data presents critical failure rate, repair time and failure probability. It is worth noting that in the external sources, the MTTF of each component is collated from various operational experiences and industry experts (SINTEF, 2015). This method applies external failure database to top down approaches such as fault tree or probabilistic graphical method to analyse failures, starting with a potential undesirable event (accident) called a Top event, and then determining all the ways it can happen. Once the initial modelling is performed using general methods and initial data, a systematic methodology is applied that uses advanced modelling.

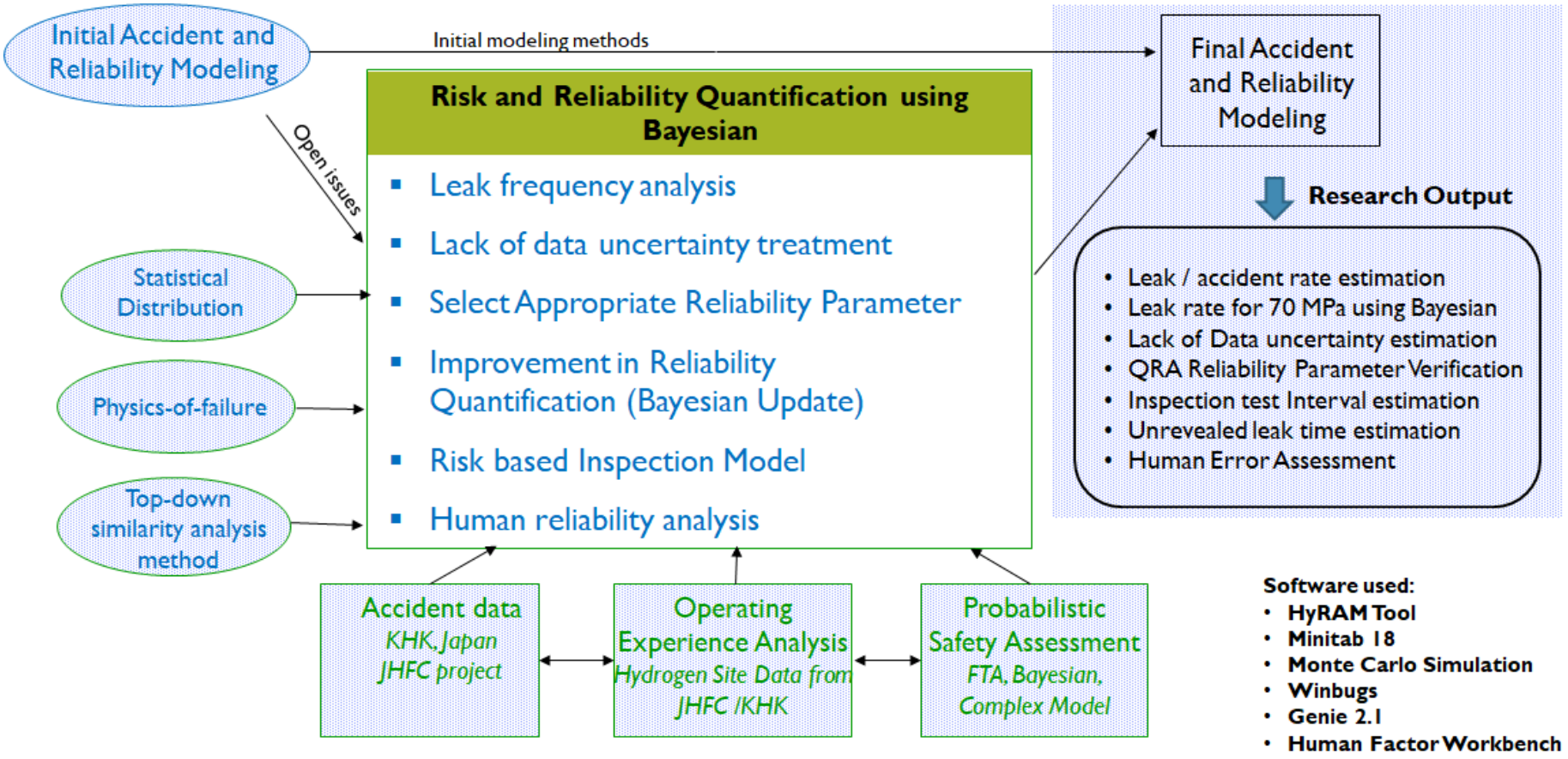


Figure 4. Research Framework: Accident and Risk and Reliability Quantification

The research framework is shown in Fig.4. The input provided to the model is based on the Data analysis. Failure data analysis was carried out based on the project report related to hydrogen and accident reports. When an accident takes place with respect to the high-pressure gas, a notification report shall be submitted to the prefectural governor or police official due to the High Pressure Gas Safety Act. Due to the Act, the accident is defined as follows:(i) Explosion, (ii) Fire, (iii) Leak, (iv) Degradation, (v) Others. Even if minor leak occurred, that event is treated as an accident related to the Act. Therefore, most of the accidents at HRS are leak of hydrogen. In this study, the following two data sources were referred to collect failure and operating data. The initial input data for the analysis were taken mainly from two data sources:

1. The Japan Hydrogen and Fuel Cell Demonstration Project

Data for estimation of failure rate were taken from the reports of the Japan Hydrogen and Fuel Cell Demonstration Project (JHFC, 2017). JHFC is a project sponsored by the Minister of Economy, Trade and Industry (METI) and started in FY2002.

2. High Pressure Gas Safety Institute of Japan

The High Pressure Gas Safety Institute of Japan has collected accidents related to the High Pressure Gas Safety Act in Japan from 1965 and published white paper on the review of accidents at HRS (KHK, 2015).

The failure and accident statistical data collected from these two sources are applied to the model. The model is related to the development of methods, techniques and frameworks for reliability and safety analysis. It specifically addresses the requirements to overcome uncertainties associated with risk and reliability quantifications that mainly can be used by researchers, reliability analysts, design and end users in risk assessment. Each of these methods and techniques used in the research model will be described in Part II in the form of six case studies.

The input data to the model mainly relies on KHK and JHFC database in Japan. This is mainly due to the nature of the project, funding agency and availability of data. It is understood that data collection and analysis for a new technology system determine the amount of uncertainty in the research output. The data selected in this research is limited however thoroughly examined and more realistic.

4.3 Research Design Flow

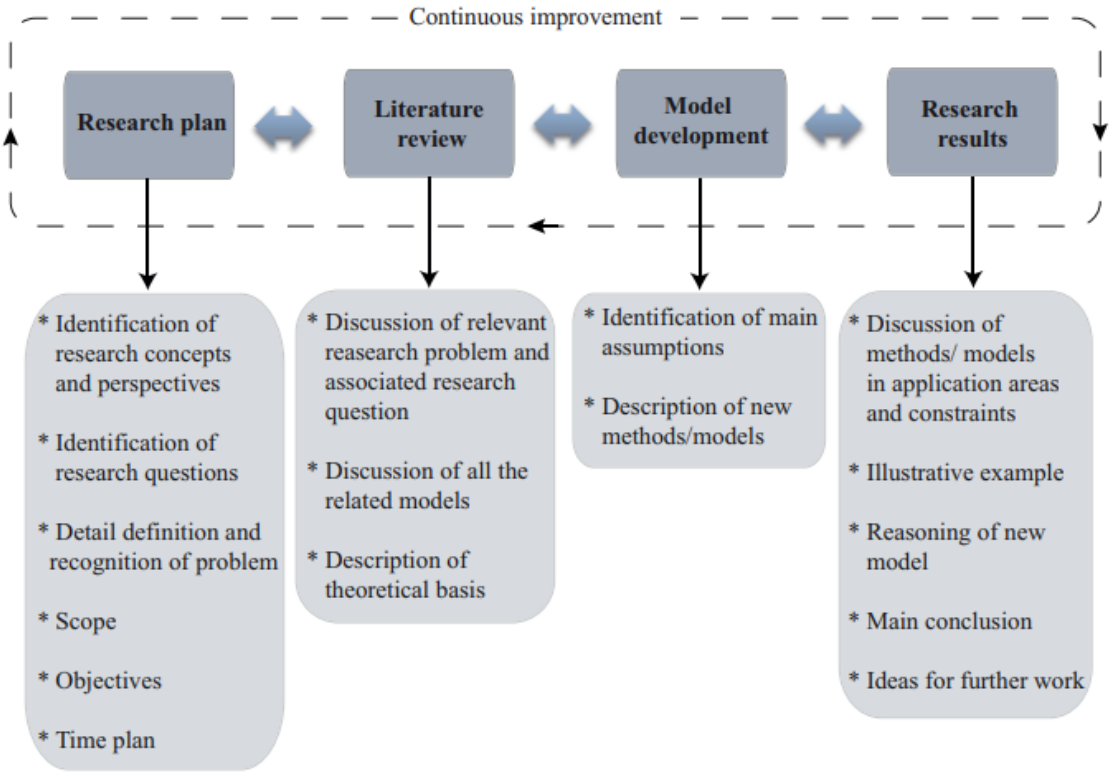


Figure 5. Research Design Flow

It is complicated to adopt one research method that will suit all requirements of the industry. A logical and documented design of the research project is the basis for any high quality research. A research project is a sequence of tasks or steps that are integrated to achieve a single objective. The research starts with defining the basis of the research, research questions and ends up with the research results. Fig.5 illustrates research design and process flow used for completing present research study and related articles. Research process has four main stages (1) research plan and challenges, (2) literature review, (3) model development, and (4) research results.

4.3.1 Research Plan

At the early stage of the design process, a research plan needs to be developed in order to understand current industry limitations, define research challenges and to provide a method for further investigation. The research plan describes the principles as a basis for research, stating its importance and implementation strategy. The research plan should answer the following questions:

- What is the ultimate intention of the research?

- What is the impact and benefits of the research on the risk society?
- Recent developments in the risk fields?
- How to incorporate a solution to address the research questions?

A typical research plan includes:

I. Specific aims: The specific aims are statements of the objectives and milestones of a research project. The purpose of this part is to clearly and concisely propose the research strategy.

II. Background: The background section states the research problem including the proposed rationale, the current state of knowledge and potential contributions and significance of the research to the field.

III. Research design and methods: The research design and methods are describing how the research will be carried out. This section is critical in order to demonstrate that the study design is developed under a clear, organized and thoughtful scheme.

4.3.2 Literature Review

The initial research activity has briefly reviewed the literature and developed research questions. The literature review spanned the body of journals, abstracts, relevant book sections, published reports and recommended practices by industry, and within the scope of reliability qualification, accident analysis, and other relevant subjects. Croom (2009) advised a strong emphasis on existing sources of evidence, especially systematic reviews that should be considered carefully prior to undertaking research. State of the art, ongoing research and development (R&D) reports, and industry practices are carried out in order to obtain sufficient knowledge about the latest needs of both in the scientific as well as in the practical point of view. Some academic institutions in Japan, mainly Yokohama National University has developed comprehensive social risk assessment guidelines that mainly adhere to the needs of qualification of new technology system. These guidelines are based on the risk assessment guidelines of Yokohama National University's Center for Creation of Symbiosis Society with Risk. They have been adapted for hydrogen fueling stations.

The general basis for this study and the topics it addresses have been established through literature surveys. These surveys provide a starting point for the research and support all the further activities. In addition, the professional experience from my main supervisor has contributed valuable inputs in the identification and solution of problems.

4.3.3 Model development

Risk and reliability engineering has two main aspects. First is to develop a model and second is to input failure or relevant data to the model to quantify the risks. Developing models are a good way to start refining all the information gathered so far. A risk model can be described as a risk analyst's attempt to represent a system and incorporate methods to address the uncertainties in the system (Parry, 1996). The model is therefore strongly dependent on the characteristic of the system and the analyst's competence. The risk analyst has to struggle with the trade-off between the need to simplify and safety. Creating model has an iterative process until an appropriate model has been developed. The level of detail or suitability of a model is restricted by the time, approximation formulas, distribution models and software availability. Models can be classified as statistical or dynamic in nature. The choice of model forces the analyst into a system structure that more or less is in accordance with the real life system. Due to the limitations in including the natural variability in the real life system, a model most likely only be an approximation (NASA, 2002). Model uncertainty to a certain degree will always exist. Standards, guidelines and internal company policies may often require or recommend specific types of models. In order to achieve the research objectives, a new framework would be developed under specific assumptions, aiming to overcome the shortages and challenges have found in the earlier steps.

4.3.4 Research Results

Research results should include the application area of the developed models, methods, or frameworks, discussion about constraints, and suggestions for new perspectives and ideas for future works. In most cases, application of case analysis on hydrogen-based technology is used for systematic description of the situations regarding how and why events occur and for demonstration of framework/model usability. The information acquisition is based on open data. However, in the context of developing a new technology system, the industry data is highly confidential and therefore presenting any real case is not

possible. In addition, due to data unavailability and complexity, it is difficult to cover all components or their failure modes in the case study and into the calculations/models.

The research results are presented to the academia and the industry through publication in international journals and proceedings of the conferences with referees and double blind peer review process. In addition, the reasoning of the models has been confirmed by sharing research ideas and results at international conferences. The purpose of the communication of the research results is both for risk communication, and for acquiring comments and feedback from risk experts. It was communicated to competent personnel who can further progress the analysis using all the available information and data. These principles of risk communication have contributed to the evaluation and quality assurance of the research results, since the input from the "outside world" has influenced the research work and thus influenced the results presented in this thesis. All the topics that are covered in my case analysis and their related areas are subjected to detailed discussion and verification of information from the academic and industry professionals. Public authorities should ensure that the outcomes of risk communication are incorporated into policies, and businesses should ensure that they are incorporated into their business plans.

5. MAIN HIGHLIGHTS, CONTRIBUTIONS AND FINDINGS

This chapter gives a summary of the main results from the research case studies. More specific information about the results are presented in the research case studies in part II of the thesis. Six research challenges were stated in Section 2. The purpose of this chapter is to evaluate to what extent these challenges have been considered. The relationships between the case studies and the research challenges are summarized in Table 4.

Table 4. Research challenges and related contributing case studies

No.	Research Challenges	Case Study No.
1	Leak frequency Analysis and Accident rate estimation	1
2	Lack of accident data uncertainty modelling	2
3	Unrevealed Leak time estimation	2
4	Verification of Risk assessment through appropriate selection of reliability parameter	3
5	Improvement in reliability quantification	4
6	Non-constant failure rate of mechanical products	4
7	Risk based Inspection prediction for new hydrogen-based systems	5
8	Human Factors influence on hydrogen-based systems	6
9	Root cause Analysis of hydrogen leak incident	6

5.1 Contribution to Research Challenge 1

Highlights:

- Accident at HRSs was analyzed with respect to operation time.
- Accident rate was modeled using a log-normal and Weibull function over time.
- The failure probability and unrevealed leak time were calculated for different inspection test intervals from the accident rate estimation.
- Failure probability and availability was modelled using Monte Carlo Simulation.

Contributions and Findings:

A quantitative based study on leakage-based analysis of accidents in Japan was conducted to understand the characteristic of leak rate. Three different models were studied and compared to understand the trend. Firstly, time based evaluation methods that utilize historical HRS accident information was proposed to estimate the leak rate. Then the leak frequency estimate from the other two methods i.e.

non-parametric based and leak hole size-based was examined. In the non-parametric approach, the leak frequency is estimated based on Bayesian update. Thereafter, a comparison of these three approaches were made to understand the trend of leak rate data. The results describes the trend of the leak rate; increasing or decreasing along the operation time, or peaking and declining.

The leak rate is estimated to be 0.16 per year, 0.20 per year, and 0.42 per year based on the time-based, leak-hole-size, and non-parametric methods, respectively. The leak rate data from time-based method shows similar trend with leak size based method however, non-parametric method tends to be conservative due to high failure observations (new evidence) during Bayesian update.

In addition, unrevealed leak time is calculated as a function of leak rate and inspection interval. For example, in the case of the time series method, when the leak rate is 0.16 per year and the inspection interval is 24 h (daily inspection), the unrevealed leak time is 19.08 s. It means that hydrogen sensors are required to detect minor leaks at short intervals to reduce the unrevealed leak time. It can be concluded that if the leak rate is estimated to be high, the inspection interval should be more frequent to reduce the unrevealed leak time and increase the process safety. The quantitative insights of this study can be used to set performance standards for availability and reliability of safety critical systems such as leak detectors in operation and maintenance of the HRS.

5.2 Contribution to Research Challenge 2

Highlights:

- Accident at HRSs was analyzed with respect to operation time.
- Accident rate was modeled using a time correlation model.
- Uncertainty in the estimation due to the lack of accident data was discussed.
- Benefits of the model adopted is discussed in comparison to traditional models.

Contributions and Findings:

This article examined the manner in which accident rate is modelled and described for HRSs. Unlike conventional statistical models in which the accident rate changes according to overall time function, Conditional autoregressive (CAR) model estimates the accident rate per month, and is constrained by the condition that the adjacent accident rate is similar to each other. Another result is that of the intrinsic

Gaussian CAR model, which represents the uncertainty in the estimation due to lack of data. The CAR result succeeded in showing that the uncertainty in the estimation increases when the operation time is long owing to the decreasing data. A model with accident rate following the intrinsic Gaussian conditional autoregressive model has the following advantages:

- Suitable to show if the estimate uncertainty is increasing owing to lack of data
- Estimates the accident rate per month and thus the graph is continuous without any gaps in the data between stations
- Support in decision making for new process systems

The CAR model is different from the other lifetime distribution models because its main aim is to reveal the estimate's uncertainty. A new system such as HRS has very little accident information, and so future predictions are inevitably unreliable. One approach to rectify this problem is to wait until enough data have been collected, or utilize the accident data of similar systems to increase its reliability. However, the Gaussian conditional autoregressive model does not aim to reduce the uncertainty; rather it discusses the effect of lack of information on the estimation. This new way of dealing with and interpreting accident information can be utilized to evaluate new systems such as HRS in the future.

5.3 Contribution to Research Challenge 3

Highlights:

- Estimate the failure rate based on the number of fillings and survival time of HRS.
- Employ a non-parametric approach to estimate cumulative failure as a function of number of fillings.
- Use a parametric approach to estimate cumulative failure as a function of survival time.
- Compare both parameters to choose correct life parameter for reliability quantification.

Contributions and Findings:

It is critically important to use the correct parameters for accurate reliability estimation. Field failure data of HRS is used as a case study to compare failure analysis based on two parameters i.e. survival time vs. number of fillings at the station. A non-parametric approach is used to estimate cumulative failure function based on number of fillings. The cumulative hazard using the Nelson-Aalen estimator showed a linear relationship with the number of fillings. A parametric approach using 2-parameters (β

and η) Weibull distribution function is employed to estimate cumulative probability of failure with the survival time. The study demonstrates that the failure rate can vary by a small to large margin based on the life parameter chosen for reliability predictions.

The study found that the failure rate estimated as a function of number of fillings is more reliable and realistic than the estimation based on survival time. Moreover, the number of fillings is more representative of the true failure rate as it considers the actual station's usage and loading. The survival time do not always represent the actual usage of the stations.

Using a case study, it is observed that two stations can have similar survival time but small to large difference in the usage (i.e., number of fillings). Thus, if the failure rate is estimated as a function of time, the mean failure rate will be roughly the same for both stations. However, if failure rate is estimated by number of fillings, the failure rate will vary depending on the actual usage of the station. The actual usage conditions are discarded when using the survival time and this may lead to uncertainty in the failure estimation.

5.4 Contribution to Research Challenge 4

Highlights:

- Introduction of dynamic modelling to IEC 61511 functional safety standard.
- Application of bayesian technique to IEC 61511 using gate valve as a case study.
- Modelling failure data uncertainty using Monte Carlo simulation.
- Sensitivity analysis on failure probability using Monte Carlo method.

Contributions and Findings:

International functional safety standards such as BS EN 61511 specifies the use of realistic and credible failure data in failure probability analysis. The proposed Bayesian framework addresses the requirements by allowing industry knowledge about failure rates to be incorporated in a prior gamma distribution and periodic updating process with new survival data as it becomes available. Monte Carlo simulation is adopted which makes it practical to solve uncertainty in the failure rate estimation and update these models with many trials in seconds. The result shows that the process of updating failure rate with more samples of new observations and modelling failure data uncertainty using Monte Carlo

simulation can be effective in improving reliability quantifications in the existing BS EN 61511 standard.

The study found that the process of updating failure rate with new observations and modelling failure data uncertainty using Monte Carlo simulation will result in lower uncertainty and narrower posterior distribution. It is observed that with less number of new observations, the updated failure rate is sensitive to generic uncertainty data which does not provide realistic result. In order to improve the sensitivity of updated failure rate, more number of observations subject to modelling using Monte Carlo method will be beneficial.

5.5 Contribution to Research Challenge 5

Highlights:

- Developed advanced RBI methodology to decide inspection time in relation to the risks
- System-categorized accidents in an HRS by operation time
- Understand the risk based influence of each critical component on the system
- Inspection interval estimated based on three risk categories i.e. minor, major and critical

Contributions and Findings:

A probabilistic graphical model, based on an acceptable level of risk, is proposed to avoid under and over estimation of inspection time interval. It presents an advanced RBI methodology to decide inspection time in relation to the risks. Bayesian Network (BN) is applied to model the risk and the associated uncertainty. Results show that the most critical components are the shut-off valve and hose/flow nozzle connection in case of minor risk. In case of major risk, flow gauge has the shortest transition from minor to major risk and thus makes it a most critical component. Pipelines have the shortest inspection time compared to other components and thus makes it the most critical component for critical risk. The developed method can assist the risk analyst and asset managers to work out the optimum inspection time for each component according to the risk level.

In addition, accident data evaluation based on operation time and system category revealed that that dispenser and accumulator failure was more evident during the early stage of HRS operation period whereas compressor and interconnection system had accidents late in the operation period.

5.6 Contribution to Research Challenge 6

Highlights:

- Developed semi-quantitative graphical method of human factor analysis for the refueling station liquid hydrogen releases
- Deriving causal Bayesian networks from human reliability analysis data
- High pressure gas accidents analysis in Japan
- Human task critical analysis are categorized and prioritized based on the risk they possess

Contributions and Findings:

A methodology is developed to analyse a liquid hydrogen transfer leak incident in the refueling station with respect to human factors as root causes. It presents a semi-quantitative graphical method of human factor analysis for the refueling station liquid hydrogen releases. The probabilistic graphical method helps to prioritise the causes that need to be analyzed first and/or in the greatest level of detail, based upon the degree of anticipated risk that they pose. As a result of analysis, events related to safety valve failure, improper connection of mechanical components, incompetency and no planning prior to the task has been found as some of the key issues in a transfer leak operational incident at a HRS. From the study, more awareness of hydrogen system among public, operator training (competency), use of correct policies and procedures are emerging as key contributions towards increased safety of the hydrogen service stations. In addition, a good performance (high integrity) safety system is required to prevent hydrogen releases.

Quantitatively, it is found that the chance of hydrogen leak incident is 15%. However, the leak event probability is drastically reduced to 0.03 per year because of the protection layer – safety system. This indicates that the current operation of the station is heavily dependent on safety system design and operation on demand to reduce the risk likelihood to 0.03 per year. The safety system functions as an emergency shutdown system where the primary function is to deactivate the source of release by automatically or manually isolating the liquid hydrogen flow. However in this case, most of the functions are dependent on human rather than system, appropriate care should be taken knowing that there is a possibility of leak in case the procedure is not followed. Standard operating procedure must be followed at all times. Assumptions are made at great risk. Risk also increases with complacency.

6. REFERENCES

Abaei, M.M., Arzaghi, E., Abbassi, R., Garaniya, V., Chai, S., Khan, F. (2018). "A robust risk assessment methodology for safety analysis of marine structures under storm conditions". Ocean Engineering, 156, 167–178, 2018.

Abbassi, R., Bhandari, J., Khan, F., Garaniya, V., Chai, S. (2016). "Developing a quantitative risk-based methodology for maintenance scheduling using Bayesian network". Chemical Engineering Transactions Vol. 48, 235–240, 2016.

Althaus, C. E. (2005). "A Disciplinary Perspective on the Epistemological Status of Risk." Risk Analysis 25 (3): 567–588.

Aven, T. (2010). "On How to Define, Understand and Describe Risk." Reliability Engineering & System Safety 95 (6): 623–631. DOI: 10.1016/j.ress.2010.01.011.

Aven, T. (2012). "The Risk Concept—Historical and Recent Development Trends." Reliability Engineering & System Safety 99 (Supplement C): 33–44. DOI: 10.1016/j.ress.2011.11.006.

Aven, T. (2014). "Fundamental Ideas and Concepts in Risk Assessment and Risk Management". London: Routledge Taylor & Francis Group.

Aven, T., Renn, O. (2009). "On risk defined as an event where the outcome is uncertain". Journal of Risk Research, 12 (2009), pp. 1-11.

Aven, T., O. Renn, and E. A. Rosa. (2011). "On the Ontological Status of the Concept of Risk". Safety Science 49 (8–9): 1074–1079.

BahooToroody, A., Abaei, M.M., Arzaghi, E., Abbassi, R. (2019). "Multi-level optimization of maintenance plan for natural gas system exposed to deterioration process". Journal of Hazardous Material Vol.362, 412–423, 2019.

Bhandari, J., Abbassi, R., Garaniya, V., Khan, F. (2015). "Risk analysis of deep water drilling operations using Bayesian network". Journal of Loss Prevention in Process Industries, Vol.38, 11–23, 2015.

Bouloiz, H., Garbolino, E., Tkiouat, M., Guarnieri, F. (2013). "A system dynamics model for behavioral analysis of safety conditions in a chemical storage unit". Safety Science. 58. 32-40. 10.1016/j.ssci.2013.02.013.

Bradley, G., Leverenz, F., Rose, S. (1999). "Contribution of Human Factors to Incidents in the Petroleum Refining Industry". Process Safety Progress, V01.18, No.4, 1999.

Casamirra, M., Castiglia, F., Giardina, M., Lombarado, C. (2009). "Safety studies of a hydrogen refueling station: Determination of the occurrence frequency of the accidental scenarios". International Journal of Hydrogen Energy, Vol. 34, pp. 5846-5854.

Croom, S. (2009). "Introduction to research methodology in operations management". In Karlsson, C., editor, Researching Operations Management, pages 42–83. Routledge, New York.

Crowe, R.M., Horn, R.C. (1967). "The meaning of risk". The Journal of Risk and Insurance, 34 (3) (1967), pp. 459-474.

DFI. (2007). "Evaluating Methodologies In Support of Homeland Security R&D Investment Decision-Making". DFI International Government Services, Washington, DC.

DNV Recommended Practice DNV-RP-A203. (2011). "Qualification of new technology". Det Norske Veritas, Høvik, Norway, July 2011.

Droguett, E.L., Groen, F.J., Mosleh, A. (2006). “Bayesian assessment of variability of reliability measures”. Pesquisa Operacional.

Fabiano, B., Parentini, I., Ferraiolo, A., Pastorino, R. (1995). “A century of accidents in the Italian industry-Relationship with the production cycle”. Safety Science 21, 65-74.

Foucher, B., Boullie, J., Meslet, B., and Das, D. (2002). “A review of reliability prediction methods for electronic devices”. Microelectronics Reliability, 42(8):1155–1162.

Garg, A., Deshmukh, S. (2006). “Maintenance management: literature review”. Journal of Quality and Maintenance Engineering.12, 205–238, 2006.

Gheriani, M., Khan, F., Chen, D., Abbassi, R. (2017). “Major accident modelling using spare data”. Process Safety and Environmental Protection, Volume 106, Pages 52-59, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2016.12.004.

Goerlandt, F., Khakzad, N., Reniers, G. (2016). “Validity and validation of safety-related quantitative risk analysis: A review”. Safety Science, Vol. 99, Part B, 2017, pp. 127-139, 2016.

Health and Safety Executive, UK. (1999). “Human factors assessment of safety critical task”. Offshore technology report 0992, HSE, UK.

IEC 61508 (2010). “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems”. International Electro technical Commission, Geneva, 2.0 edition.

IEC 60300-3-4 (2007). “Dependability management: Application guide - Guide to the specification of dependability requirements”. International Electro technical Commission.

International Energy Agency (IEA), Technology Roadmap Hydrogen and Fuel Cells, 2015.

Jafari, M., Mohammad & Zarei, E., Naser, B. (2012). “The quantitative risk assessment of a hydrogen generation unit”. International Journal of Hydrogen Energy. 37. 2012. 10.1016/j.ijhydene.2012.09.082.

Japan Hydrogen & Fuel Cell Demonstration Project, http://www.jari.or.jp/portals/0/jhfc/station/index.html; [accessed September 2017].

Jones, N. (1984). “A Schematic Design for a HAZOP Study on a Liquid Hydrogen Filling Station”. International Journal of Hydrogen Energy, Vol. 9, pp. 115-121.

Kalantarnia, M., Khan, F., Hawboldt, K. (2009). “Dynamic risk assessment using failure assessment and Bayesian theory”. Journal of Loss Prevention in the Process Industries, Volume 22, Issue 5, 2009, Pages 600-606, ISSN 0950-4230, https://doi.org/10.1016/j.jlp.2009.04.006.

Kaplan, S., Garrick, BJ. (1981). “On the quantitative definition of risk”. Risk Analysis, 1981; 1:11–27.

Karuiki., S.G, Lowe., K. (2007). “Integrating human factors into process hazard analysis”. Reliability Engineering & System Safety 2007; 92:1764-73. doi:10.1016/j.ress.2007.01.002

Kessler, A., Schreiber, A., Wassmer, C., Deimling, L., Knapp, S., Weiser, V. (2014). “Ignition of hydrogen jet fires from high pressure storage”. International Journal of Hydrogen Energy, 39 (35) (2014), pp. 20554-20559.

Khakzad, N., Reniers, G. (2016). “Application of bayesian network and multi-criteria decision analysis to risk-based design of chemical plants”. Chemical Engineering Transactions, 48, 223-228 DOI: 10.3303/CET1648038.

Khalil, Y. (2017). “A probabilistic visual-flowcharting-based model for consequence assessment of fire and explosion events involving leaks of flammable gases”. Journal of Loss Prevention in the Process Industries 50 (2017) 190–204.

Khalil, Y. (2018). “Science-based framework for ensuring safe use of hydrogen as an energy carrier and an emission-free transportation fuel”. Process Safety and Environmental Protection, Volume 117, Pages 326-340, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2018.05.011.

Khan, F., Abbasi, S.A. (1998). “Techniques and methodologies for risk analysis in chemical process industries”. Journal of Loss Prevention in the Process Industries, 11 (1998), pp. 261-27.

Khan, F.I., Haddara, M. (2004). “Risk based maintenance (RBM): a new approach for process plant inspection and maintenance”. Process Safety Progress 23 (4), 252–265, 2004.

Kikukawa, S., Mistuhashi, H., Miyake, A. (2009). “Risk assessment for liquid hydrogen fueling stations”. International Journal of Hydrogen Energy, Vol. 34, pp. 1135-1141, 2009.

LaChance, J. (2009). “Risk-informed separation distances for hydrogen refueling stations”. International Journal of Hydrogen Energy, Vol. 34, 5838-5845.

Leva, M. C., Naghdali, F., Alunni, C. (2015). “Human Factors Engineering in System Design: A Roadmap for Improvement”. The Fourth International Conference on Through-life Engineering Services, 2015.

Leveson, N. (2004). “A new accident model for engineering safer systems”. Safety Science, Volume 42, Issue 4, 2004, Pages 237-270, ISSN 0925-7535, https://doi.org/10.1016/S0925-7535 (03)00047-X.

Lundteigen, M., Rausand, M. (2009). “Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study”. International Journal of Reliability, Quality and Safety Engineering - IJRQSE. 16. 10.1142/S0218539309003356.

MacLean, H., Lave, L. (2003). “Evaluating automobile fuel/propulsion system technologies”. Progress in Energy and Combustion Science, Volume 29, Issue 1, 2003, Pages 1-69, ISSN 0360-1285, https://doi.org/10.1016/S0360-1285(02)00032-1.

Manca., D, Brambilla., S. (2012). “Dynamic simulation of the BP Texas City refinery accident”. Journal of Loss Prevention in the Process Industries, Volume 25, Issue 6, November 2012, Pages 950-957. doi:10.1016/j.jlp.2012.05.008.

Markowski, A., Siuta, D. (2017). “Selection of representative accident scenarios for major industrial accidents”. Process Safety and Environmental Protection, Volume 111, Pages 652-662, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.026.

Martins, M.R., Schleder, A.M., Droguett, E.L. (2014). “A methodology for risk analysis based on hybrid Bayesian networks”. Risk Analysis 34 (12), 2098–2120, 2014.

Matthijsen, A., Kooi, E. (2006). “Safety distances for hydrogen filling stations”. Journal of Loss Prevention in the Process Industries. Vol. 19, pp. 719-723.

Meel, A., Seider, W. (2006). “Plant-specific dynamic failure assessment using Bayesian theory”. Chemical Engineering Science, Volume 61, Issue 21, 2006, Pages 7036-7056, ISSN 0009-2509, https://doi.org/10.1016/j.ces.2006.07.007.

Milazzo, M., Giuseppe, M., Uguccioni, G. (2010). “The influence of risk prevention measures on the frequency of failure of piping”. International Journal of Performability Engineering.

Ministry of Economy, Trade and Industry. Strategic Road Map for Hydrogen and Fuel Cells, http://www.meti.go.jp/press/2015/03/20160322009/20160322009-c.pdf; 2014, revised in 2016 [accessed September 2017].

Ministry of Economy, Trade and Industry (METI). (2015). The condition of reviewing regulations corresponding

to the demand of a new era (related to hydrogen and fuel cell vehicle), http://www.meti.go.jp/committee/sankoushin/hoan/koatsu_gas/pdf/007_05_01.pdf; March 2015 [accessed September 2017].

Mohammadfam, I., Zarei, E. (2015). "Safety risk modelling and major accidents analysis of hydrogen and natural gas releases: A comprehensive risk analysis framework". International Journal of Hydrogen Energy, Volume 40, Issue 39, 2015, Pages 13653-13663, ISSN 0360-3199, https://doi.org/10.1016/j.ijhydene.2015.07.117.

