Universitetet
i Stavanger

FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme/specialisation: OFFSHORE TECHNOLOGY/ RISK MANAGEMENT	Spring / ~~Autumn~~ semester, 2017.. Open/~~Confidential~~-
Author: NUR RAMADHANIA	(signature of author)
Programme coordinator: ASSOCIATE PROFESSOR ROGER FLAGE Supervisor(s):	
Title of master's thesis: RISK CONCEPTUALIZATION AND DESCRIPTION IN INHERENT RISK ASSESSMENT AS A NEW CONCEPT OF RISK ASSESSMENT AND COMPARISON TO QRA PRACTICE IN NORWAY	
Credits: 30 ECTS	
Keywords: Inherent Risk Assessment Inherent Safety Design Principle Quantitative Risk Assessment Risk Concept Risk Description ALARP Principle	Number of pages: 59 + supplemental material/other: - Stavanger, 15 June 2017 date/year

Title page for Master's Thesis
Faculty of Science and Technology

ABSTRACT

In 2009, Shariff and Leong [1] introduced a new concept named as Inherent Risk Assessment (IRA). The concept integrates quantitative risk analysis and to a process design simulator called HYSYS aiming to provides essential data as early as possible so that modification based on inherent safety principles can still be incorporated into the design. By doing so, the evaluation of inherent risk can be easier and faster. Thus, an inherently safer design can be obtained.

On the other hand, in Norway, Quantitative Risk Assessment (QRA) studies has been extensively implemented in the petroleum industry for more than two decades. In performing the QRA, a guideline called NORSOK Standard Z-013 Risk and Emergency Preparedness Assessment [2] is utilized by the Norwegian petroleum industry and this standard is regarded as the most detailed standard. QRA is regarded as a well-establish and well-proven method in risk assessment.

Based on the key facts related to the risk assessment methods described above, it is interesting to understand further about how is risk conceptualized and described in Inherent Risk Assessment and NORSOK Z-013 [2] as the guideline of QRA practice in Norway compared to uncertainty-based risk conceptualization. Another interesting point is to discuss the key differences of Inherent Risk Assessment compared to Quantitative Risk Assessment practice in Norway based on NORSOK Z-013 [2].

In this work, several fundamental issues found in IRA, which most of them appears as disadvantages when compared to QRA in Norwegian petroleum industry. The first issue is the lack of attention given to uncertainty aspect as a consequence of Shariff and Leong [1] seems to have a mixed up understanding of probability and uncertainty. The second issue related to the risk picture presentation where ALARP region is excluded because the ALARP principle is seen can only be exclusively applied to the add-ons risk-reducing measures. The third issue the ‘mechanistic’ approach demonstrated by the study cases where the assessment is focused on the satisfying the risk tolerable limit. The other issues are related to the fact that IRA is designated to be performed in the preliminary design stage so that the implementation of inherently safer design principles can only be optimized on a fix design concept and there is a need for another risk assessment as complementary to assessed risk in the following stages.

In comparison, QRA in Norwegian petroleum industry put a consideration of uncertainty aspect in its study and NORSOK Z-013 [2] covered the introduction of ALARP principle and

evaluation even tough it is part of risk treatment which is out of the standard's scope. Moreover, QRA studies can be performed as early as concept selection phase so it has the greatest opportunity to give influence to the design and it does not need a complementary risk assessment.

The only notable advantage of IRA compared to QRA in Norway is the high integration of the risk assessment in the form of quantitative risk analysis to a process design simulator. The integration allows for the automation in the knowledge transfer between the designers and the risk assessor. Therefore, the risk level can be obtained faster compared to typical QRA studies.

The practice in Norwegian petroleum industry shows that by performing QRA thoroughly and carefully in different phases of the project, all risk in the design will be assessed since the earliest phase and the need for a complementary risk assessment can be eliminated.

Acknowledgement

This thesis is prepared as the final work to fulfill the requirement for Master of Science degree in Offshore Technology with specialization in Risk Management at University of Stavanger.

I owe my deepest gratitude to my supervisor Assistance Professor Roger Flage. Without his guidance, valuable knowledge and insight, encouragement, and positive attitude this thesis would have been possible.

I am grateful to have my two supportive best friends Nadhira and Ariefina who helped me in writing process of this thesis.

I am indebted to my husband who has been enthusiastically and endlessly encouraging me to pursue my master's degree.

Finally, I would like to express my appreciation to my daughter who has been showering me with unconditional love so that I have something to look forward to in every day.

Stavanger, 15 June 2017

Nur Ramadhania

Table of Contents

Table of Figures

1 Introduction

1.1 Background

In 2009, Shariff and Leong [1] introduced a new concept to evaluate inherent risk named as Inherent Risk Assessment (IRA). This risk assessment is described as a proactive measure to eliminate or minimize risk based on inherent safety principles by integrating quantitative risk assessment technique of quantifying risk to a process design simulator called HYSYS. It is described further that the high integration allows for automation in data extraction from design process to the risk assessment so that information related to the risk level can be obtained faster than a typical QRA study. By having the risk level in the earlier design stage, modifications based on inherent safety principles to obtain an inherently safer design can be incorporated into the design.

The inherent safety design concept was first proposed by Kletz [3] in late 1970's as a fundamental approach to hazard management focusing in avoiding or limiting the hazard at the source, and not to rely on to add-on safety features or management systems and procedures to control the hazard. [4] The inherent safety principles formalized by Kletz includes intensification, substitution, attenuation, simplification, limitation of effects, and error tolerance. [1]

Shariff and Leong [1] explains that the fundamental difference of Inherent Risk Assessment and Quantitative Risk Assessment is the stage of the assessment taken places since IRA also utilizing quantitative risk analysis approach. Shariff and Leong [1] argues that where a traditional QRA (in general) is carried out after a detailed engineering design has been completed, IRA can be performed as early as process simulation begins during the preliminary design stage in parallel with the selection of process route and development of heat and material balances. Thus, IRA results can be utilized to provoke design modifications to obtain inherently safer design.

From the technical perspective, due to its extensive and time-consuming nature, QRA only study and document the most representative scenarios. Shariff and Leong [1] further mentioned that in QRA all information for process conditions also need to be manually transferred due to lack of integration between risk assessment software and process design simulator. Meanwhile, IRA technique proposes integration between risk models and process design simulator, such as

HYSYS, so that that data can be automatically transferred. By using this integrated model, inherently safer design options can be quickly evaluated. [1]

This implementation of inherent safety design in the preliminary design stage is expected to minimize residual risk. Thus, higher cost savings can be realized as the overall design will not need add-ons safety measures as much as what have been seen in a typical QRA practice. [1]

The IRA technique presented by Shariff and Leong [1] is appealing because it addresses some of the QRA limitations. For instance, in the process leak case, typical QRA calculation will focus only on the leak frequency based on statistical data without considering the human intervention. This in contrary with Vinnem and Røed [5] research with 60% of hydrocarbon leak with a rate higher than 0.1kg/s in 2008-2014 occurred during manual intervention with the dominating activity is preventive maintenance.

IRA is expected to also address this concern due to its focus on minimizing potential leak source through reducing the complexity of the design in the first place. This is important because the plant designers have a tendency to think that any amount of flanges in the design is acceptable for plant connectivity and isolation, while at the same time these flanges are the potential leak sources. [6]

Further, Shariff and Leong [1] mentioned that IRA is not to be taken as a better technique than QRA, but rather as a complement to each other since it has different purpose and requirement and can be used in various timing along the process design stages.

Considering several key facts about Inherent Risk Assessment above; it is interesting to understand further:

1) How is risk conceptualize and described in Inherent Risk Assessment and NORSOK Standard Z-013 Risk and Emergency Preparedness Assessment [2] as the guideline of QRA practice in Norway compared to uncertainty-based risk concept?
2) What are the key differences of Inherent Risk Assessment compared to Quantitative Risk Assessment practice in Norway based on NORSOK Z-013 [2]?

1.2 Objective

The purpose of this thesis is to understand further and contribute to risk assessment studies trough:

- Analysis of how risk is conceptualized and described in the Inherent Risk Assessment and NORSOK Z-013 [2] as the guideline of QRA practice in Norway compared to uncertainty-based risk concept.
- Comparison of IRA to the practice of Quantitative Risk Assessment in Norway based on NORSOK Z-013 [2].

1.3 Scope and Limitation

The scope of this thesis is on risk conceptualization and description in Inherent Risk Management presented in Shariff and Leong [1] and NORSOK Z-013 [2] as the guideline for Quantitative Risk Assessment in Norway compared to uncertainty-based risk concept. The key difference between these two risk assessment methods also covered in this thesis. The discussion is limited to the QRA practice in Norway based on NORSOK Z-013 [2] and IRA concept presented by Shariff and Leong [1] and study case featured in Shariff and Zaini [7]. The practice of Quantitative Risk Assessment in other countries and technical issues of IRA are not covered in this thesis.

1.4 Report Structure

The structure of this thesis is as follows:

- Chapter 2: presents literature study related to the development of risk concept and description throughout the time as well as ALARP principle which to some extent is in line with the inherently safer design principles
- Chapter 3: presents the risk assessment methods subjected to the discussion of this thesis which is Quantitative Risk Assessment in Norwegian petroleum industry and Inherent Risk Assessment as introduced by Shariff and Leong [1] and Shariff and Zaini [7].
- Chapter 4: analyses how risk is conceptualized and described in IRA based on the risk definition presented in Shariff and Leong [1] as well as the risk description in QRA

based on the risk definition by NORSOK Z-013 [2] as the guideline of performing QRA.

- Chapter 5: analyses the key differences identified between QRA in Norway and IRA. The comparisons are made based on NORSOK Z-013 [2], as the guideline of performing QRA, and articles by Shariff and Leong [1] and Shariff and Zaini [7] as the developer of IRA concept and study cases.
- Chapter 6: discusses the implications of the results presented in Chapter 4 and 5 as well as analyses the advantage and disadvantage of IRA concept compared to QRA
- Chapter 7: presents the recommendation of which risk assessment method shall be implemented based on the discussion in Chapter 6
- Chapter 8: concludes the thesis

2 Theory

This chapter presents basic risk theory related to risk concept and risk description together with possible interpretations of probability and the explanation why probability *P* cannot replace uncertainty *U* in the (*A*, *C*, *U*) risk concept. A brief introduction to ALARP principle also covered in this chapter, because this principle appears to be in line with the inherently safer design principles in prioritizing risk-reduction measures at the source.

2.1 Risk Concept and Risk Description

"Risk" as a term is being used broadly in various fields, including professional or scientific. As such, there is limited consent of standard definition of risk to date. For instance, the definition of risk in accounting would not be equal with the definition of risk in engineering. This is expected because typically each field defines risk based on the type of condition they are facing. However, the lack of consent in the definition of risk pose a challenge for risk study to be able to establish a strong foundation in discussing risk.

First, to better understand what a risk is, it is important to have a clear distinction between these three categories, which are: [8]

a) Risk as a concept based on events, consequences, and uncertainty

This category covers the uncertainty of the occurrence of a future event and its consequences.

b) Risk as a modeled and quantitative concept

This category covers the frequentist-interpreted probability of an event.

c) Risk descriptions

This category covers the probability, both the estimation of frequentist probability or a subjective probability.

According to Aven [8], it is aimed to have a risk as a concept (a) as the overall concept is because the risk exists even when a model and subjective probability are not assigned. For instance, one is facing a risk of a car crash when one is driving or a risk of cancer even when there is no probability assigned. The probability only needed when a risk assessment performed, and not required when risk is seen as a general concept.

Aven [9] presents a classification system for risk descriptions to cover those big number of risk definitions as follows:

1) Risk=Expected value (loss) (*R=E*)
2) Risk=Probability of an (undesirable) event (*R=P*)
3) Risk=Objective Uncertainty (*R=OU*)
4) Risk=Uncertainty (*R=U*)
5) Risk=Potential/possibility of a loss (*R=PO*)
6) Risk=Probability and scenarios/Consequences/severity of consequences (*R=P&C*)
7) Risk=Event or consequences (*R=C*)
8) Risk=Consequences/damage/severity of these+Uncetainty (*R=C&U*)
9) Risk is the effect of uncertainty on objective (*R=ISO*)

From these nine risk categories, Aven [9] identified six development paths of risk concept evolution throughout history. The development paths are started from a risk concept by De Moivre [10] in 1711 where risk considered as an expected value, from which the risk concept evolves to six different ways. The six development paths are illustrated in **Figure 2.1** which includes:

1) Development path 1 (D1): Risk equals to expected value (of loss) (*R=E*).
2) Development path 2 (D2): Risk become the probability of a loss (*R=P*), then also cover the consequences (*R=C&P*) as the probability alone failed to serve as a general definition of risk.
3) Development path 3 (D3): This path quite similar to the D2, with an extension of *C&P* perspective to *C&U* perspective, with *U* represent the uncertainty. The *C&U* perspective allows a clear distinction between the risk as a concept and how to measure it.
4) Development path 4 (D4): Risk equals to uncertainty perspective (*R=U*).
5) Development path 5 (D5): Risk is based on the idea that there is a risk in the case that an objective probability distribution can be obtained (and uncertainty otherwise) (*R=OU*).
6) Development path 6 (D6): Based on a pragmatic view where risk is defined using different perspectives of risk depends on which perspective is the most suitable one. It includes *P* and *U*, Po, *C&P* and *C&U*, and ISO definitions.

Form these six development paths of risk, the most relevant path for the discussion in this thesis is development path *D3*. The reasoning behind this statement is presented in **Section 2.1.2** which explains why *C&P* risk perspective needs to be replaced with *C&U* perspective.

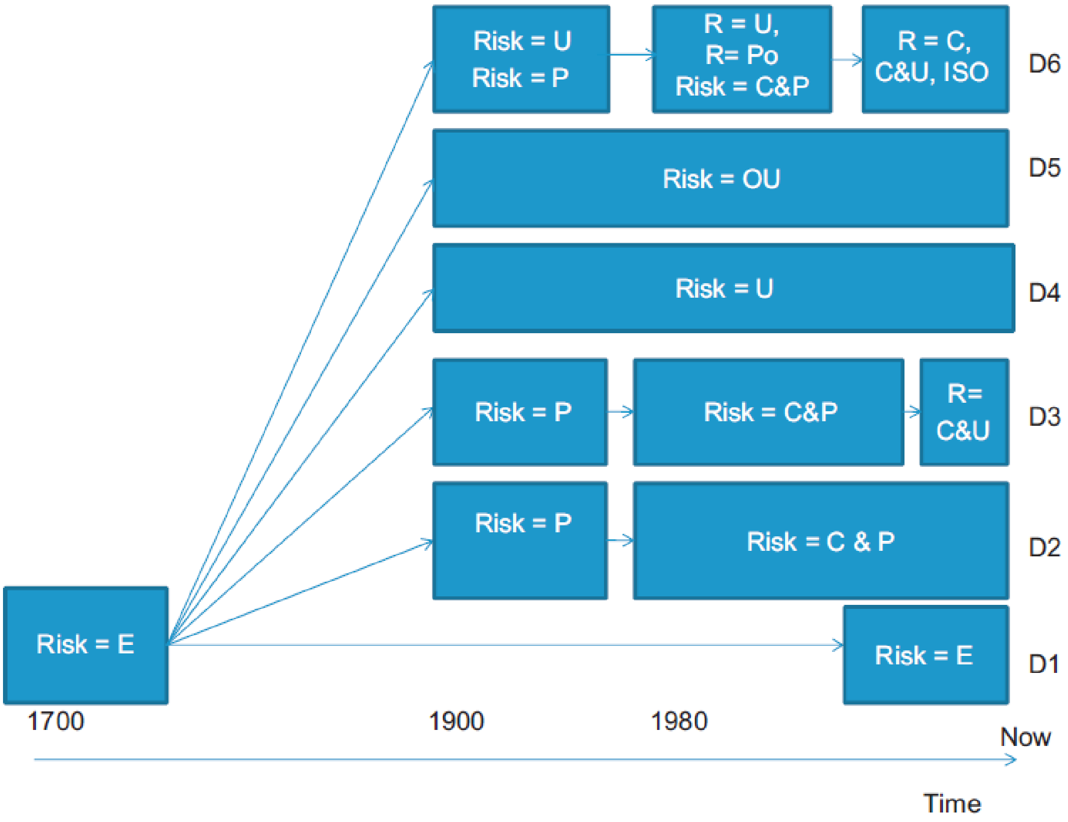


Figure 2.1 *Six development path of risk concept (Aven [9]: p. 40)*

2.1.1 Probability and Expected Value Interpretation

Aven [9] further discuss that to define risk based on probability and expected value, more explanation is needed as these terms can be interpreted in different ways. First, there are two ways to interpret a probability of event *A* which are: [9]

i) Using frequentist probability ($P_f(A)$) to express the fraction of times occurrence of event A when considering an infinite population of similar situations or scenarios to be analyzed. It is a model concept where the true value of $P_f(A)$ is unknown and need to be estimated as $P_f(A)$ *

ii) Using subjective (knowledge-based) probability (*P*) to express the assessor's degree of belief of the occurrence of the event A. Thus, it can also be denoted as $P(A|K)$ which means that this probability is conditional on some background knowledge, *K*. For instance, the probability of event *A* equals to 0.1; it means that the assessor compares his/her degree of belief for the occurrence of event *A* with the standard of drawing one specific ball from an urn contains ten balls randomly.

