# Can We Stop Learning Safety by Accident?

by

© Howard Pike

A Thesis submitted to the

School of Graduate Studies

in partial fulfillment of the requirements for the degree of

**Master of Engineering**

**Faculty of Engineering and Applied Science**

Memorial University of Newfoundland

May, 2020

St. John’s, Newfoundland and Labrador

# ABSTRACT

The question has been asked in many forums, why are major accidents still occurring? Awareness is an important basic learning factor to properly manage the lessons to be learned from major accidents. Over time, the recommendations made following an accident may be forgotten, procedures allowed to lapse, changes are made to equipment and the accident is just waiting to happen again. The memory within an organization that should help to prevent process safety accidents decays thus allowing accidents to repeat. It has been 38 years since the loss of all 84 crew members on the *Ocean Ranger*, the largest mobile offshore drilling unit of its day. At 1:10 a.m. EST on February 15, 1982, the *Ocean Ranger*'s crew sent a mayday call and abandoned the rig at 1:30 a.m. No one survived. There were no eye witnesses to tell what happened. Investigators were left with some technical evidence and the testimony from others. While the investigation report and recommendations from a Royal Commission into the *Ocean Ranger* tragedy changed the offshore safety regime of the time, can we learn more by re-examining the past? Can we stop learning safety by accident?

Safety and environmental risk go hand in hand with industrial development. However, it is unclear whether there is a linear or nonlinear relationship between risk and industrial development. Perhaps, it is case dependent. Some industrial endeavors such as offshore development, activities in a harsher environment, or development requiring new technologies (untested and untrusted technologies) may pose a higher risk (nonlinear) than more conventional industrial development activities (e.g., petroleum refineries,

petrochemical plants, pipeline transportation, and the like). Public perception plays a critical role in defining the risk versus development relationship. The public perception of risk is dependent on awareness and understanding of potential hazards and their likelihood of occurrence, and most importantly, effective communication of these along with the associated uncertainty. Public awareness can have a profound effect on the development of public policy, which in many cases is driven more by perception rather than by sound science. Two commonly used concepts of policy and decision-making will be investigated, the Precautionary Principle (PP) and As Low As Reasonably Practicable (ALARP). A clearer understanding of both approaches with an illustrative example will be provided. A process to help readers understand where and when PP versus ALARP would be most applicable is proposed.

# ACKNOWLEDGEMENTS

I would like to recognize my gratitude towards my supervisor Dr. Faisal Khan for his comments, mentorship, patience, and guidance through the learning process of this master thesis. Furthermore, I would like to thank him for his insightful support and constructive criticism to endlessly push me to become a better engineer, researcher, and person. To him, I am eternally thankful.

I would also like to recognize our co-author on the paper, *Precautionary Principle (PP) versus As Low As Reasonably Practicable (ALARP): Which One to Use and When*, Dr. Paul Amyotte for his comments, support and constructive criticism though the development of the paper.

I would like to gratefully acknowledge the assistance of graduate student Mohammad Zaid Kamil for the production of the graphics in the paper, *Precautionary Principle (PP) versus As Low As Reasonably Practicable (ALARP): Which One to Use and When*.

I would like to acknowledge the support and editorial assistance of my sister, Barbara Pike, during my graduate program.

Additionally, I would like to thank my wife, Bonnie, for her undying support, constant source of love, and encouragement to pursue of this degree. Her patience and understanding were essential to its completion. Without her help, I would not be the person I am today.

# Table of Contents

# List of Tables

# List of Figures

# List of Symbols, Nomenclature or Abbreviations

$\lambda$ – average rate of occurrence

X – distance traveled before first occurrence

$F_X(x)$ – cumulative distribution function

$x$ – discrete random variable

ABS – American Bureau of Shipping (Chapter 1)

ABS – Anti-lock Braking System (Chapter 2)

ALARP – As Low As Reasonably Practicable

BN – Bayesian Network

BT – Bow Tie

CPF – Cumulative Density Function

ETA – Event Tree Analysis

ESC – Electronic Stability Control

FTA – Fault Tree Analysis

IE – Initiating Event

MODU – Mobile Offshore Drilling Unit

VHF – Very High Frequency Radio Band

# Introduction and Overview

With thousands of people affected by major industrial disasters in the twentieth century, the public demanded improved standards in industrial sectors and has come to expect that industrial activity operate safely from the perspective of both health and safety and environmental protection. Governments implemented rules to reduce major industrial accidents and nongovernmental agencies developed standards and guidelines. Although the number of major industrial disasters has been reduced, they still occur occasionally, even with the higher level of standards and guidelines. Traditionally, experience played a large part in improving safety and regulatory development, but can we learn more by re-examining past disasters? Can we stop learning safety by accident?