Nakayama, J., Sakamoto, J., Kasai, N., Shibutani, T., Miyake, A. (2015). "Risk assessment for a gas and liquid hydrogen fueling station". In Proceedings of the 49th Annual Loss Prevention Symposium 2015, LPS 2015—Topical Conference at the AIChE Spring Meeting and 11th Global Congress on Process Safety, Austin, TX, USA, 27 April 2015; pp. 138–150.

Nakayama, J., Sakamoto, J., Kasai, N., Shibutani, T., Miyake, A. (2016). "Preliminary hazard identification for qualitative risk assessment on a hybrid gasoline-hydrogen fueling station with an on-site hydrogen production system using organic chemical hydride". International Journal of Hydrogen Energy, Vol. 41, pp. 7518-7525.

NASA. (2002). "Probabilistic risk assessment". Procedures guide for NASA managers and practitioners, volume Version 1.1. NASA Headquarters, Washington, DC.

OREDA (2009). "Offshore Reliability Data". Det Norske Veritas, Høvik, Norway, 5th edition.

OREDA (2015). "Offshore and Onshore Reliability Data Handbook". SINTEF Technology and Society: Department of Safety Research, Trondheim, Vol 1, 6th edition, 2015, Norway.

Paltrinieri, N., Khan, F. (2016). "Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application". Butterworth-Heinemann, 2016.

Parry, G. (1996). "The characterization of uncertainty in probabilistic risk assessments of complex systems". Reliability Engineering and System Safety, 54:119–126.

Pasman, H., Rogers, W. (2012). "Risk assessment by means of Bayesian networks: A comparative study of compressed and liquefied H2 transportation and tank station risks". International Journal of Hydrogen Energy, Vol. 37, pp. 17415-17425, 2012.

Pörn K. (1996). "The two-stage Bayesian method used for the T-Book application". Reliability Engineering & System Safety, Volume 51, Issue 2, Pages 169-179.

Rademaeker, E., Suter, G., Pasman, H., Fabiano, B., (2014). "A review of the past, present and future of the European loss prevention and safety promotion in the process industries". Process Safety and Environmental Protection, Volume 92, Issue 4, Pages 280-291, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2014.03.007.

Rahimi, M., Rausand, M. (2013). "Prediction of failure rates for new subsea systems: a practical approach and an illustrative example". Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 227(6), 629–640. https://doi.org/10.1177/1748006X13492954.

Redbook, CPR 12E. (1997). "Methods for determining and processing probabilities". Committee for the Prevention of Disasters, The Hague, The Netherlands, 1997.

Sakamoto, J., Sato, R., Nakayama, J., Kasai, N., Shibutani T., Miyake, A. (2016). "Leakage-type-based analysis

of accidents involving hydrogen-fueling stations in Japan and USA". International Journal of Hydrogen Energy, Vol. 41, pp. 21564-21570.

Sakamoto, J., Misono, H., Nakayama, J., Kasai, N., Shibutani, T., Miyake, A. (2018). "Evaluation of Safety Measures of a Hydrogen Fueling Station Using Physical Modelling". Sustainability 2018, 10, 3846.

Simon, E., Oyekan, J., Hutabarat, W., Tiwari, A., Turner, C. (2018). "Adapting Petri Nets to DES: Stochastic Modelling of Manufacturing Systems". International Journal of Simulation Modelling. 17. 10.2507/ijsimm17 (1) 403.

Takano, K., Okabayashi, K., Kouchi, A., Nonaka, T., Hashiguchi, K., Chitose, K. (2007). "Dispersion and explosion field tests for 40 MPa pressurized hydrogen". International Journal of Hydrogen Energy, 32 (13) (2007), pp. 2144-2153.

Tanaka, T., Azuma T., Evans, J., Cronin, P., Johnson, D., Cleaver, R. (2007). "Experimental study on hydrogen explosions in a full-scale hydrogen filling station model". International Journal of Hydrogen Energy, 32 (13) (2007), pp. 2162-2170.

The High Pressure Gas Safety Institute of Japan (KHK), (2012). "The high pressure gas incidents database". https://www.khk.or.jp/english/accident_reports.html; [accessed Feb 2017].

The High Pressure Gas Safety Institute of Japan (KHK). (2015). "Notes on Accidents related to Hydrogen Refueling Stations". (in Japanese).

Thompson, K., Deisler, R., Schwing, R. (2005). "Interdisciplinary vision: The first 25 years of the Society for Risk Analysis (SRA), 1980–2005". Risk Analysis, 25 (2005), pp. 1333-1386.

Threadgold, I. M. (2011). "Reducing the Risk of Low-Probability High-Consequence Events". Society of Petroleum Engineers. DOI: 10.2118/141763-MS.

Tsunemi, K., Yoshida, K., Yoshida, M., Kato, E., Kawamoto, A., Kihara, T., Saburi, T. (2017). "Estimation of consequence and damage caused by an organic hydride hydrogen refueling station". International Journal of Hydrogen Energy, Vol. 42, Issue 41, pp. 26175-26182.

Walker, W. E., Harremoes, P., Rotmans, J., J. P van der Sluijs, M. B. A. van Asselt, Janssen, P., Krayer von Krauss, M. (2003). "Defining Uncertainty: A Conceptual Basis for Uncertainty Management in Model-Based Decision Support." Integrated Assessment 4 (1): 5–17.

Wood, O.G. (1964). "Evolution of the concept of risk". Journal of Risk and Insurance, 31 (1) (1964), pp. 83-91.

Yamada, T., Kobayashi, H., Akatsuka, H., Hamada, K. (2015). "Analysis of high pressure gas incidents in hydrogen fueling stations". Journal High Pressure Gas Safety Institute Japan, 52 (10) (2015), pp. 23-29 [in Japanese].

Yang, M., Khan, F., Lye, L. (2013). "Precursor-based hierarchical Bayesian approach for rare event frequency estimation: A case of oil spill accidents". Process Safety and Environmental Protection, Volume 91, Issue 5, Pages 333-342, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2012.07.006.

Yeo, C., Bhandari, J., Abbassi, R., Garaniya, V., Chai, S., Shomali, B. (2016). "Dynamic risk analysis of offloading process in floating liquefied natural gas (FLNG) platform using Bayesian Network". Journal of Loss Prevention in the Process Industries, Volume 41, 2016, Pages 259-269, ISSN 0950-4230, https://doi.org/10.1016/j.jlp.2016.04.002.

CASE ANALYSIS PART II

CASE STUDY 1. Leak Frequency Analysis for Hydrogen-based Technology using Bayesian and Frequentist Methods

1.1 Introduction

One of the important accident characteristic of hydrogen energy system is the leak occurrence data. Leak rate analysis can reveal trend of accident occurrence in the hydrogen-based technology. This involves operation start time, failure cause, number of failures, minor to major leaks and consequences. This case study is chosen to support the core concept of the research by focusing all three aspects: i.e. new technology system, treatment of uncertainties in risk and reliability quantification and bayesian dynamic modelling. This case study utilizes the originality of the research through application of dynamic modelling for treatment of uncertainties in the field of risk and reliability quantification for new technology system.

Focusing on the case study, dealing with hazardous environments such as hydrogen poses considerable risks to property, people, and the environment. Leak frequency analysis is a method of understanding the characteristics of risks at hydrogen refueling stations (HRSs). Sakamoto et al. (2016) carried out a qualitative study on leakage-based analysis of accidents in Japan. In their study, leakage was classified based on the components and cause of accident. One of the characteristics of HRS accidents in Japan is that a high percentage of leak accidents occur at pipe joint sections. Because there are many joints and seals in a hydrogen refueling station, and the station's hydrogen compressor produces mechanical vibrations, small leaks from joints and seals are a major concern at HRSs. The results revealed that the main cause of leakage among flanges, valves, and seals is screw joint failure. Leakage associated with the filling hose and dispenser is mainly due to human error. Although their study makes an important contribution to leakage analysis of HRSs, it is limited to only a qualitative assessment of the leakage analysis.

The leak frequency of HRSs has been reported by several researchers. One of the ways to estimate leak frequency is based on the hole size. LaChance et al. (2009) developed a Bayesian model for leak frequency in various components used in HRSs. The leak frequency is assumed to be a function of the

fractional flow area of the leak. The leak frequency was estimated as a function of leak size, which is the ratio of the leak area divided by the total cross-sectional flow area. For a leak area of 0.1% of the total flow area, the corresponding system leakage frequency would be 0.03 per year and 0.06 per year for the 20.7 MPa and 103.4 MPa systems, respectively. Since even a small leak from joints and seals are a major concern at HRSs, most leak failures can be classified as a very small leak with leak area of 0.01% of the total flow area. When the leak area is 0.01% of the total flow area, the system's leak frequency would be 0.2 per year.

A more traditional approach to leak frequency estimation is provided in the Dutch Redbook model (Redbook, 1997). The model employs a non-parametric approach using the Nelson–Aalen estimator. By using a non-parametric approach, the leak rate can be estimated as a function of the number of fillings in the HRS. The relationship between the cumulative hazard and the number of fillings should be understood and equated to calculate the leak rate of the system. The method developed is quite generic, and is often implemented in the oil and gas industry where more traditional approaches using constant failure rates are widely adopted in leak and failure analysis. However, the characteristics of HRSs are different from those of the oil and gas industry. For example, in the oil and gas industry, accidents can occur due to a wide range of causes resulting in leaks, toxic effect, fire, and/or explosions. However, in HRSs, fire and/or explosions are not observed on a large scale. As mentioned earlier, leakage is a major event in accidents reported in HRSs.

Focusing on the HRS operation time from its start may reveal characteristics of leak occurrence. In other words, collecting data about leaks from the past will allow better understanding of the trend in the possibility of leaks by identifying its operation time. Under such circumstances, time-based evaluation is important. Studies have been performed on HRS accidents or leak frequency by organizations such as Sandia National Laboratories (LaChance et al., 2009). However, only a few studies have been conducted on the time series effect. This is one of the reasons why the operation time is given more importance and is discussed at length in this study.

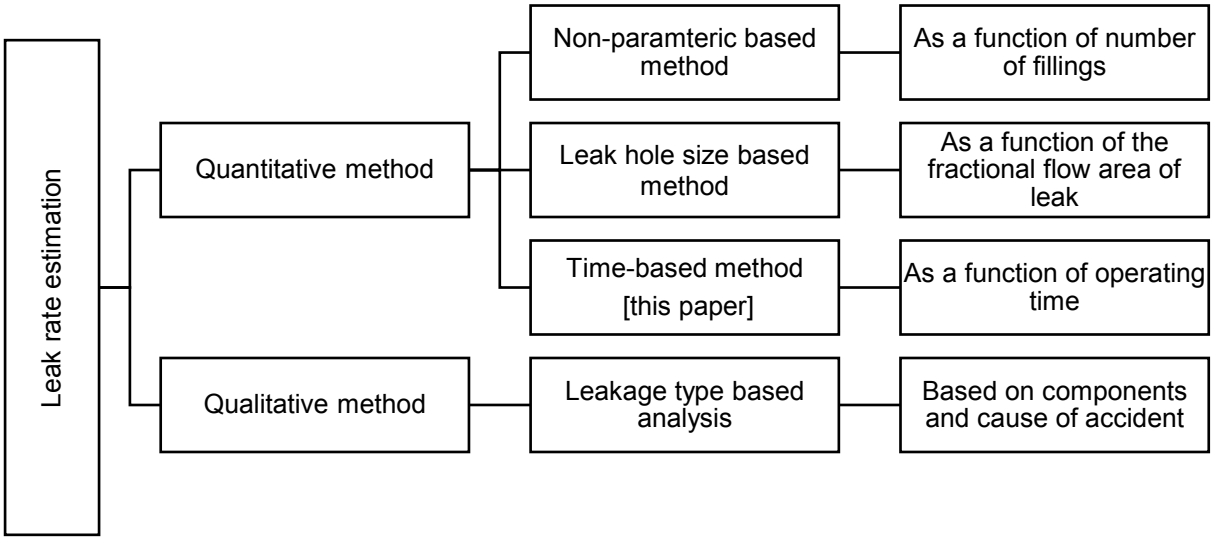


Figure 6. Review of methods developed for estimating leak frequency estimation

Fig.6 summarizes various methods that are currently adopted in the leak frequency estimation of HRS. The leak-rate estimation methods can be classified as follows:

1. Qualitative method
    a. Leakage-type-based analysis (Sakamoto al., 2016)
2. Quantitative method
    a. Leak-hole-size method (LaChance et al., 2009)
    b. Non-parametric method (Redbook, 1997)
    c. Time-based method (this study)

Note: All of the above quantitative methods employ Bayesian update for leak data evaluation

In this study, the models described above are analyzed to identify trends. Failure and operating data of HRSs are collected and analyzed in detail to estimate the leak rate using frequency (time series effect) and Bayesian based evaluation methods. The results will describe trends in the leak rate: whether they increase or decrease over operation time, or whether they are peaking and declining. Leak frequency estimations from various methods are examined with the present method to understand the different ways of modelling leak frequency. The algorithm based model implemented through statistical interpretation and WINBUGS tool provides a new way of dealing with accident data in safety and risk management. The study results will help asset managers make an engineering judgement on the appropriate leak rate data of systems.

In addition, unrevealed leak time is calculated as a function of leak rate and inspection interval. Unrevealed leak time is one area within safety and risk management of hydrogen stations that has not yet been addressed in any research study. The authors believe that in addition to process safety time, unrevealed leak time is an equally critical parameter that needs to be considered in the engineering safety designs. It determines the time period when the leak exists at the installation due to an unrevealed leak failure. This is considered to be an important characteristic of HRSs. The quantitative insights of this study can be used to set performance standards for the availability and reliability of safety critical systems, such as leak detectors, during the operation and maintenance of the HRS.

1.2 Leak data analysis

1.2.1 Leak data evaluation at HRSs based on operation time

In this case, the number of accidents (leaks) at an HRS over time was determined from the start of its operation. The term "leak rate" is used in this study in reference to the accident occurrence per unit time per HRS. "HRS operation start" denotes the start of HRS operation used in either test research or commercial operation. The operation start time of the HRS does not include the construction time of the HRS infrastructure. "Through operation time" indicates that the data is treated with the time elapsed from the start of operation. The accident count is based on the events listed in the high-pressure gas incidents database of The High-Pressure Gas Safety Institute of Japan (KHK, 2012). Operation time is the period between the operation start month and the accident occurrence month. In this study, a "month" signifies a unit of time measurement.

Kodoth et al. (2018) has already collated data based on the events listed in the high-pressure gas incidents database (KHK, 2012) to determine the data uncertainty in accident rate estimation. The same data will be referred to in this paper, because the data source is common to both studies. In total, 26 accidents were reported for these HRSs. The data source is limited to 35 MPa and 70 MPa systems. The original data contains information on when the station operated and when an accident happened for each HRS. The length of time that elapsed from the operation start time to the accident occurrence is calculated using these data. Although the starting periods differ among the stations, they are assumed

to be the same point for accident analysis. The unit of time is “month”. The accident count for each month is estimated as “[Event count per station-month]”.

However, the data collated from the database by Kodoth et al. (2018) contain many no-accident months. The statistical model that will be introduced in Sections 1.3.2.1 and 1.3.2.2, in which the function $f(x)$ describes each month’s accident rate, is not suitable for the original data, which contains many no-accident months. Consequently, the input data were modified as follows: if the first accident occurred in the second operation month, it is distributed evenly over the first and second operation months, resulting in the input accident count for each month being 0.5 [event per (station-month)]. In brief, the number of accidents in an operation month is divided by the length of the non-accident period starting from the earlier accident and is estimated as the average accident input data over the period.

The converted input data are shown in Fig.7. A relatively large value for the input data corresponds to accidents in rapid succession, whereas a relatively small value for the input data corresponds to accidents occurring over a long period. Although the data presented in Fig.7 are similar to the original data collated by Kodoth et al. (2018), note that there is no zero-accident month in Fig.7. This study emphasis lack of data treatment and re-organizing them to make it suitable for the model.

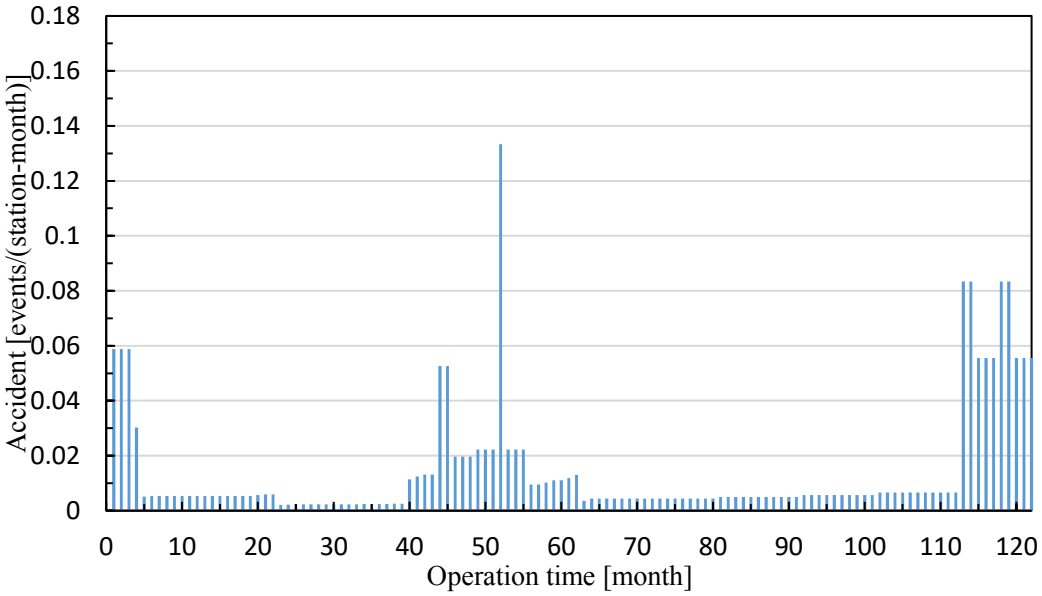


Figure 7. Input data for estimation by function of time

1.3 Methods for estimation and interpretation of leak rate

In this section, two statistical models (Lognormal and Weibull) are applied to the time series station events data in order to understand their characteristics. As each model has a different application, suitable care should be taken to apply the correct model to the data.

1.3.1 Flow of accident rate analysis as a function of time

The flow of accident rate analysis by function of time is shown in Fig.8. The analysis flow is divided into the two parts. Part 1 is related to organizing data in the format suitable to the model. The input data (referring to accident data in Fig 7) is analyzed by operation time (mean). Input data is given as an input to Part II. Part II performs statistical analysis based on the model described in Section 1.3.2. The output from the model is the posterior data.

1. Part I: Input data preparation for statistical analysis software - Data processing is needed in accident analysis using either the log-normal function or the Weibull function of time. The prior distribution for the dataset is represented in Fig.7. The prior data reported is given as an input to the model.
2. Part II: Statistical analysis using WINBUGS software (Ntzoufras, 2009) - Using the prior (input) data, the accident rate for each month is estimated. The model in WINBUGS is written in a series of commands as shown in Appendix A/B.

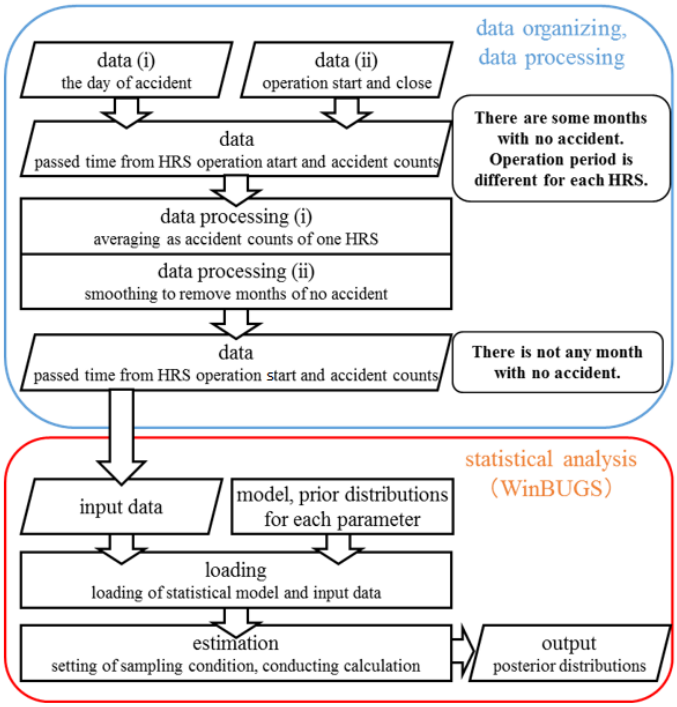


Figure. 8. Flow of analysis using the log-normal function or Weibull function of time

1.3.2 Estimation of leak rate based on time function

In the early stages of a hydrogen station's operation, human factors can cause accidents because workers may not operate or maintain the system well, and this may cause frequent accidents. During the intermediate stages of the operation, equipment component failures may cause leaks. Thus, the leak rate can be considered to be variable. This is similar to the bathtub curve used in reliability engineering. It is intuitively supposed that when computing leak data, as shown in Fig.7, the result of the early operation period is reliable, but the estimation of the late operation period is not very convincing. The conditionally autoregressive (CAR) model described in Kubo (2014), which is often used to describe spatial correlations, is suitable for application to these data (Barua, 2014).

It should be noted that the question is not whether the leak rate is constant. Perhaps, the method of estimation and modelling of the leak rate leads to the differences. The non-parametric method presented in Redbook treats "leak rate" as a constant value. However, the leak rate under certain conditions can change with time, which will not be taken into account in that method. If the constant value is sufficiently appreciated, time series analysis need not be conducted. To estimate the leak rate change over time, two time-based methods are adopted in this study. Both methods use statistical models to describe the leak rate as a function of time (NIST, 2012).

1.3.2.1 Leak rate description by function of time: A log-normal function

First, a log-normal function is introduced that models the time-changing leak rate. The variable has a log-normal distribution if the logarithm of the variable follows the normal distribution. The probability density function for log-normally distributed positive x is shown in Eq. (1):

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma x} \exp\left(-\frac{(\ln x - \mu)^2}{2\sigma^2} \right), 0 < x < \infty \tag{1}$$

where,

μ - Log-normal distribution mean value parameter

σ - Log-normal distribution standard deviation parameter

x - Positive random variable

The accident rate $f(x)$ is described by multiplying the function in Eq. (1) by a coefficient a:

$$f(x) = a\frac{1}{\sqrt{2\pi}\sigma x}\exp\left(-\frac{(\ln x-\mu)^2}{2\sigma^2}\right), 0 < x < \infty \tag{2}$$

In Eq. (2), coefficient a is multiplied by the original distribution. The operation time and leak rate correspond to x and $f(x)$, respectively. A detailed explanation of estimation is presented in Appendix A.

1.3.2.2 Leak rate description by function of time: Weibull function

Weibull distribution can take a more flexible shape of a graph than the log-normal distribution, even a nearly constant one. In this case, estimation is conducted with the Weibull function instead of the log-normal function. The probability density function for Weibull distributed positive x is shown in Eq. (3):

$$f(x) = \left(\frac{\alpha}{\beta}\right)\left(\frac{x}{\beta}\right)^{\alpha-1}\exp\left(-\left(\frac{x}{\beta}\right)^{\alpha}\right) \tag{3}$$

where,

α - Weibull distribution shape parameter

β - Weibull distribution scale parameter

x – Positive random variable

The equation applied to estimate the leak rate using the Weibull function model is shown below:

$$f(x) = a\left(\frac{\alpha}{\beta}\right)\left(\frac{x}{\beta}\right)^{\alpha-1}\exp\left(-\left(\frac{x}{\beta}\right)^{\alpha}\right) \tag{4}$$

This is the function in Eq. (3) multiplied by coefficient a. As in Eq. (2), operation time and leak rate correspond to x and $f(x)$, respectively. A detailed explanation of estimation is presented in Appendix B.

1.4 Results and Discussions

1.4.1 Leak rate estimation by time function: log-normal function

The result of leak rate estimation via the log-normal function is shown in Fig.9. Although the estimated values are individual points for each month, they are represented using a smooth curve, as shown in the figure.

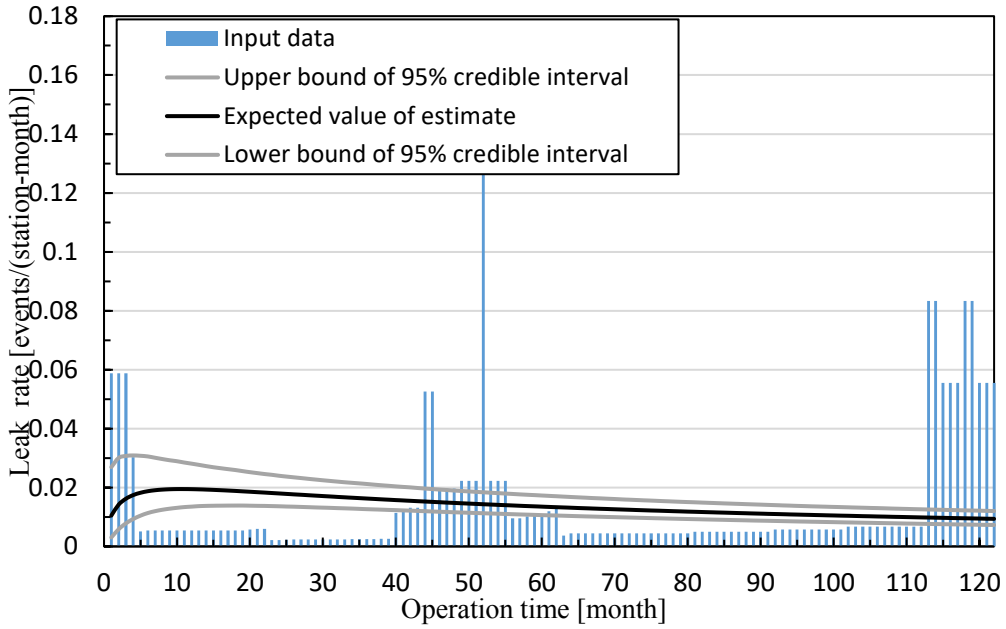


Figure 9. Leak rate estimation via log-normal time functon

The horizontal axis in the graph of Fig.9 is the operation time from the beginning of the HRS. The vertical axis is the leak rate, i.e., the average number of accidents per station per month. In the graph legend, the expected value of the estimate (shown in black) is the value that the leak rate is expected to follow, and the 95% interval is the range within which the leak rate is likely to lie with a 95% credibility. For example, from the graph, the estimated 10th operation month's expected value of leak rate is 0.0194 [event per (station-month)]. In addition, because the lower bound of the 95% credible interval in the 10th month is 0.01336 [event per (station-month)] and the upper bound is 0.0284 [event per (station-month)], there is a 95% probability of the leak rate having a value between these two bounds. As shown in the graph, the peak of the expected value of estimation falls on the 10th and 11th month. The leak estimate of 0.0132 [event per (station-month)] is estimated by the lognormal type function. This equates to 0.16 leaks per year.

1.4.2 Leak rate estimation by time function: Weibull function

The result of the Weibull type function estimation is shown in Fig.10. The input data used are the same as that for log-normal function estimation. As with the log-normal curve, this estimation resulted in a smooth curve for the overall time.

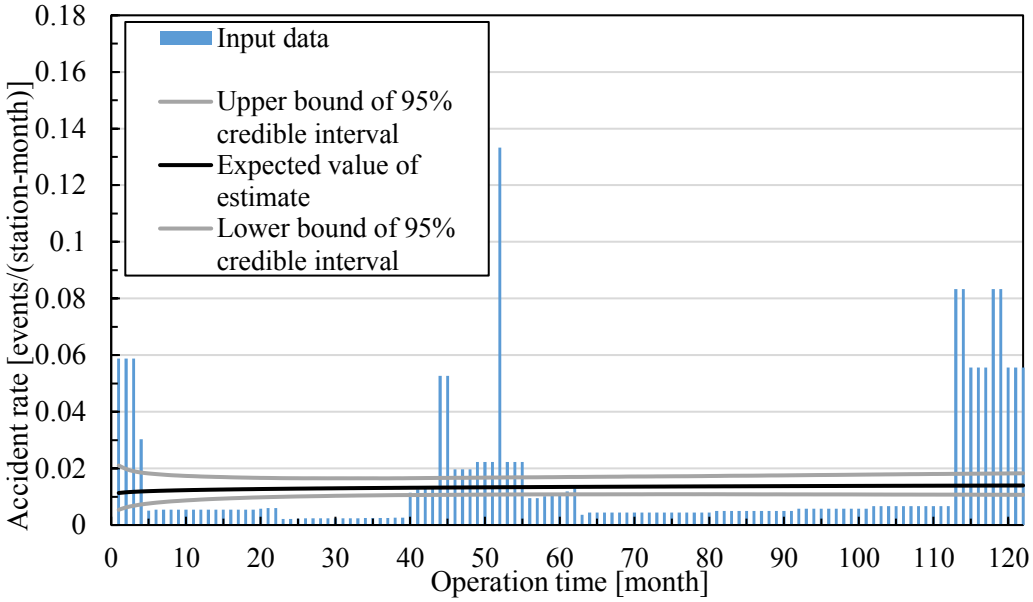


Figure 10. Accident rate estimate using Weibull function of time

From Fig.10, it can be observed that the expected value of estimation is virtually constant. Compared to the log-normal distribution, Weibull distribution's form is flexible in accordance with the parameter value. Thus, the steady result may suggest that the leak rate does not increase or decrease gradually but has a virtually constant value. It should be noted that the selected input data might have an impact on the expected value estimated, as there are many periods with equal input data, for example, the data from the 5th to the 19th month. Processing of the input data may affect the result. A leak estimate of 0.0134 [event per (station-month)] is estimated by the Weibull type function.

1.4.3 Total leak rate estimation using a non-parametric approach with the Bayesian update

A non-parametric approach was employed by Kodoth et al. (2019) to estimate the failure data of the HRS. It adopted a non-parametric analysis to estimate the leak frequency as a function of the number of fillings using JHFC data for 35 MPa systems (JHFC, 2011). To be consistent with the time-based approach, the non-parametric failure analysis results for the 35 MPa systems will be used as the initial data and succeeded by the Bayesian update approach for the 70 MPa systems in this study. Bayesian update is used to update the initial failure information and provide updated failure data based on new observations and evidences. This study employs the Bayesian update in accordance with the Dutch model (Redbook, 1997). The probability density function of gamma distribution takes the form,

$$f(x) = \frac{\beta^{\alpha}}{\Gamma(x)} x^{\alpha-1} e^{-\beta x} \quad \text{for } x > 0 \tag{5}$$

Here, α and β of the parameters can be determined by the mean and variance of the prior failure rate.

$$\alpha = \frac{E(\lambda)^2}{V(\lambda)} \tag{6}$$

$$\beta = \frac{E(\lambda)}{V(\lambda)} \tag{7}$$

The total failure rate $E(\lambda)$ of 6.7×10^{-4} per day and its variance $V(\lambda)$ of 6.0×10^{-8} per day estimated from Kodoth et al.'s (2019) findings will be used as prior knowledge in the Bayesian update. Substituting these figures in Eq. (6) and Eq. (7), the initial values of α and β are calculated to be 7.48 and 11166, respectively. Bayesian update is performed by calculating the parameters of posterior distribution, α' and β' based on new observations summarized in Table 5. The parameters can be updated as follows:

$$\alpha' = \alpha + n_f \tag{8}$$

$$\beta' = \beta + T_s \tag{9}$$

Here, nf is the number of failures and Ts is the observed time. By using Eq. (6–9), the posterior distribution's mean and variance can be obtained from the updated parameters. Table 5 summarizes the number of accidents in the 70 MPa stations based on new observations. The observed time and number of leaks are collected from January 2011 to December 2015 extracted from the literature (KHK, 2015).

Table 5. Accidents in the 70 MPa hydrogen refueling stations in Japan from 2011 to 2015

ID	Observed time [days]	Number of leaks	Leak rate [day^{-1}]	
			E(λ)	V(λ)
1	30	2	8.4×10^{-4}	7.5×10^{-8}
2	50	1	7.5×10^{-4}	6.7×10^{-8}
3	11	2	8.4×10^{-4}	7.5×10^{-8}
4	409	1	7.3×10^{-4}	7.0×10^{-8}
5	126	1	7.5×10^{-4}	6.6×10^{-8}
6	2374	2	7.0×10^{-4}	1.0×10^{-8}
7	1678	1	6.6×10^{-4}	5.1×10^{-8}
8	1585	2	7.4×10^{-4}	5.8×10^{-8}
9	71	1	7.5×10^{-4}	6.7×10^{-8}
Sum.	6334	13	1.1×10^{-3}	6.6×10^{-8}

Table 5 shows the updated leak rate and its variance for each station. Since the number of leaks for each station is one or two, Bayesian update depends on the prior distribution. When the total number of leaks and observed time are used as specific data for the 70 MPa stations, the updated leak rate is 1.1×10^{-3} per day, which is about twice the leak rate estimated from other methods.

1.4.4 Summary of results from three methods

The results from time series method can be verified with those of the other two methods to make an engineering judgement on the leak rate estimation. The obtained results are summarized as follows:

1. Time-based method: The leak rate follows lognormal distribution with a mean value of 1.84×10^{-5} per hour. The estimated leak rate as a function of time is 0.16 per year.
2. Non-parametric (Bayesian) method: The leak frequency is estimated from failure data by means of Bayesian update. The total leak rate using the non-parametric approach is estimated to be 1.1×10-3 per day, which is equivalent to 0.42 per year. This value is conservative and almost twice the leak rate compared to the results from other two methods. It should be noted that the initial data used in this approach and time based method is same however, the evidence (posterior data) of 70MPa for bayesian update is different from the time-based method. Based on the evidence, the result can vary by small to large margin.
3. Leak-hole-size method: The observed failure data (collated from the JHFC project report) is associated with leaks from threaded joints and seals. Under such conditions, it is assumed that the failure rate is equivalent to the leak frequency. Most of the failures are classified as "very small leak" of which the leak area is 0.01% of the total flow area, and the system frequency can be estimated to be 0.20 per year in line with the study by LaChance et al. (2009).