Second on expected value, if the frequentist probabilities are used then the expected values can be interpreted as the arithmetic mean of the quantities generated by considering an infinite population of similar situations or scenarios to the one analyzed. In this case, then definitions categories (1), (2), and (6) are based on a model concept. On the other hand, if subjective probabilities are used, then the expected value would represent the center of gravity of the distribution. [9]

2.1.2 Risk (*A*,*C*,*P*) and (*A*,*C*,*U*) Concepts

In the engineering field, typically risk is considered as a combination of probabilities and losses which follow the risk *C&P* perspective and (*A*, *C*, *P*) concept. The most notable definition of risk in the nuclear industry is defined by Kaplan and Garrick [11] where risk is described as equals to the triplet (s_i, p_i, c_i) with s_i is the *i*th scenario, p_i is the probability of the respective scenario, and c_i is the consequences of that scenario, i=1,2,…*N*. In this definition, the loss is represented by the scenario and the consequences.

Many analyst and researcher criticizes that the *C&P* perspective, which is a probability-based approach, is too narrow for assessing risk and uncertainty [9] because the risk exists even there is no probability associated with the risk.

Aven [12] explained why the definition of risk could not be the same and follow the (*A*, *C*, *P*) by clarifies what the *P* means since there are two interpretations of probability as mentioned in **Section 2.1.1**. The natural interpretation of *P*, in this case, is that the probability refers to the frequentist probability. This interpretation of probability is problematic since the frequentist probability is based on a hypothetical probability distribution which cannot always be justified and not exists in the real-life. Many situations, such as accidental event, cannot be repeated in the long run.

Aven [12] presented an example taken from Aven and Renn [13] which shows that in term of risk of terrorist attack when the frequentist probability interpretation is used then the probability model have no meaning. This happens as it it not possible to define an infinite population of similar situations. Therefore, according to the (*A, C, P*) concept, risk would not exist.

Based on this argument, there are several experts including Aven [8] argued the probability-based risk perspective need to be replaced with a new broader risk perspective which is not linked to the probability as one of the uncertainty measures. The new perspective then later known as *C&U* perspective with *U* represents the uncertainty. The more detailed discussion related to this argument can be found in Aven and Zio [14].

2.1.3 Risk (*A, C, U*) Concept and Description

As discussed in Aven [15], there are some cases where risk definitions are not suitable to define risk in certain conditions. Further, Aven [12] suggested the (*A*, *C*, *U*) concept as the more appropriate risk concept since a unified framework for presenting risk using both probabilistic and non-probabilistic approaches can be achieved.

The (*A*, *C*, *U*) concept states risk is equals to a two-dimensional combination of events/consequences (*C*) (of an event (*A*)) and associated uncertainties (*U*). An initiating event *A* can initiate a consequence *C*, but there is an uncertainty *U* whether the consequence *C* will happen or not. For instance, when a random person travels by car, he/she may or may not killed in a traffic accident. Another example, when a person buys some product at an online website he/she might receive the product safely, or the product lost/damaged during shipment or he/she got fraud and never receive the product he/she bought. These examples show that for each initiating event there are several consequences and since its occurrence happens in the future, there is uncertainty in whether these consequences will happen or not.

Therefore, the (*A*, *C*, U) risk concept will be used as the foundation to describe risk where *U* represent the uncertainty of event *A* and consequence *C*. Risk description is then obtained by specifying initiating event *A'* and its consequences *C'* and using a measure of uncertainty *Q*. The most common tool to measure uncertainty is probability *P*. The background knowledge *K* as the based for *Q* and specifying *C'*, also need to be included in the description. Then a general risk description can be written (*A', C', Q, K*). [16]

2.1.3.1 Describing Initiating Events

In risk assessment, the assessor specifies initiating event *A'* which is a list of incidents that might occur when an activity took place. This list of incidents may be associated both with opportunity or hazard/threat, but in this case the focus is on the hazard/threat. For instance, when someone is going to travel abroad, one can make a list of specific initiating event *A'* that might occur to him/her. The list may comprise these following events, such as stuck in traffic jam on the way to the airport, caught an endemic virus, lost our passport and others consequences with hopes that if there is an initiating event *A* occurs in real life, it has been identified in the list.

2.1.3.2 Describing Consequences

The initiating event *A* will lead to a consequence *C*. Therefore, in risk assessment, the assessor also has to specify the consequences *C'*. This *C'* represents a set of consequences that might occur if an initiating event *A* took place. Using the example above, when one got stuck in a traffic jam on the way to the airport, there are several specified consequences *C'* that may or may not happen to him/her. One might lose his/her flight, and both the ticket and the hotel booked are not refundable, so one suffers some financial loss. Another example, when one caught an endemic virus he/she might get killed within 24 hours after infected, might be hospitalized for a period of time of time and got recovered, or might have to suffer permanent damage to his/her health condition.

In risk description, a prediction of consequences (*C**) is often used. The prediction is a forecast to quantify the value of this occurrence will take in real life. [16] As an example, one might say that after infected by the virus, one will recover in one week. Alternatively, one can also use a prediction interval [*a*,*b*] to be less specific about the quantity using a probability as degree of belief. Here, one might say that he/she will be recovered in [1,2] weeks with a probability of 90%.

2.1.3.3 Describing Uncertainties

Uncertainty in the risk concept is related to both initiating event and the consequence, as one does not know whether an initiating event will occur or not and what is the consequence. The uncertainties are described by a measure, *Q*. The most common tool to measure the uncertainty is by using probability *P*.

Some people may argue that probability *P* is a good tool for measuring the uncertainty. However, as previously explained in **Section 2.1.2**, the probability *P* cannot replace the uncertainty *U* in the risk concept (*A, C, U*). When the probability replaced the uncertainty, the risk concept becomes too narrow as risk exists even without a probability assigned to the consequence. Moreover, probability *P* may have uncertainty hidden in the in the background knowledge *K* on the phenomena assessed. For instance, Aven [17] illustrated that the probability of an attack at a certain location and time is assigned to be 0.01. The issue identified from this situation is that the assigned value of probability does not provide an informative description of uncertainties related to the attack.

It has repeatedly been mentioned in different studies that probability *P* is not the only form of uncertainty measures *Q* in the risk description. The uncertainty measures also cover the judgments of the strength of knowledge (*SoK*) to capture the uncertainty which is not reflected by the probabilistic analysis. In consequence, the uncertainty description is broadened from *Q=P* to *Q=(P, SoK)*. Further, the uncertainty assessment expands from a quantitative analysis into a semi-quantitative analysis as the judgments of strength of knowledge (*SoK*) on which *P* is based a qualitative analysis [18]

In another study, Flage and Aven [19] suggested a semi-quantitative method to perform uncertainty assessment. The uncertainty factors are analyzed based on effect on risk and vulnerability which depends on the degree of uncertainty. In this assessment, the uncertainty factors are classified as “high” if one or more of the following conditions are met: [19]

- There is a strong simplification in the assumptions used
- Lack of/unreliable data
- Lack of agreement among experts
- The phenomena studied are not well understood

On the contrary, the uncertainty factors are classified as “low” when following conditions are satisfied: [19]

- The assumptions used are reasonable and justified
- Significant amount of reliable data

- Broad of agreement among experts
- The phenomena studied are well understood

For conditions which fall in between the “high” and “low” conditions, such as the phenomena involved are well understood, but to models used are considered simple, are referred as the “medium” condition.

In a more recent study by Askeland et al. [18] the uncertainty assessment is referred as strength of knowledge assessment. Further, the categories of “low”, “medium”, and “high” are presented as “strong”, “moderate”, and “weak”. These changes are adopted because the terms of “strength of knowledge” and the as “strong”, “moderate”, and “weak” categories are considered to be more precise terms to be used in this context.

As a next step, it is necessary to perform the sensitivity assessment to the uncertainty factors which has been classified based on its degree of uncertainty. If an uncertainty factor with a weak strength of knowledge is sensitive to relatively small change in the base case values, then the uncertainty factor has a significant effect on the risk. In contrary, if an uncertainty factor is a strong strength of knowledge but only affected by an unrealistic large change in the base case values, the uncertainty factor has a minor effect on the risk.

2.1.3.3.1 Uncertainty Assessment and Sensitivity Analysis

The main objective of the risk assessment is to support the decision-making process, makes the risk assessment as a time-sensitive activity. It is essential that the risk assessment provides a useful information needed to be used as one of the considerations in time the decision-making takes place.

The data availability in time of the assessment issue is a common issue faced by any risk assessment, because of the assessment is carried out ahead before the actual activities conducted. Moreover, when the risk assessment is done using a quantitative method, it is necessary to transfer all data into quantitative data. Here, the assumptions are used to fill the data that is not available at the time the risk assessment performed.

The use of assumptions is a common thing, especially in engineering calculation, and there is nothing wrong with it as long as the assumptions used are justifiable and reasonable. In a typical engineering design process, it is a responsibility for the engineer to stated and documented all assumptions used in the calculation in the design process. In the risk assessment, it is the responsibility of the risk assessor to assess the strength of the knowledge of these assumptions. Therefore, the uncertainty analysis and sensitivity analysis are two essential assessment as they are aimed to ensure that the assumptions used are reasonable.

2.2 ALARP Principle

The ALARP principle holds that risk shall be reduced to As Low As Reasonably Practicable (ALARP) level. This principle justifies the “reasonably practicable” concept for a risk-reducing measure by weighing the cost, trouble, and time to implement risk-reducing measure against the benefits obtained. If the cost, trouble, and time implementation of risk-reducing measure cannot be demonstrated to be grossly disproportionate to the benefits gained, then the risk reducing measure should be implemented. [20] [21]

In the United Kingdom, ALARP principle is the key to the tolerability of risk framework, which has been widely adopted by the UK Health and Safety Executive (UK HSE) as well as by the companies in managing risks of hazardous facilities. [20]

In implementing ALARP principle, UK HSE uses the concept of “reasonably practicable” to set goals for relevant stakeholders rather than being prescriptive. The same concept also used to justify that it does not need to achieve zero risks, as long as the risk is ALARP. **Figure 2.2** illustrates the three regions of risk according to ALARP principle, which are:

- Unacceptable risks, shown in unacceptable region, in which ALARP cannot be justified and risk reducing measure should be implemented regardless the time, cost, and trouble
- Tolerable risks, shown in ALARP region, in which risk is considered acceptable and at the level of as low as reasonably practicable
- Broadly acceptable risks, shown in broadly acceptable region, in which risk is so low that is negligible

In Norway, the ALARP is also used and included in NORSOK Standard Z-013 Risk and Emergency Preparedness Assessment [2] with a similar approach to the UK HSE approach. The main different is that in NORSOK Z-013 [2] the standard does not distinguish the risk in the ALARP region with the risk in the tolerable region so that the limit being used is the intolerable limit. The ALARP principle according to Norwegian legislation is presented in **Figure 2.3**.

In consequence of not setting the tolerable limit in the implementation of ALARP principle, no risk considered too low so that it is negligible. Therefore, all risk shall be demonstrated to be ALARP regardless of the risk level.

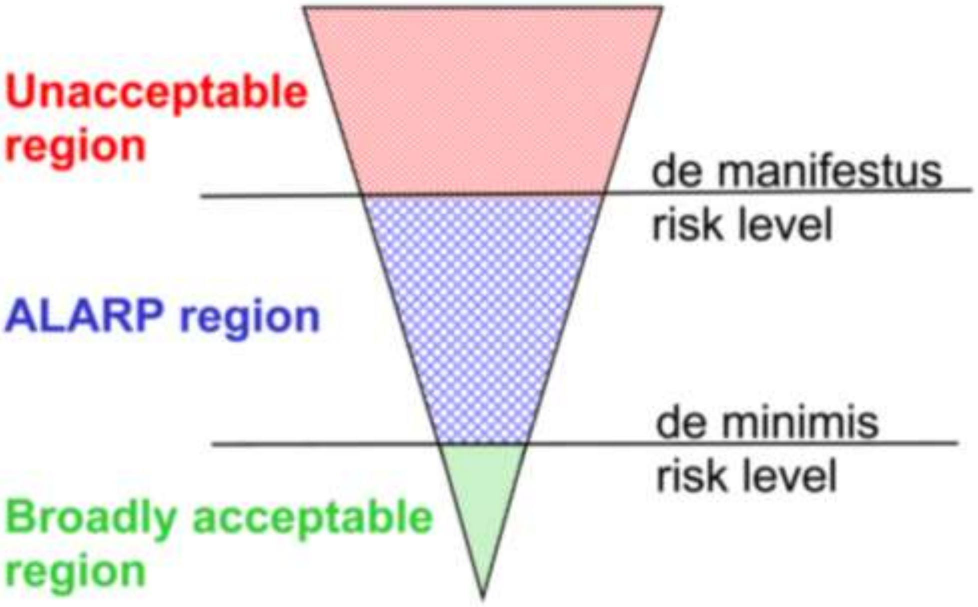


Figure 2.2 *Three risk regions based on UK HSE (Baybutt [20]: p. 37)*

For risk that categorized in the intolerable region, various actions need to be taken to reduce the risk, such as avoidance, adopting an alternative approach, or increasing the number and effectiveness of controls. [2]

Implementation ALARP principle seems closely related to the use of risk acceptance criteria. In risk acceptance criteria, a predetermined value is set to limit the risk tolerability. If the calculated risk is higher than the predetermined value, then the risk is considered to be unacceptable, and action needs to be taken to lower the risk. On the contrary, when the calculated risk is lower than the pre-determined value, then the risk is considered tolerable.