Whenever a major industrial disaster occurs we are usually told that "lessons will be learned" (Mannan & Waldram, 2014). Major accident inquiries are established into cause and essentially establish a new case study. "Lessons learned" from major industrial disasters are publicized by writing reports, making presentations at conferences, and writing up case studies in journal articles or books. All these activities suffer from many of the limitations of case studies, in particular, the difficulties involved in trying to generalize the specific causes of the disaster. Given that a major accident inquiry is a case study, we need to think carefully about how such an investigation can generate recommendations going beyond the particular causes of the case (Hopkins, 2014). Though some accidents may have been prevented from re-occurring, years of experience have not eliminated repeat accidents. The value of accident analysis lies not so much in the conclusions about the causes of the accident investigated, but in the way the whole investigation process draws

attention to safety issues that can usefully be made the subject of recommendations. Over time, the recommendations made following an accident may be forgotten, procedures may be allowed to lapse, changes are made to equipment and the accident is just waiting to happen again (Throness, 2014). The memory within an organization that should help to prevent process safety accidents decays thus allowing accidents to repeat.

Trevor Kletz, one of the pioneers of safety science, was described as a wonderfully articulate and compelling storyteller (Amyotte, 2014). Stories are used to transmit causal information and lessons among people, as well as to share experiences, and to organize a community's collective memory (Sloman & Fernback, 2017). When a community agrees to buy into a particular story, they are accepting the attitude implied by the story. Storytelling is our natural way of making sense of sequences of events and perhaps the most common way we pass causal information to one another. A good story goes beyond just describing what actually happened. It has lessons that apply not just to the incident but also to other industrial activity.

Storytelling requires that we use our understanding of causal mechanisms to build scenarios to think about. Storytelling helps us to imagine how a scenario could change if something were different. When we tell stories about the past – we can learn. When we tell stories about the future – we can predict. And when we tell stories about the present – we analyze the situation. All of this can help identify causes and foresee consequences – that allows risk assessment to produce more effective actions.

The question has been asked in many forums, why are major accidents still occurring? Silva (2016) poses the thesis that loss of technical knowledge is an important contributing

factor to why a major accident occurs. This loss occurs due to: (i) new technology, (ii) inadequate training, procedures and information, and (iii) failure to incorporate new knowledge such as lessons learned. After a major disaster occurs, attention will immediately give rise to expectation for improved health and safety measures, and environmental protection. Governments will act to reduce the risk, though not necessarily in a consistent way. The lessons learned from the accident investigation report will be disseminated. New safety methods will be implemented to industrial activities, thereby reducing the risks. However, new risk can emerge when changes are made which create new gaps in technological knowledge.

Paltrinieri et al. (2012) have built on Donald Rumsfeld's quote that distinguished different kinds of knowledge: "There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know." In addition, Paltrinieri et al. (2012) have added "Unknown Known", the things we should have known but didn't.

Awareness is an important basic learning factor to properly manage the lessons to be learned from major accidents, "Known Known" scenarios have become "typical" risk scenarios and their effect identified in the level of risk. Effective knowledge management would make possible the transfer from "Unknown Known" events to "Known Known" ones, i.e., to events that have been studied, analyzed, and assimilated into the process of risk analysis. Known unknowns might not be easily handled, but at least it is clear what to prepare for. There will always be some potential events that have never been experienced.

We have to predict not only events that are unlikely but also events that we can't even formulate clearly enough to know that we should be worried about them. It is these Unknown Unknowns that present real problems. How can you prepare for something when you don't know what you're preparing for? Then we shift from prevention issues to precaution principles. We can make assumptions as to the nature of the risk, which may be open to debate, and may need to be refined as more information becomes available, but we can make a start in assessing the risks.