1.5 Unrevealed leak time forecast based on leak frequency estimation

In general, an odorant is added to the gas (such as natural gas), to make it easy to detect leaks. However, pure hydrogen is used for FCV and it is not easy to detect a hydrogen leak. Then, the sensors used to detect hydrogen are used to detect leaks. Unrevealed leaks can occur at HRSs. There are two possibilities for hydrogen leak: either the leak will be detected by the hydrogen leak sensor within the inspection interval or the leak will not be revealed until the next scheduled inspection interval, as shown in Fig.11. Based on these two possibilities, the parameter of interest from a safety point of view is unrevealed leak time.

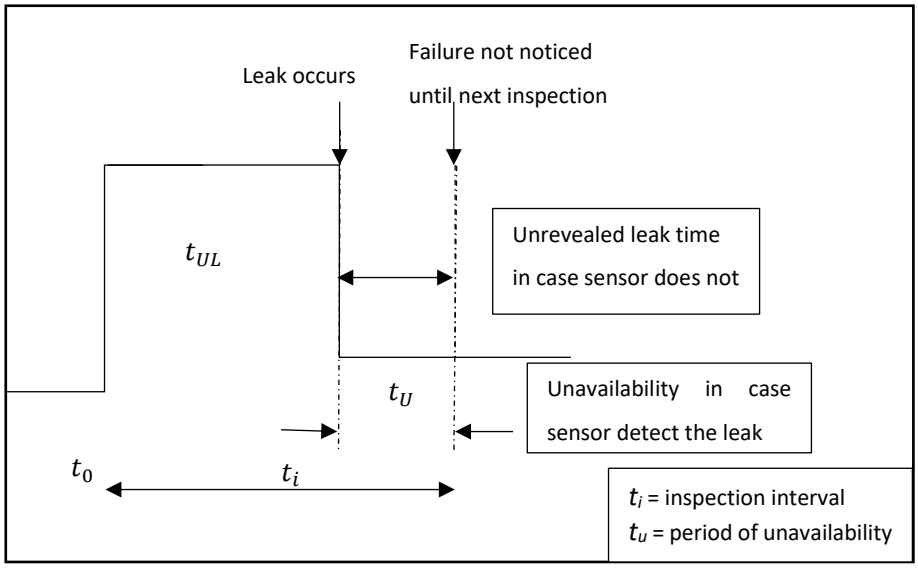


Figure 11. Inspection cycle for revealed and unrevealed leaks

For unrevealed failures, the failures become obvious only after regular inspection. Unrevealed leak time is the difference from the point when the unrevealed leak occurs and the next inspection time. Failure probability is the measure of unreliability of the installation. The unavailability is the downtime of the process when the sensor detects the leak resulting in station shutdown.

1.5.1 Unrevealed leak time based on leak rate estimate

Using the leak estimate per station-month given by the lognormal type function from the previous section, the unrevealed leak time t_{UL} is obtained from the failure rate λ and inspection interval t_i.

$$t_{UL} = \int_0^{t_i} \lambda(t_i - t)dt = \frac{1}{2}\lambda t_i^2 \quad (10)$$

The leak rate estimated value from the previous section is used as a basis for λ. The unrevealed leak time forecast based on leak rate estimation and inspection interval is presented in Table 6.

Table 6. Unrevealed leak time forecasts based on leak rate and inspection interval

Methods	Leak Rate (per year)	Inspection Interval	Unrevealed leak time
Log-Normal (time-based)	0.16	Daily	19.08 s
Weibull (time-based)		Monthly	17043 s
Non-parametric Analysis	0.42	Daily	49.70 s
		Monthly	44738 s
Leak-Hole-Size Approach	0.20	Daily	21304 s
		Monthly	23.67 s

The unrevealed leak time is directly proportional to the leak rate and inspection interval. For example, in the case of the time series method, when the leak rate is 0.16 per year and the inspection interval is 24 h (daily inspection), the unrevealed leak time is 19.08 s. It means that hydrogen sensors are required

to detect minor leaks at short intervals to reduce the unrevealed leak time. The unrevealed leak time using the non-parametric approach is estimated to be 49.70 s, which is conservative and almost twice the value compared to the results from other two methods. Perhaps this is due to the influence of evidence posterior data used in the non-parametric method for 70 MPa system. In leak hole size method, most of the failures are classified as “very small leak” of which the unrevealed leak time is estimated to be 23.67 s, which is significantly lower than the non-parametric method. In addition, for each method, the unrevealed leak time can increase drastically if the inspection interval is moved from daily to monthly routine. All these factors should be taken into account during the leak rate analysis and design of hydrogen sensors. The leak rate and unrevealed leak time data estimated with respect to inspection test in the paper can provide useful insights to engineers working in the reliability quantification of hydrogen energy system.

1.6 Conclusions

This study examined the manner in which the leak rates are modelled using various methods. A time-based Bayesian estimate method was proposed, in which leak rates were modeled using operating time data on HRSs. One of the main results is that for the log-normal and Weibull models, the leak rate changes according to the time function. Parameters for the two statistical models were determined based on a Bayesian update. Even if accident events are rare, two statistical models can provide a range of leak rates as a function of time. The results from the time series method were then examined with other two methods to make an engineering judgement on the leak rate estimation.

To summarize, the leak rate is estimated to be 0.16 per year, 0.20 per year, and 0.42 per year based on the time-based, leak-hole-size, and non-parametric methods, respectively. It can be observed that even though the values do not exactly match, there is no large margin between the results obtained by the time-based and leak-hole-size methods. However, the leak rate obtained from the non-parametric method is the most conservative among the three. Perhaps, this is because of the more frequent failures observed in the new evidences for the 70 MPa system. The leak rate data from the time-series method shows a similar trend with the non-parametric and leak-hole-size method. The asset manager can select

appropriate leak rate data based on the accident data and method availability. One of the possible solutions is to consider a conservative value for the design, in which case, the non-parametric model leak rate of 0.24 per year can be used. The base value selected can be used in design to set performance standards for the availability and reliability in the operation and maintenance of HRSs.

Unrevealed leak time was assessed from the estimated leak frequency. It can be concluded that if the leak rate is estimated to be high, the inspection interval should be more frequent to reduce the unrevealed leak time and increase the process safety. The unrevealed leak time can be used to the specification of hydrogen sensors to detect leaks of hydrogen. This will ensure the component and process both meet the requirements in the performance standard, leading to increased process safety in HRSs.

1.7 Acknowledgement

Funding: This research was supported by the Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Energy carrier” (Funding agency: Japan Science and Technology Agency (JST)). Authors would like to thank technical experts of IEA Hydrogen Safety Task 37 for fruitful discussion.

1.8 References

Barua, S., Basyouny, K., Islam, MT., 2014. A full Bayesian multivariate count data model of collision severity with spatial correlation. Anal Methods Accid Res, 2014; 3-4:28–43.

Bedrick, J., Christensen, R., Johnson, W., 2017. A new perspective on priors for generalized linear models. J. Am. Stat. Assoc. 1996; 91(436):1450–1460, http://www.jstor.org/stable/2291571/; [accessed September 2017].

Casamirra, M., Castiglia, F., Giardina, M., Lombarado, C., 2009. Safety studies of a hydrogen refueling station: Determination of the occurrence frequency of the accidental scenarios, International Journal of Hydrogen Energy, Vol. 34, pp. 5846-5854.

Redbook Dutch Model, 1997. Methods for determining and processing probabilities, Committee for the Prevention of Disasters (CPR 12E), The Hague, The Netherlands.

Gheriani, M., Khan, F., Chen, D., Abbassi, R., 2017. Major accident modelling using spare data, Process Safety and Environmental Protection, Volume 106, Pages 52-59, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2016.12.004.

International Energy Agency (IEA), Technology Roadmap Hydrogen and Fuel Cells, 2015.

Japan Hydrogen and Fuel Cell Demonstration Project (JHFC Phase2), 2011. http://www.jari.or.jp/Portals/0/jhfc/data/report/pdf/tuuki_phase2_01.pdf

Japan Nuclear Technology Institute (JNTI). Estimation of domestic general equipment failure rate considering uncertainty of failure counts (1982~2002, for 21 years, 49 plants data), http://www.genanshin.jp/archive/failure_rate/; March 2009 [accessed September 2017].

Japan Nuclear Technology Institute (JNTI). Estimation of domestic general equipment failure rate considering uncertainty of failure counts (1982~2010, for 29 years, 56 plants data), http://www.genanshin.jp/archive/failure_rate/; June 2016 [accessed September 2017].

Khalil, Y., 2017. A probabilistic visual-flowcharting-based model for consequence assessment of fire and explosion events involving leaks of flammable gases. Journal of Loss Prevention in the Process Industries 50 (2017) 190–204.

Kodoth, M., Aoyama S., Sakamoto, J., Kasai, N., Shibutani, T., Miyake, A., 2018. Evaluating uncertainty in accident rate estimation at hydrogen refueling station using time correlation model, International Journal of Hydrogen Energy, Volume 43, Issue 52, 2018, Pages 23409-23417, ISSN 0360-3199,https://doi.org/10.1016/j.ijhydene.2018.10.175.

Kodoth, M., Khalil, Y., Shibutani, T., Miyake, A., 2019. Verification of appropriate life parameters in risk and reliability quantifications of process hazards, Process Safety and Environmental Protection, 2019, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2019.05.021.

Kubo, T., 2012. Introduction to statistical modeling for data analysis (generalized linear model, hierarchical Bayesian model, Markov chain Monte Carlo method). Tokyo: Iwanami; 2012.

LaChance, J., Houf, W., Middleton, B., Fluer, L., 2009. Analyses to support development of risk-informed separation distances for hydrogen codes and standards. SAND2009-0874 Sandia National Laboratories; 2009. http://prod.sandia.gov/techlib/access-control.cgi/2009/090874.pdf; [accessed September 2017].

NIST/SEMATECH, 2012. E-Handbook of Statistical Methods, http://www.itl.nist.gov/div898/handbook/,April 2012.

Ntzoufras, I., 2009. Bayesian Modeling Using WinBUGS. John Wiley & Sons, Inc., Hoboken, NJ, USA, January 2009.

Sakamoto, J., Sato, R., Nakayama, J., Kasai N., Tadahiro, S., Miyake, A., 2016. Leakage-type-based analysis of accidents involving hydrogen fueling stations in Japan and USA. Int. J. Hydrogen Energy, 2016; 41(46):21564–21570.

The High Pressure Gas Safety Institute of Japan (KHK), 2012. The high-pressure gas incidents database, https://www.khk.or.jp/english/accident_reports.html; [accessed Feb 2017].

The High Pressure Gas Safety Institute of Japan (KHK), 2015. Notes on Accidents related to Hydrogen Refueling Stations, 2015 (in Japanese).

Yamada, T., Kobayashi, H., Akatsuka, H., Hamada, K., 2015. Analysis of high-pressure gas incidents in hydrogen fueling stations. J High Press Gas Safety Institute Japan, 52 (10) (2015), pp. 23-29 [in Japanese].

Yang, M., Khan, F., Lye, L., 2013. Precursor-based hierarchical Bayesian approach for rare event frequency estimation: A case of oil spill accidents. Process Safety and Environmental Protection, Volume 91, Issue 5, Pages 333-342, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2012.07.006.

Appendix

Appendix A. Detailed explanation of estimation using a log-normal time function

This appendix gives a detailed explanation of Section 1.3.2.1. In order to calculate accident rate over time, each parameter in Eq. (2) is estimated to describe the accident data. In Eq. (2), parameters a, σ, and μ are considered random variables. Bayesian statistics estimate a parameter's value by updating its distribution by some data; thus, each parameter is first given prior distribution. If prior information is available about these parameters, the prior distribution reflects this information and is usually called "informative prior" (e.g., (Bedrick, 1996)). In contrast, when there is no prior information, prior distribution with little information (e.g., normal distribution with mean zero and variance 10^4) is used as a "non-informative prior." In this case, no prior information is available, and thus, a non-informative prior is used.

The value for each parameter was estimated using the Bayesian statistics supporting software WinBUGS. To calculate the posterior distribution by updating the prior distribution with the accident data, WinBUGS uses Markov Chain Monte Carlo simulation, and it needs an initial value for each parameter. An appropriate initial value was chosen by judgement or automatically selected by software, and it was checked for calculation errors.

For this estimation, the following Bayesian model is introduced. Note that other methods such as least squares fitting can also suffice and so there is no special reason to use the Bayesian model. However, using the Bayesian model often enables complex modeling and utilization of other information in addition to the observed data. The time-series accident rate is described by following logical relationship:

$$\overline{\lambda}_j = a \frac{1}{\sqrt{2\pi}\sigma t_j} \exp\left(-\frac{\left(\ln t_j - \mu\right)^2}{2\sigma^2} \right) \tag{A1}$$

where,

$\overline{\lambda_j}$: expected value of accident rate for the jth month

a: coefficient

σ, μ: parameters of the log-normal function

tj: jth operation time

j: index of the operation time

Each month's accident rate is considered as a random variable following the log-normal distribution below:

$$\lambda j \sim LN(\mu 2, j, \tau) \quad \text{(A2)}$$

where,

λj: accident rate of the jth operation time tj

LN(μ2, j,τ): log-normal distribution with mean μ2, j and inverse square of standard deviation τ

μ2, j: expected value of the log-normal distribution of the accident rate for the jth operation month

τ: inverse square of the standard deviation of the log-normal distribution

To connect Eq. (A1) and (A2), the relation between parameter μ2, j and the expected value of accident rate $\overline{\lambda_j}$ is utilized as follows:

$$\mu_{2,j} = \ln\left(\overline{\lambda}_j\right) - \frac{1}{2\tau} \quad \text{(A3)}$$

Prior distribution ("non-informative prior") of each parameter is set as follows:

$a \sim Gamma(1,1)$

$\tau \sim Gamma(1,1)$

$\sigma \sim Unif\ (0,10)$

$\mu \sim Unif\ (0,10)$

where,

Gamma(a,b): gamma distribution with shape parameter a and rate parameter b

Unif (a,b): uniform distribution with lower bound a and upper bound b

Using this statistical model and the accident data, the accident rate was estimated as shown in Fig.9.

Appendix B. Detailed explanation of estimation using a Weibull time function

This appendix gives a detailed explanation of Section 1.3.2.2. It differs from Appendix A in its description of the time-series accident rate and each parameter's prior distribution and initial value, but the flow of modeling and estimation are virtually the same as in Appendix A. Firstly, the time-series accident rate is described by following logical relationship:

$$\overline{\lambda_j} = a\left(\frac{\alpha}{\beta}\right)\left(\frac{t_j}{\beta}\right)^{\alpha-1} \exp\left(-\left(\frac{t_j}{\beta}\right)^{\alpha}\right) \quad \text{(B1)}$$

where,

$\overline{\lambda_j}$: expected value of the accident rate for the jth month

a: coefficient

α, β: parameters of the Weibull function

tj: jth operation time

j: index of the operation time

Each month's accident rate is considered as a random variable following the log-normal distribution below:

$$\lambda_j \sim LN(\mu_{2,j},\tau) \quad \text{(B2)}$$

where,

λj: accident rate of operation time tj

LN(μ,τ): log-normal distribution with mean μ and inverse square of standard deviation τ

μ2, j: expected value of the log-normal distribution of accident rate for jth operation month

τ: inverse square of the standard deviation of the log-normal distribution

To connect Eq. (B1) and (B2), the relation between parameter $\mu_{2,j}$ and the expected value of accident rate $\overline{\lambda_j}$ is utilized as follows:

$$\mu_{2,j} = \ln\left(\overline{\lambda_j}\right) - \frac{1}{2\tau} \quad \text{(B3)}$$

Prior distribution ("non-informative prior") of each parameter is set as follows:

$$a \sim Gamma(1,0.00001)$$
$$\alpha \sim Gamma(0.1,0.00001)$$
$$\beta \sim Gamma(0.1,0.00001)$$
$$\tau \sim Gamma(1,0.00001)$$

where,

Gamma(a,b): gamma distribution with shape parameter a and rate parameter b

Using this statistical model and the accident data, the accident rate was estimated, as shown in Fig.10.

CASE STUDY 2. Evaluating Uncertainty in Accident Rate Estimation at Hydrogen Refueling Station using Time Correlation Model

2.1 Introduction

Collecting data about accidents in the past will provide a hint to understand the trend in the possibility of accidents occurrence by identifying its operation time However, in new technology; accident rate estimation can have a high degree of uncertainty due to absence of major accident direct data in the late operational period. The uncertainty in the estimation is proportional to the data unavailability, which increases over long operation period due to decrease in number of stations. This case study utilizes the originality of the research through treatment of uncertainties due to lack of data in risk and reliability quantification for new technology system. To address this issue, a suitable time correlation model is adopted in the estimation to reflect lack (due to the limited operation period of HRS) or abundance of accident data.

There is a possibility of abnormal events occurring at an HRS due to increased activities and operations performed at the HRS. In Japan, as HRSs store and dispense hydrogen are at a relatively high pressure, they are controlled by the High Pressure Gas Safety Act. Accident information such as hydrogen leakage at an HRS is available in the high-pressure gas incidents database of The High Pressure Gas Safety Institute of Japan (KHK, 2016). This database contains a compilation of high-pressure gas accidents, including the accident information for HRSs. In the law, explosions, fires, spouting or leak, rupture or damage, and loss or burglary are defined as “accidents” (METI, 2017). One of the characteristics of HRS accidents in Japan is that a high percentage of leak accidents occur at the joint section of the pipe (Sakamoto et al., 2016). Note that even a small leakage has to be reported based on the guidelines described in the High Pressure Gas Safety Act. This is because in the case of hydrogen fuel, even a small leak can lead to catastrophic events. In this study, “accident” refers to that defined in the High Pressure Gas Safety Act. Considering the accident statistics of natural gas stations, there are concerns that HRS accidents may increase as more HRSs are implemented in the future (Yamada et al., 2015).

Focusing on the HRS operation time from its start may reveal important characteristic of accident occurrence. In other words, collecting data about accidents in the past will provide a hint to understand the trend in the possibility of accidents occurring by identifying its operation time. However, the estimation of accident rate is only as good as the data availability. Under such circumstances, addressing uncertainty in the statistical data through time series effect is important. In this study, a suitable time correlation model is adopted in the estimation to reflect lack (due to the limited operation period of HRS) or abundance of accident data, which is not well supported by conventional approaches. The model adopted in this study shows that the uncertainty in the estimation increases when the operation time is long owing to the decreasing data.

2.1.1 Relevant safety studies

There are recent quantitative risk assessment (QRA) studies on hydrogen refueling stations and storage infrastructure to consider the application of accident scenario modelling (Dadashzadeh et al., 2018). The first step in the risk analysis is to conduct hazard and operability (HAZOP) study to liquid hydrogen fueling station (Jones, 1984). Failure mode and effects analysis (FMEA) is then reported for hydrogen fueling systems to understand component failures and their effects on the system. These two techniques are used in a study that performed the FMEA and HAZOP to identify possible accident scenarios for liquid hydrogen fueling station (Kikukawa et al., 2009). Pasman and Rogers (2012) performed risk assessment for compressed and liquefied hydrogen transportation and tank station by means of Bayesian networks. Nakayama et al. (2016) carried out the preliminary hazard identification to a hybrid gasoline-hydrogen fueling station with an on-site hydrogen production system using organic chemical hydride.

Studies have also been performed on HRS accident and leak frequency by major organizations such as Sandia National Laboratories (LaChance et al., 2009a). There are few research studys discussing on the application of accident scenario frequency modelling in risk analysis (Esmaeil et al., 2017; Nima et al., 2014; Ali et al., 2014). Accident rate estimation can provide a crucial input to Quantitative risk assessment (QRA) to quantify risks numerically. Matthijsen et al. (2006) performed risk assessment of hydrogen filling stations with the generic data taken from references (Schüller et al., 1997). LaChance

et al. (2009b) performed QRA to determine separation distances for hydrogen refueling stations. Tsunemi et al. (2017) estimated consequence and damage caused by an organic hydride hydrogen refueling station numerically.

Risks are measured from the combination of frequencies and consequences of the scenarios. Estimation of accident rates provides a key input to reliability and risk assessment quantification. Unfortunately, however, hydrogen failure data is extremely limited. One possible way is to use surrogate failure data from other settings such as commercial nuclear power plants, chemical plants, and offshore oil and natural gas platforms (Schüller et al., 1997). A study uses the fault tree analysis (FTA) to determine frequency of the accident scenarios based on generic failure data (Casamirra et al., 2009). Another way is to employ a Bayesian statistical approach to estimation of failure rate from prior accident data. A study developed a Bayesian model to estimate leak frequency leading to accidents in various components used in a hydrogen refueling stations (LaChance et al., 2009a).

2.2 Objective

Accident rate estimation plays a vital role in the determination of the occurrence frequency of the accidental scenarios. The work can conclude whether the refueling station taken into consideration is safe enough from frequency point of view or any additional refined studies are required. However, a drawback in the analysis could be lack of experience and the scarcity of the relevant data collection (Casamirra et al., 2009). The data scarcity drawback can be solved by understanding the uncertainty in the estimation due to data unavailability.

Compared to the risk analysis, the accident data uncertainty has not been so well-established, partly due to low probabilities involved and partly due to the complexity of such accidents (Nima et al., 2014). For this purpose, we have introduced a study on the accident data uncertainty based on time correlation model. This is also one of the reasons for using operation time as the basis of analysis in this study. This study estimates the uncertainty and accident rate by time correlation model that are fundamental to the challenge of lack of data, and not been addressed in previous models. This new way of dealing with and interpreting accident information can be utilized to evaluate new systems such as HRS in the future.

2.2.1 Accident data evaluation at HRSs based on operation time

The accident data for HRS is collected and counted based on the events listed in the high-pressure gas incidents database (KHK, 2016). The number of accidents at an HRS over time from the start of its operation is determined. “HRS operation start” denotes the start of operation of the HRS used in either test research, or commercial operation. The operation start time of the HRS does not include the time the HRS infrastructure was built. Operation time is the period between the operation start month and the accident occurrence month. This study uses “month” as the unit of time measurement.

Thirty-four HRSs operating from 2002 to 2014 in Japan, including onsite and offsite type, for test research and commercial use, were investigated. The operation start time for all HRSs is considered together at the same time in the analysis. The overall number of accidents recorded for these HRSs is 26. Out of these 26 accidents, 23 accidents resulted in leakage, 3 accidents resulted in explosion. Further details on the operating time and accident information for each of the 26 accidents is provided in Appendix C.

Firstly, the accident data for each HRS were investigated with respect to operation time and summed for total accidents, as shown in Fig. 12.

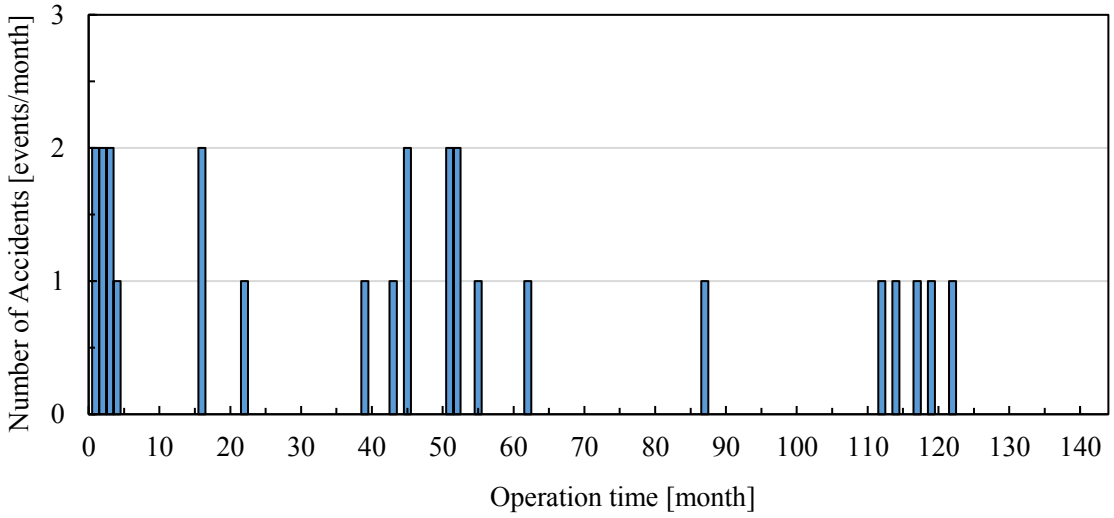


Figure 12. Accidents in HRS by operation time (total count)

The graph in Fig. 12 can be categorized into the following three cases:

- Case I: Events occurred in the short period. Looking across the operation time, some event occurred in short period (i.e., 10 accidents in the first 24 months).
- Case II: Events occurring at the intermediate operation time. This includes 10 accidents that occurred between the 25th month and the 85th month.
- Case III: Events occurring at the later operational time. This includes 6 accidents that occurred between the 86th month and the 144th month.

Note that the length of operation for each station differs; hence, the number of stations differ at each operation time (Fig.13). For example, there are 15 stations at the 50th month, but only 7 remaining at the 100th month. Fig.13 shows the number of existing stations at each operation month. It can be concluded from the below chart that the data availability is decreasing with increasing operation period.

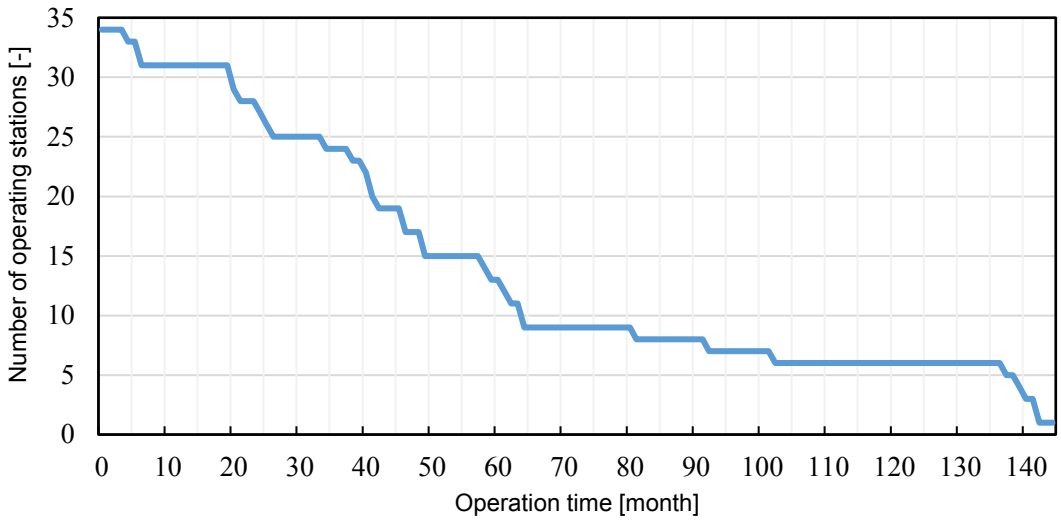


Figure 13. Number of stations operating in each month

The next step is to divide accident counts by the number of existing stations. Dividing the accident count by the number of existing stations results in the mean accident count shown in Fig.14. The trend in Fig.14 is an increase in accidents in the later operation time, but this is because the number of stations has decreased. The accident data is available up to 122 months based on the high-pressure gas incident database (KHK, 2016). However, this study analyses data up to 144 months.

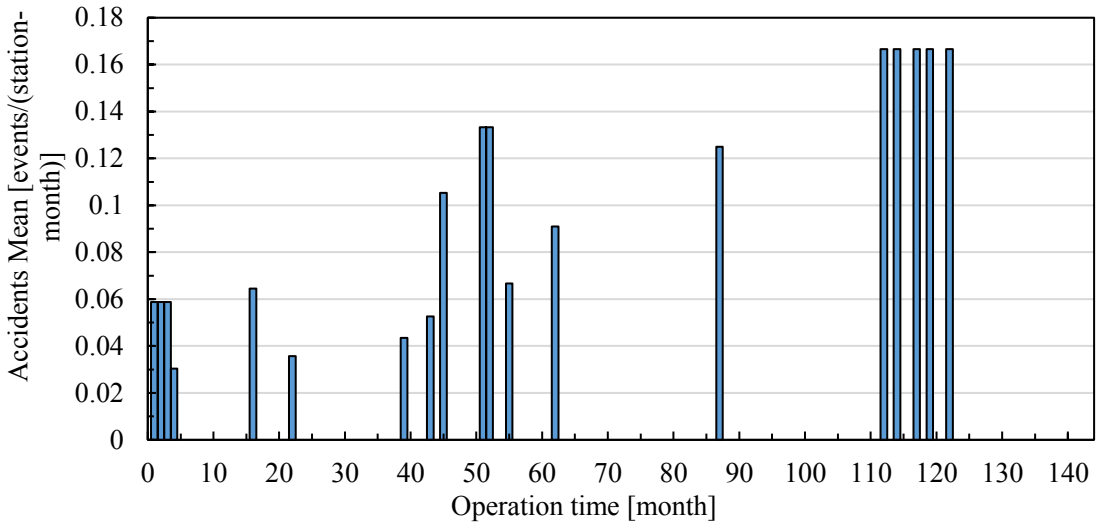


Figure 14. Accidents in an HRS by operation time (mean)

There are several drawbacks in the data represented in Fig.14. These are:

1. The data availability is decreasing over time due to less number of existing stations. This introduces large uncertainty in the estimation at the late operational period.
2. The data collected from multiple HRSs is that each station has dissimilar operation period. The availability of data varies for two stations with different operating hours. For e.g. a station operated for 1 year will have limited data compared to the station operated for 10 years. This implies that the data are all mixed and not based on common requirements. This leads to a large uncertainty in the result after modelling theory is applied.
3. There is no accident data between some months. For e.g. there is no accident data between 25thmonth to 38th month.

2.3 Method of uncertainty evaluation

2.3.1 Application of intrinsic CAR model to estimate Uncertainty

In order to address the above issue, conditionally autoregressive (CAR) model is applied (Kubo, 2012). Conditional autoregressive (CAR) model is a graphical or network model designed to specifically model spatially auto correlated data based on neighborhood relationships (Barua et al., 2014). Due to its benefit to describe spatial correlations, it is suitable for application to accident data such as in Fig.14. As observed in Fig.14, there are missing data for several months which can lead to uncertainty in accident rate estimation. Prediction of random variable in off-sample (missing) areas using is

unambiguous since it is not obvious how to specify the adjacent structure of just the in-sample (observed) areas ignoring the off-sample areas. As illustrated by Banerjee et al. (2004) for the case of a CAR model fitted to point level (rather than area) data, prediction at a missing location can be achieved by constructing a CAR model for the full set of observed and missing location. In this study, a CAR model is specified for the full set of spatial random variable in the in-sample and off-sample areas, and simply treat the response data in the off-sample areas as missing. This leads to a modified set of full conditional distributions for the spatial random effects in off-sample areas in the Markov Chain Monte Carlo (MCMC) scheme used to estimate the posterior distribution (Kubo, 2012). This study utilizes this method to estimate uncertainty in the accident data. The accident rate is estimated to have similar value to the adjacent month by utilizing the intrinsic Gaussian CAR model. The variable under observation are assumed to follow Poisson, and autocorrelation is modelled by a set of random effects that are assigned a CAR prior distribution (Bedrick et al., 1996)

2.3.2 Accident rate description using time correlation model

The problem that arises when using time series data collected from multiple HRSs is that each station has dissimilar operation period. The availability of data varies for two stations with different operating hours. For e.g. a station operated for 1 year will have limited data compared to the station operated for 10 years. It is intuitively supposed that when computing accident data shown in Fig.13, the result of the early operation period is reliable, however the estimation of the late operation period is not very convincing.

In order to address the above issue, CAR model is applied. Firstly, in the case of the 34 HRSs with accident data, the start operation time for all stations are considered together. However, the numbers of accidents for the stations are not summed; instead, they are treated separately for each station. Accident occurrence is modelled using Poisson distribution for each month per station. Poisson distribution has been found advantageous for describing count data (i.e., 0, 1, 2 …) for each month and each station (Fairos et al., 2010). Thus, accident rate on i^{th} month for j^{th} station is considered as a random variable following the Poisson distribution:

$$Y_{i,j} \sim Poisson\ (\lambda_i) \tag{11}$$

where,

$Y_{i,j}$: accident occurrence for each month per station

i: operation time index

j: station index

λ_i: expected value of the Poisson distribution of the accident rate for each month

In addition, to make changes with time, the mean of the Poisson distribution is considered and described using two parameters, β and r_i. The β parameter considers the overall-time accident rate whereas the r_i parameter considers only the individual month's accident rate. It takes the form of the generalized linear model shown in Eq. (12), where the left-side function is called the logarithmic link function and the right side is called the linear predictor.

Here, the expected value of the accident rate λi is described by generalized linear model below:

$$Log\ (\lambda_i) = \beta + r_i \tag{12}$$

where,

Log (λi): logarithmic link function of λi

B: global parameter and

r_i:: local parameter

The characteristic of this model is such that the accident rate may change; however, the value is relatively similar to the adjacent month. Time correlation was set to the statistical model by utilizing the intrinsic Gaussian CAR model. In this model, each local parameter ri does not take a value independently. To connect each local parameter ri, their prior distribution must be described by Eq. (13). The local parameter ri follows the prior distribution given that μi is true. μi is calculated as equal to the mean of two values, ri-1 and ri +1, of the adjacent operation time. Parameter s represents the overall dispersion. If s is small, ri does not vary widely and the accident rate is smooth overall. Conversely, if s is large, ri varies widely and the accident rate fluctuates significantly. Equations (13) and (14) are applied to estimate the accident rate using the time correlation model. In the simplest form, the density

of an intrinsic CAR model for r = (r1…rn) is

$$p(r_i \mid \mu_i, s) = \sqrt{\frac{n_i}{2\pi s^2}} \exp\left\{ -\frac{(r_i - \mu_i)^2}{2s^2/n_i} \right\} \quad (13)$$

$$\mu_i = \frac{r_{i-1} + r_{i+1}}{2} \quad (14)$$

where,

μi is the mean of the value of the two local parameters r_i -1 and r_i +1

s is the parameter representing overall dispersion. It is the precision parameter that determines the amount of smoothing and it is commonly estimated from data

In other words, the prior distribution of the i[th] local parameter r_i should be a normal distribution with mean μ_i and standard deviation $s/\sqrt{n_i}$. The prior distribution ("non-informative prior") of the other parameter is set as follows:

$\beta \sim N(0,0.0001)$

$s \sim Unif(0, 10000)$

where,

N(μ,τ): normal distribution with mean μ and inverse square of its standard deviation τ

Unif (a,b): uniform distribution with lower bound a and upper bound b

2.3.3 Flow of accident rate analysis using the conditional autoregressive model

The flow of accident rate analysis using the conditional autoregressive model is shown in Fig.15. The analysis flow is divided into the two parts. Part 1 is related to organizing data in the format suitable to the model. Part II performs statistical analysis based on the model described in Section 2.3.2.