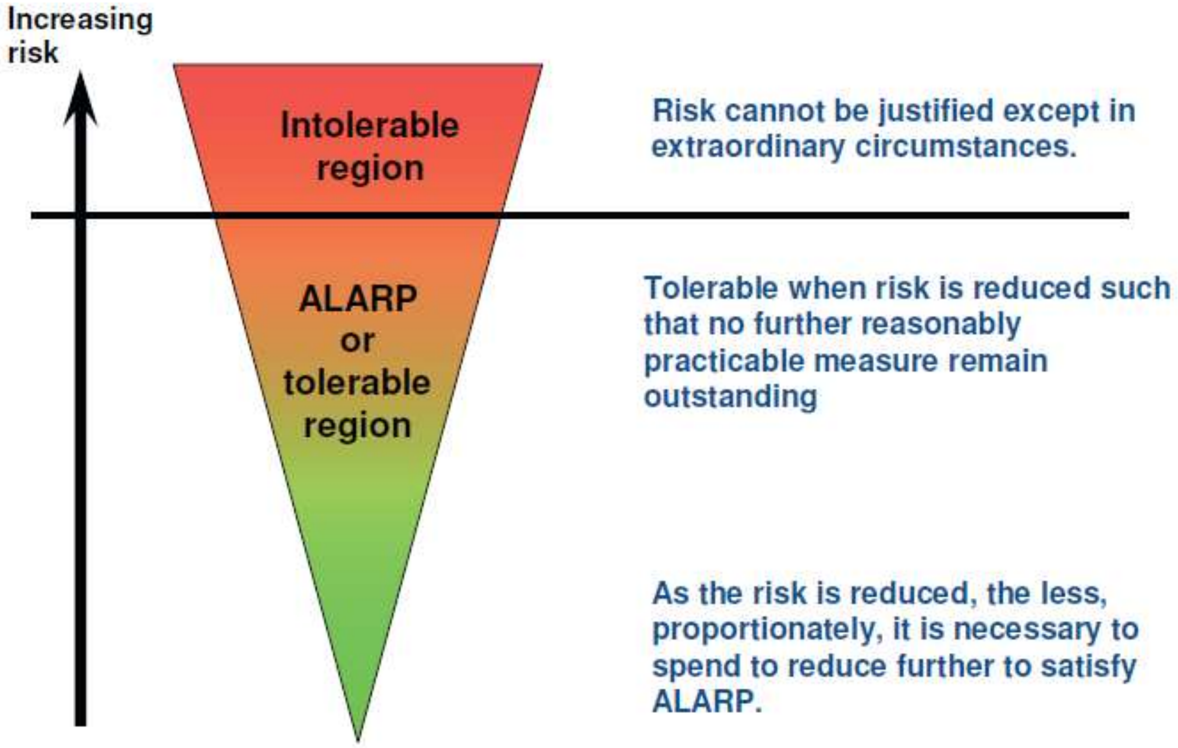

Increasing risk
Intolerable region
ALARP or tolerable region
Risk cannot be justified except in extraordinary circumstances.
Tolerable when risk is reduced such that no further reasonably practicable measure remain outstanding
As the risk is reduced, the less, proportionately, it is necessary to spend to reduce further to satisfy ALARP.

Figure 2.3 *ALARP principle in Norway legislation (Standard Norway [2]: p. 68)*

NORSOK Z-013 [2] require that ALARP process should be performed using a ‘reserved onus of proof’ thinking, which means that documentation is needed to prove that it is justifiable not to implement a proposed risk reduction measure. Further, the standard provides a list of minimum items to be considered in the risk and ALARP evaluation including: (Standard Norway [2]: p. 68-69) “

a) Are authority requirements satisfied?

b) Are all corporate and local requirements, guidelines and philosophies as well as national and international standards and recommended practices satisfied?

c) Is the quantified risk level at least on par with risk levels of similar concepts?

d) If there are solutions that do not meet the conditions of item b) or item c) above, can it be satisfactory demonstrated that no significant increase in risk level would result as a consequence of these deviations?

e) Where quantitative requirements have been defined, is there a sufficient margin, which may allow some increases later in the design process to be absorbed without the massive need for improvement?

f) Is best available technology (BAT) being utilized?

g) Have inherent safe solutions been chosen whenever possible?

h) Are precautionary and cautionary principles considered?

i) Are there unsolved aspects relating to risk to personnel and/or working environment, or possibly areas where there is a conflict between these two aspects?

j) Are there unsolved aspects relating to risk of major oil spill?

k) Is the concept chosen robust with respect to safety?

l) Are the latest research and development results and mew technology aspects reflected in solutions that are adopted?

m) Are societal concerns met, if required to consider?

n) Are the associated costs significantly disproportionate to the risk reduction achieved?"

NORSOK Z-013 [2] also add few notes to these points for consideration, that item a) is a precondition of ALARP evaluation that needs to be satisfied since the beginning of the project. Further, the item d) can only be applied to item b) and c), but not to any matters related to item a). For instance, the normally unmanned installation which has some deviations to the item b) and c).

3 Risk Assessment

Risk assessment is one of the key elements in risk management. It comprises risk analysis and risk evaluation with the principal objective is to generate a risk picture which is later used as a supporting document in the decision-making process. There are different techniques of risk assessment available in the current risk management practice includes qualitative analysis such as Hazard and Operability Study (HAZOP) and quantitative analysis such as Quantitative Risk Assessment and Bayesian Network.

In the following, Quantitative Risk Assessment (QRA) and Inherent Risk Assessment (IRA) will be presented further. The presentation of Quantitative Risk Assessment is focused on the practice in Norway Offshore Oil and Gas Industry based on NORSOK Standard Z-013 Risk and Emergency Preparedness Assessment [2]. Meanwhile, the presentation of Inherent Risk Assessment is focused on Inherent Risk Assessment as presented by Shariff and Leong [1] and Shariff and Zaini [7]. There is a difference in the quality of information as the QRA in Norway has been established for decades so that there is a comprehensive guideline available. On the other hand, IRA is a new concept proposed which is developed based on specifics study cases.

3.1 Quantitative Risk Assessment (QRA)

QRA can refer to Quantitative Risk Assessment or Quantitative Risk Analysis depends on which of these terms applicable. When there are risk analysis and risk evaluation involved, then the Quantitative Risk Assessment term is used. Meanwhile, when it only comprises risk analysis then the Quantitative Risk Analysis term is used. However, in practice "analysis" and "assessment" are used interchangeably. In this thesis, the distinction of both terms will be applied to obtain some consistency.

QRA can also be referred using these terms which are: (Vinnem [22]: p. 3) "

- *Quantitative Risk Assessment (QRA)*
- *Probabilistic Risk Assessment (PRA)*
- *Probabilistic Safety Assessment (PSA)*
- *Concept Safety Evaluation (CSE)*
- *Total Risk Analysis (TRA*)"

This report will be focusing on the term of Quantitative Risk Assessment or Quantitative Risk Analysis (QRA) in Norway which is more relevant to Total Risk Analysis (TRA). From this way further, when the term QRA is used, then it is meant QRA in Norway as explained before.

3.1.1 QRA practice in Norway

Vinnem [22] explained the development of QRA studies in Norwegian petroleum industry was started in second half of the 1970s. The studies began as a few pioneer projects in research to investigate whether analysis methodologies and data of sufficient sophistication and robustness were available. In the research, the methods and data used were adapted from WASH 1400 which had been utilized by the nuclear power generation industry in the United States.

In 1981, Norwegian Petroleum Directorate (NPD) issued a guideline for safety evaluation of platform conceptual design which marked the next step of the QRA development. The guidelines are applied for all new offshore installations and require them to perform QRA in the conceptual design phase. [22]

At the early years, Norway was the only country that utilizing QRA in offshore oil and gas industry systematically. The critics to the QRA method was declared persistently by the UK offshore industry and authorities saying that such method is inappropriate for improving safety. [22]

However, then, when the Piper Alpha accident happened in 1988, Lord Cullen [23] as the lead investigator of the accident recommended to introduced QRA into UK legislation in a similar way as in Norway. It was a significant acknowledgment for QRA, but it does not remove the skepticism of the QRA method entirely. [22]

The regulations related to the QRA are changes several times since 1981 with the most updated version of the regulations are amended in January 2016. The current Norwegian safety regulations cover not only offshore petroleum activities but also onshore petroleum facilities.

3.1.1.1 NORSOK Standard Z-013 Risk and Emergency Preparedness Assessment

Developed by the Norwegian petroleum industry, NORSOK Z-013 [2] is established to provide requirements for effective planning and execution of risk and/or emergency preparedness assessment.

NORSOK Z-013 [2] standard covers:

- the planning and implementation of risk and emergency preparedness assessment and not the risk treatment.
- the risk of a major accident. Thus, the analysis of occupational fatalities and injuries are not included in this standard.

NORSOK Z-013 [2] is developed based on normative and informative reference from national and international standards which includes, but not limited to, ISO, IEC, other NORSOK standards, and DNV reports. [2]

NORSOK Z-013 [2] standard can be considered as a well-established guideline because it comprises a follow-through requirement, for instance:

- it provides the objective and the scope of the assessment
- the steps in risk approach, and
- the additional requirements for the assessment across the three phases of a project.

However, the requirements in the NORSOK Z-013 [2] standard are not prescriptive requirements. Thus, there is no strong enforcement by the authorities.

3.1.1.1.1 Risk Assessment Process

In the general requirement of NORSOK Z-013 [2], it is stated that a risk assessment process shall always cover these following points:

a) Identification hazardous situations and potential accidental events
b) Identification of initiating events and describe the potential causes
c) Analysis of accidental sequences and their possible consequences
d) Identification and assessment of risk-reducing measures
e) Provision of a nuanced and overall picture of the risk, presented using suitable method for the target groups/users

The risk assessment process by NORSOK Z-013 [2], as presented in **Figure 3.1**, comprises these following steps:

1. **Establishing the context**

The first phase of the risk assessment process is the establishing the context. As the main purpose of risk assessment is to support decision-making, it is essential to determine the context before performing the risk analysis to ensure the analysis is suitable for its intended objectives and purpose. It is done by defining the objective, the scope, responsibilities, methods, models, and tools to be used, system boundaries and system basis, risk acceptance criteria, deliveries, and the execution plan for the rest of process. [2]

After the context established, the risk analysis can be carried out using the qualitative or quantitative technique as suited to the purpose and objective of the risk assessment. Here, the discussion is focused on the quantitative risk analysis (QRA).

2. **Hazard Identification (HAZID)**

Hazard Identification (HAZID) is a critical step in QRA, as a hazard that is not identified at this stage will be excluded from further assessment. Thus, it is crucial to perform a comprehensive and thorough identification and recording of hazard. [2]

Before the HAZID is performed, all relevant information and data related to the system observed should be gathered. This information could be obtained from accident database, previous internal/external report, literature, experts, and all available material which can provide useful information. It is also important to check the quality of the information gathered before it is used as the basis for the studies.

After all potential hazards and important factors for accident mitigation are identified and listed, a comprehensive illustration of relevant hazard that may occur in each are of observed can be obtained. There will be a copious number of potential hazards identified which will need a screening to select the most relevant potential hazards to represent the whole system. In the next steps, the list of hazards produced will be used as the basis for more detailed analysis.

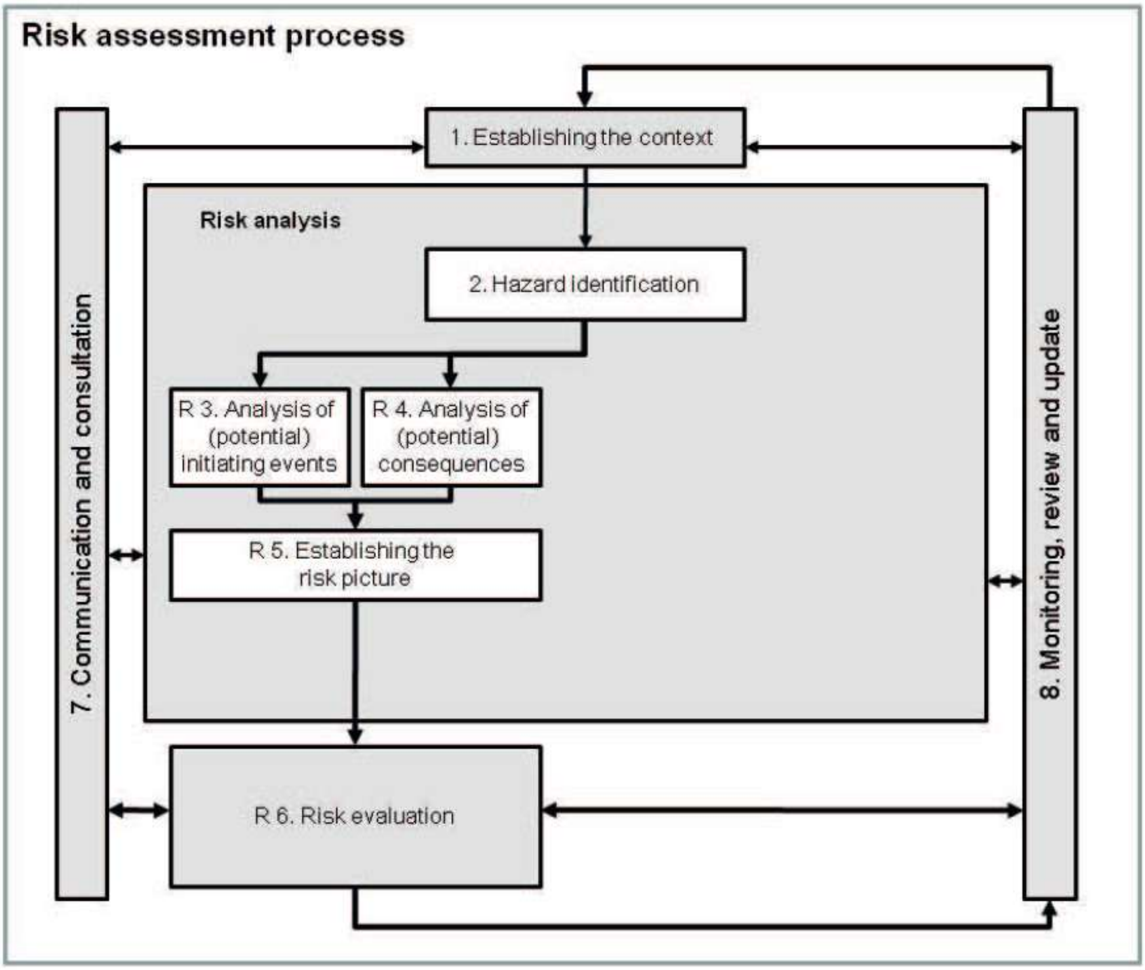

Risk assessment process
1. Establishing the context
Risk analysis
2. Hazard identification
R 3. Analysis of (potential) initiating events
R 4. Analysis of (potential) consequences
R 5. Establishing the risk picture
R 6. Risk evaluation
7. Communication and consultation
8. Monitoring, review and update

Figure 3.1 *Risk Assessment Process based on NORSOK Z-013 (Standard Norway [2]: p. 19)*

3. Analysis of Initiating Event

The objective of this step is to identify the potential causes of initiating events and to assess the probability/frequency of initiating event occurring. [2] For instance, in the scenario of a gas leak from process area, the initiating event will be a gas leak. Therefore, all potential leak sources should be identified, and the data of frequency leak from each leak source should be gathered.

4. Analysis of Potential Consequences

In this step, the possible consequences analyzed covers the entire accidental sequence or sequences that may be the outcome if an initiating event should occur. [2] The analysis can be performed in detailed modeling by using extensive event-trees analysis to coarse judgmental assessment of expert based on experimental studies and available data, depends on the objective and the scope of the risk assessment.

The potential consequences then analyzed in accident sequences, which is made up of series steps which define the various escalation possibilities. Each step is usually related to the possible function, or failure of, the barriers involved. [24] The most common method to perform a modeling of accident sequences is Event Tree Analysis (ETA). Even though this analysis regarded as static analysis, which is a disadvantage, it has been developed into a more dynamic system.

5. Establishing Risk Picture

After the initiating event identified and the potential consequences analyzed in accidental sequences, risk picture can be established. When establishing the risk picture, it is should also reporting the risk assessment process it underwent. For a quantitative risk analysis, there are two requirements need to be fulfilled which are the calculation necessary to establish the risk picture and the presentation of the risk picture.

The sensitivity analysis also should be carried out to the risk picture to identify the most important aspects and assumptions in the analysis. Further, the effect of changes in the assumptions/aspects and potential risk reducing measures are evaluated.

6. Risk Evaluation

Based on the scope, requirement for risk evaluation in NORSOK Z-013 [2] only cover the part of decision basis that may be used for such assessments and decisions which the risk assessment process can and should provide. One of them is if the consequences are expressed using quantitative analysis, the risk shall also be expressed as the cumulative frequency for all consequences. [2]

7. Communication and consultation

Communication and consultation in the risk assessment process are carried out to involve the relevant stakeholders, both internal and external, so that the quality of risk assessment process can be improved and suitable to meet the intended purpose(s). As this part is crucial to the overall process, the communication and consultation are performed in every step of risk assessment process in different time and different level of involvement for the relevant stakeholders.