While the risk of suffering harm is an inescapable aspect of all human activity, loss of life, serious illness, and degradation of the environment are no longer acceptable consequences from any industrial development. Increased levels of awareness of environmental and development issues and greater engagement on the part of the public have led to a much keener interest in industrial risk management practices, policies, and effectiveness. Regulatory interventions and risk management use two widely recognized principles for risk reduction approaches: the "Precautionary Principle" (PP) and the "As Low As Reasonably Practicable" (ALARP) principle (TRB, 2018). The importance of the precautionary principle (PP) in the public review process cannot be ignored. Three public reviews of hydraulic fracturing in Atlantic Canada have used the principle in recommending, if not a moratorium, then a suspension of further development. These recommendations resulted from elements of uncertainty of a range of issues related to the risk of unconventional oil and gas development.

The public interest in environmental and development issues derives principally from notable public policy conflicts over industrial development believed to be hazardous or environmentally unfriendly and the implicit promise that we can keep technological risks

thoroughly under control. This promise has driven an increased expectation for a society free of involuntary risks. However, risk as a concept perceived by the general public appears to be rather poorly understood. The word risk has become an emotionally charged word, used and abused repeatedly in the media and on the internet in ways that polarize discussions and create antagonism. The communication of risk to the public is a challenging task, made more so when trying to balance risks in one domain with benefits in another. All the progress and benefits that technology has brought in social development would not have been achieved if society were indeed to stop development at the first suggestion of any problem. The challenge is how to recognize the problem as an impending threat, to analyze the signs, to identify the hazard, and then to manage the potential risk.

**Problem Statement**

The management of risks associated with potentially hazardous industrial activities has been and continues to be the subject of considerable development in the range and extent of regulatory activity associated with the authorization of industrial activity (Melchers, 2001). If regulatory activity is to employ rational decision-making, it requires a clear and quantitative way of presenting risk so that it can be adequately weighed, along with all other costs and benefits. Risk analysis seeks to quantify risk as much as possible in terms not only of the probability of an event in time and space, but also the probability of a particular level of consequences. The scientist or professional engineer will readily admit that risks of a technical nature cannot be reduced to zero, but they can be reduced to very low values, from either or both aspects of probability and consequence, for almost all industrial activities. While risk assessment techniques help to measure the safety and

environmental threat of a particular activity, evaluation methods use risk assessment techniques to assess the adequacy of the layers of protection provided for an activity. New approaches aim to reduce uncertainty over time through system monitoring that is iterative, structured, and systematic.

This thesis explores the answers for two pertinent questions:

1. Have we learned from past accidents? If so, then why do accidents continue to occur with significant consequences? Can we stop learning safety by accident?
2. What are the principles of risk reduction ALARP and PP? When, where and how to use them?

**Research Objectives**

One objective of this thesis was to review a past accident to see if further recommendations can be drawn from the re-examination of an accident investigation. The fundamental ideas on accident causation and system safety have evolved over the last few decades, and they are strongly intertwined with the concepts and tools of risk analysis on the one hand, and accident models on the other hand. Can we learn more from past accidents?

Another objective of this thesis was to examine risk acceptance principles. If the risk of suffering harm is an inescapable aspect of all human activity, then how do we know when the activity is safe enough? What is safety? The term in its human context has no meaning except in relation to potential risk of harm. It is essentially a relative term, the complement of risk. How do we present risk in a clear and quantitative way so that it can be adequately weighed, along with all other costs and benefits?

## Research Scope

The scope of the current study is from an Oil and Gas development perspective with emphasis on offshore and frontier areas. While the research may be applicable to other hazardous activities such as the nuclear industry, aerospace or other high-risk processes, these are not explored in the current work. This work has examined one aspect of effective knowledge management that would make possible the transfer from "Unknown Known" events to "Known Known" ones, i.e., to re-examine events that had previously been studied, analyzed, from the perspective of more recent ideas on accident causation and system safety. The work also examines two of the possible principles of risk acceptance. The two widely recognized principles for risk reduction approaches used in regulatory interventions, ALARP and PP.

## Thesis Composition

The definition of risk used in this thesis incorporates the likelihood that a hazard will cause adverse effects, together with the measure of those effects. Two approaches to risk management are considered: the "Precautionary Principle" (PP) and the "As Low As Reasonably Practicable" (ALARP) principle. The relationship between them with respect to risk management of industrial activity is explored along with how they can be better utilized. The primary objective is to encourage transparency and accountability in the application of risk management as embodied by the PP and ALARP to industrial activity to promote greater confidence in the risk management process.