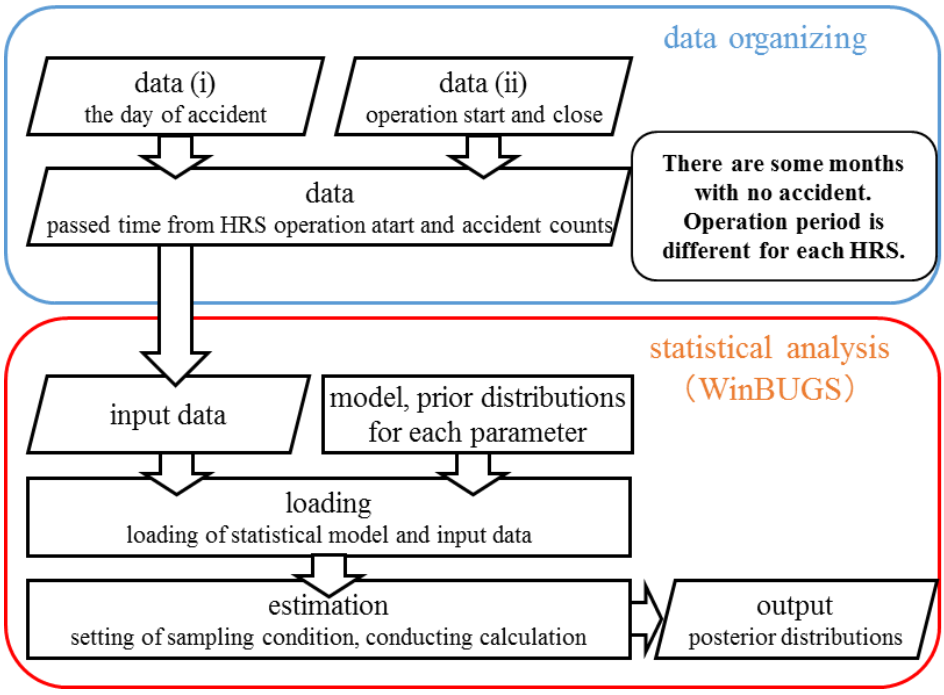


Figure 15. Flow of analysis using conditional autoregressive model

Part I: Input data preparation for statistical analysis software - Unlike accident rate analysis using traditional method, data processing is not needed in the conditional autoregressive model. This means the statistical data shown in Fig.14 can be directly used as an input data to CAR model without any data processing. The prior distribution for the dataset is represented in Fig.14. The prior (input) data reported is given as an input to the model. However, the important thing to note is that there are several problems associated with the prior data. There are some months with no accident and operation period is different for each HRS.

Part II: Statistical analysis using WINBUGS software - Using the prior (input) data, the accident rate for each month is estimated. To calculate the accident rate through updating of the prior distribution with the accident data, WinBUGS uses Markov Chain Monte Carlo simulation, and it needs an initial value for each parameter. The model in WINBUGS is written in a series of commands. The statistical model used in this study will overcome the problems by:

1. Estimating accident rate for each month by the condition that the adjacent accident rate is similar to each other
2. Estimating uncertainty associated with data over operation period

The model output is obtained from the WINBUGS and is represented in the form posterior distribution. The posterior distribution is further analyzed to understand the uncertainty associated with the data. Fig.16 shows a posterior output from the model and thereafter several comparisons and conclusions are made.

2.4 Results - Accident rate Estimation and Uncertainty Analysis

The interpretation from the outcome of this model is important. The accident rate estimation provided by the time correlation model is based on the interpretation of the reality. The accident rate estimation using the lognormal type function or Weibull function estimates the accident rate change over time. This model estimates the accident rate per month, and is constrained by the condition that the adjacent accident rate is similar to each other.

In Fig.16 the results of accident rate for each month have been plotted. The distribution shows the expected (mean) value of the accident rate for each month. In addition to the mean value, the upper bound and lower bound of 95% credible interval are plotted in the same distribution. The three peaks obtained in Fig.16 can be related to the 3 cases described in section 2.2. Peak 1 is a result of events occurring in the short period. i.e., seven accidents in the first four months. Peak 2 is a result of events occurring at intermediate operation time. Finally, Peak 3 is a result of events occurring at late operational time. This model approximates accident data for some months that originally does not have any accident data. The estimated accident data for each month is adjacent to its predecessor month thereby obtaining non-discrete distribution.

In addition to the uncertainty estimation, the graph in Fig.16 has two main differences compared to Fig.14. Firstly, the bar graph in Fig.14 shows only discrete values whereas in Fig.16, the graph is continuous without any gaps in the data between each stations. Secondly, no-accident months exist in Fig.14, whereas in Fig.16, each month has a positive value. Thirdly, in Fig.14, the bar graph does not define the probability of accident occurrence.

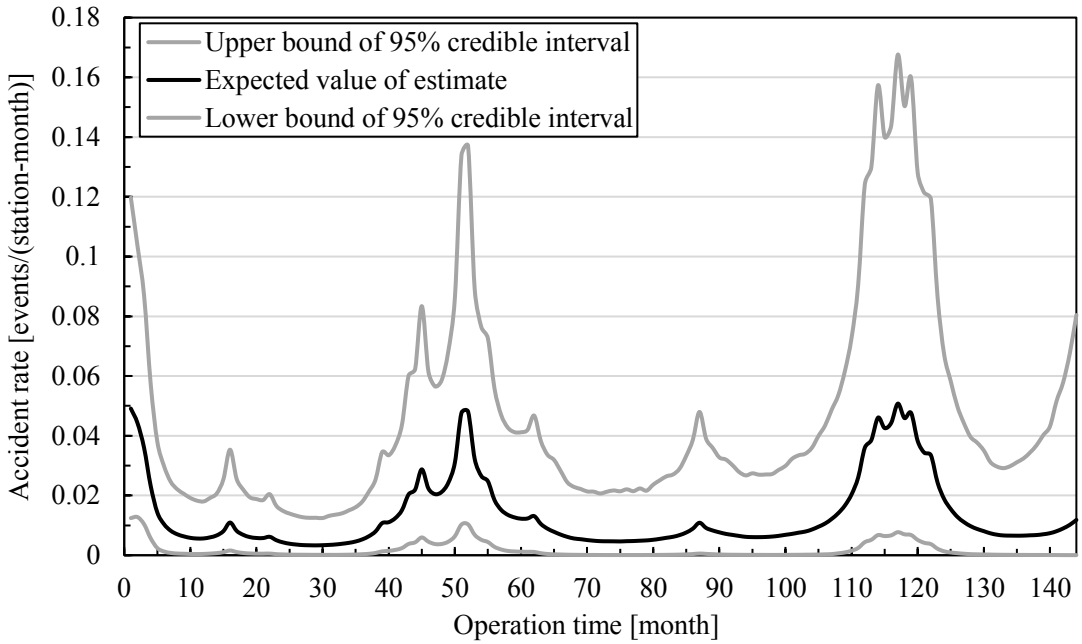


Figure 16. Results - Accident rate in an average HRS across its operation time, estimated using the intrinsic Gaussian conditional autoregressive model

It can also be noticed that the credible interval is narrower during the start operation period of the HRS. Remarkably, the credible interval tends to expand as the operation time elapses. This is because the amount of available data decreases as the operation time increases, as mentioned in Section 2.2. There is a wider distortion between the expected value and lower/upper bound credible interval at the late operational period for e.g. after 80th operating month. The wider the credible interval, the higher uncertainty in the accident rate estimation. In order to demonstrate this numerically, we have assigned an error factor (EF) which is the difference between the upper bound and lower bound. Error factor as defined in the red book on probability estimation is given by (Schüller et al., 1997):

$$EF = \sqrt{\frac{x'0.95}{x'0.05}} \tag{15}$$

Where,

$x'_{0.95}$ = upper bound of 95% credible interval

$x'_{0.05}$ = lower bound of 95% credible interval

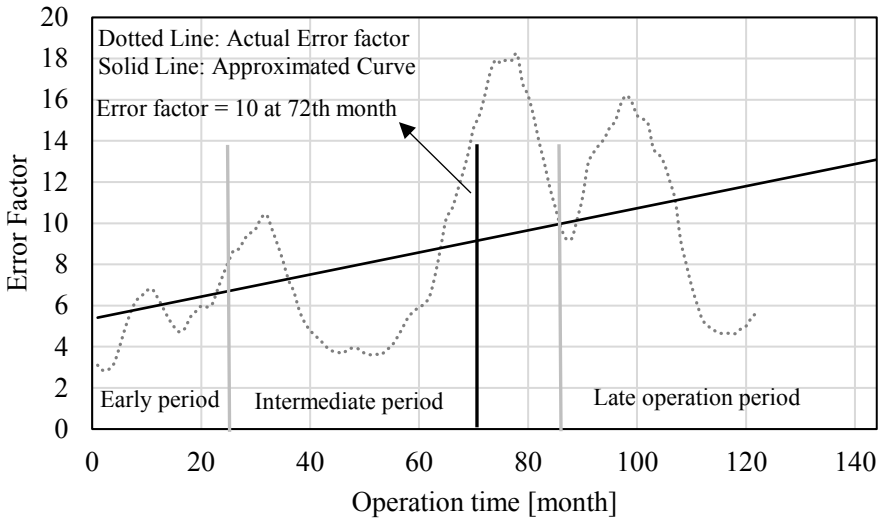


Figure 17. Result and Interpretation – Evaluation of Uncertainty by means of Error Factor

The result of the error factor starting from 1st month till 144th month is shown in Fig.17. The lower bound and upper bound of accident rate for each month can be calculated from Fig.16. The plotting of error factor vs operation month is shown in Fig.17. As the original data has random data for each month with some months having no data, the graph is non-uniform. The operation time is divided into early, intermediate, late operation period based on the 3 cases categorized in section 2.2. An interpretation of the results is developed using approximate curve as shown by solid line. The solid line is taken as the linear smooth curve from the plotted points. This shows an increasing trend for error factor over the operation month. The error factor can be related to decreasing data over the longer operation period. The average error factor is less than 10 from the beginning of the operation period until the mid-operation month i.e. till 72th month approximately. However in the late operation period, it can be noticed that the error factor shoots well above 10 pointing towards higher uncertainty in the data as a result of no enough data available during that period.

Furthermore, using CAR model offers some advantageous such as it can directly use accident data of HRS with different lengths of operation month without any data processing. In CAR model, the total number of HRSs is not considered. Even though the number can be more or less than reality, the result is not significantly affected. However, less information than target may cause uncertainty in the estimation.

2.5 Conclusions

This study examined the manner in which accident rate is modelled for HRSs. Unlike conventional statistical models in which the accident rate changes according to overall time function, CAR model estimates the accident rate per month, and is constrained by the condition that the adjacent accident rate is similar to each other. Another result is that of the intrinsic Gaussian CAR model, which represents the uncertainty in the estimation due to lack of data. The CAR result succeeded in showing that the uncertainty in the estimation increases when the operation time is long owing to the decreasing data.

A model with accident rate following the intrinsic Gaussian conditional autoregressive model has following advantages:

- Suitable to show the estimate uncertainty is increasing owing to lack of data
- Estimates the accident rate per month and thus the graph is continuous without any gaps in the data between stations
- Support in decision making for new process systems

2.6 Acknowledgement

Funding: This research was supported by the Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Energy carrier” (Funding agency: Japan Science and Technology Agency (JST)).

2.7 References

[1] The High Pressure Gas Safety Institute of Japan (KHK). The high-pressure gas incidents database, https://www.khk.or.jp/english/accident_reports.html; Version 2016.

[2] Ministry of Economy, Trade and Industry. The incident response manual of the High Pressure Gas Safety Act, http://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/files/manual250226.pdf; [accessed September 2017].

[3] Sakamoto J, Sato R, Nakayama J, Kasai N, Tadahiro S, Miyake A. Leakage-type-based analysis of accidents involving hydrogen fueling stations in Japan and USA. International Journal of Hydrogen Energy, Vol. 41, pp. 21564-21570, 2016.

[4] Yamada T, Kobayashi H, Akatsuka H, Hamada K. Investigation and analysis of accident cases in gas stations. The High Pressure Gas Safety Institute of Japan, 2015; 52(10); 23-9 [in Japanese].

[5] Dadashzadeh M, Kashkarov S, Makarov D, Molkov V. Risk assessment methodology for onboard hydrogen storage. International Journal of Hydrogen Energy, Volume 43, Issue 12, 2018, Pages 6462-6475, ISSN 0360-3199, https://doi.org/10.1016/j.ijhydene.2018.01.195.

[6] Jones N. A Schematic Design for a HAZOP Study on a Liquid Hydrogen Filling Station. International Journal of Hydrogen Energy, Vol. 9, pp. 115-121, 1984.

[7] Kikukawa S, Mistuhashi H, Miyake A. Risk assessment for liquid hydrogen fueling stations. International Journal of Hydrogen Energy, Vol. 34, pp. 1135-1141, 2009.

[8] Pasman H, Rogers W. Risk assessment Risk assessment by means of Bayesian networks: A comparative study of compressed and liquefied H2 transportation and tank station risks. International Journal of Hydrogen Energy, Vol. 37, pp. 17415-17425, 2012.

[9] Nakayama J, Sakamoto J, Kasai N, Shibutani T, Miyake A. Preliminary hazard identification for qualitative risk assessment on a hybrid gasoline-hydrogen fueling station with an on-site hydrogen production system using organic chemical hydride. International Journal of Hydrogen Energy, Vol. 41, pp. 7518-7525, 2016.

[10] LaChance J, Houf W, Middleton B, Fluer L. Analyses to support development of risk-informed separation distances for hydrogen codes and standards. SAND2009-0874 Sandia National Laboratories; 2009. http://prod.sandia.gov/techlib/access-control.cgi/2009/090874.pdf; [accessed September 2017].

[11] Esmaeil Z, Ali A, Nima K, Mostafa M, Iraj M. Dynamic safety assessment of natural gas stations using Bayesian network. Journal of Hazardous Materials, Volume 321, 2017, Pages 830-840, ISSN 0304-3894,

https://doi.org/10.1016/j.jhazmat.2016.09.074.

[12] Nima K, Faisal K, Nicola P. On the application of near accident data to risk analysis of major accidents. Reliability Engineering & System Safety, Volume 126, 2014, Pages 116-125, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2014.01.015.

[13] Ali A, Arshad A, Faisal K. Accident modelling and analysis in process industries. Journal of Loss Prevention in the Process Industries, Volume 32, November 2014, Pages 319-334.

[14] Matthijsen A, Kooi E. Safety distances for hydrogen filling stations. Journal of Loss Prevention in the Process Industries, Vol. 19, pp. 719-723, 2006.

[15] Schüller J, Brinkman J, Van Gestel P, Van Otterloo R. Red Book - Methods for determining and processing probabilities. Committee for Prevention of Disasters Second edition, The Hague, The Netherlands, 1997.

[16] LaChance J. Risk-informed separation distances for hydrogen refueling stations. International Journal of Hydrogen Energy, Vol. 34, 5838-5845, 2009.

[17] Tsunemi K, Yoshida K, Yoshida M, Kato E, Kawamoto A, Kihara T, Saburi T. Estimation of consequence and damage caused by an organic hydride hydrogen refueling station. International Journal of Hydrogen Energy, Vol. 42, Issue 41, pp. 26175-26182, 2017.

[18] Casamirra M, Castiglia F, Giardina M, Lombarado C. Safety studies of a hydrogen refueling station: Determination of the occurrence frequency of the accidental scenarios. International Journal of Hydrogen Energy, Vol. 34, pp. 5846-5854, 2009.

[19] Kubo T. Introduction to statistical modeling for data analysis (generalized linear model, hierarchical Bayesian model, Markov chain Monte Carlo method). Tokyo: Iwanami; 2012.

[20] Barua S, El-Basyouny K, Islam MT. A full Bayesian multivariate count data model of collision severity with spatial correlation. Analysis Methods Accid Res, 2014;3-4:28–43.

[21] Banerjee S, Carlin B, Gelfand A. Hierarchical Modeling and Analysis for Spatial Data. Chapman & Hall/CRC, Boca Raton, Florida (2004).

[22] Bedrick J, Christensen R, Johnson W. A new perspective on priors for generalized linear models. J. Am. Stat. Assoc. 1996; 91(436):1450–1460, http://www.jstor.org/stable/2291571/; [accessed September 2017].

[23] Fairos W, Mohamad A, Yap B. A Practical Approach in Modelling Count Data. Proceedings of the Regional Conference on Statistical Sciences 2010 (RCSS'10) June 2010, 176-183.

Appendix C. Detailed explanation of 26 accidents collated from database (KHK, 2016)

ID	Acc. Code (KHK-ID)	Accident Name	Failure Date	Number of elapsed months
1	2005-120	Hydrogen leakage from filling hose	13-05-2005	2
2	2005-222	Hydrogen leakage at hydrogen station	28-07-2005	4
3	2005-415	Explosion of hydrogen at hydrogen station	07-12-2005	1
4	2006-216	Hydrogen leakage at hydrogen station	17-06-2006	39
5	2006-433	Hydrogen leakage in compressed hydrogen gas	24-10-2006	3
6	2007-532	Hydrogen gas leakage accident	17-10-2007	55
7	2007-557	Hydrogen gas leakage accident	07-08-2007	51
8	2007-574	Hydrogen gas leakage accident	28-09-2007	51
9	2010-122	Hydrogen leakage from filling hose during filling operation	12-05-2010	2
10	2010-135	Inhalation of hydrogen station, hydrogen leakage from discharge valve mounting part	15-06-2010	87
11	2011-066	Hydrogen leakage from dispenser joint due to earthquake	12-03-2011	3
12	2012-090	Hydrogen leakage from the cap nut of the connection part of the card	09-04-2012	16
13	2012-224	Hydrogen leakage from hydrogen station pressure gauge	10-07-2012	62
14	2012-226	Leakage from hydrogen station dispenser and hose attachment	18-07-2012	16
15	2012-314	Leakage from valve mounting part of hydrogen stand	17-10-2012	22
16	2012-339	Hydrogen leakage from the valve connection	05-11-2012	114
17	2012-362	Hydrogen leakage from the check screw ground thread portion of compressor discharge	30-10-2012	112
18	2013-037	Hydrogen leakage from the accumulator base valve	06-02-2013	119
19	2013-063	Leakage from liquid hydrogen receiving lower valve at hydrogen station	09-03-2013	117
20	2013-115	Leakage from overflow preventing valve connection of hydrogen station	22-05-2013	1
21	2014-173	Hydrogen leakage from the shutoff valve	03-07-2014	52
22	2014-182	Hydrogen leakage from filling hose after completion of filling test	17-07-2014	52
23	2014-299	Hydrogen leakage from the connecting part of the compressor unit	24-10-2014	43
24	2014-349	Explosion during inspection of opening of accumulator	09-12-2014	45
25	2013-356	Hydrogen leakage from suction valve of compressor	31-07-2013	122
26	2013-376	Rupture of hydrogen filled hose during filling test	03-12-2013	45

CASE STUDY 3. Verification of appropriate life parameters in risk and reliability quantifications of process hazards

3.1 Introduction

Verification of QRA can be performed in several ways. One of the method is to verify the selection of appropriate parameters in risk assessment. This case study is chosen to support the core concept of the research by focusing on mainly two aspects: i.e. new technology system and verification of uncertainties in risk and reliability quantification. This case study utilizes the originality of the research through treatment of uncertainties in the field of risk and reliability quantification by verification of appropriate parameters for new technology system.

QRA methods contain a large amount of uncertainty due to the lack of field failure data. This recognizes a need of collecting sufficient and improved reliability data for new technology systems (Rademaeker et al., 2014) .The verification and validation of QRA has become a great concern to public acceptance of HRSs. The validity of QRA was reviewed by Goerlandt et al. (2016). Generic validity approaches such as benchmark tests have been proposed, but it was pointed out that an evidence-based approach is needed to support the validity of QRA results.

Moreover, failure frequency estimation is one of the important measures of risk quantification. In traditional reliability assessment, mean time to failure (MTTF) is one of the most common approaches to field failure data analysis. MTTF is a unit of measuring reliability that treats failure as a constant value. It can lead to uncertainty because process failures are not always constant in nature. For example, gradual deterioration of process vessel, cylinder corrosion or erosion of pipelines are non-constant failures in reality. This kind of failures should not be measured using MTTF concept which at the moment not all industries follow. This makes it critically important to use the correct parameters for accurate reliability estimation.

In the past, Sandia National Laboratories reported on hydrogen leak frequency for HRSs (LaChance et al., 2009). They used the Bayes approach for statistical modeling to determine hydrogen leak frequency data in refueling facilities. In the report, leak frequency is determined through a functional relationship

between leak size and leak frequency. In other words, a part of a pipe is likely to have more small hole leaks than a large hole leak (Sakamoto et al., 2016). The present study uses a different approach compared to the leak size approach as it expresses failure rate with respect to survival time and number of fillings.

This study discusses verification of appropriate parameter in failure estimation and its influence on the reliability assessment to offset the limitations associated with data scarcity and QRA uncertainty problems. Selection of the appropriate parameter in reliability assessment can be one of the possible ways to verify and validate the accuracy of QRA results. Field failure data of hydrogen refueling stations (HRS) is used as a case study to compare failure analysis based on two parameters i.e. survival time vs. number of fillings at the station. A non-parametric approach is used to estimate cumulative failure function based on number of fillings. The cumulative hazard using the Nelson-Aalen estimator showed a linear relationship with the number of fillings. A parametric approach using 2-parameters (β and η) Weibull distribution function is employed to estimate cumulative probability of failure with the survival time. The present study demonstrates that the failure rate can vary by a small to large margin based on the life parameter chosen for reliability predictions. Accordingly, the objectives of this study are as follows:

1) Estimate the failure rate based on the number of fillings and survival time of HRS.
2) Employ a non-parametric approach to estimate cumulative failure as a function of no. of fillings.
3) Use a parametric approach to estimate cumulative failure as a function of survival time.
4) Compare both parameters to choose correct life parameter for reliability quantification.

3.2 Analysis of failure data

Analysis of failure data has been carried out based on the hydrogen and accident reports. When an accident takes place with respect to the high-pressure gas, a notification report shall be submitted to the prefectural governor or law enforcement pursuant to the High Pressure Gas Act (METI, 2017). According to the law, the accident is classified as follows:(i) Explosion, (ii) Fire, (iii) Leak, (iv) Degradation, (v) Others. In this study, the Japan Hydrogen and Fuel Cell Demonstration Project (JHFC) data source was used to collect failure and operating data. JHFC demonstration project was mainly carried on 35MPa systems built to study HRS related accidents. Thus, accidents reported during the

demonstration phase of HRSs is related to 35MPa systems. It should be noted that the estimated failure rate depends on failure data of 35 MPa systems and not 70 MPa commercial systems.

3.2.1 Description of the Japan Hydrogen and Fuel Cell (JHFC) Demonstration Project

Data for estimation of failure rates are taken from the reports of the Japan Hydrogen and Fuel Cell Demonstration Project (JHFC). JHFC is a demonstration project sponsored by the Minister of Economy, Trade and Industry (METI) and started in Fiscal year (FY) 2002 (JHFC, 2011). HRS is a relatively new technology and thus the failure data is extremely limited. The data collected from the demonstration project report considers a total of 28 stations. These 28 stations, which includes three corporation stations, were established and operated to collect operating data from FY2002 to FY2013 (NEDO, 2014). Seventeen failure data (i.e.17 failure events) were collected from FY2002 to FY2013. The number of fillings and survival days to failure are calculated from the failure date. Censored data are also collected from the stations without a failure until the end of FY2013. The failure data of all 28 stations collated from JHFC report is listed in Appendix D.

3.3 Methods

In this section, various parameter-based models are applied to refueling stations' accident data to understand their characteristics. As each model has a different application, care should be taken to apply the correct model to the data. For this reason, the models are compared.

3.3.1 Estimation of failure rate, λ(t), based on assumed constancy over time

Herein, the failure rate is estimated based on the assumption that it remains constant over time. Accordingly, the failure rate (λ) is calculated by dividing the total number of failures by the total survival time. Here, the sum of all failures that occurred, (namely, 17 failure events) in 28 hydrogen fueling stations (S1, S2… S28) represents the total failure count 'Y', and the whole survival time for each station is summed up to give the total survival time 'T'. The total failure count 'Y' is divided by the total survival time 'T' to yield the average failure rate (λ) as described by Eq. (16):

$$\lambda(t) = \frac{Y}{T} = \frac{17\ \text{[failure events]}}{127.69\ \text{[survival years]}} = 0.13\ \text{[failure events/(station-year)]} \qquad (16)$$

In Eq. (16), the calculated value of 0.13 can be viewed as the average value for all 28 stations. Assuming

that this failure rate is constant over time, the number of failures can be predicted. In this case, it is about one failure in 7.69 years.

One of the studies associated with constant failure over time was conducted by JANSI (2009) that focused on an estimation method for failure rate calculated the equipment failure rates of a Japanese nuclear power plant from its probabilistic risk assessment (PRA). Japan Nuclear Technology Institute employed the Bayesian methodology to enable the uncertainty band of failure rate to be updateable with data storing, which until then had a fixed value (JANSI, 2017). This methodology is also used in the latest report (Jones, 1984). The report by Jones (1984) considers the failure rate to be constant over time and the probabilistic variance is updated by new data. In addition, the observation probability {p} is taken into account for the purpose of failure rate estimation. In cases where abundant and reliable field failure data and operating time data are available and operating time, then Eq. (16) can be applied to calculate the failure rate.

3.3.2 Non-Parametric Distribution Analysis using Nelson-Aalen estimate

Total failure rate of components and systems in HRS was estimated from JHFC data (NEDO, 2014). JHFC reported not only failure data but also operating data such as the total number of fillings per month. The easiest method to apply this non-parametric approach is to divide the total number of failures by the total number of fillings. Here, the sum of all failures that occurred, i.e. 17, in 28 hydrogen fueling stations defines the total failure count 'Y,' and the total number of fillings for each station is summed up into a total number of fillings 'N.' The total failure count Y is then divided by the total number of fillings N to calculate the average failure rate per fillings 'f (n)' as described by Eq. (17).

$$f(n) = \frac{Y}{N} = \frac{17\ [failure\ events]}{24063\ [number\ of\ fillings]} = 0.0007\ [failure\ events/(filling)] \quad (17)$$

The number of fillings and survival time data can be collated to understand the number of fillings performed per day at a station. The number of fillings per day is calculated as described by Eq. (18).

$$n_a = \frac{24063\ [number\ of\ fillings]}{47549\ [survival\ time]} = 0.5\ [fillings/day] \quad (18)$$

The cumulative failure function as a function of number of fillings is obtained by Nelson-Aalen estimate. The maximum likelihood estimation (MLE) and variance of the cumulative failure function is obtained by Nelson-Aalen estimate (Nelson, 2000). The Nelson-Aalen estimator for the cumulative failure function takes the form shown in Eq. (19).

$$F(t) = \sum_{t_j \le t} \frac{d_j}{r_j} \tag{19}$$

Where d_j is the number of individuals who failed at t_j and r_j is the number of individuals at risk just prior to t_j. The variance of the estimator is also defined by Eq. (20).

$$V[F(t)] = \sum_{t_j \le t} \frac{d_j}{r_j^2} \tag{20}$$

In this study, the number of fillings, N was employed instead of time, t since the number of fillings per day depends on the station. The result of this analysis is shown in section 3.4.1.

3.3.3 Parametric Distribution Analysis using Weibull Plot

The primary advantage of using Weibull Analysis is the ability to obtain more flexible distribution even with small number of samples. The 2-parameter Weibull distribution can take a more flexible shape of a graph to estimate failure rate, even a nearly constant one. The cumulative distribution function (CDF) for a two parameter Weibull distributed positive x is given by Eq. (21):

$$F(x) \; = \; 1 - e^{-(\frac{x}{\eta})^{\beta}} \tag{21}$$

Where β is the slope parameter (shape parameter), η is the characteristic life (or the scale parameter) and x is a positive random variable.

The slope of the 2-parameter Weibull plot, beta, β, determines which member of the family of Weibull failure distributions best fits or describes the data. The Weibull plot is the CDF plotted against the survival time. The horizontal axis is the age to failure, i.e., survival time. The vertical axis of the plot is the CDF, describing the percentage that will fail at any given age. The complement of the CDF scale, (100 - CDF) is reliability. The characteristic life η is defined as the age at which 63.2% of the units will have failed, the (indicated on the plot with a horizontal dashed line). Strictly speaking, for β = 1, the mean-time to-failure (MTTF) is equal to η. For β > 1.0, MTTF and η are almost equivalent.

The survival time data was used for all 28 stations from the JHFC project. The Weibull function estimates the two parameters β and η. Once the two parameters are determined, the CDF plot can be obtained using Eq. (21). The result of this analysis is shown in section 3.4.2.

3.4 Results and discussion

3.4.1 Failure rate estimation as a function of number of fillings (Non-parametric analysis)

Figure 13 shows the cumulative failure rate, F, plotted against the number of fillings, N, using Eq. (19). Seventeen failure data are plotted by using the Nelson-Aalen estimator. As can be seen from Fig.18, the cumulative hazard shows linear relationship with the number of fillings and the failure rate can be estimated as slope of the linear approximation of plotted data.

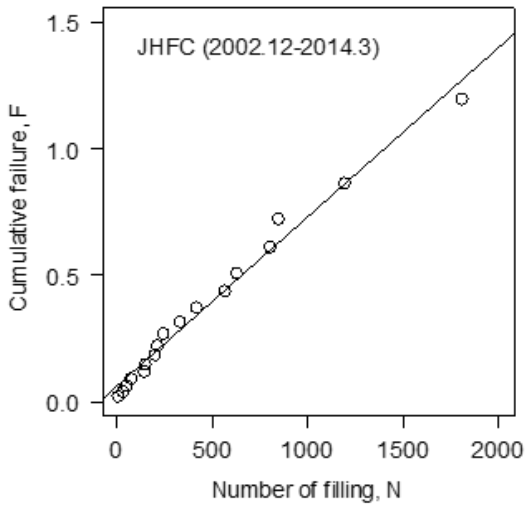


Figure 18. Total failure rate of hydrogen refueling stations in Japan

Total failure rate, λ, is the slope of the cumulative failure vs. number of fillings and its value is approximated 6.7×10^{-4} per filling. This value is almost equal to the value of 7.0×10^{-4} failures per filling estimated from dividing the total number of failures by the total number of fillings. The value of 6.7×10^{-4} per filling is equivalent to 1 failure in 1490 fillings. Considering an average of 0.5 fillings performed per day at a station per Eq. (18), it can be stated that one failure is likely to happen in 2980 days at a station based on the number of fillings. This valve is equivalent to one failure per 8 years which equates to a failure rate of 0.12 per year for small leak.

If the cumulative failure function, F (N), is assumed to be a linear function, the variance of failure rate is obtained as follows:

$$V(\lambda) = \frac{1}{N^2} V[F(N)] \tag{22}$$

Fig.19 shows the variance of failure rate, V(λ), calculated by the above equation. The plotted data converges to a constant value of about 6×10^{-8} for N > 500. This observation demonstrates that the failure rate, λ, assumes a constant value for N > 500.

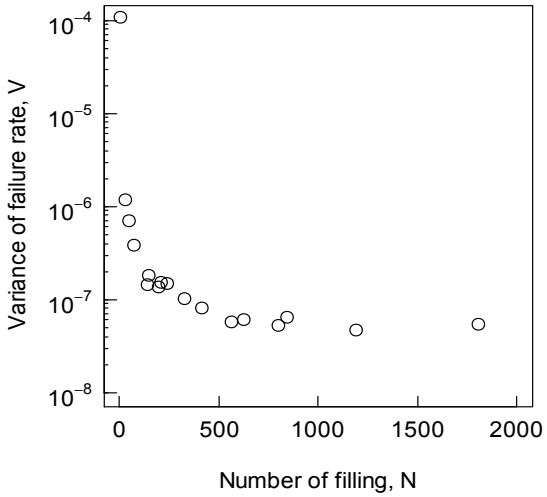


Figure 19. Variance of failure rate of hydrogen refueling stations in Japan

All observed failure events are related to hydrogen leaks. In such cases, it can be assumed that the failure rate is equivalent to leak frequency. LaChance et al. (2009) estimated the total leak frequency for two types of hydrogen refueling stations. The leak frequency was estimated as a function of leak size, which is the ratio of the leak area divided by the total cross-sectional flow area. For a leak area of 0.1 % of total flow area, the corresponding system leakage frequency would be 0.03 per year and 0.06 per year for the 20.7 MPa and 103.4 MPa systems, respectively.

Eleven of 17 failures plotted in Fig.18 represent leaks from threaded joints and four failures are leaks from the seals. Since many joints and seals are typically used the hydrogen refueling station and the station's hydrogen compressor produces mechanical vibrations, small leak from joints and seals are major concern at HRSs (Sakamoto et al., 2016). Accordingly, most of the leak failures can be classified

as very small leak with leak area of 0.01 % of total flow area (LaChance et al., 2009). When the leak area is 0.01 % of total flow area, the system's leak frequency would be 0.2 per year.

3.4.2 Failure rate estimation as a function of time (Parametric Analysis)

The survival time data for all 28 stations (S1, S2…, and S28) are used as an input data to the 2-Parameter Weibull Analysis. The collated data are taken from the JHFC project (JHFC, 2011). The field data of n units (28 stations herein) consists of the failure times for the failed units and the running times (censoring) times for the units with no failures. The 'n' sample were ordered from smallest to largest without regard to whether they are censoring or failure times. A censored data was used to distinguish failure times from the censoring times (units without failures), which are marked "0". In total, there were 17 failures observed.