8. **Monitoring, review and updating risk assessment**

Since the risk assessment can be performed in several phases, such as concept selection phase and the engineering phase, changes may occur to the project subjected to the risk assessment. Increased level of details also will occur as the project developed which means that there is a need to monitor, review, and updating the risk assessment throughout the project life.

3.1.1.1.2 Quantitative Risk Analysis in Different Phases of Project

As an addition to the general requirement of risk assessment process presented above, NORSOK Z-013 [2] also provide requirements for quantitative risk analysis (QRA) in different phases of the project. There are three different phases discussed in this NORSOK standard includes QRA in concept selection phase, QRA in concept definition, optimization, and detailed engineering phases, and QRA in the operational phase. [2]

1. **Requirements to QRA in concept selection phase**

The objective of the assessment in this phase is to compare the different concepts and identify any potential showstopper for each concept. [2] Since this assessment is carried out in the early phase of the project, then the level of information details is assumed to be limited. The assessment can be carried out in qualitative, quantitative, or combination of both techniques, which depends on the complexity, applicable hazards, exposed system, and information available.

The additional requirements in this phase are presented using the same structure to the general ones. One of the significant additional requirements is related to the risk picture. Risk picture presented in this phase shall be clear to avoid any difficulties or violation to the company and/or the authority regulations that might stop the whole project. Thus, it is crucial to identify the showstopper as early as possible. Another requirement for the risk picture is it shall be comparable to each concept thus it is possible to rank between the concept in a risk perspective. Further, the opportunity for inherently safety design, robustness, and risk reducing measures implementation shall be identified when establishing the risk picture. Using the risk picture, the items to be focused on in the next phase should be identified.

2. **Requirements to QRA in concept definition, optimization, and detailed engineering phases**

The requirements presented in this part are applied to the assessment performed late in the concept definition and optimization phase. The level of details vary, and the objective will typically differ during these phases. The design is assumed to be mature enough, but it can still be modified. The layout drawings and P&IDs for process and essential safety systems are assumed to be available at the time of the assessment carried out. The analysis does not cover the construction work and installation activities.

The requirements in this phase are more detailed and specifics, such as on the compliance with acceptance criteria, ALARP evaluation, establishment of DSHAs, designs, and layouts, barriers, and operations. The risk analysis performed is more comprehensive compared to the previous phase with detailed modeling and assessment of causes and probabilities of initiating events.

Here, the risk-reducing measures identification and assessment shall be performed in the risk evaluation step. From which, the result is used as an input to ALARP evaluations.

3. **Requirements to QRA in operational phase**

The requirements to QRA in operational phase are applied to the assessment of a facility that has been in operation for a period of time. It is assumed that some operational experience with the facility has gained. Thus, an assessment should be performed during the detailed engineering phase, as the focus of the assessment in operational phase be to update the assessment in detailed engineering phase after operational experiences gained. The result of the assessment shall be used as a support for decision-making in the operational phases, such as planning and performing operational and maintenance work and small modifications. The assessment also shall be able to be documented the deviations of assumptions and presuppositions that have not been subjected to sensitivity analysis are to be treated.

3.2 Inherent Risk Assessment (IRA)

Inherent Risk Assessment (IRA) is a new concept to evaluate risk in preliminary design stage introduced by Shariff and Leong [1] in 2009 and extended by Shariff and Zaini [7]. The concept is developed with the objective to detect hazard proactively early in the design stage and to allow for the opportunity to reduce their magnitude or likelihood of occurrence proactively. [1] The main feature of this assessment is the implementation of inherent safety principles formalized by Kletz [3] in late 1970's. Shariff and Leong [1] further explained that the IRA method allows the engineer/process designer to obtain the risk level at the preliminary design stage by utilizing a similar approach to the conventional QRA so that the industry can adopt the concept easily.

The inherent safety is a proactive approach to hazard/risk management during process plant design and operation. The aim of inherent safety is to reduce or eliminate the root causes of the hazards by modifying the design of the plant itself instead of relying on additional engineered safety systems and features, and procedural controls which can and do fail. [1] There are several principles of inherent safety (IS) formalized by Kletz [25] such as intensification, substitution, attenuation, simplification, limitation of effects, and error tolerance.

The important aspect in the assessment is the time of introducing the inherent safety principles. As the time goes on in the design stage, then the opportunity to implement the principles declined. As illustrated in **Figure 3.2** taken from Shariff and Zaini [7], as the knowledge of process grows throughout the project, the opportunities for installing inherently safer features is at its maximum point in the research phase and declining throughout the other phases and at its minimum point in the operation phase. Thus, this concept needs a perfect tool so that the risk level of the design could be obtained as early as possible at the beginning of the project. Based on this idea, Shariff and Leong [1] developed a tool by using a process design simulator, such as HYSYS, with integrated inherent risk assessment model to make data transfer to the risk model easier.

Shariff and Leong [1] then refer to Mohd Shariff et al. (2006) for more technical details related to the integration of consequences and probability models with process design simulator, HYSYS which is not covered in this thesis as the article discuss the technical detail which is irrelevant to this report.

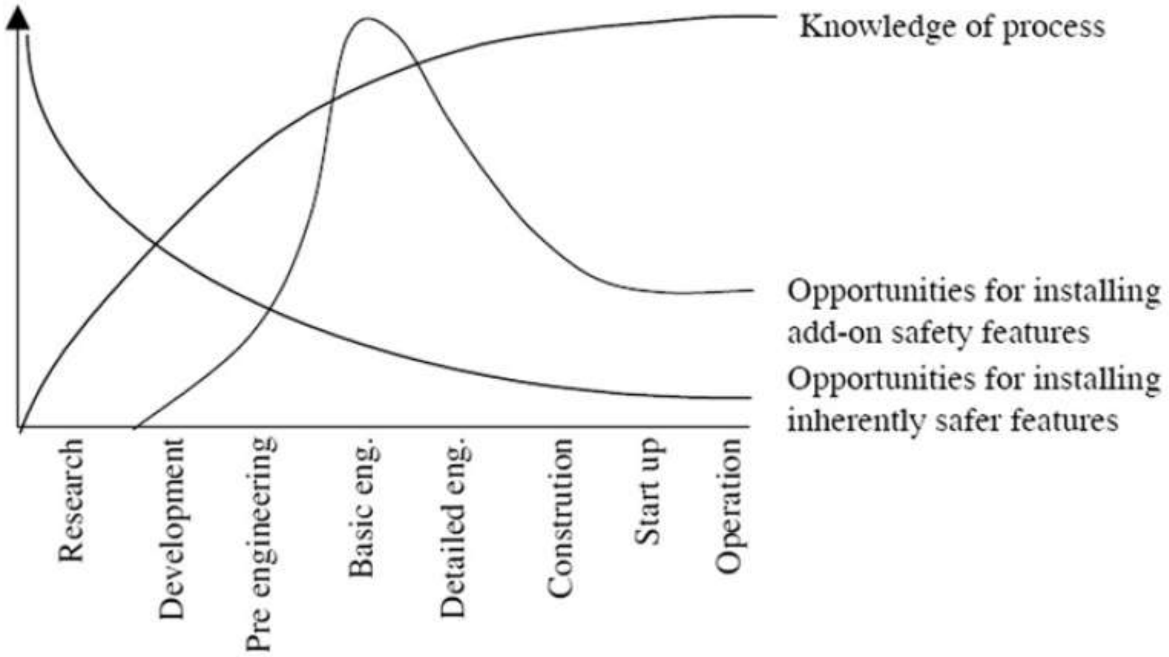


Figure 3.2 The design impossibility and inherently safety design by (Hurme and Rahman [26]: p. 239)

3.2.1 Inherent Safety

The term of inherent safety in the engineering field is frequently used in the loss prevention in process industry among engineered safety and procedural safety. Engineered safety covers the addition of safety measures at the end of the design process, while procedural safety covers procedural or administrative controls to reduce risk. Lastly, the inherent safety covers on the utilization of properties of a material or process to eliminate the hazard. Inherent safety is focusing on eliminating the hazard at source rather than accepting it and try to mitigate the consequences. [27]

Inherent Safer Design or Inherent Safety principles are formalized by Kletz [3] in late 1970's after the explosion in Flixborough [28] in 1974 in which 38 workers killed and 36 suffered injuries. There are fourteen principles of inherently safer design presented in Kletz and Amyotte [25], with four fundamental principles which are commonly used in the practice since they are more general and widely acceptable as follows:

- **Minimization**: this principle is based on the most famous basic idea by Kletz , which is "*what you don't have, can't leak*". It is an obvious common sense but not all plant designer aware and utilized it when designing a process plant. Any inventory required by the design plan is accepted and used with confidence to control all of it. By using the minimization principle, engineers/plant designers are shall be able to reconsider the inventory design and identify the most crucial ones so that only materials or procedures which are not avoidable are used. The minimization principle also referred as the intensification principle.

- **Substitution**: If the minimization is not possible, then a replacement of hazardous material/processing route/procedure to a safer one needs to be considered as an alternative.
- **Moderation**: This is another option to the minimization principle if the hazardous material and/or process cannot be replaced, then the hazardous material should be utilized in their least hazardous forms and/or the process should involve the less severe processing conditions. This principle may result in a contrary effect to the minimization principle as to create a less severe processing condition might need a longer a residence time and larger inventory. [25]
- **Simplification**: This principle is to simplify the design processes, equipment, and procedures so that the error possibilities and equipment which can fail to be eliminated from the system.

It can be seen that the Inherent Safety principles are applied according to preferred order in which minimization is the most preferred one. As concluded in Amyotte et al. [27], inherent safety is not a stand-alone concept; it works through a hierarchical arrangement of risk-reducing measures consideration - from most to least effective - inherent, passive engineered, active engineered, and procedural safety. Further, Amyotte et al. [27] stated that the key to inherently safer design is early and frequent consideration of the four key principles.

3.2.2 Inherent Safety Studies Development

In the development of inherently safer design, there have been many studies which discuss how to implement the principles into the real-life practice. According to Khan and Amyotte [4], the outstanding efforts has started since 1985 after Kletz [3] formalized the inherent safety principles in late 1970’s. Most of the studies mentioned in Khan and Amyotte [4] facing the same challenge in implement inherently safer design principles which are the lack of systematical methodologies and tools to translate the principles from concept to implementation.

IRA concept is developed as one of the attempts to provide methodologies and tools to implement the inherently safer design principles and expanded the scope of the study by integrating it with the risk assessment. This concept was not the first attempt to integrated the risk assessment techniques to the safety engineering, as recorded by Khan and Amyotte [4], in 1994 there is a study which incorporated HAZOP and other techniques in safety assessment.

3.2.3 Risk Definition in IRA

In defining risk, Shariff and Leong [1] is referring to risk definitions by:

- Center for Chemical Process Safety [29] where risk is defined as "*a measure of human injury, environmental damage or economic loss in terms of both the incident likelihood and the magnitude of the loss or injury*"
- Health and Safety Executive UK [30] where risk is referred as "*the chance that someone or something that is valued will be adversely affected in a stipulated way by the hazard*".

Shariff and Leong [1] also refer to a mathematical function of risk by Wentz [31] as follows:

$$Risk = f(probability\ or\ frequency, consequences) \tag{3.1}$$

From the risk definitions and the mathematical function presented above, Shariff and Leong [1] concluded that:

"*risk has components of probability (uncertainty) of the event and consequences (effects) resulting from the event*".

There is no further explanation regarding the inherent risk determination in the article. However, the authors refer to a systemic approach by Crowl and Louvar [32] to estimate risk parameters which are presented in the following.

3.2.4 Hazard Identification and Risk Assessment Procedure in IRA

Crowl and Louvar [32] presented four questions that need to be asked in each chemical plant processes which are: "

1) *What are the hazards?*
2) *What can go wrong and how?*

3) *What are the chances?*

4) *What are the consequences?*”

From these four questions, Crowl and Louvar [32] further explain that the question number 2 – 4 are associated with risk assessment, while the question number 1 is related to the hazard identification. When a hazard identification and risk assessment is combined, then it is categorized as a hazard evaluation.

Figure 3.3 illustrates the hazard identification and risk assessment procedure presented by Crowl and Louvar [32] which comprises:

1. **Hazard Identification**

Hazard identification is started after the system description is finished. This step can be performed independently from the risk assessment, but the best result is achieved by conducting both studies. [32] There are several hazard identification methods described by Crowl and Louvar [32] which includes process hazard checklists, hazards surveys, hazard and operability (HAZOP) studies, and safety review.

2. **Scenarios Identification**

In this step, as described by Crowl and Louvar [32] as the risk assessment, which includes the incident identification and consequence analysis. The incident identification step describes how an accident occurs and frequently includes the studies of accident probability. Meanwhile, the consequences analysis describes the expected damage of loss of life, damage to the environment or capital equipment, and days outage.

3. **Risk Determination**

The result of studies conducted in scenarios identification step is used in a final risk assessment to determine whether the risk acceptable or not. If the risk is acceptable, then the study is finished and can proceed to the construction or operational phase. However, if the risk is considered unacceptable, then a modification to the system must be performed, and the procedure is restarted.

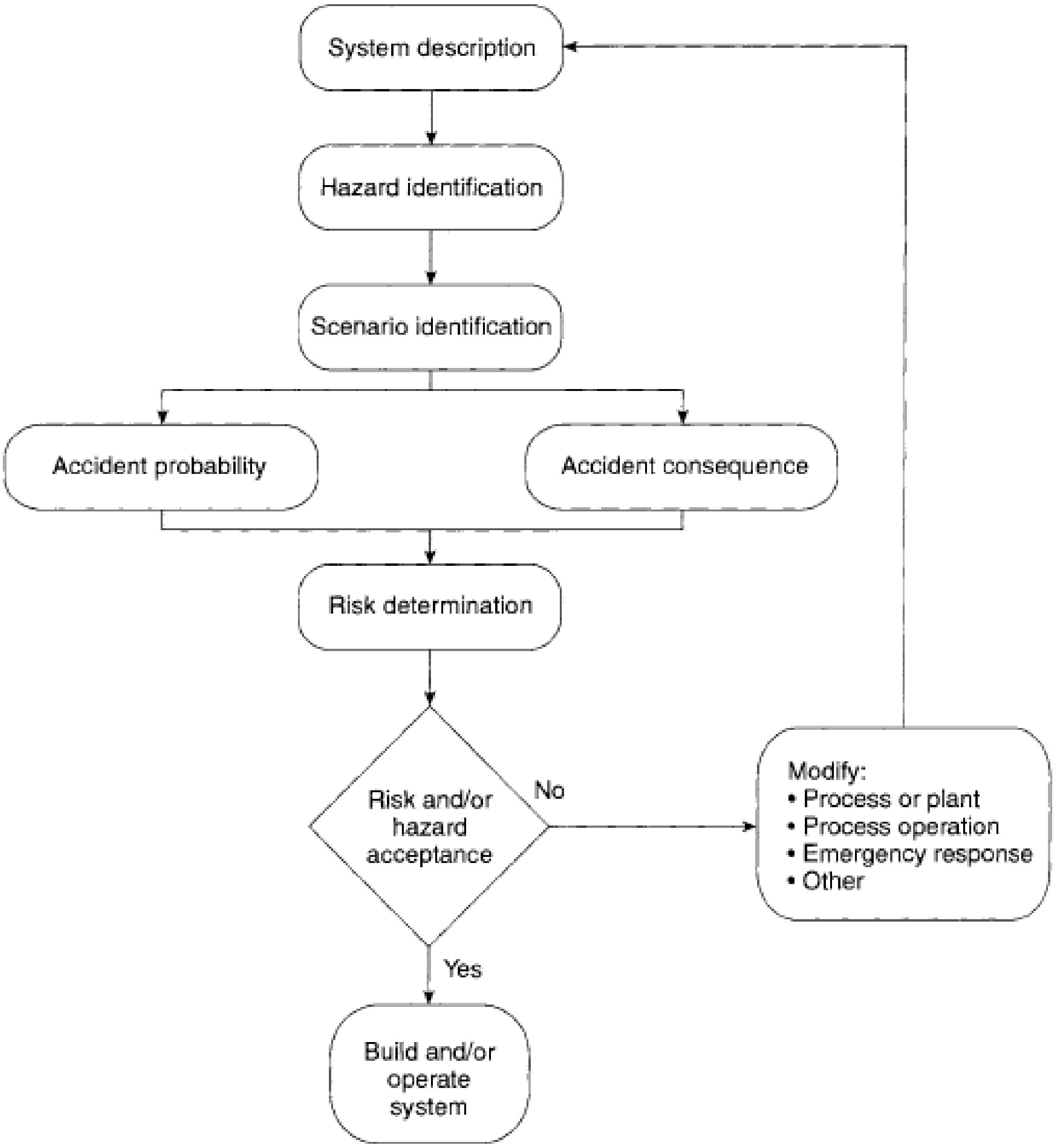


Figure 3.3 *Procedure of hazard identification and risk assessment (Crowl and Louvar [32]: p. 430)*

3.2.5 Study Cases

Currently, there are two study cases in which the application of IRA is developed. Shariff and Leong [1] first introduced IRA concept customized for the explosion of flammable material in 2009, then Shariff and Zaini [7] use IRA on a case study of toxic release.