The thesis consists of two manuscripts: the first is a paper submitted as part of a presentation made at the 2nd International Conference on Advances in the Field of Health,

Safety, Fire, Environment, Allied Sciences & Engineering held at the University of Petroleum and Energy Studies, Dehradun, India in November 2018 and the second is a paper that has been published in the Journal of Process Safety and Environmental Protection, volume 137 (May 2020) pages 158 – 168.

Chapter 1 comprising the first paper reflects on the loss of the *Ocean Ranger* mobile offshore drilling unit and what additional lessons can be learned by re-examining this disaster. It has been 38 years since the loss of all 84 crew members on the *Ocean Ranger,* the largest mobile offshore drilling unit of its day. At 1:10 a.m. EST on February 15, 1982, the *Ocean Ranger*'s crew sent a mayday call and abandoned the rig at 1:30 a.m. No one survived. There were no eye witnesses to tell what happened. Investigators were left with some technical evidence and the testimony from others. While the investigation report and recommendations from a Royal Commission into the *Ocean Ranger* tragedy changed the offshore safety regime of the time, can we learn more by re-examining the past? Can we stop learning safety by accident?

Chapter 2 comprising the second paper presents the challenges and opportunities associated with establishing risk acceptance for risk assessment and management. Safety and environmental risk go hand in hand with industrial development. However, it is unclear whether there is a linear or nonlinear relationship between risk and industrial development. Perhaps, it is case dependent. Some industrial endeavors such as offshore development, activities in a harsher environment, or development requiring new technologies (untested and untrusted technologies) may pose a higher risk (nonlinear) than more conventional industrial development activities (e.g., petroleum refineries, petrochemical plants, pipeline

transportation, and the like). Public perception plays a critical role in defining the risk versus development relationship. The public perception of risk is dependent on awareness and understanding of potential hazards and their likelihood of occurrence, and most importantly, effective communication of these along with the associated uncertainty. Public awareness can have a profound effect on the development of public policy, which in many cases is driven more by perception rather than by sound science. This chapter sheds light on this crucial issue. It investigates two commonly used concepts of policy and decision-making, the Precautionary Principle (PP) and As Low As Reasonably Practicable (ALARP). The chapter provides a clearer understanding of both approaches with an illustrative example. It proposes a process to help readers understand where and when PP versus ALARP would be most applicable.

Chapter 3 concludes the thesis and discusses future scope of work.

## Co-authorship Statement

I hereby declare that the manuscript titled Precautionary Principle (PP) versus As Low As Reasonably Practicable (ALARP): which one to use and when, (Pike, H., Khan, F., Amyotte, P.) in the Journal of Process Safety and Environmental Protection, volume 137 (May 2020), pages 158 - 168. As primary author, I led the development of the framework, its implementation, and analysis of the results with the help of co-authors, Dr. Faisal Khan and Dr. Paul Amyotte. I have drafted the initial manuscript, which was reviewed and commented by co-authors. Their suggestions were later incorporated in the final manuscript. As co-authors, Faisal Khan and Paul Amyotte helped developing the framework, and supported in finalizing the methodology. They also contributed in reviewing and revising the manuscript.

.

# Chapter 1 - Can we stop learning safety by accident?

“Those who cannot remember the past are condemned to repeat it” appeared in “The life of reason”, Santayana (1905).

# Can we stop learning safety by accident?

Howard Pike[1,*]

[1]Centre for Risk, Integrity and Safety Engineering, Faculty of Engineering, Memorial University, St. John's, NL, Canada. p79hlp@mun.ca

**Preamble.** The chapter was a paper submitted as part of a presentation made at the 2nd International Conference on Advances in the Field of Health, Safety, Fire, Environment, Allied Sciences & Engineering held at the University of Petroleum and Energy Studies, Dehradun, India in November 2018.

**1.0 Abstract**. It has been 38 years since the loss of all 84 crew members on the *Ocean Ranger,* the largest mobile offshore drilling unit of its day. At 1:10 a.m. EST on February 15, 1982, the *Ocean Ranger*'s crew sent a mayday call and abandoned the rig at 1:30 a.m. No one survived. There were no eye witnesses to tell what happened. Investigators were left with some technical evidence and the testimony from others. While the investigation report and recommendations from a Royal Commission into the *Ocean Ranger* tragedy changed the offshore safety regime of the time, can we learn more by re-examining the past? Can we stop learning safety by accident?