The 2-parameter Weibull plot for the given age to failure data is shown in Fig.20. The seventeen failures are plotted on the graph and Weibull parameters (β and η) are graphically estimated on plot papers using Minitab 16 software (Minitab, 2010). The β value of 1.41 suggests that the stations have failure rates that increase with age; that is, they have a wear out pattern and safety critical components should be replaced or repaired at some age to prevent wear out failures. The age of failure is represented as a survival time in days. Thus, the horizontal scale is the age to failure, i.e., survival time in days. The vertical scale is the cumulative failure probability plot in percent.

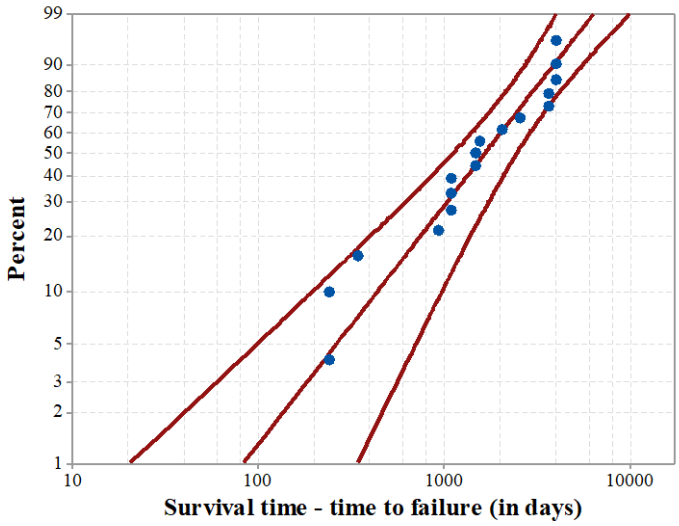


Figure 20. The 2-parameter Weibull Probability plot for age to failure

The Weibull plot in produced with a 95% confidence interval as shown in Fig.20. The censoring information was used to distinguish failed and units without failures. A total of 17 failures were obtained. The β and η parameters of the Weibull distribution from the given JHFC dataset is provided in Table 7.

Table 7. Characteristics of the 2-parameter Weibull distribution based on JHFC dataset

Characteristics of Distribution	Estimate	95.0% Confidence Interval	
		Lower	Upper
Shape parameter (β)	1.41	0.96	2.08
Scale parameter (η)	2158.77	1516.53	3073.01
Mean time to failure (MTTF)	1964.08	1398.61	2758.17
Standard deviation	1406.39	891.209	2219.38

The results of the Weibull based estimation is shown in Fig.21. The employed input data is the same as those used with the Nelson-Aalen estimator, with the exception of using the survival times in lieu of number of number of fillings. The mean time to failure (MTTF) is estimated to be 1964 days. The characteristic life (η) is equal to 2158 days. The lower bound and upper bound of the estimates are generated with a 95% confidence interval.

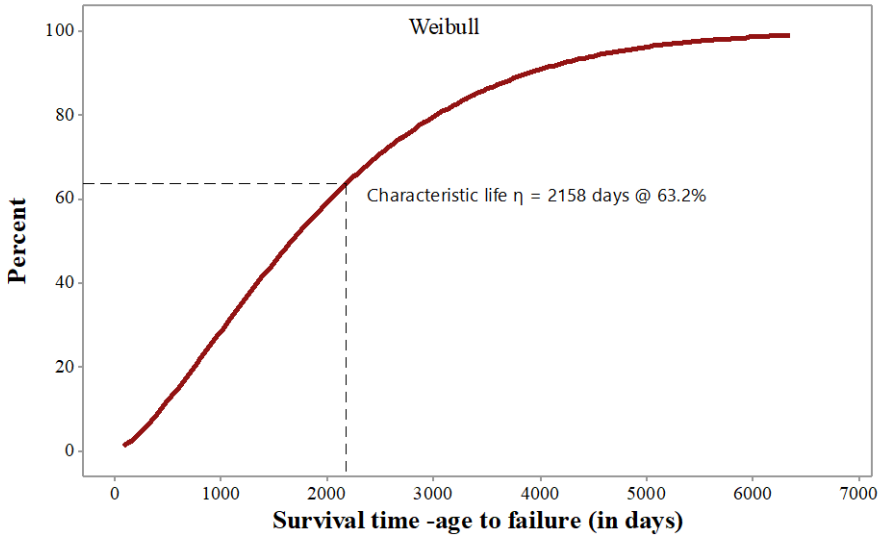


Figure 21. Cumulative failure plot for age to failure

The cumulative failure plot for the given age to failure data using Weibull distribution is shown in Fig.21. An estimate of the population of percentage failing for a given age can be obtained from this figure. For example, the estimate of the percentage of station failing by 1480 days is 44% based on the data collated for 28 stations (S1, S2… S28) from JHFC project report (JHFC, 2011; NEDO, 2014). The characteristic life (η) represents an age at which 63.2% of the total population must have failed and as

Fig.21 shows, 63.2% of the units would have failed at the time of 2158 days. In 2-parameter Weibull distribution, when $\beta > 1$, the characteristic life (η) is almost equivalent to mean life. The failure rate is estimated to be 0.17 based on the mean life of 2158 days.

3.4.3 Comparison of estimation methods: Survival time vs. number of fillings

To numerically demonstrate the difference between the two estimation methods, Station S4 and Station S11 are used as an example. In the JHFC input data, S4 and S11 have similar survival times, but they have a large difference in the usage (i.e. number of fillings). S4 has 2385 fillings in 2678 days whereas S11 has 662 fillings in 2738 days. The comparison between the two estimation methods is summarized in Table 8. The failure rate as a function of time to failure (Weibull) is estimated using the mean failure rate calculated in Section 3.4.2. The failure rate by number of fillings (Nelson-Aalen) is estimated using the cumulative failure calculated in Section 3.4.1.

Table 8. Failure rate data for Station S4 and S11 using both methods

Station	Number of Fillings	Survival Time	Failures by survival time (Weibull)	Failures by number of fillings (Nelson-Aalen)
S4	2385	2678 days	1.24	1.67
S11	662	2738 days	1.27	0.46

From Table 8, it can be seen that there is a difference in the failure rate estimation from both methods. The failure rate estimated as a function of survival time is almost same for both stations, i.e. around 1.24 failures. However, failure rate estimated by number of fillings could be more or less conservative depending on the number of fillings. Based on the assumption of 0.5 fillings per day, the failure rate is found to be conservative for S4 (namely, 1.67 failures) in comparison to S11 (namely, 0.46 failures) as S4 has much higher number of fillings then S11.

3.5 Conclusions

This study provides failure rate estimation methodology for hydrogen refueling stations in Japan using two parameters, namely, survival time and number of fillings. The generated results can be summarized as follows:

1. The non-parametric approach suggests that the cumulative failure, F (N), can be estimated as a linear function of number of fillings (N). The estimated failure rate seems to converge to a constant

value for N > 500. Considering an average of 0.5 fillings per day, the estimated failure rate is 0.12 per year.

2. In parametric approach, the cumulative failure is estimated from the failure and survival data using the 2-paramter Weibull Analysis. The 28 HRS are assessed using the number of failures and survival time data. The Weibull probability plot and cumulative failure plot are obtained to estimate mean failure rate. The estimated failure rate as a function of time is 0.17 per year.
3. The observed failure data (collated from the JHFC project report) is associated with leaks from threaded joints and seal. Under such conditions, it is assumed that the failure rate is equivalent to leak frequency. Also, most of the failures are classified as "very small leak" of which the leak area is 0.01 % of total flow area and the system frequency can be estimated to be 0.2 per year in line with the study by LaChance et al. (2009).

Using a case study, it is observed that two stations can have similar survival time but small to large difference in the usage (i.e., number of fillings). Thus, if the failure rate is estimated as a function of time, the mean failure rate will be roughly the same for both stations. However, if failure rate is estimated by number of fillings, the failure rate will vary depending on the actual usage of the station. The actual usage conditions are discarded when using the survival time and this may lead to uncertainty in the failure estimation.

The study concludes that the failure rate estimated as a function of number of fillings is more reliable and realistic than the estimation based on survival time. Moreover, the number of fillings is more representative of the true failure rate as it considers the actual station's usage and loading. The survival time do not always represent the actual usage of the stations.

3.6 Acknowledgements

Authors would like to thank technical experts of IEA Hydrogen Safety Task 37 for fruitful discussion.

3.7 References

Casamirra, M., Castiglia, F., Giardina, M., Lombarado, C., 2009. Safety studies of a hydrogen refueling station: Determination of the occurrence frequency of the accidental scenarios. International Journal of Hydrogen Energy, Vol. 34, pp. 5846-5854.

Goerlandt, F., Khakzad, N., Reniers, G., 2016. Validity and validation of safety-related quantitative risk analysis: A review. Safety Science, Vol. 99, Part B, 2017, pp. 127-139, 2016.

Japan Nuclear Technology Institute (JANSI), 2009. Estimation of domestic general equipment failure rate considering uncertainty of failure counts (1982~2002, for 21 years, 49 plants data), http://www.genanshin.jp/archive/failure_rate/; March 2009 [accessed September 2017].

Japan Nuclear Technology Institute. (JANSI), 2017. Estimation of domestic general equipment failure rate considering uncertainty of failure counts (1982~2010, for 29 years, 56 plants data), http://www.genanshin.jp/archive/failure_rate/; June 2016 [accessed September 2017].

Jones, N., 1984. A Schematic Design for a HAZOP Study on a Liquid Hydrogen Filling Station. International Journal of Hydrogen Energy, Vol. 9, pp. 115-121.

Khalil, Y., Nosher D., 2008. Probabilistic treatment of expert judgment on aleatory and epistemic uncertainties associated with on-board vehicle hydrogen storage systems. Proceedings of the ANS PSA 2008 Topical Meeting – Challenges to PSA During the Nuclear Renaissance Knoxville, Tennessee, September 7–11, American Nuclear Society (ANS), LaGrange Park, IL.

Khalil, Y., 2017. A probabilistic visual-flowcharting-based model for consequence assessment of fire and explosion events involving leaks of flammable gases. Journal of Loss Prevention in the Process Industries 50 (2017) 190–204.

Khalil, Y., 2018. Science-based framework for ensuring safe use of hydrogen as an energy carrier and an emission-free transportation fuel, Process Safety and Environmental Protection, Volume 117, Pages 326-340, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2018.05.011.

Kikukawa, S., Mistuhashi, H., Miyake, A., 2009. Risk assessment for liquid hydrogen fueling stations. International Journal of Hydrogen Energy, Vol. 34, pp. 1135-1141, 2009.

LaChance, J., 2009. Risk-informed separation distances for hydrogen refueling stations. International Journal of Hydrogen Energy, Vol. 34, 5838-5845.

LaChance, J., Houf, W., Middleton, B., Fluer, L., 2009. Analysis to Support Development of Risk-Informed Separation Distances for Hydrogen Codes and Standards. SANDIA REPORT, SAND2009-0874, 2009.

Matthijsen, A., Kooi, E., 2006. Safety distances for hydrogen filling stations", Journal of Loss Prevention in the Process Industries. Vol. 19, pp. 719-723.

Ministry of Economy, Trade and Industry (METI). 2017. The incident response manual of the HP Gas Safety Act, http://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/files/manual250226.pdf; [accessed September 2017].

Minitab 16 Statistical Software, 2010 [Computer software]. State College, PA: Minitab, Inc. (www.minitab.com).

Nakayama, J., Sakamoto, J., Kasai, N., Shibutani, T., Miyake, A., 2016. Preliminary hazard identification for qualitative risk assessment on a hybrid gasoline-hydrogen fueling station with an on-site hydrogen production system using organic chemical hydride. International Journal of Hydrogen Energy, Vol. 41, pp.

7518-7525.

Nelson, W., 2000. Theory and Applications of Hazard Plotting for Censored Failure Data. Techno metrics, Vol. 42, No. 1, pp. 12–25.

New Energy and Industrial Technology Development Organization (NEDO), 2014. Technical and Social Demonstration Project (JHFC3), Accident Database. 2014.

Pasman, H., Rogers, W., 2012. Risk assessment Risk assessment by means of Bayesian networks: A comparative study of compressed and liquefied H2 transportation and tank station risks. International Journal of Hydrogen Energy, Vol. 37, pp. 17415-17425, 2012.

Rademaeker, E., Suter, G., Pasman, H., Fabiano, B., 2014. A review of the past, present and future of the European loss prevention and safety promotion in the process industries. Process Safety and Environmental Protection, Volume 92, Issue 4, Pages 280-291, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2014.03.007.

Redbook, CPR 12E, 1997. Methods for determining and processing probabilities. Committee for the Prevention of Disasters, The Hague, The Netherlands, 1997.

Sakamoto, J., Sato, R., Nakayama, J., Kasai, N., Shibutani T., Miyake, A., 2016. Leakage-type-based analysis of accidents involving hydrogen fueling stations in Japan and USA. International Journal of Hydrogen Energy, Vol. 41, pp. 21564-21570.

The Japan Hydrogen and Fuel Cell Demonstration Project (JHFC Phase2), 2011. http://www.jari.or.jp/Portals/0/jhfc/data/report/pdf/tuuki_phase2_01.pdf.

The High Pressure Gas Safety Institute of Japan (KHK), 2015. Notes on Accidents related to Hydrogen Refueling Stations. (In Japanese).

The California Energy Commission (CEC), 2004. Technical Consultant Report on Failure Modes and Effects Analysis for Hydrogen Fueling Options. CEC-600-2005-001, Nov 2004.

Tsunemi, K., Yoshida, K., Yoshida, M., Kato, E., Kawamoto, A., Kihara, T., Saburi, T., 2017. Estimation of consequence and damage caused by an organic hydride hydrogen refueling station. International Journal of Hydrogen Energy, Vol. 42, Issue 41, pp. 26175-26182.

Yamada, T., Kobayashi, H., Akatsuka, H., Hamada, K., 2015. Analysis of high pressure gas incidents in hydrogen fueling stations. J High Press Gas Safety Institute Japan, 52 (10) (2015), pp. 23-29 [in Japanese].

Appendix D

Detailed explanation on 17 failure accidents collated from database with censored failure data (JHFC, 2011; NEDO, 2014)

Station ID	Failed Date	Failure Frequency	Total Survival Time (days)	Total Survival Time (years)
S1	18-07-2012	1	1094	3.00
S2	17-06-2006	1	929	2.55
S3	No failure	0	4136	11.33
S4	No failure	0	2678	7.34
S5	15-06-2010,06-02-2013	2	3651	10.00
S6	No failure	0	417	1.14
S7	17-10-2007	1	4016	11.00
S8	No failure	0	1095	3.00
S9	05-11-2012	1	2036	5.58
S10	07-08-2007,30-07-2013	2	3998	10.95
S11	No failure	0	2738	7.50
S12	No failure	0	1795	4.92
S13	No failure	0	2435	6.67
S14	No failure	0	2372	6.50
S15	28-07-2005	1	240	0.66
S16	13-05-2005	1	240	0.66
S17	24-10-2006	1	1551	4.25
S18	10-07-2012	1	2572	7.05
S19	No failure	0	1218	3.34
S20	No failure	0	849	2.33
S21	No failure	0	394	1.08
S22	No failure	0	394	1.08
S23	30-10-2012, 09-03-2013	2	1465	4.01
S24	09-04-2012, 17-10-2012	2	1094	3.00
S25	No failure	0	1095	3.00
S26	No failure	0	1095	3.00
S27	22-05-2013	1	344	0.94
S28	No failure	0	667	1.83

Note: Total Stations: 28, Total failures: 17, Total Survival time (in years): 127.69

CASE STUDY 4. Improvement in reliability quantification to support BS EN 61511 failure probability analysis

4.1 Introduction

Functional safety engineers are actively involved in safety and reliability engineering applications of various facilities to conform with IEC 61508/11 standard. These standards are used as a best practice in the design and implementation of safety systems in process applications. In order to improve the requirements of the standard, a dynamic risk based approach is recommended to be integrated into the standard in order to bring improvement to the existing static approach. Hence, the core concept of this research is utilized in practical aspects of IEC 61511 in this case study, where transformation from static to dynamic approach is suggested.

Probabilistic risk assessment (PRA) has been widely adopted within the process industries to provide performance based design of the safety instrumented systems (SIS). PRA gained widespread attention since the introduction of the ANSI / ISA S84 (1996) standard. To ensure that the probabilistic calculations in the PRA and SIS design are relevant and meaningful, validation of PRA is necessary. The international standard for functional safety BS EN 61511 (2016) specifies for using credible, traceable and realistic failure rate data in failure probability analysis. However, in reality, these requirements have proven difficult for end-users because of the lack of failure data records and large amount of sample data required for frequentist methods. Lack of failure data leads to uncertainty in risk and reliability quantifications making risk assessment decisions weak.

In BS EN 61511 reliability assessment, mean time to failure (MTTF) is one of the most common approaches to field failure data analysis. MTTF and similar metrics are used for situations with a constant failure rate. In other words a piece of equipment has the same chance to failure at any point in time i.e. the chance of failing at 11th hour and the chance of failing at 110th hour is the same. However, this is generally not true for systematic failures encountered in hazardous sites. The most common mechanism of failures in the industry is erosion, corrosion, fatigue, cracks etc. When the right conditions exist, corrosion starts, grows and eventually over time leads to failures. Mahmoodian (2014) describes

the older the equipment the more likely it will fail due to corrosion, thus not a constant failure rate. This shows that an overall MTTF may alter the risk assessment results. Over the past several decades, enough information has been collected on MTTF from several sources to estimate failure rates. OREDA (2015), one of the largest data source, combines data from multiple sources. The OREDA data distribution is very wide and uncertainty intervals span 1 or 2 orders of magnitude. One reason for the variability in rates is that these datasets include variations on the environment and service conditions.

Moreover, new technology or major accident hazards with low probability has limited or no failure data. Under such circumstances, traditional methods are not of much benefit. Even the life data distribution to model the time to failure is not of much use because the time to failure data is not available for new systems. Under such condition, the users are constrained from using traditional approach to reliability engineering.

This study draws conclusions on how failure rates and failure probability can be controlled in practice. The proposed Bayesian framework addresses the above requirements by providing a periodic updating process that allows industry knowledge about failure rates to be incorporated in a prior distribution and cyclical updated with new survival data as it becomes available. A sensitivity analysis is further carried out to perform uncertainty modelling on failure rate using Monte Carlo simulation. The outcome of this work would help to predict maintenance intervals. The results can be integrated with predictive and preventive maintenance strategies as suggested by Abbassi et al. (2016) whilst maintaining overall system availability and safety.

4.2 Estimation and interpretation of failure rate using statistical model

The BS EN 61511 standard recognizes the impact of lack of quality reliability data on the PRA result. Justification of failure data is an important measure to provide verification of risk analysis as proposed as reviewed by Goerlandt et al. (2016). The standard demands that:

"Reliability data used in quantifying effect of random failures should be credible, traceable, documented and justified based on field feedback"

BS EN 61508- Part 2 (2010) states that:

"The reliability data uncertainties shall be taken into account when calculating the target failure measure"

There are basically two types of model that can be applied to reliability modelling. Frequentist approach is commonly used in reliability calculation but one disadvantage is that they do not consider prior knowledge. The Bayesian approach is adopted in this study to provide more benefits and will be discussed in detail hereafter. As each model has a different application, suitable care should be taken to apply the correct model to the data.

4.2.1 Estimation of failure rate based on Gamma approximation (Bayesian method)

In reference to the note in Clause 11.9.2 of BS EN 61511-1 regarding confidence in reliability data, mean time to failure (MTTF) is typically determined by recording the number of failures (n) which occur in a sample of components during an accumulated number of operating hours (T). However, the failure data can be extremely limited, which in this case, will not be taken into account and can lead to uncertainty in reliability modelling. Japan Nuclear Technology Institute (2017) introduced the Bayesian method to enable the uncertainty width of failure rate to be updateable with data storing, which until then had a fixed value. The nuclear report considers the failure rate as constant over time and the probabilistic variance is updated by new data. Similar approach is adopted in this study for BS EN 61511 application and discussed in detail hereafter.

Data scarcity and constant failure rate uncertainty problem can be addressed using gamma approximation with Bayesian inference to estimate the failure rate. The model presented uses gamma approximation to produce prior distribution with uncertainty. The likelihood function (new observation) is modelled using Poisson function. Based on the joint likelihood of Poisson distribution and the parameters of the gamma approximation, Bayesian inference is established to analyze survival data. The sensitivity analysis is then performed on the updated failure rate to reduce the uncertainty to as low as possible.

4.2.2 Prior Distribution

There are many techniques and considerations to be taken when selecting a prior distribution. For the purpose of this study, the main focus is on feasibility, simplicity and mathematical traceability for engineers. For these reasons, a Gamma approximation was chosen as the prior distribution. Prior knowledge will be assigned from external industry data sources. The parameters α and β are estimated using Dutch red book model (1997) as:

$$\alpha = \frac{x^2}{Var} \tag{23}$$

$$\beta = \frac{x}{Var} \tag{24}$$

Where, x - Positive random variable, Var - Variance of the sample data

4.2.3 Likelihood (evidences)

In reality, BS EN 61511 reliability calculations are typically based on the exponential distribution, which is a special case (i.e. where x = 0) of the more general Poisson distribution. The Gamma distribution is a "conjugate prior" of the Poisson likelihood function which enables Bayesian equation to be solved analytically and elegantly. Given a constant failure rate (λ), the Poisson distribution gives the probability of failures (x) per time (t), as shown below.

$$P(xi\,, ti\,|\lambda) = e^{-\lambda t}\,\frac{(\lambda t)^x}{x\,!} \tag{25}$$

In the completed model, the variables x and t will take the place of the evidence $f\ (T_1 \mid \lambda)$ in Eq. (26). The survival time and number of failures data will be obtained through new observations from failure records.

4.2.4 Sampling of Survival Data using Bayesian Inference

Based on the Bayes' theorem, the relationship between the prior, the posterior, and the likelihood function is written as:

$$\mathrm{f}\,(\lambda \mid \mathrm{T_1}) = \frac{f\ (T_1 \mid \lambda) * f_0\,(\lambda)}{\int_0^\infty f\ (T_1\,|\lambda) * f_0\,(\lambda)} \tag{26}$$

Note: $\mathrm{T_1}$ is the first occurrence of failure or survival time. In Eq. (26), λ is the unknown parameter of interest distributed with posterior f (λ |T_1), $f_0\ (\lambda)$ is the prior distribution of λ. Subsequently, $f\ (T_1 \mid \lambda)$

is the likelihood function that updates a prior distribution. Using the standard equation of Bayesian update from the Dutch Red book (1997), the gamma parameter update is given by,

$$\alpha' = \alpha + n_f, \tag{27}$$

$$\beta' = \beta + T_s, \tag{28}$$

Where, n_f is number of failures and T_s is survival time.

The updated mean and variance can be calculated using Maximum Likelihood method (MLE) with the formula:

$$x = \frac{\alpha'}{\beta'} \tag{29}$$

$$Var = \frac{\alpha'}{\beta'^2} \tag{30}$$

Using Eq. (27), (28), (29) and (30), the posterior distribution mean can be expressed as

$$\mathrm{E}\ \{\mathrm{f}\ (\lambda \mid \mathrm{T}_1) = \frac{\alpha'}{\beta'} \tag{31}$$

In other words, α parameter can be converted to number of failures, β can be converted to the total survival time. The initial prior parameters are denoted as α_0 and β_0. After the first update of these parameters based on new observation, the parameters are called α' and β'.

4.3 Practical application of proposed model to BS EN 61511

4.3.1 Estimating Initial value of Gamma parameters

The prior value of gamma parameters α_0 and β_0 should be carefully chosen as they have large impact on Bayesian updating process. To make this selection, data for valve failure rates was gathered from a variety of industry data sources such as OREDA (2016). A total of 20 independent dangerous failures for operating valves were collected to produce prior distribution and obtain values for $_0$, β_0. These data are only used as informative prior to establish prior distribution. Based on the 20 independent failure data for valves, the mean and variance is calculated as:

- Mean (x) = 0.0335 failures / year,
- Variance = 0.0015

Now, the initial values, α_0 and β_0 are calculated using Eq. (23) and Eq. (24) as α_0 = 0.75, β_0 = 22.33.

4.3.2 Bayesian Update

After describing how to calculate Bayesian model in Section 4.3, we are presenting some examples to illustrate the application of this model for case specific scenarios. We have obtained case specific data from the Japan Hydrogen and Fuel Cell Demonstration Project – Phase 2 (2011) and Phase 3 (2014). The project analyzed 17 failures that were observed in the various Hydrogen stations operated from FY2002 to FY2013. 6 out of 17 failures were related to process valves. The survival time data chosen are for 6 process valves. The data on valve failures were further analyzed and reliability related information were extracted for use in this study. The data extracted from the JHFC Phase 2 (2011) project is shown below:

Table 9. Valve survival data from JHFC report

ID	Component	Start Date	Failure Date	Survival (days)	Survival (years)	KHK - ID
1	Check Valve	2003/2/7	2010/6/15	T1 = 2685	7.4	2010-135
2	Suction Valve	2007/8/8	2013/7/30	T2 = 2183	6.0	2013-356
3	Gate Valve	2003/4/1	2007/10/17	T3 = 1660	4.5	2007-532
4	Gate Valve	2010/6/16	2013/2/6	T4 = 966	2.6	2013-037
5	Gate Valve	2012/4/9	2012/10/17	T5 = 191	0.5	2012-314
6	Check Valve	2013/4/19	2013/5/22	T6 = 33	0.1	2013-115

The survival data chosen to demonstrate different aspects of updating in chronological order is: 7.4, 6.0, 4.5, 2.6, 0.5, and 0.1. The six survival time (in years) reported occurs independently and are assumed to follow Poisson distribution (Likelihood function). As illustrated in Section 4.3.2, the Gamma parameters Alpha and beta are converted to number of failures and survival time respectively. Bayesian update is performed by calculating the parameters of posterior distribution, α' and β'. Table 10 also shows the updated α', β', posterior mean and variance for each component based on Eq. (27) and Eq. (28).

Table 10. Bayesian update result

Component ID	Component	Survival (in years)	α'	β'	Updated variance	Updated failure rate λ (per hour)
1	Check Valve	7.4	1.75	29.73	2.26×10^{-7}	6.72×10^{-6}
2	Suction Valve	6.0	1.75	28.33	2.49×10^{-7}	7.05×10^{-6}
3	Gate Valve	4.5	1.75	26.83	2.78×10^{-7}	7.45×10^{-6}
4	Gate Valve	2.6	1.75	24.93	3.21×10^{-7}	8.01×10^{-6}
5	Gate Valve	0.5	1.75	22.83	3.83×10^{-7}	8.75×10^{-6}
6	Check Valve	0.1	1.75	22.43	3.97×10^{-7}	8.91×10^{-6}

From Table 10, it can be noticed that there is no significant difference in the failure rates for all six components. All failure rates are within the same order of magnitude. One of the reason could be the updated failure rate is sensitive to generic data uncertainty due to less number of new observation. In order to obtain more realistic data, more observations should be analyzed in order to improve the sensitivity of updated failure rate. For this reason sensitivity analysis using Monte Carlo is performed. Gate valve has minimum three data cases (shown in Table 10) which is chosen as an example for illustration purpose. In total, three failures occurred at 4.5, 2.6 and 0.5 years respectively. The new values of α', β' and λ is calculated as:

α' = 3.75 β' = 29.93 λ = 1.43 x10^{-5}

4.4 Sensitivity analysis on failure probability using Monte Carlo method

The initial values of α_0 and β_0 can result in uncertainty in the distribution of failure rate due to generic data and therefore a Monte Carlo simulation is adopted in this study for the uncertainty analysis on the failure rate. In the field of reliability engineering, BS EN 61511 (Ed.2 2016) commonly uses probability of failure on demand (PFD) metric for understanding the performance of safety. The PFD is calculated from the failure rate based on equation in the BS EN 61508 (2010). The uncertainty analysis on 1oo2 valve system for PFD is shown below:

4.4.1 Failure Probability Modelling for 1oo2 Final elements Configuration (Valve)

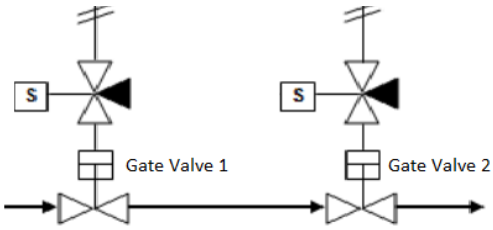


Figure 22. 1oo2 Configuration of final element (Gate valve)

In the process sector industry, the safety function PFD is dominated by the final elements due to relatively higher failure rate and architectural constraint. With 1oo2 valve configuration, the PFD is calculated as:

$$\text{PFD1oo2} = (1 - CCF)\ \frac{\lambda^2 \,.\, {t_i}^2}{3} + \frac{CCF \,.\, \lambda \,.\, t_i}{2} \qquad (32)$$

Where, λ - Failure rate, CCF - Common cause factor (Beta), t_i - Inspection interval in hours

The total failure rate for gate valve is estimated to be 1.43×10^{-5} failures per hour. The lambda λ is assigned gamma distribution with Mean: 1.43×10^{-5}, Variance: 4.77×10^{-7}. The inspection interval t_i is assigned triangular distribution with minimum value of 8400, likeliest value of 8760 and maximum value of 9000. The inspection period is 8760 hours (annual test). The CCF is assigned uniform distribution with minimum value of 0.01 and maximum value of 0.04. This means the CCF ranges between 1% and 4%. The failure probability calculation computed using Eq. (32) in Monte Carlo simulation after 1000 trials is shown below:

Table 11. Failure probability on demand calculation

Parameter	Value	Distribution	Comment
λ	1.43×10^{-5}	Gamma	Failure rate of dangerous undetected failures (per hour)
M	1	NA	Minimum number of component failures causing system failure
N	2	NA	Number of redundant "channels" of sub function
CCF	0.02	Uniform	Common cause factor
t_i	8760	Triangular	Inspection interval in hours
PFD($1_{oo}2$)	2.51×10^{-3}	Output	Total failure probability on demand

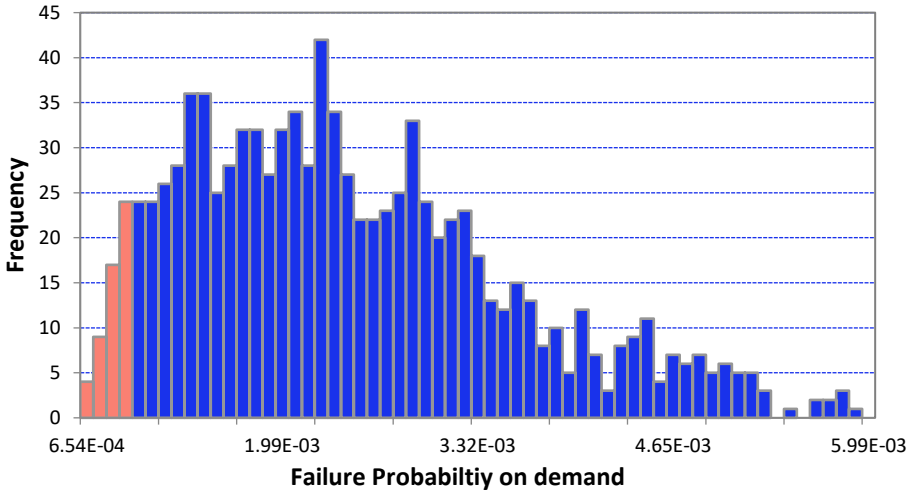


Figure 23. PFD Uncertainty Analysis using Monte Carlo

The PFD forecasts using the Monte Carlo simulation is executed for 1000 number of trials for acceptable uncertainty analysis on failure rate. The blue area in the graph is the certainty range for the estimated value of PFD. The red area is the uncertainty range. Fig.23 shows the PFD certainty range is from 1.00×10^{-3} to 1.00×10^{-2} (SIL 2) based on annual inspection and certainty level of 90%. The base value of PFD for this configuration is estimated to be 0.00251. This is equivalent to SIL 2 classification as per BS EN 61511 SIL classification. The forecasts of failure probability for different inspection intervals is presented is Table 12.

Table 12. Valve Failure Probability Forecast based on failure rate estimation

Failure rate, λ (per hour)	**Inspection Interval**	**Inspection Interval (hours)**	**Failure Probability on demand**	**BS EN 61508 SIL Class [Achieved]**
	Monthly	720	2.06×10^{-4}	SIL 3
1.43×10^{-5} (Gamma function)	Quarterly	2160	6.18×10^{-4}	SIL 3
	6 months	4320	1.24×10^{-3}	SIL 2
	Yearly	8760	2.51×10^{-3}	SIL 2

The Montel Carlo simulation allows to model failure probability for all possible values of λ and t_i put together in the calculation. The final PFD certainty range is estimated to be in SIL 2 range with base value of 0.00251 based on 1 year inspection interval and 90% certainty level.

4.5 Conclusion

The Bayes framework expands on the single-stage model and allows data from available sources to be leveraged in the updating process. The Bayesian methodology provides a flexible, coherent framework for managing failure rate data for any component. Monte Carlo simulation make it practical to solve uncertainty in the failure rate estimation and update these models in seconds. The process of updating failure rate with new observations and modelling failure data uncertainty using Monte Carlo simulation will result in lower uncertainty and narrower posterior distribution. It is observed that with less number of new observations, the updated failure rate is sensitive to generic uncertainty data which does not provide realistic result. In order to improve the sensitivity of updated failure rate, more number of observations subject to modelling using Monte Carlo method will be beneficial. The final PFD certainty range for 1oo2 gate valve is estimated to be in SIL 2 range with base value of 0.00251 based on 1 year inspection interval and 90% certainty level. In order to achieve failure probability in the range of SIL 3, the inspection interval on valve across installations should be carried out at least once in 3-6 months interval. The appropriate base value can be used in design set performance standards for availability and reliability in operation and maintenance of the component.

4.6 References

Abbassi R., Bhandari J., Khan F., Garaniya V., Chai S., 2016, Developing a quantitative risk-based methodology for maintenance scheduling using bayesian network, CET, 48, 235-240 DOI:10.3303/CET1648040

ANSI/ISA S84.01, 1996, Application of Safety Instrumented Systems for the process control industry, ISA, USA.