3.2.5.1 IRA for explosion flammable material study case

Using **Equation 3.1** as the basis to estimate risk, the IRA is performed by assessing two aspects which are the probability of the explosion and the consequences. Information required in part is simulation data and prediction of piping and equipment sizing. The simulation is performed using pipe or equipment leak as the basic scenario.

The estimation of explosion probability is developed using Event Tree Analysis (ETA) as shown in **Figure 3.3**. It is important to be noted that there is a possibility of different mechanisms in any other explosion scenario from the one presented in **Figure 3.3** since this figure only represents a simplified basis to describe the probability of an explosion in the event of loss of containment. By using ETA, consistency in factors being considered in each case can be ensured. The consistency is needed so that each variation in the process options and modifications are comparable on an equal basis, thus leaving only the chemical and process conditions aspects as a variable used in the IRA. [1]

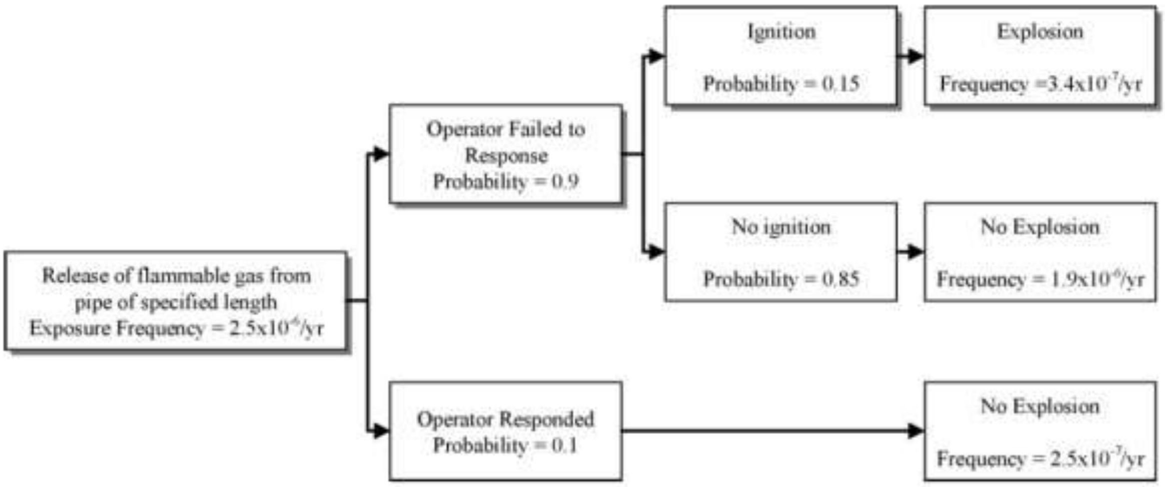

Release of flammable gas from pipe of specified length
Exposure Frequency = 2.5x10^{-6}/yr
Operator Failed to Response
Probability = 0.9
Operator Responded
Probability = 0.1
Ignition
Probability = 0.15
No ignition
Probability = 0.85
Explosion
Frequency =3.4x10^{-7}/yr
No Explosion
Frequency = 1.9x10^{-6}/yr
No Explosion
Frequency = 2.5x10^{-7}/yr

Figure 3.4 Even Tree Analysis for potential explosion of flammable materials release (Shariff and Leong [1]: p. 374)

The frequency and probability numbers in **Figure 3.4** are for illustrative purpose only and not based on real data. In the real world during the simulation stage, the data needed such as actual sizing of pipe diameter and length is not yet available. Thus, a good engineering judgment and estimation is necessary to fill such data gap.

The next assessment is related to the consequences of an incident which is developed in a spreadsheet that is integrated with HYSYS – a process simulation software – as illustrated in **Figure 3.5**.

In the study case, Shariff and Leong [1] uses a series of distillations columns with 27 process streams which are screened based on their rank on the potential of causing damages in cases of the explosion. From these 27 process flows, only top five streams are further analyzed for their inherent risk based on the chemicals used and process conditions of the design as the inherent properties. [1]

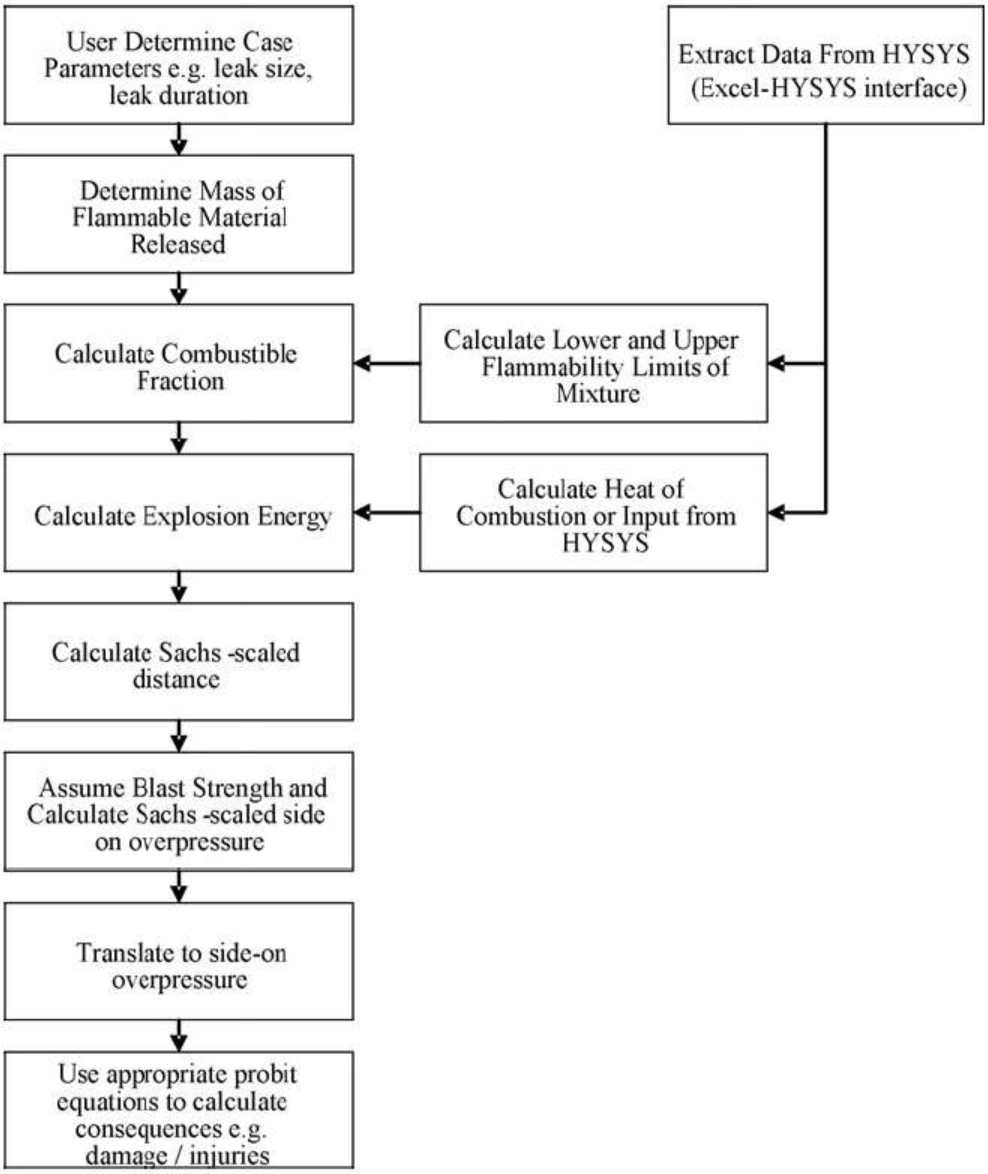

User Determine Case Parameters e.g. leak size, leak duration
Determine Mass of Flammable Material Released
Calculate Combustible Fraction
Calculate Explosion Energy
Calculate Sachs -scaled distance
Assume Blast Strength and Calculate Sachs -scaled side on overpressure
Translate to side-on overpressure
Use appropriate probit equations to calculate consequences e.g. damage / injuries
Extract Data From HYSYS (Excel-HYSYS interface)
Calculate Lower and Upper Flammability Limits of Mixture
Calculate Heat of Combustion or Input from HYSYS

Figure 3.5 *Integrated consequences estimation model (Shariff and Leong [1]: p. 375)*

Here, the risk picture is presented using F-N curve with F represent the overall event frequency, and N represents the number of fatalities based on the assumption 100 workers are exposed to the hazard due to the explosion. The number of workers exposed used in this case study is a random number. However, in the real assessment, an actual headcount should be utilized. The illustration of FN curve for this study case is presented in **Figure 3.6**. As shown in **Figure 3.6**, the FN curve only shows the intolerable region and not the ALARP region. As explained by Shariff and Leong [1], the ALARP region is not represented in the IRA result since the safety measures and control mechanism to reduce risk to As Low As Reasonably Possible is not yet introduced in the preliminary stage.

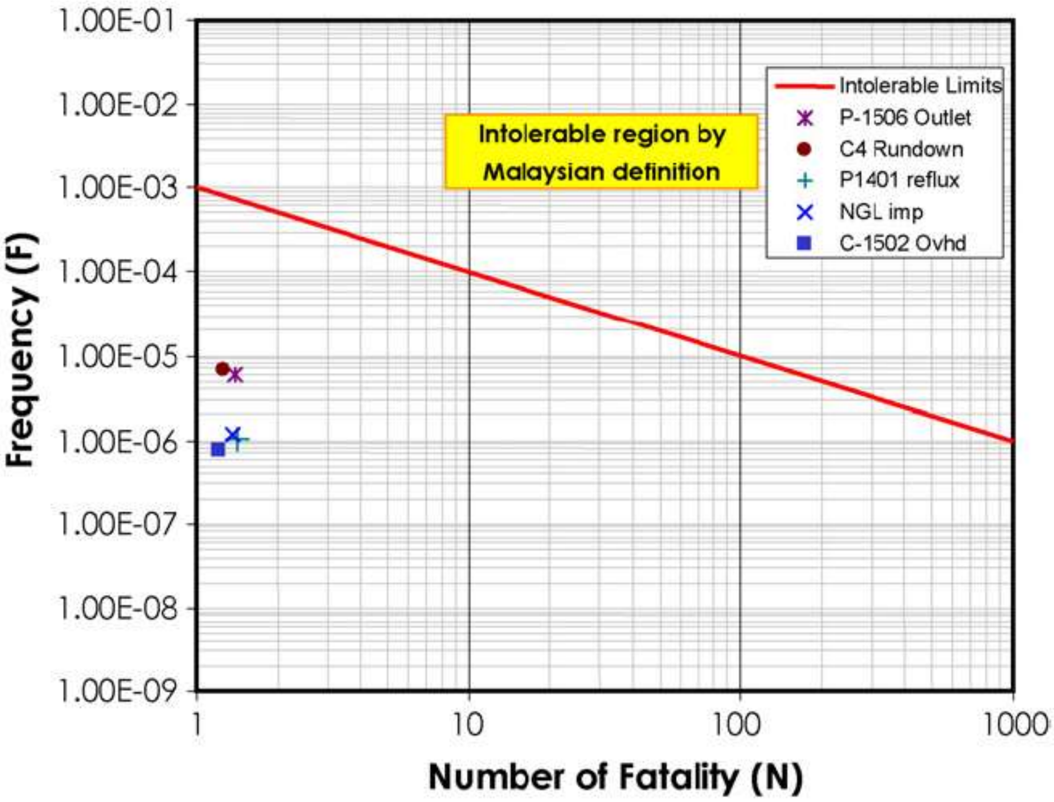


Figure 3.6 FN Curve for explosion study case (Shariff and Leong [1]: p. 375)

3.2.5.2 IRA for toxic release study case

In this study case, Shariff and Zaini [7] presents the IRA and the design improvement for toxic release based on the framework in **Figure 3.7**. This particular technique is named Toxic Release Inherent Risk Assessment (TRIRA). [7] This technique uses the similar approach to the IRA for explosion study case with a slight modification in the risk picture representation.

Shariff and Zaini [7] defined risk as the product of severity and likelihood in which the likelihood is further defined, as refer to DOSH (2008) as an event likely to occur within a given period of time. The severity of the released materials is obtained from the consequences analysis due to the toxic accident using a prototype tool named TORCAT as explained in Shariff and Zaini [33].

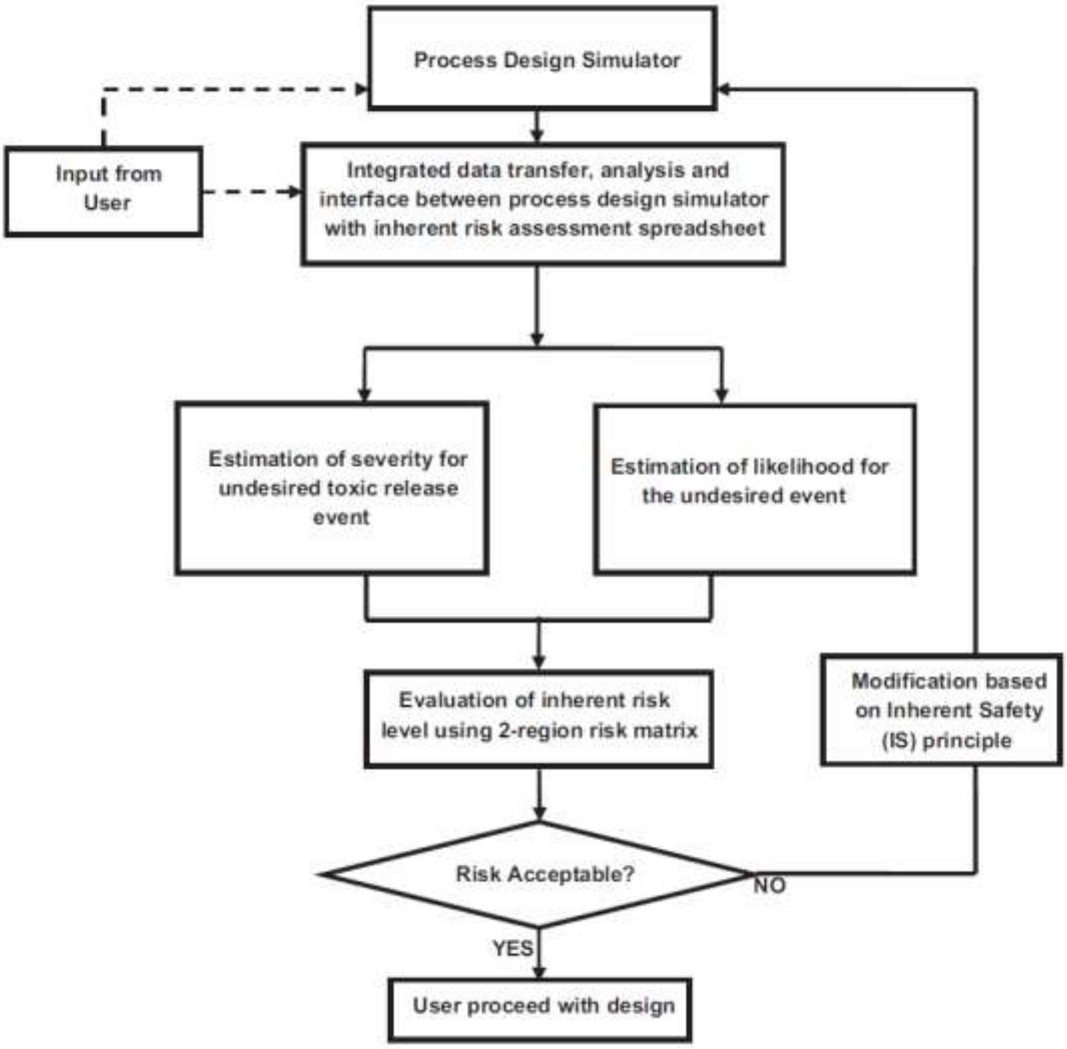

Process Design Simulator
Input from User
Integrated data transfer, analysis and interface between process design simulator with inherent risk assessment spreadsheet
Estimation of severity for undesired toxic release event
Estimation of likelihood for the undesired event
Evaluation of inherent risk level using 2-region risk matrix
Modification based on Inherent Safety (IS) principle
Risk Acceptable?
NO
YES
User proceed with design

***Figure 3.7** Toxic Release Inherent Risk Assessment (TRIRA) Framework (Shariff and Zaini [7]: p. 608)*

Figure 3.8 shows the framework of TORCAT in which it is integrating the consequences analysis of toxic release and the modification of the design based on the inherent safety principle. The tool utilizes a process simulation software named iCON to develop of process flowsheets based on process requirement. [33]

In TRIRA, the risk picture is presented by 2-region risk matrix as shown in **Figure 3.9**. The matrix uses the same principle as the FN curve in the explosion study case in which the safety measures and control mechanism are not yet introduced to reduce risk As Low As Reasonably Possible. Therefore, the risk matrix only features 2-region which represents "UNACCEPTABLE" and "ACCEPTABLE" risk.