**Keywords:** *Ocean Ranger*, accident analysis, training, safety management, safety culture

## 1.1 Introduction

With thousands of people affected by major industrial disasters in the twentieth century, the public has demanded improved standards in industrial sectors and has come to expect that industrial activity operate safely from the perspective of both health and safety and environmental protection. Governments implemented rules to reduce major industrial accidents and nongovernmental agencies developed standards and guidelines. Although the number of major industrial disasters has been reduced, they still occur occasionally, even with the higher level of standards and guidelines. Traditionally, experience played a large part in improving safety and regulatory development, but can we learn more by re-examining past disasters? Can we stop learning safety by accident?

Whenever a major industrial disaster occurs we are usually told that "lessons will be learned" (Mannan & Waldram, 2014). Major accident inquiries are established into cause and essentially establish a new case study. "Lessons learned" from major industrial disasters are publicized by writing reports, making presentations at conferences, and writing up case studies in journal articles or books. All these activities suffer from many of the limitations of case studies, in particular, the difficulties involved in trying to generalize the specific causes of the case. Given that a major accident inquiry is a case study, we need to think carefully about how such an investigation can generate recommendations going beyond the particular causes of the case (Hopkins, 2014). Though some accidents may have been prevented from re-occurring, years of experience have not eliminated repeat accidents. The value of accident analysis lies not so much in the conclusions about the

causes of the accident investigated, but in the way the whole investigation process draws attention to safety issues that can usefully be made the subject of recommendations.

Paltrinieri et al. (2012) have built on Donald Rumsfeld's quote that distinguished different kinds of knowing:

"There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know."

In addition, Paltrinieri et al. (2012) have added "Unknown Known", the things we should have known but didn't.

Awareness is an important basic learning factor to properly manage the lessons to be learned from major accidents, "Known Known" scenarios have become "typical" risk scenarios and their effect identified in the level of risk. Effective knowledge management would make possible the transfer from "Unknown Known" events to "Known Known" ones, i.e., to events that have been studied, analyzed, and assimilated into the process of risk analysis. Known unknowns can be handled. It might not be easy, but at least it is clear what to prepare for. There will always be some potential events that have never been experienced. We have to predict not only events that are unlikely but also events that we can't even formulate clearly enough to know that we should be worried about them. It is these Unknown Unknowns that present real problems. How can you prepare for something when you don't know what you're preparing for? Then we shift from prevention issues to

precaution principles. We can make assumptions as to the nature of the risk, which may be open to debate, and may need to be refined as more information becomes available, but we can make a start in assessing the risks.

Silva (2016) poses the thesis that loss of technical knowledge is an important contributing factor to why a major accident occurs. This loss occurs due to: (i) new technology, (ii) inadequate training, procedures and information, and (iii) failure to incorporate new knowledge such as lessons learned. After a major disaster occurs, attention will immediately give rise to expectation for improved health and safety measures, and environmental protection. Governments will act to reduce the risk, though not necessarily in a consistent way. The lessons learned from the accident investigation report will be disseminated. New safety methods will be implemented to industrial activities, thereby reducing the risks. New risk can emerge when new changes are made which create new gaps in technological knowledge.

Trevor Kletz, one of the pioneers of safety science, was described as a wonderfully articulate and compelling storyteller (Amyotte, 2014). Stories are used to transmit causal information and lessons among people, as well as to share experiences, and to organize a community's collective memory (Sloman & Fernback, 2017). When a community agrees to buy into a particular story, they are accepting the attitude implied by the story. Storytelling is our natural way of making sense of sequences of events and perhaps the most common way we pass causal information to one another. A good story goes beyond just describing what actually happened. It has lessons that apply not just to the incident but also to other industrial activity.

Storytelling requires that we use our understanding of causal mechanisms to build scenarios to think about. Storytelling helps us to imagine how a scenario could change if something were different. When we tell stories about the past – we can learn. When we tell stories about the future – we can predict. And when we tell stories about the present – we analyse the situation. All of this can help identify causes and foresee consequences – that allows thinking to produce more effective actions.