Aven. T., Heide. B., 2009, Reliability and validity of risk analysis, Rel. Eng. & Sys Safe, vol. 94, pp.1862 to 1868.

BS EN 61511-1 Ed 2, 2016, Functional Safety – Safety Systems for the Process Industry, Geneva, Switzerland.

BS EN 61508, 2010, Functional Safety of Programmable Electronic Safety-Related Systems: Part 1-4. BS, UK.

Casamirra M, Castiglia F, Giardina M., Lombarado C., 2009, Safety studies of a hydrogen refuelling station: Determination of the occurrence frequency of the accidental scenarios, International Journal of Hydrogen Energy, Vol. 34, pp. 5846-5854.

Dutch Red Book, CPR 12E, 1997, Methods for determining and processing probabilities, Committee for the Prevention of Disasters, The Hague, The Netherlands.

Droguett E.L., Groen F.J., Mosleh A., 2006, Bayesian assessment of variability of reliability measures. Pesquisa Operacional.

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

Japan Nuclear Technology Institute, 2016, Estimation of domestic general equipment failure rate considering uncertainty of failure counts, http://www.genanshin.jp/archive/failure_rate/; [accessed Sept 2017].

Khakzad N., Reniers G., 2016, Application of bayesian network and multi-criteria decision analysis to risk-based design of chemical plants, Chemical Engineering Transactions, 48, 223-228 DOI:10.3303/CET1648038.

LaChance J., Houf W., Middleton B., Fluer L., 2009, Analysis to Support Development of Risk-Informed Separation Distances for Hydrogen Codes and Standards, Sandia Report, SAND2009-0874.

Mahmoodian M., Alani A., 2014, A gamma distributed degradation rate model for reliability analysis of concrete pipes subject to sulphide corrosion, International Journal of Reliability and Safety, vol. 8, no. 1, pp. 19-32.

Oreda Offshore and Onshore Reliability Data Handbook Vol 1, 6th edition, 2015, SINTEF Technology and Society: Department of Safety Research, Trondheim, Norway.

Pörn K., 1996, The two-stage Bayesian method used for the T-Book application, Reliability Engineering & System Safety, Volume 51, Issue 2, Pages 169-179.

The Japan Hydrogen and Fuel Cell Demonstration Project (JHFC Phase2), 2011, http://www.jari.or.jp/Portals/0/jhfc/data/report/pdf/tuuki_phase2_01.pdf, Japan.

CASE STUDY 5. A Risk Based Inspection Model for Hydrogen Storage Process using Bayesian Network

5.1 Introduction

The safety integrity of the technology system should be maintained through routine inspection and maintenance programme. In case of hydrogen energy systems, an appropriate inspection routine will also increase the chance of authority's approval and public acceptance, which is a pre-requisite for successful implementation and operation of new technology systems. Therefore, a probabilistic graphical model, based on an acceptable level of risk, is proposed to avoid under and over estimation of inspection time interval. This case study presents an advanced Risk-based Inspection (RBI) methodology to decide inspection time in relation to the risks through dynamic graphical modelling. Bayesian Network (BN) is applied to model the risk and the associated uncertainty.

Meanwhile, BN has been popularly used in significant areas where safety assessments are involved. Pasman and Rogers performed risk assessment for compressed and liquefied hydrogen transportation and tank station by means of BN (Pasman and Rogers, 2012). A bayesian statistical approach is also employed in the estimation of failure rate from prior data. LaChance developed a bayesian model to leak frequency in various components used in a hydrogen refueling station (LaChance, 2009). As most of the traditional risk analysis techniques (e.g. fault tree analysis (FTA) and event tree analysis (ETA)) are static and non-updatable conventional model, they regularly fail to fully capture the variation of risks during operation (Paltrinieri and Khan, 2016). Besides, conventional techniques use only binary variables and do not represent conditional dependencies (Martins et al., 2018). Based on BN, Abbassi et al. presented a RBI methodology, applied to an offshore process facility (Abbassi et al., 2016).

Results show that the most critical components are the shut-off valve and hose/flow nozzle connection in case of minor risk. In case of major risk, flow gauge has the shortest transition from minor to major risk and thus makes it a most critical component. Pipelines has the shortest inspection time compared to other components and thus makes it the most critical component for critical risk.

Despite all these ongoing efforts made on operational process, inspection interval forecast is one area within safety and risk management of HRS which has not received enough attention in research areas. The application of bayesian in the field of operation and maintenance is scarce due to complication. However an approach is highly desired for setting inspection test interval using BN. As a result, a risk-based methodology for inspection scheduling is developed in this work and demonstrated through an application of case study. The objective of this approach is to develop risk based inspection model by implementing a BN analysis. In this study, risk level is calculated via BN considering the failure probabilities (Pf) and the possible consequences. The inspection plan is determined after setting the evidence that the system operates at the lowest possible risk using BN and influence diagram.

5.2 Background

In this section, the accidents that occurred in an HRS are categorized with respect to systems. In order to categorize systems, the information in the columns "system" and "accident brief description" were divided into hydrogen dispenser, compressor, accumulator, and interconnection system. The accidents are categorized according to Table 13.

Table 13. Accident categorization by system

System	**Site of accidents**
Dispenser	Coupling, Hose, O ring
Compressor	Piping, Connecting, Valve
Accumulator	Pressure vessel, Interconnections, Valve
Interconnection	Piping, Valve, Seal, Others

A graph for accident categorization by system is shown in Fig.24. Note that the data is the mean number for a station. The event data observed in Fig.24 was obtained for a total operation time of 144 months. The event data is obtained from database maintained by the High Pressure Gas Institute of Japan (KHK, 2017). It can be noted that dispenser failure was more significant during the initial 52 months. Accumulator failure resulted in accidents during the initial 45 months. Conversely, the compressor and interconnection system had accidents late in the operation period, especially from the 112th months to the 122nd months.

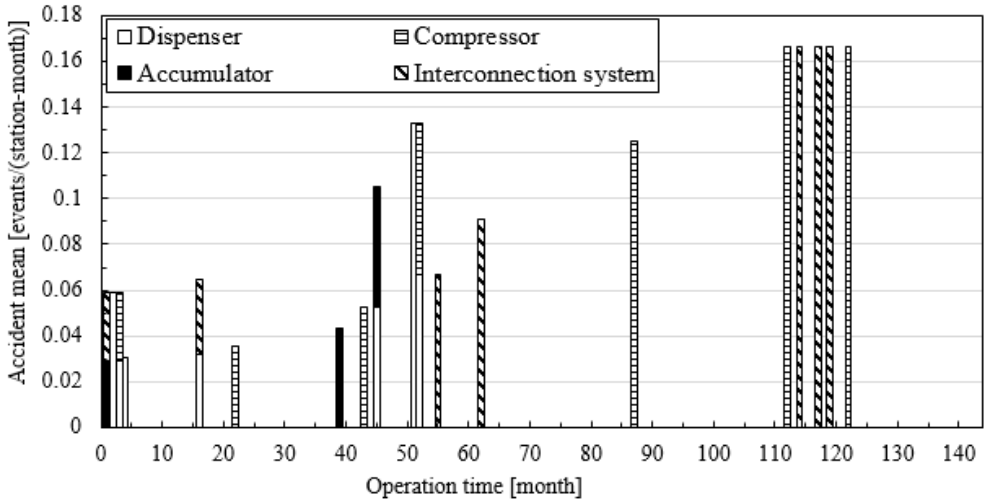


Figure 24. System-categorized accidents in an HRS by operation time (mean)

Up to this point, this study has discussed the accident information of Japanese HRSs in terms of operation time and system failure. Categorizing accidents by system gives a hint as to when a specific piece of system tends to fail. However, understanding failure characteristics of critical components within the hydrogen system is vital and should not be overlooked. The inspection interval for each critical components should be individually defined and this requires a methodology to carry out relevant analysis. The proposed methodology to solve this issue is shown in next section.

5.3 Proposed Methodology

The methodology developed in this study is based on the model that emphasizes on the scenario. The sequence of the proposed methodology for RBI in this study is illustrated in Table 14. Fig.25 shows the proposed methodology flowchart. In the first step, the system is defined and divided into its components. The relationship among the critical components is determined in step 2. Next, the associated FT is built. The top event (system failure) is broken down into sub events until all the primary events (events that could not be expanded further) are found. The scenario used as a case study is “hydrogen storage process”.

Table 14. Proposed steps in RBI Methodology

Step	Step description
1	Develop hydrogen scenario risk model and identify critical components
2	Develop FTA for the model
3	Mapping fault tree into quantitative BN graphical
4	Estimate mean time to failure and annual failure probability using BN
5	Calculate inspection interval

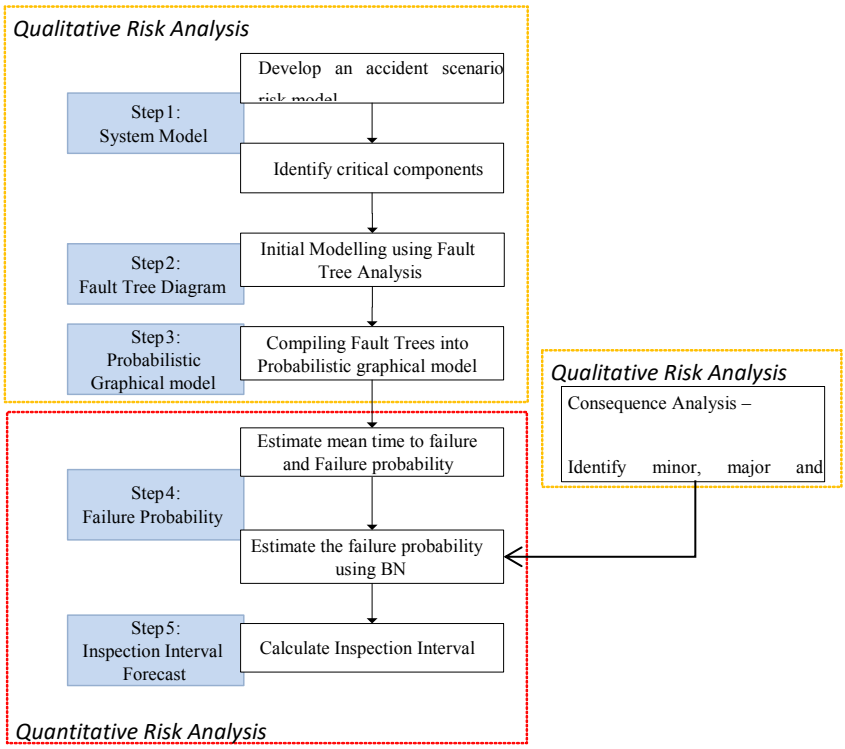


Figure 25. Proposed dynamic risk based methodology for HRS applying Bayesian Network

In the next step, mean time to failure (MTTF) of each component are found using available data. Subsequently, the annual probability of failure is worked out then. The probability table of root nodes in the BN can be filled with the irrespective failure probabilities. A risk matrix can be used to specify the consequences of system failure (top event) and risk of the operation. The level of risk can be defined in different approaches. Herein, it is divided in three categories:

1) Minor risk that is a low level of risk and it is considered acceptable in order to operate safely;

2) Major risk that is a higher level of risk that comprehends consequences that may bring damages to environment or to human beings;

3) Critical risk that is the highest level of risk and it has to be avoided.

Based on present RBI the optimum maintenance time of components is revised through probability updating. Setting the evidence that minor risk has occurred at 100% probability, a backward analysis is conducted on the BN to point out the updated probabilities of the roots (e.g. the probabilities of failure of the components when the system operates at the lowest risk possible). Finally, based on the updated probabilities the inspection interval is calculated.

5.4 Application of risk based inspection (RBI)

In order to demonstrate the applicability of the developed RBI methodology, it is applied to hydrogen storage process (HSP) as a case study. The main functions of a HSP are measuring the gas compression, storage and smooth transfer to the subsequent dispenser. A typical model of a HSP is shown in Fig.26. The compressed hydrogen gas at a higher pressure is contained in the cylinders (accumulator) at 82Pa. The compressed hydrogen is then passed through series of check valves and shut-off valves to the dispenser. Dispenser consists of pre-cooler, shut-off valves and hose/nozzle connections. The compressed hydrogen is used as per the requirement from the user. Dealing with high-pressure hazardous material inherently increases the risk due to leakage and fire and/or explosion.

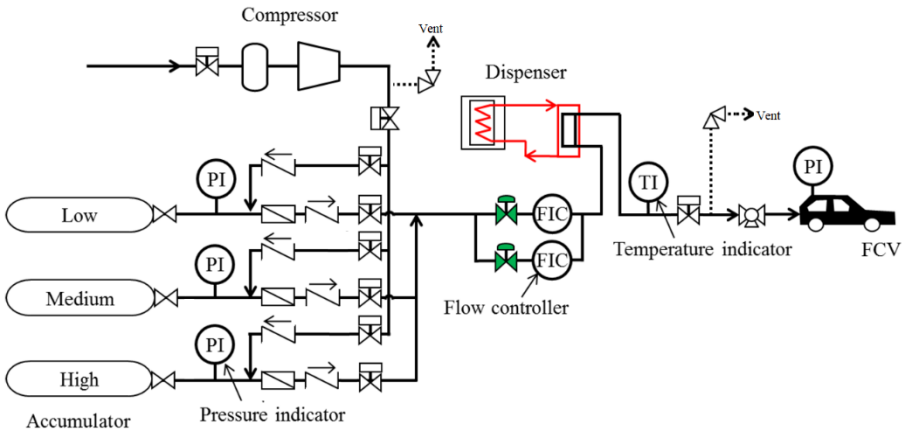


Figure 26. Hydrogen Storage Process Flow Diagram

Loss of containment is a high risk of concern with possibility of major/minor injuries. Thus, the leak is considered as a failure event in this case study. The leak equipment and location identified are as follows:

- Dispenser components such as pre-cooler, flow gauge, shut-off valve etc.
- Hose and flow nozzle connection for dispenser
- Check valve-overflow prevention valve
- Accumulator main body (high pressure, low pressure)
- Connection pipe for hydrogen holder (hydrogen purifier outlet valve to compressor inlet valve)
- Compressor and connection piping etc. (compressor inlet-check valve, outlet valve)

A HSP has four critical groups of different components that can lead to a failure of the system as shown in Table 15. The case study is simplified and only critical key components are analyzed in the study to demonstrate the methodology adopted.

Table 15. Critical components of HSP

Group	Component
Dispenser	Flow gauge
	Shut-off valve
	Hose and flow nozzle connection
Compressor	Compressor
Storage (Accumulator)	Tank (Cylinders)
Interconnection system	Pipelines
	Check valve
	Shut-off valve

Initial failure data for above components are collated from industry external sources i.e. SINTEF. The data presents critical failure rate, repair time and failure probability. It is worth noting that the MTTF of each component provided in SINTEF is collated from various operational experiences and industry experts (SINTEF, 2015). These values and corresponding failure rate are shown in Table 16.

Table 16. Failure rate of critical components of HSP

Components	MTTF (in hours)	Failure rate (per hour)
Flow gauge	270270	3.70×10^{-6}
Shut-off valve	344827	2.90×10^{-6}
Hose nozzle conn.	135135	7.40×10^{-6}
Check valve	147275	6.79×10^{-6}
Tank (Cylinders)	92592	10.8×10^{-6}
Pipelines	132450	7.55×10^{-6}
Compressor	182149	5.49×10^{-6}

Based on reported MTTF and failure rate, the probability of failure in a year is calculated. In order to consider the randomness of failures events, exponential distribution is adopted for the estimation of maintenance intervals. So the annual probabilities of failure would be achieved by Eq. (33):

$$P(t) = 1 - e^{-\lambda t} \tag{33}$$

where P(t) is the annual probability of failure when t is set equal to 8760 hour (a year) and is the failure rate expressed in failure per hour given by Eq. (34):

$$\lambda = \frac{1}{\text{MTTF}} \tag{34}$$

Fault tree representation of the model is represented in the form of BN. The developed BN for a HSP incorporating the failure of critical components is illustrated in Fig.27. The primary events are linked to four major intermediate events (i.e. dispenser failure, accumulator failure, check valves and compressor failure) which consequently may lead to top event i.e. system failure.

Table 17. Adopted Risk matrix for developing RBI

SCALE OF LIKELIHOOD	SCALE OF SEVERITY		
	Minor	**Major**	**Catastrophic**
Not Likely	Low	Low	Medium
Possible	Low	Medium	Medium
Probable	Low	Medium	High
Likely	Medium	High	High
Certain	Medium	High	Extreme

The risk of operation consisting of three aforementioned levels is integrated into the network (shown in Fig.28). In Table 17, the terms low, medium, high and extreme refers to the risk category. In addition to the fault tree, the upper part of the BN is extended to include ignition probability and leakage to consider the output effects. The output effects are classified into noise, mechanical damage, environmental impact and fire/explosion.

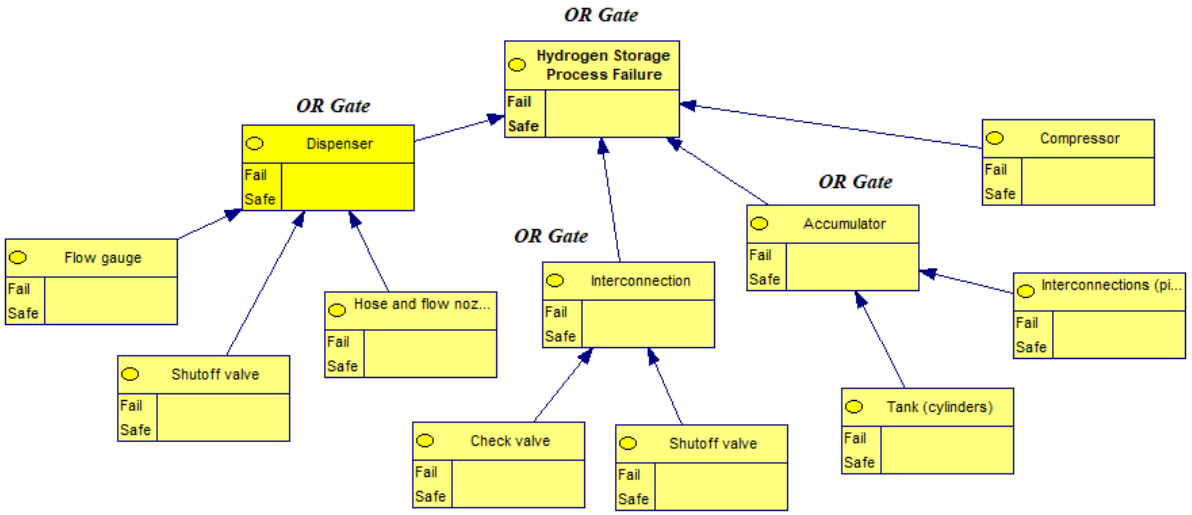


Figure 27. Fault tree of a HSP

The prior Pf of critical components calculated by Eq. (33) was assigned to root node as prior probability. The conditional probability (CP) of intermediate nodes represents the contribution factors of root nodes in the intermediate nodes. The Yes/No and Safe/Fail state of each node is assigned CP of risks using a

risk matrix shown in Table 13. It should be noted that the conditional dependencies and probability figures are based on generic data and expert judgement. Based on the assumed ignition probability of 14%, leakage of 10% probability and conditional dependencies between nodes, the physical output effects and three risk outputs are calculated.

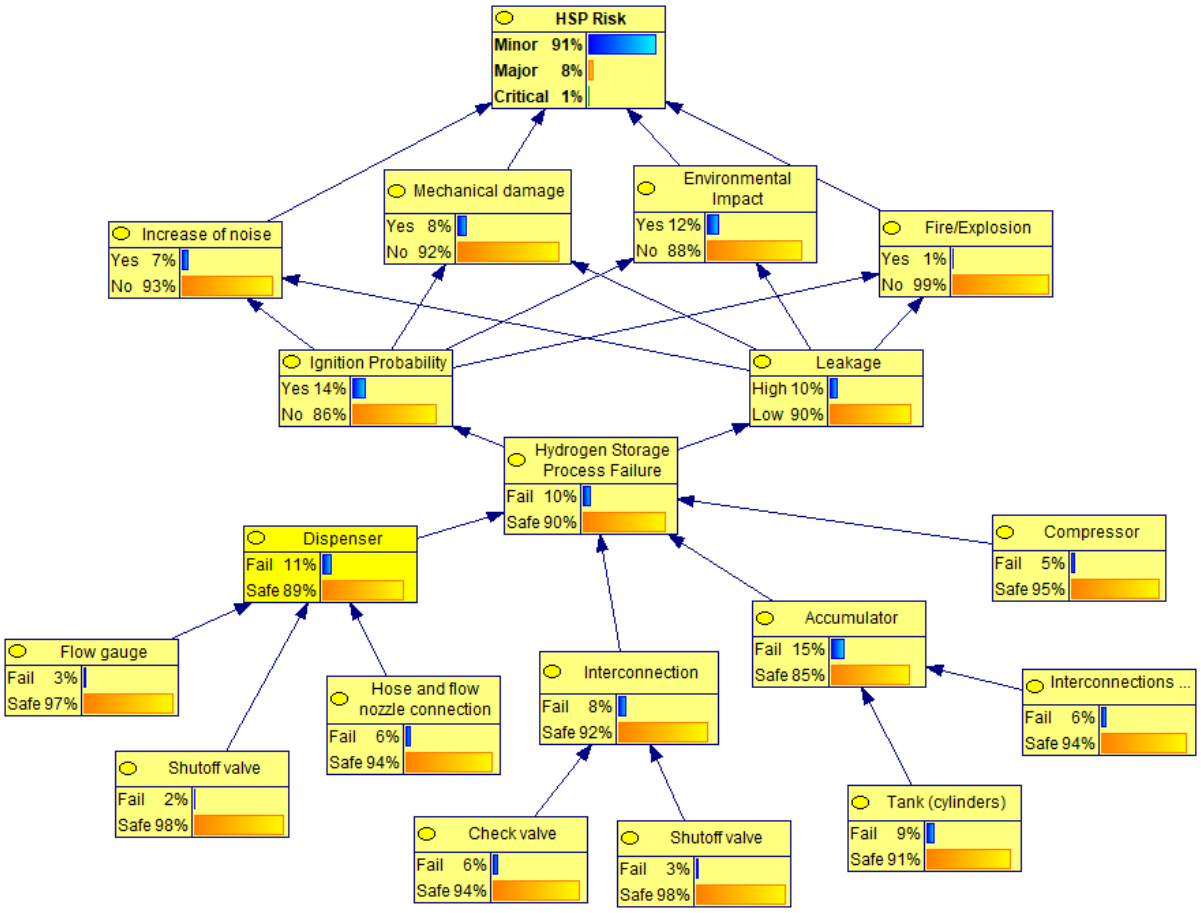


Figure 28. Developed Bayesian Network for a HSP

After mapping the possible consequences into the BN (Fig.28) using GeNIe 2.1 software, the system results to operate in minor risk with probability of 91%, in major risk with probability of 8% and in critical risk with probability of 1%. In order to generate the posterior probability of the components, the risk level of 100% minor risk was targeted. In the light of new evidence and based on posterior probability, the inspection interval is calculated as:

$$TI = \frac{\ln (1 - Pf)}{\lambda} \tag{35}$$

Where TI is the inspection interval, Pf is the posterior probability of failure, (ln) stands for natural logarithm and λ is the previous failure rate estimated by Eq. (34). Similarly, 100% major and critical risk were targeted to observe the influence of posterior probability as reported in Table 18.

5.5 Results and Discussion

Based on the relationship between the nodes conditional dependencies and probabilities the three risk outputs are calculated. Table 18 lists posterior probabilities and inspection interval of HSP components for minor, major, critical risk.

5.5.1 Minor risk level:

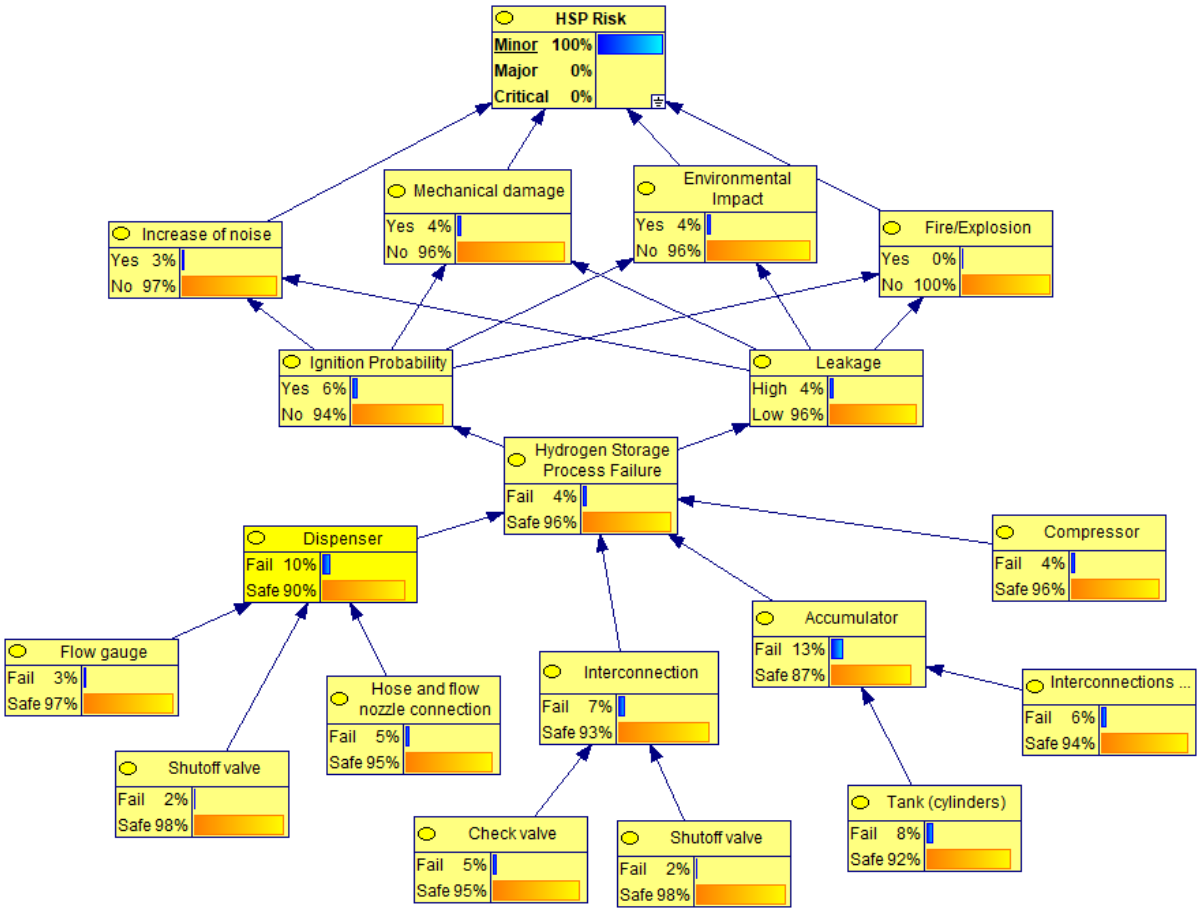


Figure 29. Minor risk posterior result

The calculations depicted that the most critical components are determined as the shut-off valve and hose/flow nozzle connection with the shortest TI of 290 and 288 days respectively. Thus, in case of shut-off valve, if the TI is 290 days, a 100% minor risk event will occur with a probability of 0.02. On the contrary, the most reliable components are the flow gauge and pipelines, which have the longest TI of 343 and 341 days respectively. For e.g. in case of flow gauge, if the TI is 343 days, a 100% minor risk event will occur with a probability of 0.03. Frequent usage of hose connection from operator will increase the minor risk.

5.5.2 Major risk level:

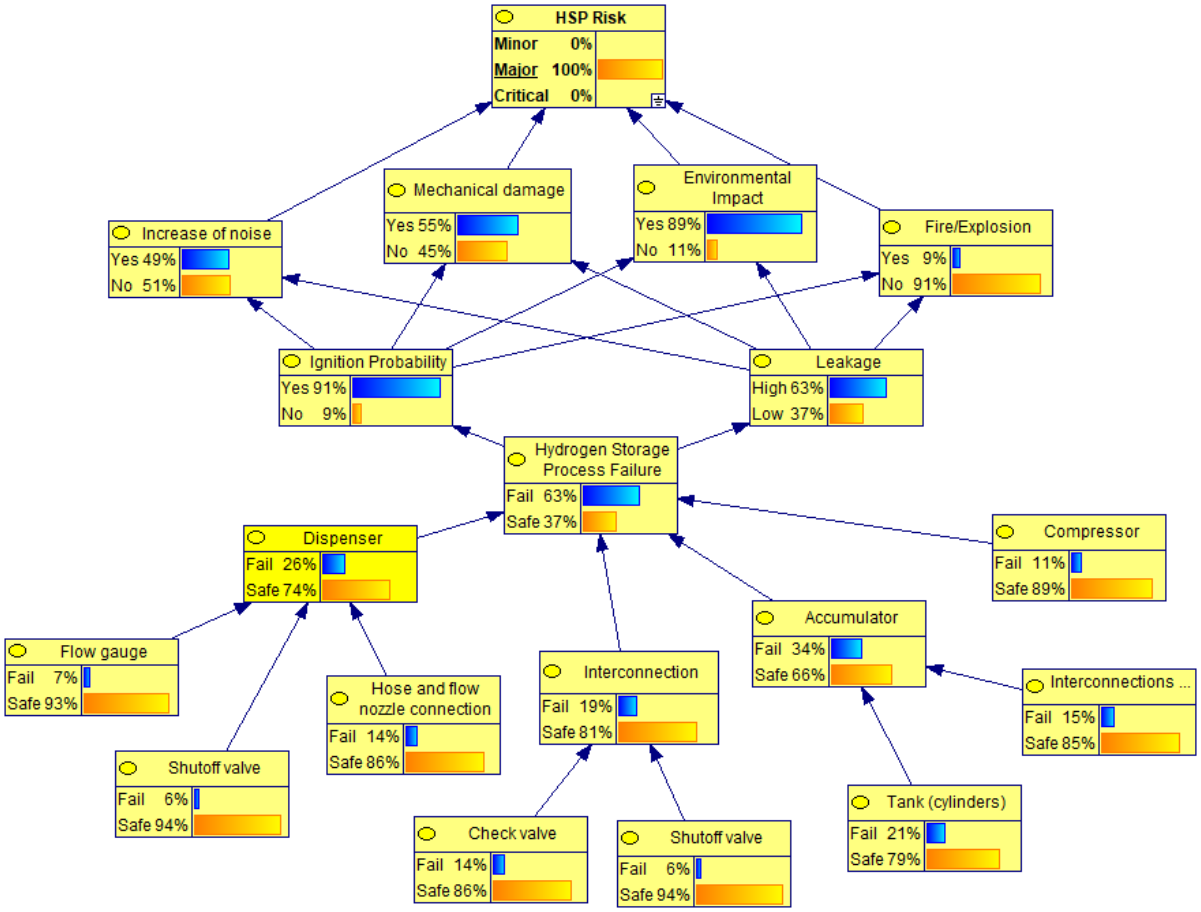


Figure 30. Major risk posterior result

In case, the policies of the system accept and tolerate major risks, the TI can be extended to wider time interval. The inspection action is required for tank before 588 days to avoid transition from minor to major risk. In case of flow gauge, the transition time from minor to major risk is the shortest i.e. 474 days. The calculation prioritize flow gauge as more critical due to shortest TI of 817 days. It should be noted that based on the influence diagram, conditional dependencies and probability, there is no change in major risk level and critical risk level TI for flow gauge.

5.5.3 Critical risk level:

The proportion of critical risk from the overall HSP risks is 1%, however critical risk with low probability can lead to high consequences. It can be noticed that compared to major risk, there is no significant difference in TI as critical risk. In case of pipelines, the transition time from minor to critical risk is the shortest i.e. 427 days compared to other components. The pipelines also has a relatively short inspection time compared to other components and thus becomes more critical under this category. If

the inspection period for pipeline is 768 days, a 100% critical risk event will occur with a probability of 0.13. The pipelines are associated with all major system installed in the HSP. A small to large leak on high-pressure system can release a huge amount of hydrogen thereby resulting in flammable air/gas.