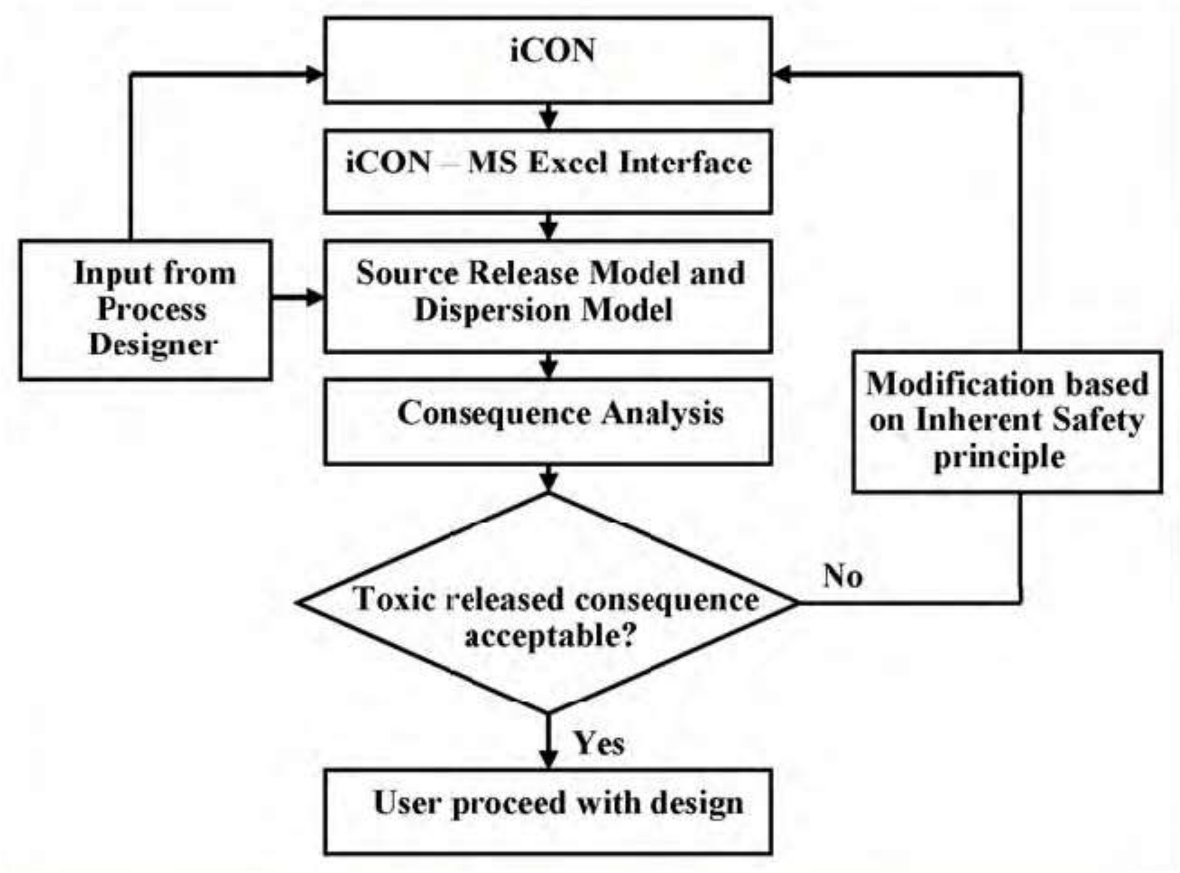
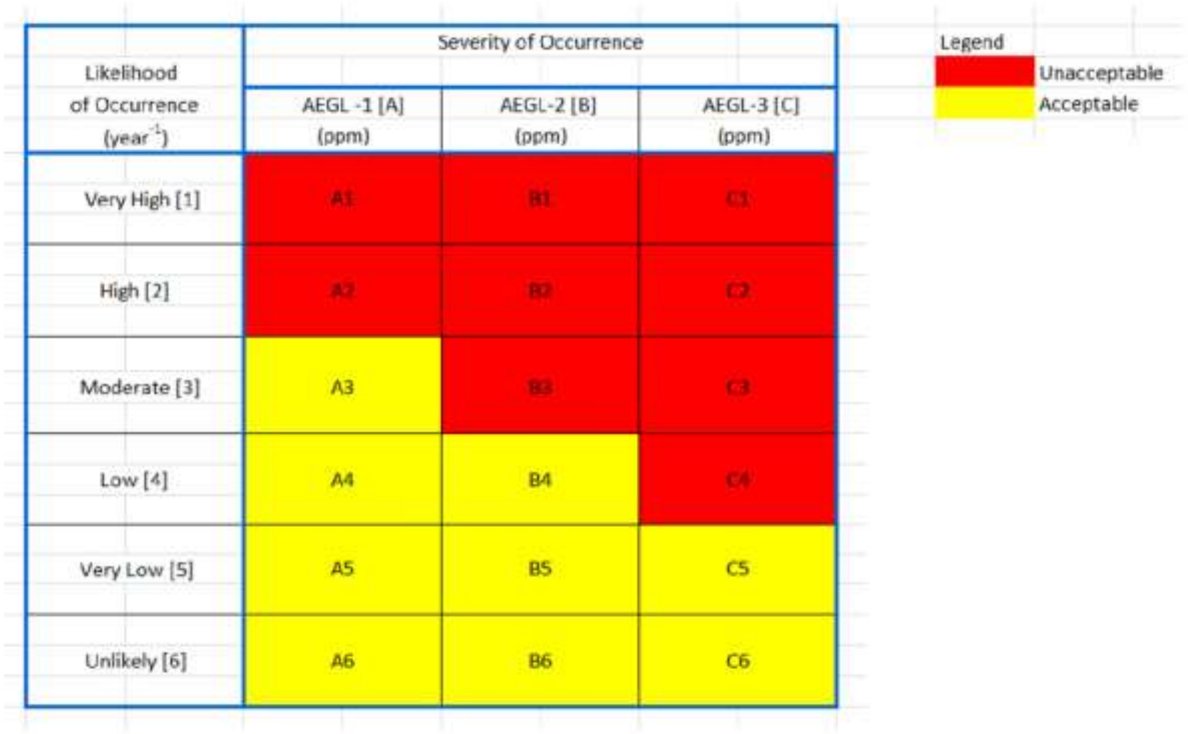

iCON
iCON – MS Excel Interface
Input from Process Designer
Source Release Model and Dispersion Model
Consequence Analysis
Modification based on Inherent Safety principle
Toxic released consequence acceptable?
No
Yes
User proceed with design

Figure 3.8 *Framework of TORCAT (Shariff and Zaini [33]: p.397)*

Similar to the explosion study case, the TRIRA presented in Shariff and Zaini [7] is specified to the particular case and cannot be used as general scenarios. On the other hand, the inherent risk assessment should cover all items in the process flow sheet in order to obtain an overall inherently safer design.

Another major challenge in TRIRA application is the assessment required the size of unit operations in which it is not available in the early stage of the project. This challenge is to be addressed in the future work by adding the conceptual models to estimate the size of unit operations. [7]



Likelihood of Occurrence (year^{-1})	Severity of Occurrence		
	AEGL -1 [A] (ppm)	AEGL-2 [B] (ppm)	AEGL-3 [C] (ppm)
Very High [1]	🟥 A1	🟥 B1	🟥 C1
High [2]	🟥 A2	🟥 B2	🟥 C2
Moderate [3]	🟨 A3	🟥 B3	🟥 C3
Low [4]	🟨 A4	🟨 B4	🟥 C4
Very Low [5]	🟨 A5	🟨 B5	🟨 C5
Unlikely [6]	🟨 A6	🟨 B6	🟨 C6

Legend	
🟥	Unacceptable
🟨	Acceptable

***Figure** 3.9 2-region Risk matrix of TRIRA result (Shariff and Zaini [7]: p. 608)*

4 Risk Concept and Description in QRA and IRA

In this chapter, the comparison on how risk is conceptualized and described in IRA by Shariff and Leong [1] and in NORSOK-Z013 [2] as the guideline of QRA practice in Norway is presented. The article by Shariff and Zaini [7] is not included in this chapter since the article is an extended study of IRA concept by Shariff and Leong [1] and does not discuss any risk description in it.

4.1 Comparison on Risk Concept and Description

4.1.1 In QRA Norwegian petroleum industry

According to NORSOK-Z013 [2], risk is described as the combination of the probability of occurrence of harm and the severity of that harm. In addition to the risk description, there is a note saying that the risk may be expressed qualitatively or quantitatively and the probability may be expressed using a probability value from 0 to 1 with no dimension or as frequency, with the inverse of time as a dimension. The risk definition by NORSOK Z-013 [2] shows that risk is described using the *C&P* perspective as it only includes the probability of occurrence and the severity of the consequences. There is no uncertainty aspect included in the risk definition.

4.1.2 In IRA by Shariff and Leong [1]

As explained in **Chapter 2**, Shariff and Leong [1] described risk by making references to risk definitions by Center for Chemical Process Safety [29] and Health and Safety Executive UK [30], as well as a mathematical function of risk by Wentz [31].

By observing the sentence of risk definition by Shariff and Leong [1] alone, there is ambiguity in the risk definition. The first interpretation is that the risk definition in IRA, to some extent, is in line with the (*A*, *C*, *U*) concept since it includes the uncertainty. However, in the risk definition Shariff and Leong [1] also mentioned probability along with the uncertainty. By observing on how Shariff and Leong [1] wrote the word "uncertainty" in a parenthesis right next to the word "probability" without any conjunction in between, implying that the authors are failed to distinct the probability and the uncertainty. From this kind of writing, several questions can be raised. Do the authors mean that the probability is same as the uncertainty? Or, do the authors say that the probability is part of or represents the uncertainty?

Further, looking closely at the risk definitions and the mathematical function Shariff and Leong [1] referred to, none of these risk definitions or mathematical function that mentioned uncertainty. The words used are just “likelihood”, “chance”, “probability”, and “frequency”. Then it is clear that Shariff and Leong [1] has failed to make a distinction between the uncertainty and the probability.

Veland and Aven [34] categorized this way of thinking as a ‘chaotic’ perspective of risk where the probability and the uncertainty are understood as the same thing. Whereas explained in **Chapter 2**, the probability is just one form of measures of uncertainty and cannot replace the uncertainty.

Based on this observation, then the suitable interpretation of risk definition by Shariff and Leong [1] is that risk is defined based on *C&P* perspective.

5 Comparison of IRA and QRA

This chapter will discuss the comparison between QRA in Norway based on NORSOK Z-013 [2] and IRA by Shariff and Leong [1] and Shariff and Zaini [7] presented in **Chapter 3**. There are seven key differences identified from these risk assessment methods as summarized in **Table 5.1** and described further in the following subsections.

Table 5.1 *Key Difference between IRA and QRA in Norway*

Key Differences	IRA	QRA in Norway
Legislative Requirement and Guideline	Not available	Available
Inherent Safety Design Principles Application	The principles are used as the basic idea of the assessment.	The principles are included in NORSOK Z-013 [2] with no further explanation on how to apply these principles.
ALARP Principle and Evaluation	ALARP principle is not yet introduced because the assessment carried out in preliminary design stage.	ALARP principle and evaluation are covered in NORSOK Z-013 [2]. However, it is out of the standard's scope as it is part of risk treatment.
Attention Given to the Uncertainty Aspect	In IRA study cases, there is not any part of the studies which mentioned an assessment conducted as the consideration of the uncertainty aspect.	NORSOK Z-013 [2] shows that the standard also includes the uncertainty aspect in the consideration.

Key Differences	IRA	QRA in Norway
Timing in Performing the Assessment	Preliminary design stage	• Concept selection phase • Concept definition, optimization, and detailed engineering • Operational phase
Transfer of Knowledge between Design Process and Risk Assessment	High integration of the risk assessment process and the process design simulator allows for the automation in the transfer of knowledge so that the risk assessment can be performed in parallel to the design process.	The assessment typically carried out through consultation and communication between the process design engineer and the risk assessor within the Safety team which means the transfer knowledge is done manually.
The need for Complementary Risk Assessment	IRA designated to be conducted in the preliminary design stage. Therefore, need another Risk Assessment for the other stages of the project.	QRA can be performed in every phase of the project. Thus, does not need a complementary risk assessment.

5.1 Legislative Requirement and Guideline

Norway is one of the countries which have legislation that calls for the use of QRA studies in the design and operation of offshore installations. [22] According to Norway's Management Regulation [35] in Section 17, Norway requires all petroleum activities both offshore and onshore to:

"*carry out risk analyses that provide a balanced and most comprehensive possible picture of the risk associated with the activities. The analyses shall be appropriate as regards providing support for decisions related to the upcoming processes, operations or phases*." (Petroleum Safety Authority [36]: Section 17)

The regulation further refers to NORSOK Z-013 [2] and ISO 31000 [37] as the standards that should be used, among other, in performing risk analyses and emergency preparedness analyses.

Even though the regulation does not specifically mention QRA as the preferred method of conducting the risk analyses, the regulation refers to NORSOK Z-013 [2] which is the guideline for planning and executing to perform risk and emergency preparedness assessment in Norway, which includes the QRA. Therefore, the regulation has indirectly required the Norwegian petroleum industry to perform QRA.

As for IRA, Shariff and Leong [1] and Shariff and Zaini [7] mentioned there is not any regulation or formalized guideline related to this assessment. It may be caused by the fact the assessment is just a new concept introduced in 2009.