While the investigation report and recommendations from the Royal Commission into the *Ocean Ranger* tragedy changed the offshore safety regime of the time, can a modern analysis be used to review this disaster to gain further insight into safety science?

### 1.2 Background to the *Ocean Ranger* disaster

None of the 84 crew on the *Ocean Ranger* that fateful morning of February 15th in 1982 survived the disaster. With no survivors, there were no eyewitnesses to tell what happened. Investigators were left with some technical evidence. There was also testimony from others. These allowed for a number of firm conclusions. But investigators also had some conclusions that were based on assumptions derived from established patterns of behavior and practice.

There have been many theories of what could have happened. Over the years, a number of stories have been written with different accounts of what may have happened. However, we will rely on the conclusions of the Royal Commission on the Ocean Ranger Marine Disaster (Hickman, 1984), and to a lesser degree the Marine Casualty Report of the United States Coast Guard (USCG, 1983).

The definition of safety that we use most often comes from the Royal Commission, "High standards of safety in the workplace are achieved when well-designed equipment is operated properly by well-managed and well-trained persons. Safety is maintained by keeping these factors in a state of positive balance, in what is normally a highly dynamic situation." (Hickman, 1985)

Those key points all played a role in the loss of 84 people in the *Ocean Ranger* disaster. There were inadequacies in the design of the equipment. There were poor operating procedures. There was a lack of training. Designing for normal or static conditions and thinking in terms of static conditions in what is a very dynamic marine environment may also have played a role.

Today, we see a positive balance maintained by Safety Culture, risk awareness and collective mindfulness. These are important factors in any successful industrial operation. Safety Culture as a term was not used in the early 1980's, but as you talk to those who worked on the *Ocean Ranger* and read the Commission Report you can see that the fundamental elements of a safety culture were missing.

Certainly, risk awareness as it relates to the marine environment was not evident from ODECO's management nor from the MODU leadership. Another missing element was collective mindfulness. In fact, workers were told when they came onboard the rig that safety wasn't their responsibility. They were told it was the responsibility of a single person onboard, the industrial relations representative.

The *Ocean Ranger* was the largest semisubmersible mobile offshore drilling unit (MODU) of its day. It was built in 1976 at the Mitsubishi Heavy Industries shipyard for OEDCO and Norwegian firm Fearnley & Eger A/S. This was just 14 years after the first semisubmersible spudded a well in the Gulf of Mexico for Shell in January of 1962. Shell had modified a submersible drilling unit called the *Blue Water 1* to go from sitting on the seabed and drilling, to floating in 90 meters of water and drilling. Shell had developed this novel technology which is generally considered the first move from land based drilling technology to floating drilling technology.

The *Ocean Ranger* was built under the supervision of the American Bureau of Shipping (ABS) and rated by ABS for "Unrestricted Ocean Operations". It was initially registered under Panamanian flag, however, in 1979, as sole owner of the *Ocean Ranger*, ODECO transferred the rig to United States registry. ABS was the first Ship Classification Society to develop rules for MODUs. Their rules were initially published in 1968 but updated in 1973. The *Ocean Ranger* was built to the 1973 rules. The first International Maritime Organization MODU code was published in 1979, but the *Ocean Ranger* would not have had to comply with it.

The *Ocean Ranger* used on-the-job training. So the loss of a partner, in this case Fearnley & Eger A/S, would have meant the potential loss of some rig knowledge held by their people.

Panama as flag state authority depended on ABS for oversight of construction and operation. The United States would have accepted the Panamanian oversight of construction. The United States Coast Guard did conduct a review and survey of the

MODU during the transfer process. However, because the rig was not operating in United States waters it was up to ODECO to arrange for the required inspections and to keep certificates current.

The Ocean Ranger was 121 metres long, 80 metres wide and 91 metres from the keel to the top of the derrick. It was designed for winds of up to 115 miles per hour (185 kilometers per hour) and waves up to 110 feet (33.5 metres). Prior to February 14th, the *Ocean Ranger* had weathered over 50 significant storms. The normal crew complement was between 80 and 85 people, although it could carry up to 100. The *Ocean Ranger* began work offshore on the Grand Banks of Newfoundland and Labrador for Mobil in November 1980 and in February 1982 was on its 4th well.