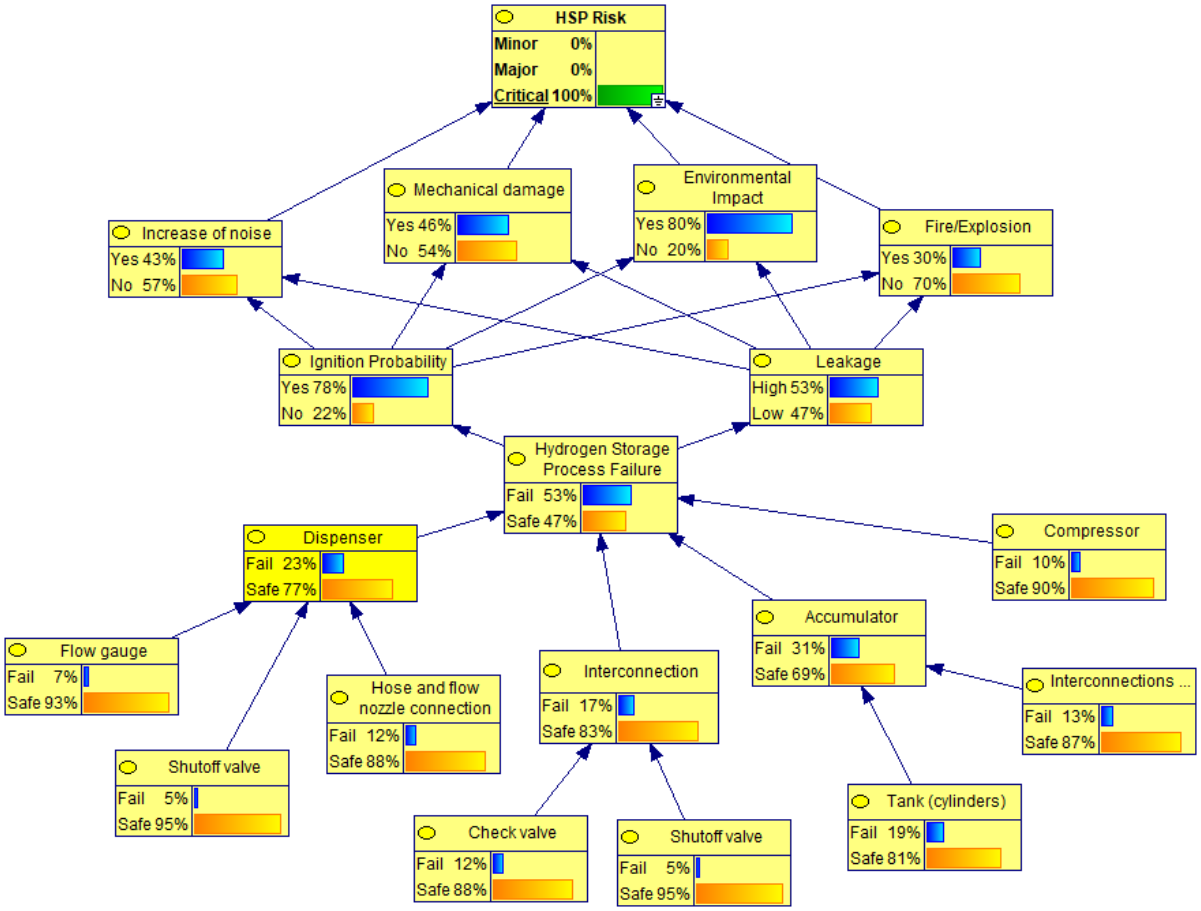


Figure 31. Critical risk posterior result

Table 18. Failure probabilities (Pf) and Inspection Interval (TI) of HSP critical components

Components	**Prior Pf**	**100% minor risk level**		**100% major risk level**		**Escalation time from minor to major risk**	**100% critical risk level**	
		Posterior (Pf)	**TI (days)**	**Posterior (Pf)**	**TI (days)**		**Posterior (Pf)**	**TI (days)**
Flow gauge	0.0319	0.03	343	0.07	817	474 days	0.07	817
Shut-off Valve	0.0250	0.02	290	0.06	889	599 days	0.05	736
Hose and flow nozzle	0.0627	0.05	288	0.14	849	561 days	0.12	719
Check Valve	0.0577	0.05	314	0.14	925	611 days	0.12	784
Tank (Cylinders)	0.0902	0.08	321	0.21	909	588 days	0.19	812
Pipelines	0.0640	0.06	341	0.15	896	555 days	0.13	768
Compressor	0.0470	0.04	309	0.11	884	575 days	0.10	800

Results show that the most critical components are the shut-off valve and hose/flow nozzle connection in case of minor risk. In case of major risk, flow gauge has the shortest transition from minor to major risk and thus makes it a most critical component. Pipelines has the shortest inspection time compared to other components and thus makes it the most critical component for critical risk.

5.6 Conclusion

This study presents a simple and creative RBI methodology to optimize the inspection test on the hydrogen system operation to model the associated risks using a BN. HSP was chosen as a case study to illustrate the methodology and its advantages. This study divides the risks in three different categories. By these categories, the inspection time is determined given that a component is overpassing the minor, major or critical level of risk. The most critical components were determined based on inspection time. In addition, accident data evaluation based on operation time and system category revealed that that dispenser and accumulator failure was more evident during the early stage of HRS operation period whereas compressor and interconnection system had accidents late in the operation period.

This methodology will be beneficial to understand the risk based influence of each critical component on the system, thereby allow prioritizing their inspection interval. In addition, the quantitative results on failure probabilities and risk based TI can be used to plan and optimize test interval for safety critical components. It should be noted that the TI calculation is based on the initial failure data assumed from external sources.

5.7 References

1) Pasman, H., Rogers, W. Risk assessment by means of Bayesian networks: A comparative study of compressed and liquefied H2 transportation. *International Journal of Hydrogen Energy*, Vol. 37, 17415-17425, 2012.

2) LaChance, J.: Risk-informed separation distances for hydrogen refueling stations, *International Journal of Hydrogen Energy*, Vol. 34, 5838-5845, 2009.

3) Paltrinieri, N., Khan, F.: Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application, *Butterworth-Heinemann*, 2016.

4) Martins, M.R., Schleder, A.M., Droguett, E.L.: A methodology for risk analysis based on hybrid Bayesian networks, *Risk Analysis,* Vol. 34, 2098–2120, 2014.

5) Abbassi, R., Bhandari, J., Khan, F., Garaniya, V., Chai, S.: Developing a quantitative risk-based methodology for maintenance scheduling using Bayesian network, *Chemical Engineering Transactions,* Vol. 48, 235–240, 2016.

6) *The High Pressure Gas Safety Institute of Japan (KHK)*, The high-pressure gas incidents database, https://www.khk.or.jp/activities/incident_investigation/hpg_incident/incident_db.html; [accessed February 2017].

7) SINTEF Offshore and Onshore Reliability Data Handbook Vol 1, 6th edition, *SINTEF Technology and Society*, Department of Safety Research, Trondheim, Norway, 2015.

CASE STUDY 6. Human Factor Analysis of Safety in Liquid Hydrogen Leak Incident using Probabilistic Graphical Model

6.1 Introduction

The human factors is of major concern and should be considered when implementing technology system. The High Pressure Gas Safety Institute of Japan (KHK, 2015) is a key organization that keeps record of high-pressure gas incidents (Yamada, 2015). This institute treats incidents, as accidents with explosion, leakage, and other ordinary disasters. The accident analysis at refueling stations carried out by the institute shows several factors that influence the initiating cause lead to flammable material (fuel) release. The chart in Fig.32 describes the statistics for the year 2015 for accident causes as recorded by the High Pressure Gas Safety Act (Yamada, 2015). In terms of accident causes, the record shows that out of 429 accidents in the year 2015, inadequate facility maintenance and management was the cause for 203 (47%) accidents, inadequate facility design and fabrication defects was the cause for 87 (20%) accidents, and 46 (11%) were caused by human factors, together contributing to 78% of the total accidents. This case study presents human error assessment through application of probabilistic graphical modelling.

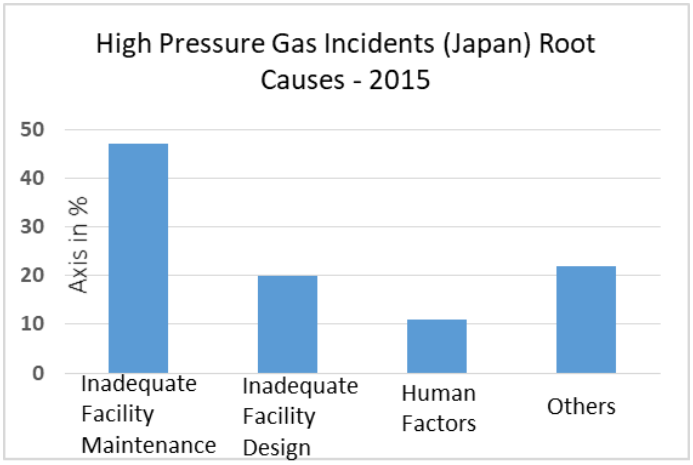


Figure 32. High Pressure as Accident Statistics in Japan 2015

Some studies reveal that organizational and human factors accounts for a considerable proportion of process accidents (Sakamoto et al., 2016; Karuiki, 2007) In addition, existing studies report that the leakage at joints in dispenser is mainly due to human error (Sakamoto et al., 2016) With regards to leakage from flexible hose and valve, the cause of all the accidents in US is human error. For the same

category, the human error and natural disaster are the leading causes in Japan. Human factors is an area which has not received as much attention as it deserves. This shows the need of a strategy to understand areas of improvement in the field of human factors to help prevent accidents.

The risk associated with the refuelling stations could change the perception of people towards accepting hydrogen as a fuel for fuel cell vehicles. Similarly, the process industry has faced some catastrophic incidents that are mostly attributed to human factors (Karuiki, 2007). The past study from UK HSE shows that human factors have contributed to several major accidents such as Piper Alpha, BP Texas refinery etc. (HSE, 1999; Manca 2012). At the most broad level of categorization, 47% of the identified accidents involved human error in one form or another (Bradley, 1999). Past studies show that more importance is given to technical aspects of systems in order to reduce the possibility of release (Leva, 2015). In spite of improvement in the performance of technical systems, it has been noted that accidents are on the rise. Thus, the technology has reached to a point where the improved safety can only be achieved through better understanding of human error mechanisms (Yamada and Leva, 2015).

The International Energy Agency (IEA) Hydrogen Implementing Agreement (HIA) in collaboration with research institutes is currently focusing on identifying and quantifying human influence on operational safety of hydrogen infrastructure (IEA, 2014). The hydrogen safety task requires a framework to model human factor issues for hydrogen safety. Thus, the focus of the study is to establish a framework to address human factor issues at hydrogen fuel station. Many quantitative approaches towards human error modelling have been developed in the past. Techniques such as SHERPA (Embrey, 2012), and THERP (Swain, 1983) were modelled to account for human factors. However, these techniques were mainly modelled for nuclear plants, chemical plants or medical devices and they do not address the human activity influence factors other than those provided in the technique itself. In addition, some quantitative methods do not thoroughly consider the factors that are suspected to contribute to human reliability (Hallbert, 2004). A new technology such as a Hydrogen Station poses a huge amount of risk due to human errors. However, the risk assessment for this station does not take into account the human factors issue as of now (Yamada, 2015). At present, there is limited research on

human factor analysis framework and classification for the hydrogen refuelling stations. Hence, the importance of this study lies on addressing human factor issues and providing solutions to quantify human error probabilities. A human factor analysis framework designed specifically for hydrogen refuelling stations would therefore be advantageous.

The purpose of this study is to develop a methodology to analyse a liquid hydrogen transfer leak incident in the refuelling station with respect to human factors as root causes. This study presents a semi-quantitative graphical method of human factor analysis for the refuelling station liquid hydrogen releases. The probabilistic graphical method helps to prioritise the causes that need to be analysed first and/or in the greatest level of detail, based upon the degree of anticipated risk that they pose. This study draws some conclusion and recommendations on multiple root causal relationships leading to gas releases focusing on human factor (HF) issues.

6.2 Research Methodology

The research methodology developed in this study is based on the model that emphasises on the scenario. The scenario used as a case study is "liquid hydrogen refuelling station transfer leak incident". A case study of liquid hydrogen release during bulk transfer process is undertaken as a scenario to analyse human related issues associated with the incident. The Human Factor Modelling (HFM) presented in this study consists of main steps as shown in Table 19.

Step	Step description
i	Development of a Hydrogen Scenario Risk Model – (Human Factor related causes only)
ii	Human Factor – Failure Mode and Effect Analysis (FMEA)
iii	Modelling the Human Factor Causes using a Fault Tree Analysis
iv	Compiling Fault tree into Probabilistic Graphical Model (PGM)
v	Human Error Probability Modelling (HEPM)
vi	Quantitative Modelling using Probabilistic Graphical Model
vii	Analysis Result

Table 19. Human Factor Modelling Process Steps

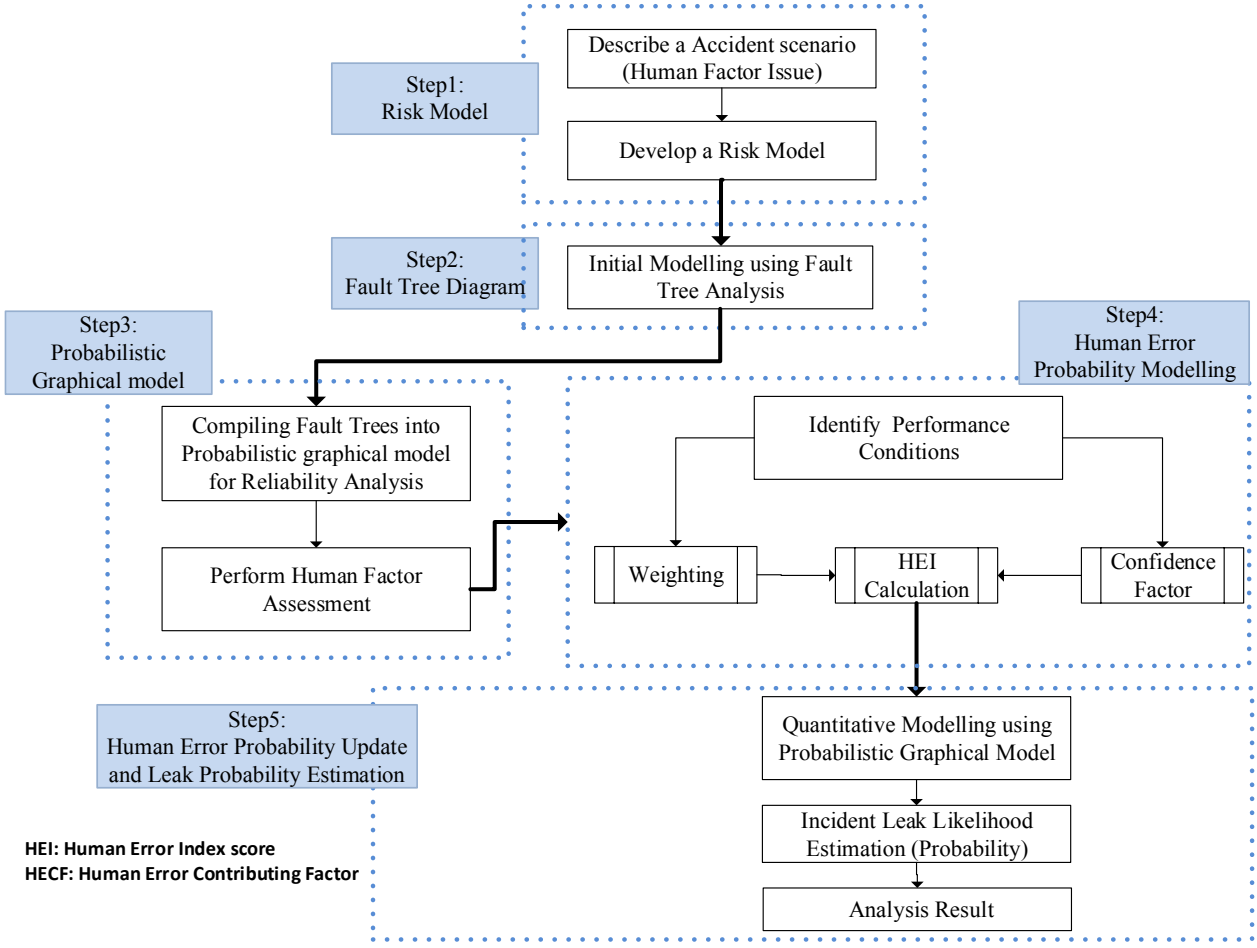


Figure 33. Human Factor Modelling Framework

A human factor modelling framework has been developed to understand the main steps involved in the process. As shown in Fig.33, the first step in the process is to develop a risk model for the scenario under investigation. Once the scenario is properly defined with all relevant information, the process makes use of multiple probability assessment techniques to model human error. The process uses probabilistic graphical model as a basis for quantitative analysis of human error. The steps involved in the assessment process are explained in detail in section 6.3 with an example of their application for a case study scenario.

6.2.1 Process Description

Liquid Hydrogen (LH2) transfer is a critical task because it involves large amounts of hydrogen. A tank truck is used to deliver LH2 to the refuelling station. A simple schematic diagram of the process is shown in Fig.34. The delivered liquid is stored in one or more storage tanks (cylinders) at temperatures

below -250°C. The operator initiates the transfer process and the supervisor is supposed to be monitoring his work. The hydrogen is transferred from the tank truck to the LH2 tank through a shut-off valve using hose pipe connection. In the later process, the hydrogen passes through a pump and is stored in pressure vessels. The shut-off valve is used for safety and isolation purposes. The hose pipe has to be correctly secured and verified in order to ensure smooth transfer of the LH2.

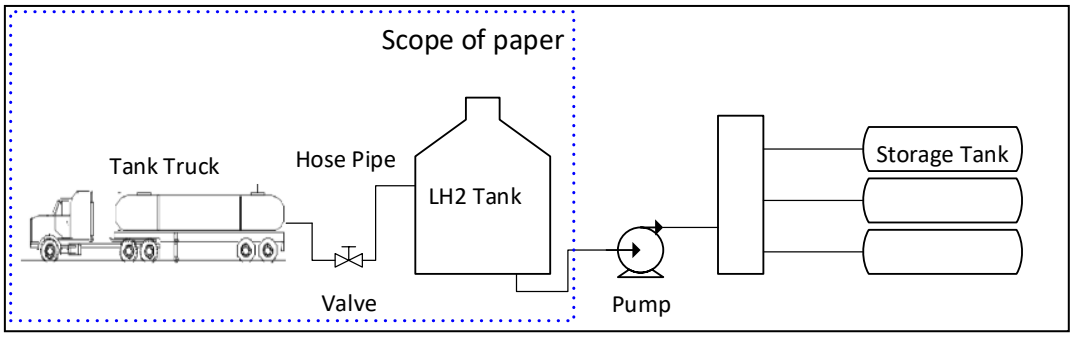


Figure 34. Liquid hydrogen delivery process

Previous study on hydrogen fuel station accidents reveals that leakage at joints is caused by human error and natural disaster in Japan (Sakamoto et al., 2016). Thus, this study attempts to focus on the process hazards from the human factor point of view, apply relevant safety methods to measure and prevent human error by fuel cell vehicle users.

6.3 Research Process and Case Study

6.3.1 Development of a hydrogen release scenario – Risk model

The first step in the research process is to extract more information about the scenario such as the causes of failure, root causes, protective layer, etc. The development of the set of release scenario will generate more information about human factors and specific conditions introduced to prevent hydrogen releases. The risk model for the scenario used as a case study is described in detail in Table 20.

Case Study Scenario:- Liquid Hydrogen Refuelling Operational Incident (Reported date: 29 Jan 2007)	
Hydrogen Type	Liquid
Probable Cause Identified	Failure to follow standard operating procedure.
Root cause	Communication, Human Error, Individual Action, Situational Awareness, Mechanical failure
Root Cause Categorization	Human and Operational Error / Procedural Failure / Mechanical Integrity
Operation Mode	Normal Operation
Detected by	Operator after the incident occurred / Detection Systems
Damage	Minor injury (The man was burned on his hands and on his stomach.)
Protective Layer	Follow the operating procedure
Purpose of Protective Layer	To ensure the steps in the procedure is not omitted while undergoing the tasks
Causes of failure	Distraction, time pressure, training, competency, procedure quality
What the industry needs to do in the future to avoid such failures	A. Hydrogen Safety Management • Facilities to establish Guidelines for the bulk transfer of liquid hydrogen from tank truck to the storage tanks. B. Engineering Design • Use of close coupled instrumentation design to avoid leaks through valve connections • Correct material selection for valves C. Human factors Engineering • Human reliability to be considered • Ensure standard operating procedures are followed

Table 20. Hydrogen Release scenario - Risk Model

6.3.2 Human Factor - FMEA

To identify human error related issues associated with hydrogen fuelling stations, bulk transfer incidents at such stations in Japan were analysed considering the failure mode, failure causes and effect analysis. Usually FMEA process is applied to mechanical equipment or component only (Gandhi, 1992). However, this study extends application of FMEA to identify human related issues. Human factor FMEA is a new area of research and this study makes an attempt to modify original FMEA to draw some conclusions. Human Factor FMEA emphasize on failure mode and failure cause for relevant process components such as hose, tank truck, shut-off valve an storage tank. The potential failure modes and their applicable HF related failure causes are captured in Table 21.

Key Process Step	Potential Failure Mode	Potential Failure Effects	Potential Causes (human error)	Current Controls
Emergency shutdown system	Shutdown failure on transfer leak	Potential Fire/explosion	Gas alarm not recognized by the operator - human error	Leak detector, visual detection by the public
		Potential Fire/explosion	Emergency shutdown not initiated by the supervisor or the operator - human error	Leak detector, visual detection by the public
		Potential Fire/explosion	Emergency shutdown not initiated by the supervisor or the operator - human error	Leak detector, visual detection by the public
Transfer Hose	Hose connection leak during unloading	Leak with potential of fire. Cryogenic burn	Mechanical failure of the hose	Inspection routines
		Leak with potential of fire. Cryogenic burn	Improper connection from the operator - human error	Quality Procedure/Checklists
	Release from hose prior to disconnect (not vented properly)	Minor Leak with potential of Cryogenic burn	Hose not vented prior to disconnect - human error	
		Minor Leak with potential of Cryogenic burn	Operator did not follow the right procedure and unloading checklists - human error	Quality Procedure/Checklists
Liquid H2 Tank Truck Leak	Liquid H2 Tank Truck Leak	Potential Fire/explosion	Mechanical failure due to road vibration	
		Potential Fire/explosion	Truck collision damages hydrogen piping while unloading - human error (collision either due to the movement of the truck itself or the nearby vehicle impact to truck)	Driver puts warning signs and caution cones near the truck and at the site
Liquid H2 shut-off valve Failure (stuck open)	Liquid H2 shut-off valve Failure (stuck open)	Potential Fire	Mechanical failure of valve - (stuck open)	Leak detector, visual detection by the public
		Potential Fire	Operator assume the valve was closed	Leak detector, visual detection by the public
	Failure to Stop release by closing stuck open valve on the trailer	Potential Fire	Operator not trained to stop liquid release	Leak detector, visual detection by the public
		Potential Fire	No planning to handle liquid release situation was done before the task	Leak detector, visual detection by the public
Bulk storage tank leak	Gas leakage from a liquid outlet valve	Potential Fire	Mechanical failure of the valve (stuck open)	Safety valve, Leak detector, Level Gauge, visual detection
		Potential Fire	Improper connection prior to unloading	Safety valve, Level Gauge, Leak detector, visual detection

Table 21. Human Factor FMEA

6.3.3 Scenario fault tree modelling

In order to analyse the human factors it is necessary to model the scenario using some modelling techniques. In this study, fault tree is introduced to model the scenario. The probability modelling makes use of several techniques such as FMEA, Fault tree analysis in risk assessment process. The failure analysis traceability can be improved by combining FMEA with Fault tree (Peeters, 2018). This is the method being utilised, which helps to analyse the failure causes and their root causes from the potential failure modes already identified through Human Factor FMEA. The fault tree model for the scenario "liquid hydrogen refuelling station leak incident" is presented in Appendix E. The causal relationship between basic events are linked using "AND" or "OR" gates. The human factor related basic events are identified as "operator" or "supervisor" in blue marks. The fault tree developed for the scenario will then be mapped to probabilistic graphical model to take advantage of several benefits offered by graphical model over conventional fault trees (Hamza, 2015; Khakzad, 2013).

The top event (T) i.e. the scenario "liquid hydrogen refuelling station leak incident" occurs when:

- P (T) = P (1) AND P (2)

The structure data of the tree and minimal cut sets are determined for evaluation of large fault trees. The minimal cut sets for the fault tree is obtained using deterministic approach (Kohda, 2006). All events in the fault tree are numbered as shown in Appendix E. The minimal cut sets for fault tree are:

- Set 1: E (1.1) E (2.1.1)
- Set 2: E (1.1) E (2.1.2)
- Set 3: E (1.1) E (2.2.1.1) E (2.2.1.2) E (2.2.2.1)
- Set 4: E (1.1) E (2.2.2.2) E (2.2.1.1) E (2.2.1.2)
- Set 5: E (1.1) E (2.3.2.1) E (2.3.2.2) E (2.3.1.1)
- Set 6: E (1.1) E (2.3.1.2) E (2.3.2.1) E (2.3.2.2)
- Set 7: E (1.1) E (2.4.1)
- Set 8: E (1.1) E (2.4.2)
- Set 9: E (1.2.1) E (1.2.2) E (2.1.1)
- Set 10: E (1.2.1) E (1.2.2) E (2.1.2)
- Set 11: E (1.2.1) E (1.2.2) E (2.2.1.1) E (2.2.1.2) E (2.2.2.1)
- Set 12: E (1.2.1) E (1.2.2) E (2.2.2.2) E (2.2.1.1) E (2.2.1.2)
- Set 13: E (1.2.1) E (1.2.2) E (2.3.2.1) E (2.3.2.2) E (2.3.1.1)
- Set 14: E (1.2.1) E (1.2.2) E (2.3.1.2) E (2.3.2.1) E (2.3.2.2)
- Set 15: E (1.2.1) E (1.2.2) E (2.4.1)
- Set 16: E (1.2.1) E (1.2.2) E (2.4.2)

Where E = Event. For event numbering refer to Appendix E.

Thus, the top event could occur if any of the set events is TRUE.

6.3.4 Compiling fault tree into probabilistic graphical model

Due to certain limitations fault tree cannot be used in dynamic risk analysis environment, where the probability needs to be updated on real time basis. Fault tree does not allow incorporating new knowledge or evidence into the system thereby making it inflexible to dynamic risk modelling (Paltrinieri, 2016; Hamza, 2015). The modelling possibilities offered by fault tree can be extended by relying on probabilistic graphical networks. Therefore, fault tree is mapped into a graphical diagram (Fig.35) to relax the limitations of fault tree and improve risk assessment process (Khakzad, 2013a, 2011b; Bobbio, 2001).

Figure 35. Hydrogen Liquid Transfer Leak Scenario Modelling using Probabilistic Graphical Model

The probabilistic graphical model was developed using software GeNIe 2.0 (Horny, 2014). The graphical model demonstrates a set of basic events (random variables) and their conditional

dependencies in the form of a directed acyclic graph (Zarei, 2017). The oval shaped node from which the arc is linked is called parent node while the node to which the arc is linked is called child node. The Fig.30 shows the relationship between various nodes leading to the top event. The relationship between different nodes are marked as "AND" or "OR". The graphical model is an exact replica of the fault tree represented in Appendix E. The top event can be identified by the black rectangle mark. In the latter part of this study, each root cause node (also known as fault node) will be provided with a human error probability based on the assessment performed in Section 6.3.5. The joint probability distribution for each child node is calculated using the equation:

$$P(X) = \prod_{i=1}^{n} P(Xi \mid Pa(Xi)) \quad (36)$$

Where,
i = 1 to n;
P (X) is the joint distribution probability;
Pa (Xi) is the parent set of Variable Xi.

The causal relationship between basic events helps to identify the most critical basic events leading to the top event (Khakzad, 2013). The model serves as a basis for identifying human factor related critical events. The nature of this structure and its ability to better model causal relationship between nodes (variables) make risk modelling more effective, transparent, and flexible (Zarei, 2017). More complex algorithms such as discrete and continuous distribution can be plotted using graphical model. However, this study limits the use of graphical model to conditional probability only.

6.3.5 Human Error Probability Modelling (HEPM)

This section of the study explains a method to estimate the human error probability for the failure events identified in FMEA. Firstly, it is difficult to analyse human error probability due to the random behaviour of humans. Practically, any activity performed by an operator can depend on several performance conditions such as training, distraction, performance, experience, stress, time pressure etc. The performance conditions that could be applicable for possible failure modes are shown in Fig.36. The human failure modes are primarily categorized as personal, group or management factors. The performance conditions are then decided based on the task activity. For example, an operator opening the wrong valve will be categorized under "Action" performance conditions. Furthermore, there are

several guidewords under each performance condition to help analyse each performance conditions in depth. The possible list of guidewords to analyse relevant performance conditions are listed in Appendix F.

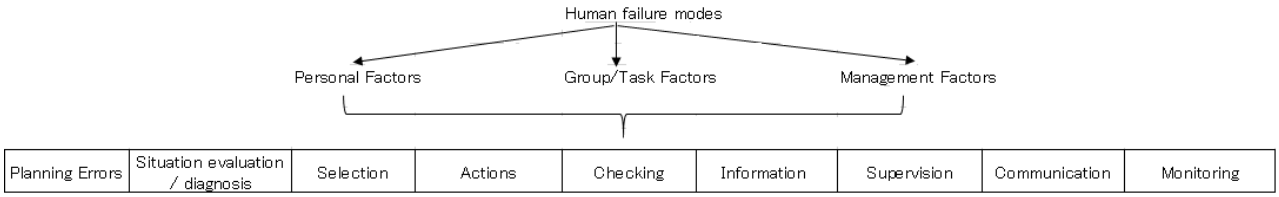


Figure 36. Human Failure mode grouping

The failure modes captured through FMEA should be reviewed by a team of experts and analysts should link each failure mode to its most applicable performance conditions. Thereafter, applicable guidewords should be extracted for each performance conditions. The Human Error Index (HEI) is calculated by adding together the products of the relative importance weights and the assessed confidence factor for each of the Performance conditions (DiMattia, 2005).

Event	Gas Alarm not recognised by the operator						
Total number of Conditions identified:	7						
Performance Conditions	Alarm management philosophy in place	The parameters that need to be monitored were not clearly defined	Definition of roles and responsibilities	Ease of access of monitoring information	Duration of monitoring	Distractions	Training
Box 1 Weighting	100	-100	100	100	-100	-100	100
Box 2 Confidence Factor	25	50	50	50	50	50	50
Total Human Error Index Sccore	0.46	Human Error Probability	0.05				

Figure 37. Human error probability modelling

Fig.37 shows HEPM for one of the failure mode i.e. “Gas Alarm not recognized by the operator” identified using the Human Factors - FMEA. This failure mode has seven performance conditions associated with it. Each performance conditions may be assigned a Weight from -100 to +100 and a confidence factor from 0 to +100. The confidence factor (shown in Box 2 marked in Orange) is a numerical value provided by the analyst which reflects the state of each performance condition in the model. This is normally on a scale from 1 (corresponding to worst-case conditions) to 100, (corresponding to best-case conditions). For some performance conditions (called reverse scales) such as time pressure or distractions, increasing the confidence factor (e.g. from low time pressure, rating 10 to high time pressure, rating 90) will increase the error probability. For these types of performance conditions, the values are subtracted from 100 in order to reverse direction of the scale. The HEPM for other failure modes are listed under Appendix G.

In case of weighting values shown in Box 1, high level of Monitoring Information is something positive and will increase the Human Error Index (HEI) value and decrease the probability of error - it therefore has a positive weight with a value of 100. In contrast, a high level of Distraction is a negative thing and will decrease HEI and increase the probability of error - it therefore has a negative weight with a value of -100. The model may be fine-tuned by adjusting the weights. For example, Training may be considered twice as important as Quality of Procedures so the later performance conditions may have a weight of +50 rather than +100.

The products of confidence factor and its corresponding weight for each performance conditions are then added to give a human error index score (the HEI) for the failure mode, which is then rescaled to fall within the range 0 - 1. This is the number shown in the bottom left hand window (0.46) of Fig.37. The HEI is obtained through a simple mathematical calculation as follows:

$$HEI=[(25/100)+(1-(50/100))+(50/100)+(50/100)+(1-(50/100))+(1-(50/100))+(1-(50/100))]\times(1/7)$$

$$HEI=[(0.25)+(1-0.50)+0.5+0.5+(1-0.5)+(1-0.50)+(1-0.50))]\times(1/7) = 0.46$$

Note the correction for reversed scales for 3 performance conditions is marked to -100.

The HEI score can be transformed to a Human error Probability HEP (the value of 0.0536 shown in the adjacent window in Fig.37) by means of a calibration relationship. Substituting the calculated HEI value of 0.46 (at the top of the failure modes of Fig.35) into Equation (37) gives a predicted HEP of 0.0536 for this failure event. The relationship between HEI and HEP are shown below:

$$HEP = -0.0999 * HEI + 0.1 \quad (37)$$

Note the HEI range from 0 to 1.0 is calibrated against HEP range of 0 to 0.1 because a proportion of the top event (leak incident) is caused due to human error. So a base factor of 10% human factor contribution leading to the top event is assumed in this study. In reality, this figure could be much higher and the calibration scale will then need to be changed accordingly. HEI and HEP values for the remaining human factor related failure modes are shown in Appendix G.

Note: In the case of a hazardous top event to be calculated is a frequency (1/time), Event 1.1 and 1.2.1 are converted to frequency.

6.3.6 Quantitative Modelling using Probabilistic Graphical Model

The graphical model in Fig.35 is used as a base for quantitative (probability) determination. The relationship between different nodes is represented through AND/OR gates based on the fault tree diagram drawn at the initial stage. Numerically, it represents the joint probability distribution among them. This distribution is described efficiently by exploring the probabilistic independences among the modelled variables (Khakzad, 2013). Each node is described by a probability distribution conditional on its direct predecessors.