5.2 Inherent Safety Design Principles Application

NORSOK Z-013 [2] as the guideline for performing QRA in Norway also includes the inherent safety principles in the standard. Several requirements related to the inherently safe design principles, as follows:

1) In Section 3 Terms, Definitions, and Abbreviations part 3.1.38,
   The standard presented and described briefly four inherently safer design principles which include reduction, substitution, attenuation, and simplification. Even though this is not a requirement, the section provides definitions of these four principles. Thus, the risk assessor can have a clear definition of what to expect when a requirement related to the inherent safety design came up.
2) In Section 5 Risk Assessment Process,
   The requirements related to inherently safer design principles are included in HAZID and risk evaluation steps of risk assessment processes. In both steps, the principles are mentioned as one of the possible risk-reducing measures that shall be identified in the design subjected to the risk assessment.
3) In Section 6 Additional requirements to QRA in concept selection phase
   It is required to identify the possible significant risk-reducing measures which allow inherently safe options to be adopted. Also, the risk picture established shall present the opportunities and the benefits of inherently safe design identified in the design concept.

4) In Annex A – Risk metrics, criteria, and ALARP evaluations

   The inherently safer design principles are mentioned in the ALARP evaluation principles, the scope of ALARP evaluation of concept selection phase, and scope of ALARP evaluation of engineering phase.

5) In Annex C - HAZID

   There is a section comprises seven items related to the application of the inherently safer design principles, which includes:

   - avoiding the usage of hazardous material or method
   - modification or replacement of dangerous substance and processes with less hazardous ones
   - implementation of high safety margins to critical operational parameters
   - using a straightforward and robust design, implementation of process safety
   - segregation of people from hazard processes/materials
   - layout settings

6) In Annex C, there is also an environmental risk section which including inherently safer design principle by Lees [38].

All of the requirements related to inherently safer design principles presented above does not require the risk assessor to implementing these principles directly but rather to identifies the possible opportunity to apply the principles in the assessed design. Moreover, the benefits gained from implementing the inherently safer design principles also needs to be presented.

On the other hand, in IRA the inherently safer design principles are used as the foundation of the assessment. The principles are applied by integrating the risk assessment to a process design simulator called HYSYS so that the risk level can be obtained in time the design process took place.

5.3 ALARP Principle and Evaluation

In **Section 4.1** of NORSOK Z-013 [2], it is stated that a complete risk reduction process which can also be referred as ALARP evaluation is not covered by this standard since it is a part of risk treatment. However, there is a section in Annex A of NORSOK Z-013 [2] which presents the ALARP evaluation as an informative index which covers enough information to perform an ALARP process. The information includes: [2]

- the objective of the ALARP process,
- ALARP demonstration process,
- ALARP evaluation principles, and
- Scope of ALARP evaluation in the concept phase, engineering phases, and operational phases.

In IRA, both Shariff and Leong [1] and Shariff and Zaini [7] remove the ALARP region in the risk picture with the argument that the safety measures and control mechanism are not yet introduced in the preliminary design stage.

5.4 Attention Given to the Uncertainty Aspect

IRA study cases presented by Shariff and Leong [1] and Shariff and Zaini [7] mainly focuses on obtaining risk level at the preliminary design stage and there is not any part of the studies which mentioned an assessment conducted as the consideration of the uncertainty aspect.

Although the assumptions used in the study cases are based on previous studies and using a well-proven method such as Event Tree Analysis, the calculation process is rather straightforward. Right after the risk level is obtained in the calculation, the risk level is directly compared to the limits set by the Malaysian government. Both Shariff and Leong [1] and Shariff and Zaini [7] did not mention any sensitivity analysis or uncertainty analysis conducted to the calculated risk. This is an unfortunate as the readers may assume that the authors have completely ignored the uncertainty aspect from the calculation.

On the other hand, NORSOK Z-013 [2] shows that the standard also includes the uncertainty aspect although it is based on *C&P* perspective. It can be seen in the requirement for establishing the context, where it is required to document which methods, models, and tools to be used in the process. The methods, models, and tools utilized in the risk assessment shall be recognized and validated method. Assumptions used, such as expert judgments, as well as the composition of the expert group shall be stated and documented.

Another requirement in NORSOK Z-013 [2] which covers the uncertainty issue is found in the establishing risk picture. The risk picture is required to include a discussion of uncertainty which comprises following items: [2]

- the risk perspective used in the assessment

- the effect and level of uncertainty given the system boundaries and system basis defined in the context of the assessment compared to the real systems
- possible meaning of the main results
- the unexpected outcomes that may occur as the result of invalid assumptions or lack of knowledge

5.5 Timing in Performing the Assessment

Shariff and Leong [1] emphasize that IRA has an advantage as the assessment is conducted at the preliminary design stage. Thus, IRA has a larger opportunity to give an influence on the process design engineer to modify the design.

On the contrary, QRA studies can be carried out in every phase of a project. According to NORSOK Z-013 [2], there are three different phases that QRA can be performed which are:

- concept selection phase,
- concept definition, optimization and detailed engineering, and
- operational phase

5.6 Transfer Knowledge between Design Process and Risk Assessment

IRA concept is integrating the inherently safer design principle and quantitative risk analysis to a process design simulator. The high integration allows for the automation in knowledge transfer from the design process to the risk assessment process. Therefore, the risk level can be obtained faster as the process design in progress.

On the other hand, QRA conducted by the safety team which consists relevant internal and external stakeholders such as the experts and the engineers in process design as well as the risk analyst. Typically, the knowledge transfer performed manually from the process design engineer to the safety team, from which an extensive review and study are carried out.

5.7 The need for Complementary Risk Assessment

As stated clearly by Shariff and Leong [1], IRA is a complement of QRA. Thus, IRA cannot replace the QRA. The main reason is that IRA is developed as a risk assessment in the preliminary design stage. On the other hand, QRA studies can be performed from the concept design phase all the way to the operational phase of the project. Therefore, by using QRA, the need for a complementary risk assessment can be eliminated.

6 Discussion

6.1 Risk Conceptualization and Description and Its Effect on the Risk Assessment Method

The explanation in **Chapter 4** shows that both IRA and NORSOK Z-013 [2], as the guideline for QRA, describe risk using the *C&P* perspective. In IRA, there is uncertainty mentioned in the risk definition. However, the uncertainty aspect and the probability seems to be used interchangeably by Shariff and Leong [1]. Meanwhile, in NORSOK Z-013 [2], the uncertainty is not even mentioned in the risk definition.

As explained in **Chapter 2**, some authors and experts believe the *C&P* perspective need to be replaced with the *C&U* perspective because the *C&P* perspective is too narrow and risk still exists even without any probability associated with the consequence. Then, as the implication of the change in the risk perspective, Aven [39] explained there is a need for additional characterizations to provide the underlying uncertainty in the background knowledge and the potential black swan phenomena.

According to Veland and Aven [34], risk perspective forms one's fundamental understanding of risk which can affect on how one communicates the risk. This statement is to some extent reflected in IRA. As Shariff and Leong [1] seems to have a mixed up understanding related to the probability and the uncertainty, IRA study cases do not mention any uncertainty assessment and/or sensitivity analysis conducted to the calculated risk. This condition is implying the authors paid no or limited attention to the uncertainty aspect.

It is a disadvantage when risk assessment studies rely too much on the probability value and give no or limited consideration to the uncertainty aspect. The frequentist probability can be considered a poor method to express the likelihood of an occurrence of an accidental event as this approach uses a hypothetical probability distribution which does not exist in real life. The accidental event happened cannot be reproduced in the long run, it only happened once.

6.2 Inherently Safer Design Principles Practicability and Its Connection to ALARP Principle

According to Khan and Amyotte [4], the fundamental idea of the inherently safer design is to avoid or eliminate hazard entirely that it will not cause any harm to people or environment under any circumstances. However, the perfect hazard-free condition is not practicable, especially in the industrial world. For instance, in nuclear and oil and gas industry, the nature of the activities involved is closely related to hazardous materials. Therefore, there is a need for establishing a context of what is an inherently safer design that is achievable with the advanced technology available today.

One way to address the issue on the impracticality of inherently safer design is by adapting the ALARP principle to the inherently safer design principles. As in ALARP principle, it is acceptable not to have a zero residual risk as long as it is as low as reasonably practicable. By doing so, the inherently safer design can be less idealistic in achieving a total risk-free condition and can settle in keeping the risk as low as reasonably practicable.

Another way to address the impracticality issue is by looking the inherently safer design term in a relative way. As suggested by Khan and Amyotte [4], this can be done by using a comparison in the design process. Design which shows the less inherent risk is the inherently safer design.

By integrating the inherently safer design principles and the quantitative risk analysis method to a process design simulator, IRA concept may motivate the process design engineer to be proactive in managing risk during the design stage. Further, IRA concept can be a powerful tool in obtaining risk reduction to ALARP level.

For instance, in managing risk of loss of containment, IRA is focusing on minimizing potential leak source by reducing the complexity of the design in the first place. The integration of the inherently safer design principles to the design process allows the plant designer to have a higher awareness that each flange used in the design have a potential to be a leak source which contributes to the overall risk level. The more flanges used, the higher the risk. Thus, the designer will use the flanges in his/her design consciously.

In comparison, a typical QRA study, the focus of assessment in managing the risk of loss of containment is of the leak frequency based on statistical data and relying on add-ons safety features. The typical QRA studies also exclude the human intervention in its calculation. Meanwhile, according to Vinnem and Røed [5] that 60% of hydrocarbon leak with leak rate higher than 0.1kg/s in 2008-2014 occurred during manual intervention with the dominating activity is preventive maintenance. Thus, it can be seen that the typical QRA studies do not address the actual cause of the risk of loss of containment.

Now, looking back to the study cases of IRA presented by Shariff and Leong [1] and Shariff and Zaini [7], it is stated that the risk picture presentation from IRA excludes the ALARP region. The authors argue that since IRA is conducted in the preliminary design stage, the ALARP principle is not yet to be introduced. It is a disadvantage for IRA because the inherently safer design principle and ALARP principle should be in line as they both serve the same purpose which is to give the highest priority to measures to eliminate or reduce causes of accidents. Moreover, ALARP principle can solve the impracticality issue of the inherently safer design principles due to its idealistic idea.

On the other hand, as presented in **Chapter 5**, NORSOK Z-013 [2] includes the inherently safer design in its requirements for risk assessment approach as well as in ALARP evaluation. These requirements stated that, in risk assessment process and ALARP evaluation, options to implement possible risk-reducing measures which include the inherently safer design principles shall be identified and the benefits gained shall be presented in the risk picture.

NORSOK Z-013 [2] may not require the risk assessor to directly applying the principles in the risk assessment, but it requires the risk assessor to assess whether the inherently safer design principles have been implemented and reflected in the design as one of the possible risk-reducing measures.

However, there is no further explanation on how to implement these principles as NORSOK Z-013 [2] only presents four principles on inherently safer design with its definition. The standard failed to include the hierarchy of controls which is the essential part of the inherent safety design principles because the inherent safety is not a stand-alone concept. [27]

The hierarchy of control provides the guideline on the order of prioritization of these principles from the most effective principle which is reduction or minimization to the least effective principle which is simplification. By using this hierarchy of control, the process design engineer can have a systematic order in prioritizing the principles instead of picking which principles to be applied randomly.

Although the inherently safer design principles included in NORSOK Z-013 [2], Vinnem [22] stated that the inherently safer design has no connection to QRA studies. This statement is contradictive considering that Vinnem [22] also regarded the principles as ‘very important’ to reduce risk to ALARP level. As QRA studies also adopting ALARP principle, therefore, to some extent QRA studies and inherently safer design principles have a connection.

The connection between QRA studies and the inherently safer design principles might seem negligible. However, considering the statement by Amyotte et al. [27] that one of the keys to inherently safer design is frequent consideration of the principles, the connection become essential. If the inherently safer design principles adopted in QRA studies, then these principles will also be used as consideration in the risk assessment process so that the principles do not exclusively adhere to the design process.

In relation to the ALARP principle, even though NORSOK Z-013 [2] includes the principle in the guideline and cover the ALARP evaluation in the annex, according to Vinnem [22] the Norwegian petroleum industry has neglected the ALARP approach for major accident prevention and more focused on risk tolerance criteria. The situation is resulting in an issue referred as 'mechanistic' approach which discussed in the next section.

6.3 IRA on 'Mechanistic' Approach found in QRA

The 'mechanistic' approach issue is found when a risk tolerance limit is introduced to the risk evaluation process. In this situation, the focus of risk analysis and evaluation is often limited to satisfying the risk acceptance limits, usually with no or small margin.

For example, on specific offshore oil and gas facility a risk tolerance limit is set that the Fatal Accidental Rate (FAR) value shall be less than 10. The 'mechanistic' approach occur when the risk analysis and evaluation are focusing on meeting this certain value, rather than to see beyond the limit and to reduce the risk as low as reasonably practicable. The implication of such exercise is that there is no or limited margin for the uncertainty aspect given the invalid assumptions or lack of knowledge.

This particular issue is found in QRA practice in Norway. As have mentioned in **Section 6.1.2.**, the Norwegian petroleum industry has neglected ALARP principle and more focus on risk tolerance limit.

IRA has the potential to address such approach as the nature of inherently safer design principle is to reduce the risk at the source and not dependent to risk tolerance limit. However, looking closer to both study cases in IRA, the focus of the assessment is too narrow on satisfying the risk limit sets by the government of Malaysia. It is shown on the assessment is conducted just by looking for the best possible combination that will result in the lowest risk level, rather than rethink the whole process and create a new design out of it. As long as the calculated risk is below the intolerable limit, then there is no need to perform an extended effort in risk reduction.

6.4 The Timing of Risk Assessment Performed and Its Effect on the Design Process

One of the highlighted features of IRA is that the assessment performed during the preliminary design stage so that there is still an opportunity to modify the plant design. However, according to Tüv Rheinland [40] that the greatest opportunity to obtain the lowest residual risk is at the conceptual stage since at this stage the consideration of the alternative options is performed. Once the concept is selected, then the attention shifts to alternative layout examination and system option in inherent safety optimization. Khan and Amyotte [4] also support the statement by stating that the design in the concept design phase is almost 'fixed' so that the authors suggested to made comments related to design even at the earlier stage to avoid major changes in the project.

Based on these arguments, QRA has an advantage compared to IRA as QRA studies can be performed as early as conceptual design. It should be noted that in a typical engineering design process, the preliminary design stage comes after conceptualization stage. [41] [42] As stated by Amyotte et al. [27], one of the key success of the inherently safer design principles implementation is an early consideration. The earlier the principles introduced to the design, the more effective these principles implemented.

For instance, in a typical project development process in the offshore oil and gas industry, there is one of the milestones called 'decision gate' between the concept selection phase and the preliminary phase, or can be referred as Front End Engineering Design (FEED). In the concept selection phase, the alternative of field development concepts such as subsea development, fixed platform, or floating production vessel are evaluated and compared with each other to find the most feasible development concept for the project. After one of the development concepts is selected in the decision gate, say a tensioned-leg platform, then in the further design process, the focus of the discussion shifted to the more detailed design such as the layout of the platform. It is no longer possible to change the other development concepts unless a major rework and waste of resources are acceptable, which is very unlikely.

6.5 Integration of Process Design Simulator and Risk Assessment in relation to Transfer Knowledge

According to Khan and Amyotte [4], the inherently safer design approach encourage the plant designers to utilize basic design feature in achieving a better balance between hazard avoidance, prevention, control, and mitigation. From this statement, it is clear that the inherently safer design principles are targeted to help the plant designers in the design process.

In order to help the process plant designers achieving such balance in their designs, IRA concept integrates the risk assessment in the form of quantitative risk analysis to a process design simulator. This high integration allows for the transfer of knowledge between the designers and the risk assessor conducted automatically. Therefore, the designers can obtain the risk level of their design much faster compared to a typical QRA study. Moreover, the integration can tackle communication issue found in the transfer knowledge process between the process designers and the safety team.

However, this integration should not replace the consultation and communication process between the design engineer and the risk assessor. There is a potential issue if the consultation process is neglected which comes from the competence of the process designer to perform a self-check to the design. According to Lotsberg et al. [43], many errors related to the calculation and lack of understanding of the methodology used for design are difficult to detect by self-checks. It is, therefore, an independent review by another person or an independent analysis is needed to detect these error in time.