**1.3 The design of the *Ocean Ranger*.**

The structure of the *Ocean Ranger* was similar to many other semi-submersible drilling units operating around the world at the time. It was an eight column two pontoon configuration with an upper hull of two decks, supported by a framework of braces and trusses, see figure 1-1. However, there was one notable difference. The location of the ballast control room. It was located in the starboard column No.3. At drilling draft, it was 28 feet above mean sea level, or just 8 and a half metres above mean sea level. Representing a static not dynamic condition.

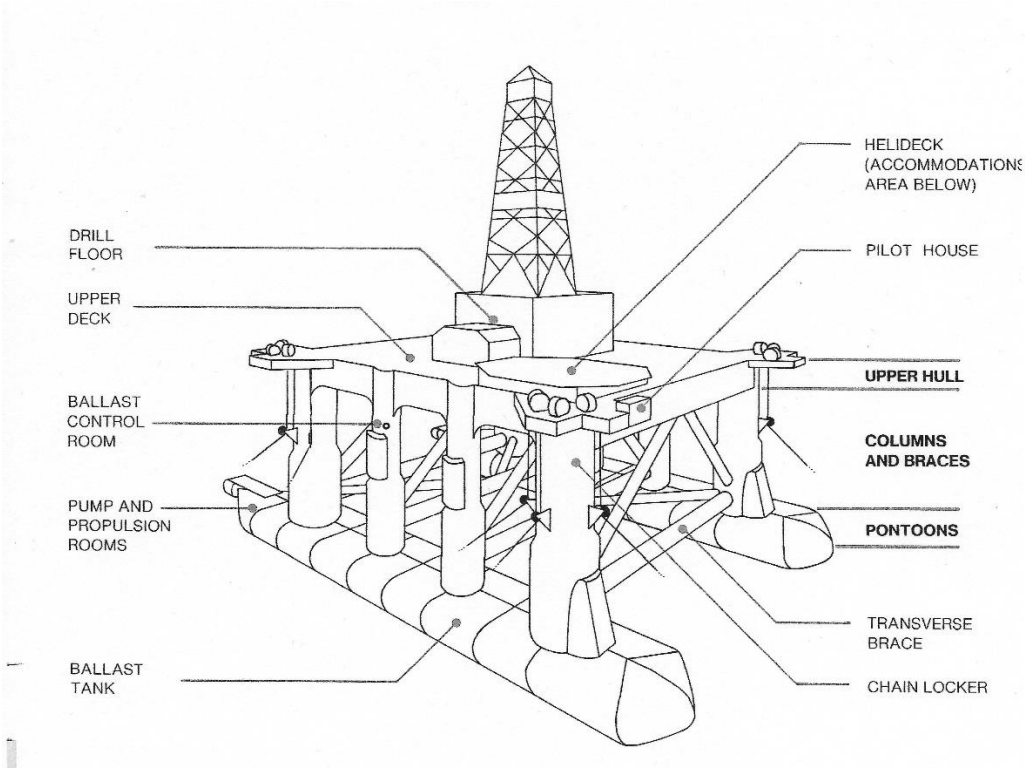


Figure 1-1 Ocean Ranger (Hickman, 1984)

It was important for drilling operations to maintain an even trim. So both pontoons contained 16 compartments or tanks with 12 used for ballast water, two for fuel oil and two for drill water, see figure 1-2. To maintain this even trim – valves on the ballast water tanks were pneumatically powered with electrical control from the ballast control room. Ballast water was transferred by pumps located in the aft pump room of each pontoon.