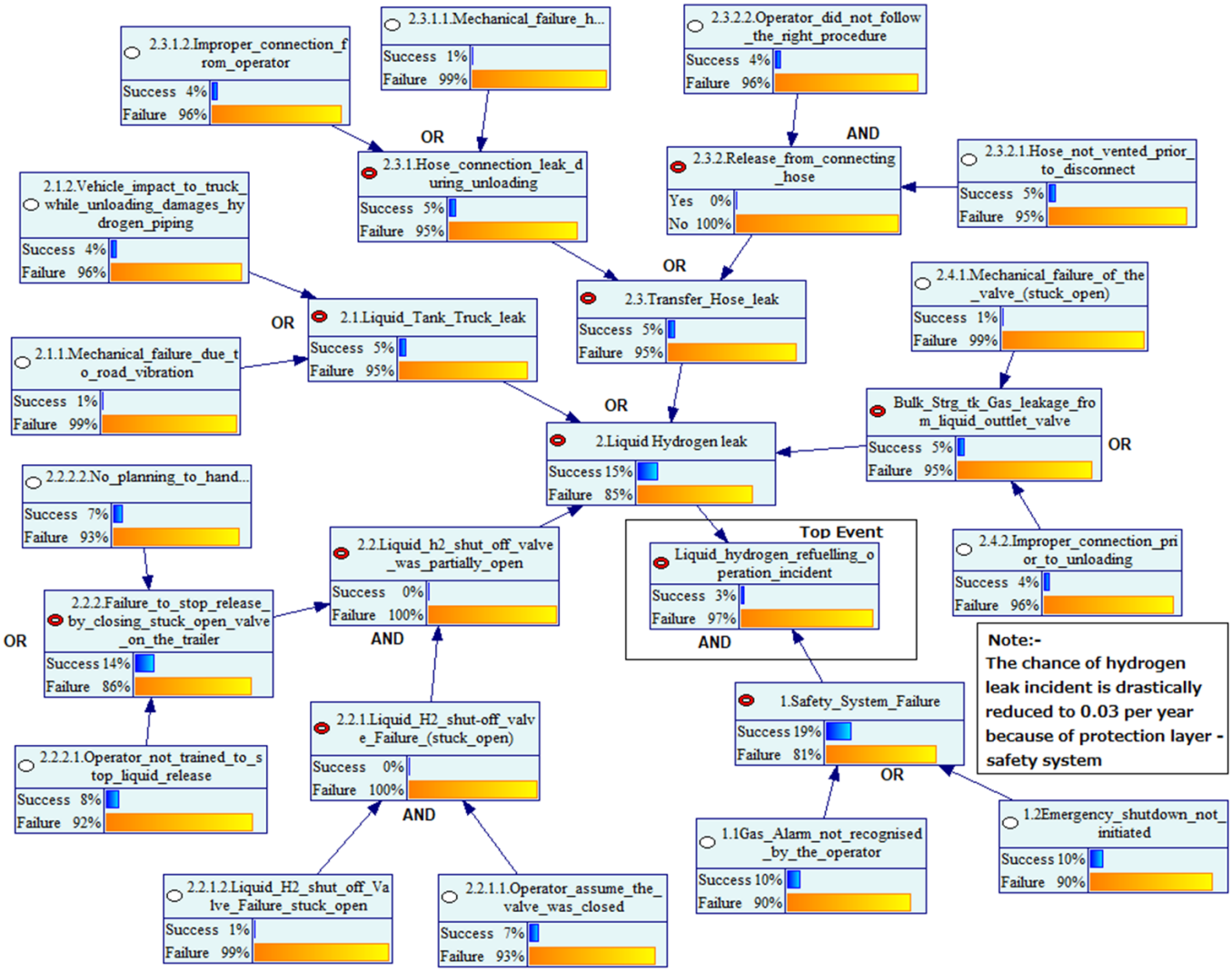


Figure 38. Human Factor Modelling of Leak Incident using Probabilistic Graphical Model

The final step is to determine the top event (gas release) probability. In the present work, the graphical modelling is simulated and run in GeNIe 2.0 software (Horny, 2014). Fig.38 shows the probabilistic graphical diagram equivalent of fault tree drawn (Hamza, 2015; Pearl, 2005; Groth, 2012). The mapped model is able to consider the common causes failures and conditional dependency among events. Once new observations are made such as new failure numbers, slip or misses of basic events, estimated top event likelihood can be updated through probability updating by means of the developed Graphical Model. It is to be noted that the probability figures estimated through the graphical model are slightly different from the values estimated through fault trees. This is because of the inclusion of conditional dependency.

The calculation sheet for the human error probability of all events, whose values were used to predict the scenario occurrence probability by means of probabilistic graphical model, is shown in Appendix G. Scenario (top event) frequency is equal to 0.03 per year after taking credit for safety system. This shows that the current operation of the station is heavily dependent on safety system design and its operation on demand in order to reduce the risk likelihood to 0.03/year.

6.4 MAIN FINDINGS AND RESULTS

One of the objectives of this study is to analyse critical events from safety point of view. This requires a coarse risk screening exercise to prioritise the causes to be analysed first and/or in the greatest level of detail, based upon the degree of anticipated risk that they pose. The graphical model developed in Fig.38 helps the analyst to understand the conditional probability distribution for each basic events to its child node. The graphical model describes the joint probability distribution efficiently by exploring the probabilistic independences among the modelled variables. Thus, the intermediate events having more influence on the top event are prioritised from Fig.38 and their relevant basic causes are further assessed based on the calculations of HEP and conditional probability distribution shown in Fig.38. A human factor analysis result is presented in the form of a table in Appendix H.

The approach used is useful to apply a coarse and relatively rapid screening process in order to focus the causal analysis on those causes that constitute the greatest source of risk. This reduce the time and effort required to reach to conclusions and also improves the quality of decision making process.

The underlying three failure events are identified as contributing to poor performance from the HEPM assessment (Appendix H):

1. Improper connection to hose from operator
2. Improper connection to liquid outlet valve prior to unloading
3. Liquid filling Vehicle collision impact damages hydrogen piping system

- **Improper connection to hose from operator**

Conditions	Recommendations that should be considered in Scope
Training	Training exercise should cover hose connection checks prior to the start of the process.
Checklist	The use of checklists should be clearly defined and understood by all personnel involved in the design, installation, maintenance, operation of bulk transfer process and the associated mechanical components.
Standard Operating Procedure & Policy	Standard procedure must be followed in all cases. A policy for use on hose and its connections should be developed, documented and implemented for new or existing installation.
Task based risk assessment	It is recommended to perform a task based risk assessment to identify potential cause of failures prior to the bulk transfer process.
Awareness Program	Good awareness program is essential to identify and record potential threats to piping's and fittings associated with the safety valves.
Clothing	Prescribed clothing must be worn at all times.
Supervision	A supervision should be mandated for hose connection checks prior to the start of the process.

- **Improper connection to liquid outlet valve prior to unloading**

Conditions	Recommendations that should be considered in Scope
Training	Training exercise should cover safety valve checks prior to the start of the process.
Checklists	The use of checklists should be clearly defined and understood by all personnel involved in the design, installation, maintenance, operation of bulk transfer process and the associated safety valves.
Standard Operating Procedure & Policy	Standard procedure must be followed in all cases. A policy for use on safety device and minimization of the fitting and piping's should be developed, documented and implemented for new or existing installation.
Task based risk assessment	It is recommended to perform a task based risk assessment to identify potential cause of failures prior to the bulk transfer process.
Awareness Program	Good awareness program is essential to identify and record potential threats to piping's and fittings associated with the safety valves.
Clothing	Prescribed clothing must be worn at all times.
Supervision	A supervision should be mandated to cover safety valve checks prior to the start of the process.

- **Liquid filling Vehicle collision impact damages hydrogen piping system**

Conditions	Recommendations that should be considered in Scope
Guardrail	The hydrogen dispenser area should have a guardrail system to prevent any collision with external vehicles.
Training	Staff should supervise the position of the vehicles and maintain safe distance from the dispenser. Staff should be trained on how to deal with minor fuel spillages in case of hazardous scenario.
Station layout	There should be an identified boundary between refuelling operation area and ancillary service area that will reduce the travel movement of the vehicles within the premises.
Fire Extinguisher	Each Dispenser should be equipped with one or more portable dry powder fire extinguishers
Standard Operating Procedure & Policy	Standard procedure must be followed in all cases. A policy for use on safety device and minimization of the fitting and piping's should be developed, documented and implemented for new or existing installation.
Task based risk assessment	It is recommended to perform a task based risk assessment to identify potential cause of failures prior to the bulk transfer process.

Probabilistic graphical model shown in Fig.38 shows that the chance of hydrogen leak incident is 15%. However, the leak event probability is drastically reduced to 0.03 per year because of the protection layer – safety system. This indicates that the current operation of the station is heavily dependent on safety system design and operation on demand to reduce the risk likelihood to 0.03 per year. The safety system functions as an emergency shutdown system where the primary function is to deactivate the source of release by automatically or manually isolating the liquid hydrogen flow. However in this case, most of the functions are dependent on human rather than system, appropriate care should be taken knowing that there is a possibility of leak in case the procedure is not followed. Standard operating procedure must be followed at all times. Assumptions are made at great risk. Risk also increases with complacency.

6.5 CONCLUSION

As a result of analysis, events related to safety valve failure, improper connection of mechanical components , incompetency and no planning prior to the task has been found as some of the key issues in a transfer leak operational incident at a hydrogen refuelling station. In the final part of this study, a quantification technique using a probabilistic graphical model quantifies the top event (gas release) probability using the HEP data. The frequency of a hydrogen leak incident is 0.03/year provided all necessary safety measures are in place. From the study, more awareness of hydrogen system among public, operator training (competency), use of correct policies and procedures are emerging as key contributions towards increased safety of the hydrogen service stations. In addition, a good performance (high integrity) safety system is required to prevent hydrogen releases.

6.6 REFERENCES

Bobbio, A., Portinale, L., Minichino, M., and. Ciancamerla, E., "Improving the analysis of dependable systems by mapping Fault Trees into Bayesian Networks", Reliability Engineering & System Safety 71 (2001), 249–260.

Bradley, G., Leverenz, F., Jr., and Rose, S., "Contribution of Human Factors to Incidents in the Petroleum Refining Industry", Process Safety Progress (V01.18, No 4) (1999).

DiMattia, D.G., Khan, F., and Amyotte, P., "Determination of Human error probabilities for offshore platform musters". Journal of Loss Prevention in the Process Industries, Vol. 18, Pages 488-501(July–November 2005).

Embrey, D., 2012, SHERPA Revisited – "A Systematic, Human Error Reduction and Prediction Approach to modelling and assessing human reliability in complex tasks", 2012 PSAM 11 & ESREL 2012 Conference, Helsinki, Finland.

Gandhi, O.P., Agrawal, V.P., "FMEA—A diagraph and matrix approach", Reliability Engineering & System Safety, Volume 35, Issue 2, 1992, Pages 147-158.

Groth, K., and Mosleh, A., "Deriving causal Bayesian networks from human reliability analysis data: A methodology and example model". Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, Volume: 226 issue: 4, page(s): 361-379 (2012).

Hallbert, B., Gertman, D., Lois, E., Marble, J., Blackman, H., Byers. J., "The use of empirical data sources in HRA". Reliability Engineering & System Safety 2004; 83(2):139–43.

Hamza, Z., and Abdallah, T., "Mapping Fault Tree into Bayesian Network in safety analysis of process system" 2015 4th International Conference on Electrical Engineering (ICEE), Boumerdes, 2015, pp. 1-5. DOI: 10.1109/INTEE.2015.7416862 (INSPEC Accession Number: 15807337).

Health and Safety Executive, UK 1999, "Reducing error and influencing behaviour". Report No. HSG48, Health and Safety Executive, UK, 1999.

Health and Safety Executive, UK 1999, "Human factors assessment of safety critical task", Offshore technology report 0992, HSE, UK.

Horny, M., Technical Report on "Bayesian Networks" Boston University School of Public Health, Arial 18, 2014. (Software GeNIe available at (http://www.bayesfusion.com).

IEA (2014b), "Technology Roadmap: Energy Storage", OECD/IEA, Paris.

Karuiki, S.G., Lowe, K., "Integrating human factors into process hazard analysis", Reliability Engineering & System Safety 2007; 92:1764-73. doi:10.1016/j.ress.2007.01.002

Khakzad, N., Khan, F., and Amyotte, P., "Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network", Process Safety Environ Protection 91 (2013), 46–53.

Khakzad, N., Khan, F., and Amyotte, P., "Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches", Reliability Engineering & System Safety 96 (2011), 925-932.

Kohda, T., "A simple method to derive minimal cut sets for a non-coherent fault tree", Int J Automat Comput (2006) 3: 151. https://doi.org/10.1007/s11633-006-0151-4

Leva, M. C., Naghdali, F., Alunni, C. C., "Human Factors Engineering in System Design: A Roadmap for Improvement". The Fourth International Conference on Through-life Engineering Services, 2015.

Manca, D., Brambilla, S., “Dynamic simulation of the BP Texas City refinery accident”. Journal of Loss Prevention in the Process Industries, Volume 25, Issue 6, November 2012, Pages 950-957. doi:10.1016/j.jlp.2012.05.008

Nakayama, J., Sakamoto, J., Kasai, N., Shibutani, T., Miyake, A., “Preliminary hazard identification for qualitative risk assessment on a hybrid gasoline-hydrogen fuelling station with an on-site hydrogen production system using organic chemical hydride”. International Journal of Hydrogen Energy, Volume 41, Issue 18, 18 May 2016, Pages 7518-7525.

Paltrinieri, N., Khan, F., “Dynamic Risk Analysis in the Chemical and Petroleum Industry”, Butterworth-Heinemann, 2016, Page IV, ISBN 9780128037652, https://doi.org/10.1016/B978-0-12-803765-2.12001-3.

Pearl, J., “Influence Diagrams – historical and Personal Perspectives", Decision Analysis, Vol. 2, no. 4, Dec 2005, pp. 232-234, DOI 10.1287/deca.1050.0055.

226:361–379, August 2012. DOI: 10.1177/1748006X11428107

Peeters, J.F.W., Basten, R.J.I., Tinga, T., “Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner”, Reliability Engineering & System Safety, Volume 172, April 2018, Pages 36-44.

Sakamoto, J., Sato, R., Nakayama, J., Kasai, N., Shibutani, T., Miyake, A., “Leakage-type-based analysis of accidents involving hydrogen fuelling stations in Japan and USA”, International Journal of Hydrogen Energy, Volume 41, Issue 46, 14 December 2016, Pages 21564-21570.

Swain, A.D., and Guttmann, H.E., “Handbook of human reliability analysis with emphasis on nuclear power plant applications”. Report No. NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, 1983.

KHK, The High Pressure Gas Safety Institute of Japan, (website: - www.khk.or.jp/english); Document available at http://www.khk.or.jp/english/dl/annual_report_lpg_2015.pdf.

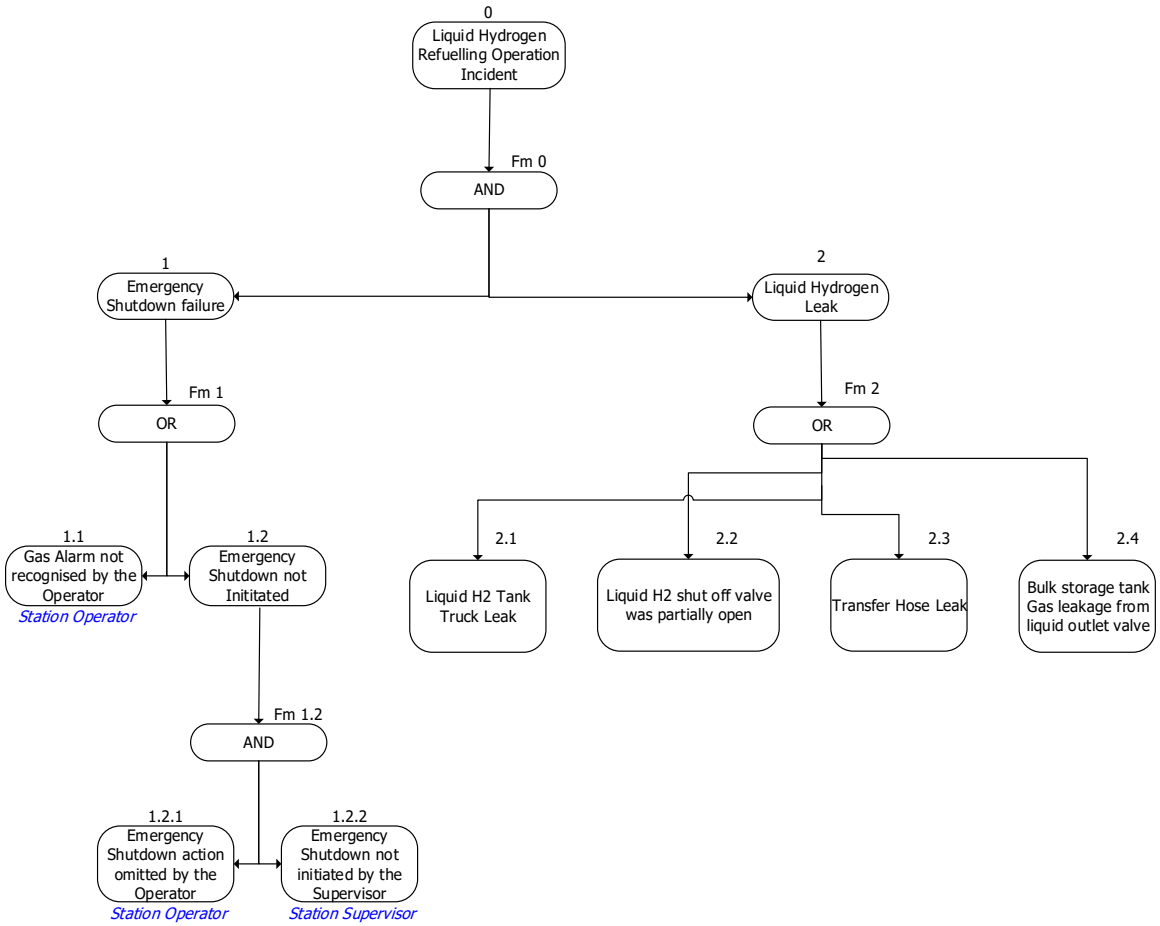
Yamada, T., Kobayashi, H., Akatsuka, H., Hamada, K.,

"Investigation and analysis of accident cases in gas stations", The High Pressure Gas Safety Institute of Japan, 2015; 52(10); 23-9 [in Japanese].

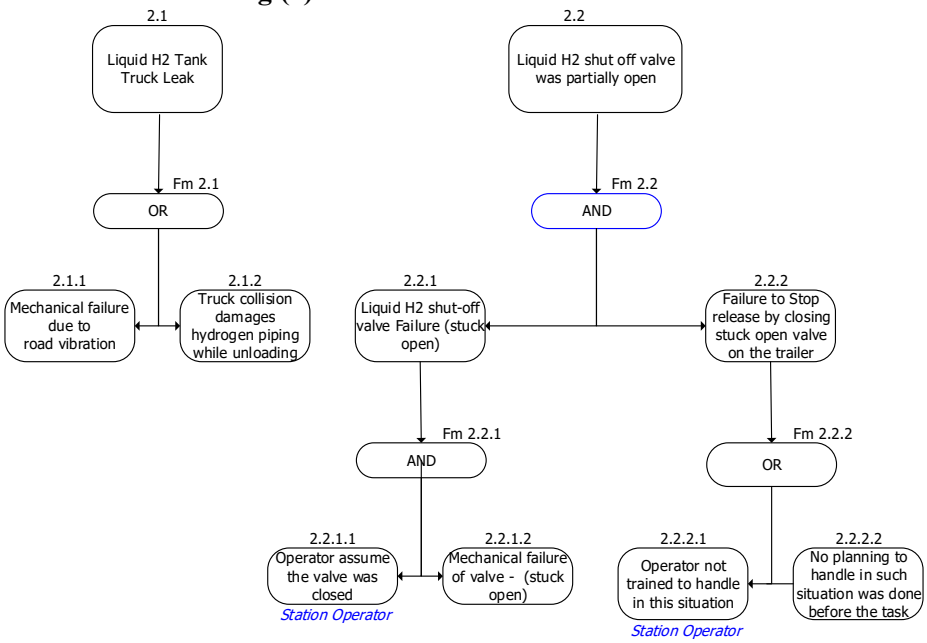
Zarei, E., Azadeh, A., Aliabadi, M., and Mohammad, I., “Dynamic Safety Risk Modelling of Process Systems Using Bayesian Network”, Published online 00 Month 2017 in Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/prs.11889.

Appendix E – Scenario Fault Tree modelling (expanded)

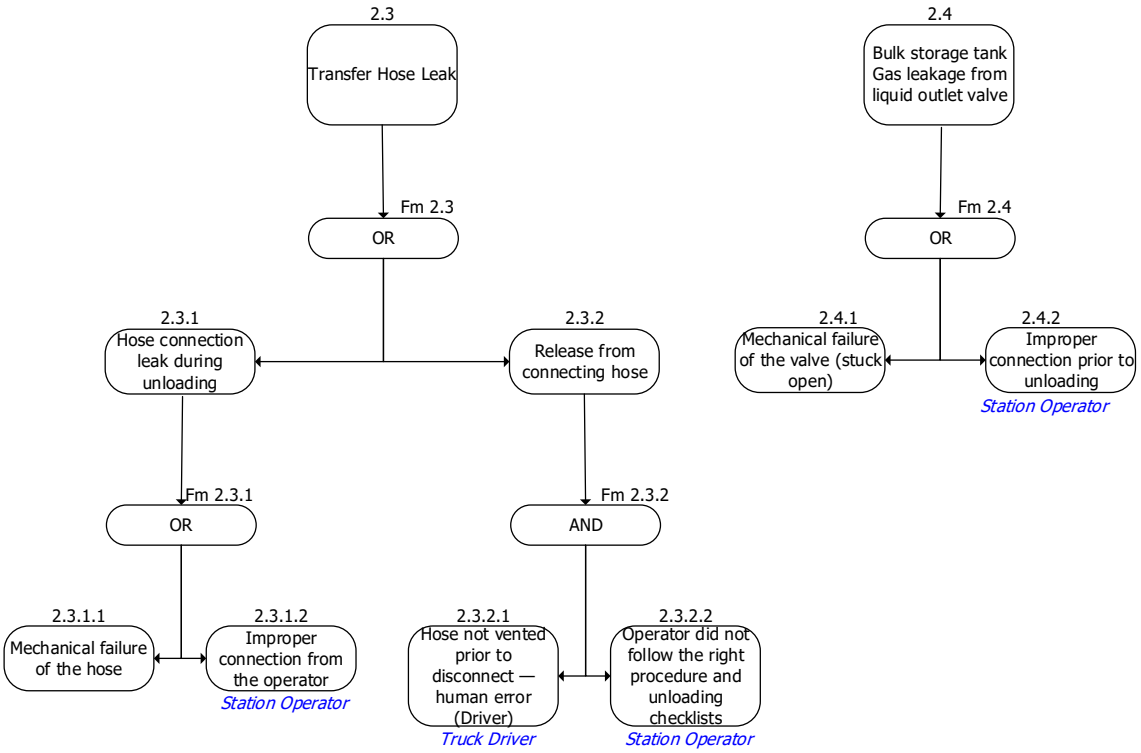
i) Top event



ii) Leak event modelling (1)



iii) Leak event modelling (2)



Appendix F – Key guidewords for performance conditions

Planning Errors	***Situation evaluation / diagnosis***	***Selection***
1 Incorrect or no plan formulated	1 SA omitted	1 Selection omitted
2 Insufficient resources allocated to activity	2 SA incorrect	2 Selection incorrect
3 Insufficient time allocated	3 SA too late	
4 Contingencies not considered		
5 Roles and responsibilities not defined		
Actions	***Checking***	***Information***
1 Action omitted	1 Check omitted	1 No Information
2 Right action wrong object	2 Check too late/early	2 Wrong information obtained
3 Action incomplete	3 Wrong object or action checked	3 Information incomplete
4 Action too early/late	4 Wrong check	4 Information content not checked/verified
5 Action too fast/slow		
6 Action too little/too much		
Supervision	***Communication***	***Monitoring***
	1 Information not communicated	1 Monitoring omitted
	2 Wrong information communicated	2 Wrong person or process monitored
	3 Ambiguous information communicated	3 Monitoring incomplete or interrupted (e.g. following a shift change)
	4 Incomplete information communicated	4 Incorrect variables monitored

Appendix G – Human error probability assessment

Event ID	Failure mode	Failure Mode HEP	Failure event Description	Individual HEP	Frequency in per year
1.1	Shutdown failure on transfer leak	0.19 per year	Gas alarm not recognized by the operator	0.0536	Approx. 0.1
1.2.1			Emergency shutdown not initiated by the supervisor or the operator - human error	0.0584	Approx. 0.1
1.2.2			Emergency shutdown not initiated by the supervisor or the operator - human error	0.0584	--
2.3.1.1	Hose connection leak during unloading	0.0809	Mechanical failure of the hose	0.0401	--
2.3.1.2			Improper connection from the operator	0.0426	--
2.3.2.1	Release from hose prior to disconnect(not vented properly)	0.0019	Hose not vented prior to disconnect - human error	0.0501	--
2.3.2.2			Operator did not follow the right procedure and unloading checklists - human error	0.0378	--
2.1.1	Liquid H2 Tank Truck Leak	0.0785	Mechanical failure due to road vibration	0.0401	--
2.1.2			Truck collision damages hydrogen piping while unloading - human error (collision either due to movement of truck itself or nearby vehicle impact to truck)	0.0401	--
2.2.1.1	Liquid H2 shut-off valve Failure (stuck open)	0.0071	Operator assume the valve was closed	0.0711	--
2.2.1.2			Mechanical failure of valve (stuck open)	0.1	--
2.2.2.1	Failure to Stop release by closing stuck open valve on the trailer	0.1432	Operator not trained to stop liquid release	0.08	--
2.2.2.2			No planning to handle liquid release situation was done before the task	0.0688	--
2.4.1	Storage Tank Gas leakage from liquid outlet valve	0.0809	Mechanical failure of the valve (stuck open)	0.0401	--
2.4.2			Improper connection prior to unloading	0.0426	--
	Top Event Likelihood		**0.03 / year frequency with safety system credit**		

Note: In the case of a hazardous top event to be calculated is a frequency (1/time), Event 1.1 and 1.2.1 are converted to frequency.

Appendix H – Human factor analysis result

Event ID	Failure events (excludes safety system failure)	HEP	% Contribution to Intermediate Event – Top Event	Performance level
2.3.1.1	Mechanical failure of the hose	0.0401	1%	Low effect
2.3.1.2	Improper connection from the operator - human error	0.0426	4%	Poor
2.3.2.1	Hose not vented prior to disconnect	0.0501	0%	-
2.3.2.2	Operator did not follow the right procedure and unloading checklists - human error	0.0378	0%	-
2.1.1	Mechanical failure due to road vibration	0.0401	1%	Low effect
2.1.2	Truck collision damages hydrogen piping while unloading - human error	0.0401	4%	Poor
2.2.1.1	Operator assume the valve was closed	0.0711	0%	-
2.2.1.2	Mechanical failure of valve (stuck open)	0.1	0%	-
2.2.2.1	Operator not trained to stop liquid release	0.08	0%	-
2.2.2.2	No planning to handle liquid release situation was done before the task	0.0688	0%	-
2.4.1	Mechanical failure of the valve (stuck open)	0.0401	1%	Low effect
2.4.2	Improper connection prior to unloading	0.0426	4%	Poor

Note: The intermediate event having more influence on the top event are prioritized and its relevant basic causes are further assessed using probabilistic graphical model.

7. MAIN CONCLUSIONS AND FUTURE WORK

The PhD initially addresses the core concept relating to risk review, safety categorization of new technology and accident analysis. At first, the term "risk" is defined for this PhD as "probability uncertainty" and the concept of the risk is reviewed in detail in Section 1.2.1. Due to the nature of the new technology, it should be categorized based on the classification and qualification in terms of safety as explained in Section 1.2.2 and 1.2.3. The qualification of a hydrogen system is classified under Category 3 due to limited knowledge of the application and extremely limited data on accidents/failures. Performance criteria for the product and/or the technologies must be specified by the developer based on various safety and reliability measure. The accident characteristic is studied to understand the trend of accident occurrence and impact of lack of data on the uncertainty in results in new systems.

A dynamic approach for addressing uncertainty in accident and risk assessment, based on the evaluation of the hydrogen system is implemented. The case study addressed several uncertainties areas in the risk and reliability quantification of hydrogen station. Research results include developed models for organizing, processing and analyzing accident data. A general systematic process flowchart is developed in Fig.3 and framework in Fig.4. The reliability prediction methods adopted in this research were classified into three categories: (1) statistical distribution methods, (2) physics-of-failure methods, and (3) top-down similarity analysis methods. The first and third category is based on statistical analysis of failure data, while the second category is based on physics-of-failure models. Case study 1 and 2 of the research deployed statistical methods, case study 3 deployed physics-of-failure method, while case study 4, 5 and 6 utilized external failure database combined with Bayesian.

In the initial phase of the research, time based evaluation methods using Weibull and log normal function were proposed for leak rate estimation using operating time data on HRSs. Even if accident events are rare, two statistical models can provide a range of leak rates as a function of time. This is found to be beneficial in case of lack of data issue. In addition, leak frequency estimates from the other two methods i.e. non-parametric based and leak hole-size based were examined. The leak rate obtained from the non-parametric method was found to be the most conservative among the three. Perhaps, this

is because of the more frequent failures observed in the new evidences for the 70 MPa system. One possible solution is to consider a conservative value for the design of HRS, in which case, the non-parametric model leak rate of 0.24 per year can be used. The base value selected can be selected in design to set performance standards for the availability and reliability in the operation and maintenance of HRSs.

Unrevealed leak time was assessed from the estimated leak frequency. It can be concluded that if the leak rate is estimated to be high, the inspection interval should be more frequent to reduce the unrevealed leak time and increase the process safety. The unrevealed leak time can be used to the specification of hydrogen sensors to detect leaks of hydrogen. This will ensure the component and process both meet the requirements in the performance standard, leading to increased process safety in HRSs. Further work can be carried out to set the performance requirement of hydrogen sensor based on the unrevealed leak time.

For accident data uncertainty assessment, we have introduced a study on the accident data uncertainty based on time correlation model (CAR model). The model estimates the uncertainty and accident rate by time correlation model that is fundamental to the challenge of lack of data. The CAR model is different from the other lifetime distribution models because its main aim is to reveal the estimate's uncertainty. A new system such as HRS has very little accident information, and so future predictions are inevitably unreliable. One approach to rectify this problem is to wait until enough data have been collected, or utilize the accident data of similar systems to increase its reliability. However, the Gaussian conditional autoregressive model does not aim to reduce the uncertainty; rather it discusses the effect of lack of information on the estimation. This new way of dealing with and interpreting accident information can be utilized to evaluate new systems such as HRS in the future.

Verification of QRA is vital topic in the field of process safety and was found necessary to choose appropriate parameters in failure estimation and understand its influence on the reliability assessment to offset the limitations associated with data scarcity and QRA uncertainty problems. Failure of hydrogen system was estimated using time function and number of filling function. The study concludes

that the failure rate estimated as a function of number of fillings is more reliable and realistic than the estimation based on survival time. Moreover, the number of fillings is more representative of the true failure rate as it considers the actual station's usage and loading. The survival time do not always represent the actual usage of the stations. The study brings to light the importance of verifying the appropriate life parameters and their associated influence on reliability assessment. The verification of appropriate parameters reveal the true estimates of failure rate for HRS. If the reliability parameter is selected based on usage and actual conditions of the HRS, it will lead to accurate estimation of risks and improved critical business decisions. Further work can be carried out to find other suitable ways for verification and validation of QRA.

For improvement in reliability assessment, a dynamic modelling was integrated to IEC 61508 functional safety standard to conclude on how failure rates and failure probability can be controlled in practice. A Bayesian framework was implemented that addressed the requirements by allowing industry knowledge about failure rates to be incorporated in a prior gamma distribution and periodic updating process with new survival data as it becomes available. It is observed that with less number of new observations, the updated failure rate is sensitive to generic uncertainty data which does not provide realistic result. In order to improve the sensitivity of updated failure rate, more number of observations subject to modelling using Monte Carlo method will be beneficial. Further work can be carried out to generate appropriate base value for all hydrogen station components that can be used in design set performance standards for availability and reliability in operation and maintenance of the component.

A simple and creative RBI methodology was implemented to optimize the inspection test on the hydrogen system based on the associated risks using a BN. The study divides the risks in three different categories. By these categories, the inspection time is determined given that a component is overpassing the minor, major or critical level of risk. The most critical components were determined based on inspection time and risk category. In addition, accident data evaluation based on operation time and system category revealed that that dispenser and accumulator failure was more evident during the early stage of HRS operation period whereas compressor and interconnection system had accidents late in

the operation period. Further work can be carried out to implement a decision support tool for integrity management using comprehensive and real failure data to reduce uncertainty and improve accuracy.

A probabilistic graphical model is proposed for human factor analysis in liquid hydrogen leak incident. From the study, more awareness of hydrogen system among public, operator training (competency), use of correct policies and procedures are emerging as key contributions towards increased safety of the hydrogen service stations. In addition, a good performance (high integrity) safety system is required to prevent hydrogen releases. It is found that such semi-quantitative graphical method of human factor analysis for the refueling station liquid hydrogen releases helps to prioritise the causes that need to be analyzed first and/or in the greatest level of detail, based upon the degree of anticipated risk that they pose. Further work can be carried out within to identify prior probability of human causes across the entire hydrogen refuelling station. This research can be further extended to accomplish standardisation of HEP data with the ultimate objective of producing an engineering database for human error risk assessment.

8. INTERNATIONAL PUBLICATIONS AND CONFERENCES

❑ International Publication (4 Published)

- Mahesh Kodoth, Shu Aoyama, Junji Sakamoto, Naoya Kasai, Tadahiro Shibutani, Atsumi Miyake. Evaluating uncertainty in accident rate estimation at hydrogen refueling station using time correlation model, International Journal of Hydrogen Energy, Volume 43, Issue 52, 2018, Pages 23409-23417, ISSN 0360-3199, https://doi.org/10.1016/j.ijhydene.2018.10.175.

- Mahesh Kodoth, Tadahiro Shibutani, Yehia F. Khalil, Atsumi Miyake. Verification of appropriate life parameters in risk and reliability quantifications of process hazards, Process Safety and Environmental Protection, Volume 127, 2019, Pages 314-320, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2019.05.021.

- Mahesh Kodoth, Shu Aoyama, Junji Sakamoto, Naoya Kasai, Yehia Khalil, Tadahiro Shibutani, Atsumi Miyake. Leak Frequency Analysis for Hydrogen-based Technology using Bayesian and Frequentist Methods, Process Safety and Environmental Protection, 2020, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2020.01.025.

- Kodoth M., Shibutani T., 2019. Improvement in reliability quantification to support BS EN 61511 failure probability analysis, Chemical Engineering Transactions, 77, 571-576, DOI:10.3303/CET1977096.

❑ Domestic Conference (2)

- Kodoth M., Shibutani T.," A Risk Based Inspection Model for Hydrogen Refueling Station using Bayesian Network", JCOSSAR 2019, Tokyo, Japan, Oct 2019.

- Mahesh Kodoth," Improving education on Safety and Risk Management in undergraduate courses in Chemical Engineering ", Japan-India YNU Symposium 2017 `Emerging Materials & Systems for Green and Life Innovations` Conference , Yokohama, Japan, Dec 2017.

❑ International Conference (2)

- Kodoth M., Shibutani T.," Application of Probabilistic Graphical Models in Human reliability Analysis", Asia Pacific Symposium on Safety (APSS 2017), Kyushu, Japan, 01st Dec 2017.

- Kodoth M., Shibutani T.," Improvement in reliability quantification to support BS EN 61511 failure probability analysis", Loss Prevention (LP 2019), Delft, Netherlands, 16th June 2019.