In QRA studies, the risk assessment is performed by the safety team led by the risk analyst and comprises relevant internal and external stakeholders from different expertise including the process design engineer.

Here, as there are different teams involved, the knowledge transfer from one team to the safety team is crucial because it is conducted manually. The process design team have the responsibility to provide and document all assumptions, model, and method used in the design to the safety team so that the risk assessment can provide a reliable risk picture.

With many people involved in the risk assessment process, the communication skills of those people involved influenced the quality of the assessment itself. As have discussed in Veland and Aven [34], different perspective and knowledge of risk will affect on how people communicate with each other. For instance, when an expert with a ‘chaotic’ perspective on risk communicates with a risk analyst who has an objective interpretation of risk, may create a resentment from the expert because he/she think the risk analyst is beeing too narrow-minded. This resentment may affect the quality of the risk assessment, and this is something that needs to be avoided.

6.6 Potential of IRA to be implemented as a Risk Assessment in real-life

As described by Vinnem [22] in **Chapter 3**, the history of the implementation of QRA studies in Norway's offshore oil and gas at the early years shows that even a well-established and well-proven method needs a continuous improvement which takes time and effort. Skepticism and critics were addressed to the use of QRA in offshore oil and gas industry by other countries do not stop the development and improvement of QRA method.

Observing on the realization of IRA concept conducted by Shariff and Leong [1] and Shariff and Zaini [7] in developing the study cases on potential explosion from flammable material release and toxic release, this is just a starting point for IRA. The concept is relatively new compared to QRA studies in Norwegian petroleum industry, since it was introduced in 2009 which is over two decades since the first development of QRA studies in Norway.

There is a potential for IRA to be improved, especially some fundamental issues identified in IRA concept realization as discussed in **Section 6.1**. However, it is too early to utilize the concept in the real-life.

7 Recommendations

The comparison and the discussions conducted in **Chapter 4**, **5**, and **6** shows that QRA practice in Norwegian petroleum industry has more advantages compared to IRA concept by Shariff and Leong [1]. By performing QRA thoroughly and carefully in different phases of the project, starting from conceptualization phase all the way to the operational phase, all risk related to the design will be assessed since the earliest phase and the need for a complementary risk assessment can be eliminated. Therefore, it is more reasonable just to perform the QRA rather than IRA.

However, it has to be acknowledged that IRA concept promotes the implementation of the inherently safer design principles by integrating quantitative risk analysis to a process design simulator. The designers can be proactive in addressing the inherent risk as the risk level can be obtained during the process design. The integration can tackle communication issue found in the transfer knowledge process between the process designers and the safety team. It would be a significant improvement if the integration method introduced by IRA adopted in QRA studies.

In relation to the NORSOK Z-013 [2] as the guideline of QRA practice in Norway, it is recommended to expand its coverage on the inherently safer design principles by adding an annex or a section in one of the annexes. In this section, a brief description of the inherently safer design principle can be added it includes the hierarchy of control which is an essential part of the principles since these principles are not stand-alone principles.

As previously explained, the hierarchy of control serves as the guideline on the order of prioritization of inherently safer design principles from the most to the least effective principle. The hierarchy of control helps the process design engineers so that they have a systematic order in prioritizing the principles instead of picking which principles to be applied randomly.

By expanding the coverage on the inherently safer design principles, it is hoped for that the risk assessor can have a higher awareness as well as a clearer illustration on what to expect when assessing whether a design has implemented the principles or not. Thus, a frequent consideration of the principles to ensure a successful implementation on achieving inherently safer design can be performed by both process design team and the risk analysts.

8 Summary and Conclusion

Inherent Risk Assessment (IRA) is a recently introduced concept of risk assessment by Shariff and Leong [1]. The concept integrates quantitative risk analysis and inherently safer design principles to a process design simulator, called HYSYS, aimed to obtain risk level as early as the preliminary design stage. IRA encourages the process designer to be proactive to reduce the risk at the source by generating a balanced inherently safer design.

Currently, there are two study cases developed for realization IRA concept. First study case is performed by Shariff and Leong [1] and focusing on the potential explosion from flammable materials release, Second study case is focused on toxic release and conducted by Shariff and Zaini [7].

In its attempt to defining risk, Shariff and Leong [1] failed to distinct the probability as the measure of uncertainty with the uncertainty itself. There are two pieces of evidence supporting this statement: first, on how the authors mentioned probability along with uncertainty in the risk definition and; second, by observing the risk definition and mathematical function the authors made reference to which none of these sources mentioned uncertainty.

Based on the risk definition presented by Shariff and Leong [1] it is concluded that IRA concept is developed based on the perspective where risk is seen as a combination of consequences and probability (*C&P* perspective). Based on the IRA study cases, the probability in IRA is interpreted as a frequentist probability. As a consequence, IRA relies too much on the frequentist probability and gives no or limited consideration to the uncertainty aspect. It is shown in IRA study cases where calculated risk is straightly compared to the intolerable limit set by the Malaysian government. Moreover, there is no part of the studies that mentioned an uncertainty analysis and/or sensitivity analysis conducted. This is implying that the authors paid no or limited attention to the uncertainty aspect. This appears to be a disadvantage when compared to QRA in Norway where NORSOK Z-013 [2] also define risk based on *C&P* perspective but the requirement to perform uncertainty assessment is also included in the standard.

IRA concept excluded the ALARP principle in its risk picture presentation. Meanwhile, according to NORSOK Z-013 [2] as the guideline to perform QRA in Norwegian petroleum industry, the ALARP evaluation is included as part of risk treatment. Shariff and Leong [1] and Shariff and Zaini [7] argue that since IRA carried out in preliminary design stage, ALARP principle is not yet to be introduced. The authors misunderstood ALARP principle as a principle that can only be exclusively applied to the add-ons risk reducing measure. However, ALARP principle should be in line with the inherently safer design principles because it has the same purpose of giving high priority to risk reduction at source. Moreover, by adopting ALARP principle to the implementation of inherently safer design principles, the idealistic foundation of inherently safer design principles to achieve zero-risk condition can be more realistic and settle with the keeping risk as low as reasonably practicable.

IRA concept also missed the opportunity to address the issue of ‘mechanistic’ approach found in QRA practice in Norway. IRA has the potential to address such approach as the nature of inherently safer design principle is to reduce the risk at the source and aiming for zero-risk condition. However, IRA study cases demonstrate that the focus of the assessment is too narrow on satisfying the risk limit sets by the government of Malaysia rather than to concentrate on reducing risk at the source. It is shown on how the assessment is conducted just by looking for the best possible combination that will result in the lowest risk level, rather than rethink the whole process and create a new design out of it. As long as the calculated risk is below the intolerable limit, then there is no need to perform an extended effort in risk reduction.

One of the highlighted features of IRA is that the assessment performed during the preliminary design stage so that there is still an opportunity to modify the plant design. However, according to NORSOK Z-013 [2], QRA can be performed as early as the concept selection phase. It is another disadvantage of IRA, as IRA can only be performed in the preliminary design stage which comes after the concept selection phase. Therefore, QRA has the greatest opportunity in influencing the design form since the conceptual design stage which is earlier than the preliminary design stage. In addition, because of QRA can be performed throughout the project life, from concept selection phase to the operational phase, it does not need a complementary risk assessment in to be carried out in other phases.

Besides the issues presented above, IRA has an advantage compared to QRA in Norway in terms of help the process plant designers achieving a balanced design since it integrates the risk assessment in the form of quantitative risk analysis to a process design simulator. The integration allows the transfer knowledge between the designers and the risk assessor conducted automatically. Therefore, the designers can obtain the risk level of their design much faster compared to a typical QRA study. Moreover, the integration can tackle communication issue found in the transfer knowledge process between the process designers and the safety team.

IRA concept is relatively new compared to QRA studies in Norwegian petroleum industry because it was just introduced in 2009. There is still time and opportunities to improve the implementation of IRA concept, especially to address some fundamental issues identified in IRA concept realization as discussed.

Based on the analyses and discussion conducted in **Chapter 4**, **5**, and **6** its is concluded that QRA practice in Norwegian petroleum industry based on NORSOK Z-013 [2] has more advantages compared to IRA because it is a well-established and well-proven methodology in risk assessment. By performing QRA thoroughly and carefully in different phases of the project, starting from concept selection phase all the way to the operational phase, all risk in the design will be assessed since the earliest phase and the need for a complementary risk assessment can be eliminated.

However, there are two items of recommendation for QRA practice in Norway that can be adopted from IRA. First item is the integration method of quantitative risk analysis and inherently safer design principles to a process deign simulator which allows the transfer knowledge can be performed automatically. Second item is to expand the coverage of inherently safer design principles in NORSOK Z-013 [2] to promotes the implementation of the principles since one of the key success in applying inherently safer design principles is frequent consideration.

9 References

1. Shariff, A.M. and C.T. Leong, *Inherent risk assessment--A new concept to evaluate risk in preliminary design stage.* Process safety and environmental protection, 2009. **87**(6): p. 371-376.
2. Standards Norway, *Risk and emergency preparedness assessment*, in *NORSOK Z-013*. 2010, Standards Norway: Norway.
3. Kletz, T.A., *Inherently Safer Plants.* Plant/operations progress, 1985. **4**(3): p. 164-167.
4. Khan, F.I. and P.R. Amyotte, *Inherent safety in offshore oil and gas activities: a review of the present status and future directions.* Journal of Loss Prevention in the Process Industries, 2002. **15**(4): p. 279-289.
5. Vinnem, J.E. and W. Røed, *Root causes of hydrocarbon leaks on offshore petroleum installations.* Journal of Loss Prevention in the Process Industries, 2015. **36**: p. 54-62.
6. Gordon, B. and R. Duncanson, *Managing Uncertainty to Deliver Sustainable Unmanned Operations*. 2015, Society of Petroleum Engineers.
7. Shariff, A.M. and D. Zaini, *Inherent risk assessment methodology in preliminary design stage: A case study for toxic release.* Journal of Loss Prevention in the Process Industries, 2013. **26**(4): p. 605-613.
8. Aven, T., *On how to conceptualise and describe risk.* Reliability: Theory & Applications, 2011. **2**(1): p. 28-37.
9. Aven, T., *The risk concept—historical and recent development trends.* Reliability Engineering & System Safety, 2012. **99**: p. 33-44.
10. De Moivre, A., *De Mensura Sortis.* Philosophical Transactions, 1711. **27**: p. 213-64.
11. Kaplan, S. and B. Garrick, *On the quantitative definition of risk.* Risk Analysis, 1981. **1**: p. 11-27.
12. Aven, T., *A risk concept applicable for both probabilistic and non-probabilistic perspectives.* Safety Science, 2011. **49**(8–9): p. 1080-1086.
13. Aven, T. and O. Renn, *The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism risk.* Risk Analysis, 2009. **29**: p. 587-600.
14. Aven, T. and E. Zio, *Some considerations on the treatment of uncertainties in risk assessment for practical decision making.* Reliability Engineering & System Safety, 2011. **96**(1): p. 64-74.
15. Aven, T., *Misconception of Risk*. 2010, Cichester: Wiley.
16. Aven, T., *Risk Analysis*. 2nd ed. ed. 2015, Chichester: Wiley.
17. Aven, T., *On how to define, understand and describe risk.* Reliability Engineering & System Safety, 2010. **95**(6): p. 623-631.
18. Askeland, T., R. Flage, and T. Aven, *Moving beyond probabilities – Strength of knowledge characterisations applied to security.* Reliability Engineering & System Safety, 2017. **159**: p. 196-205.
19. Flage, R. and T. Aven, *Expressing and Communicating Uncertainty in Relation to Quantitative Risk Analysis.* Risk Reliability, 2009. **2**(13): p. 9-18.
20. Baybutt, P., *The ALARP principle in process safety.* Process Safety Progress, 2014. **33**(1): p. 36-40.
21. Aven, T., *Risk analysis: assessing uncertainties beyond expected values and probabilities*. 2008, Chichester: Wiley.
22. Vinnem, J.E., *Offshore Risk Assessment Vol 1: Principles, Modelling and Applications of QRA Studies*. Springer Series in Reliability Engineering. Vol. 1. 2014, London: Springer.

23. Lord Cullen, H., *The public inquiry into the Piper Alpha disaster: volume 1*. 1990, HMSO: London.
24. Vinnem, J.E., *Offshore Risk Assessment vol 2. : Principles, Modelling and Applications of QRA Studies*. Springer Series in Reliability Engineering. Vol. 2. 2014, London: Springer.
25. Kletz, T. and P.R. Amyotte, *Process Plants: A Handbook for Inherently Safe Design*. 2010, Boca Raton, Fla: CRC Press.
26. Hurme, M. and M. Rahman, *Implementing inherent safety throughout process lifecycle.* Journal of Loss Prevention in the Process Industries, 2005. **18**(4–6): p. 238-244.
27. Amyotte, P.R., M.J. Pegg, and F.I. Khan, *Application of inherent safety principles to dust explosion prevention and mitigation.* Process Safety and Environmental Protection, 2009. **87**(1): p. 35-39.
28. Health and Safety Executive UK. *Flixborough (Nypro UK) Explosion 1st June 1974*. [cited 2017; Available from: http://www.hse.gov.uk/comah/sragtech/caseflixboroug74.htm.
29. Center for Chemical Process Safety(CCPS), *Guidelines for Chemical Process Quantitative Risk Analysis*. 2nd ed. 2000, New York: American Institue of Chemical Engineers.
30. Health and Safety Executive UK (HSE-UK), *Reducing Risk, Protecting People*. 2001, Health and Safety Executive UK (HSE-UK),: Crown, United Kingdom.
31. Wentz, C.A., *Safety, Health and Environment Protection*. 1999, New York: McGraw Hill.
32. Crowl, D.A. and J.F. Louvar, *Chemical Process Safety: Fundamentals with Applications*. 1990, New Jersey, USA: Prentice Hall.
33. Shariff, A.M. and D. Zaini, *Toxic release consequence analysis tool (TORCAT) for inherently safer design plant.* Journal of Hazardous Materials, 2010. **182**(1–3): p. 394-402.
34. Veland, H. and T. Aven, *Risk communication in the light of different risk perspectives.* Reliability Engineering & System Safety, 2013. **110**: p. 34-40.
35. Petroleum Safety Authority. *REGULATIONS RELATING TO MANAGEMENT AND THE DUTY TO PROVIDE INFORMATION IN THE PETROLEUM ACTIVITIES AND AT CERTAIN ONSHORE FACILITIES (THE MANAGEMENT REGULATIONS)*. 2016 [cited 2017 2 June]; Last amended 15 December 2016, cf. page 4]. Available from: http://www.ptil.no/management/category401.html#p17.
36. Petroleum Safety Authority. *REGULATIONS RELATING TO MANAGEMENT AND THE DUTY TO PROVIDE INFORMATION IN THE PETROLEUM ACTIVITIES AND AT CERTAIN ONSHORE FACILITIES (THE MANAGEMENT REGULATIONS)*. 2016 3 February 2017]; Available from: http://www.psa.no/management/category401.html.
37. ISO, *ISO 31000:2009, Risk Management - Principles and guidelines*. 2009, ISO: Switzerland.
38. Lees, F.P., *Lee's loss prevention in the process industries: hazard identification, assessment and control*. 3rd ed, ed. S. Mannan. Vol. 3. 2005, Amsterdam: Elsevier Butterworth-Heinemann.
39. Aven, T., *Practical implications of the new risk perspectives.* Reliability Engineering & System Safety, 2013. **115**: p. 136-145.
40. TUVRheinland.
41. Ertas, A. and J. Jones, *The Engineering Design Process*. 2nd ed. 1996, New York, N.Y.: John Wiley & Sons, Inc.

42. Dym, C. and P. Little, *Engineering Design*. 3rd ed. 2009, New York, N.Y.: John Wiley & Sons, Inc.

43. Lotsberg, I., et al., *Risk assessment of loss of structural integrity of a floating production platform due to gross errors.* Marine Structures, 2004. **17**(7): p. 551-573.