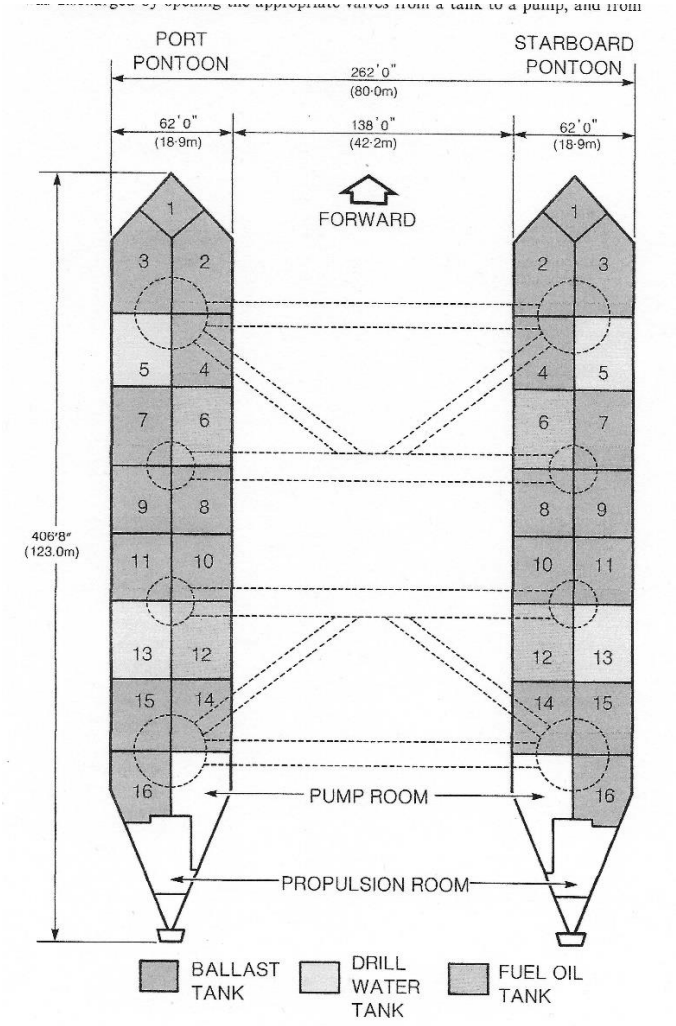


Figure 1-2 Ocean Ranger pontoon layout (Hickman, 1984)

The ballast control console had an upper vertical panel containing instruments which monitored elements of the ballast, drill water, and fuel oil systems. The lower panel was horizontal with a schematic diagram etched in it representing the tank layout, piping, pumps and valves in each of the port and starboard pontoons. Each valve was represented by an indicator light that showed red for closed and green for open. These indicator lights were set in pairs of push-button switches, labeled “open” and “close”, and the valve was

operated by pressing the appropriate switch. The pumps were each represented and operated by red “stop” and green “start” push-button switches with indicator lights. So the control console provided very limited information regarding the valves, and no information about the equipment condition. In the event of a failure in the control system, the operator could be presented with confusing or conflicting information. The original specification for the ballast control was a simpler all pneumatic system, but the subcontractor to the shipyard suggested the electric over pneumatic system.

Today such a change would trigger a management of change process to evaluate if new risks were being introduced. That wasn’t common in the era of the *Ocean Ranger* and it wasn’t done. It is significant and should be noted that other ODECO rigs had the simpler control system, the all pneumatic control system.

If electric power was lost, the valves were designed to fail-safe in the closed position. The electrician representing the owners during the construction knew that the solenoid valves could be opened by inserting a rod and closed by withdrawing the rod. Shipyard workers crafted brass rods which were used to commission the pneumatic system before the electric control panel was installed. The brass rods were then stored in a box behind one of the panels of the control console. There were no diagrams or instructions regarding the use of the rods to manually control the valves. The senior ballast control operator on the rig that night believed that inserting the rods would close an open valve during electrical failure. So the operators’ system knowledge was not only incomplete, it was wrong. With 18 of these rods inserted on the night of the loss, that belief would have serious implications.

To maintain position over the wellhead, the rig was moored to the seabed with 12 anchors. Three ran from each corner column with a combination of anchor chain and wire rope. For the storage of anchor chains, each column contained three chain lockers which were between watertight flats at the 35 foot and 70 foot elevations above the keel. These lockers were 38 feet in diameter. There were two upper deck openings leading into each chain locker; the first with an area of approximately 6 square feet at the top of the chain pipe, and the second with areas varying between 22.4 square feet and 28.3 square feet at the top of the wire box. The upper deck openings were 80 feet above mean sea level at drilling draft, see figure 1-3. Again a static not dynamic condition. The American Bureau of Shipping designated these openings as the first point above the waterline where seas could enter the hull if it were in a damaged condition. However, there were no coverings provided for these openings, no drainage system in the chain lockers, and no alarm system to indicate if flooding had taken place. Even if they knew the lockers were flooded, the only way to pump out water was by using portable pumps.

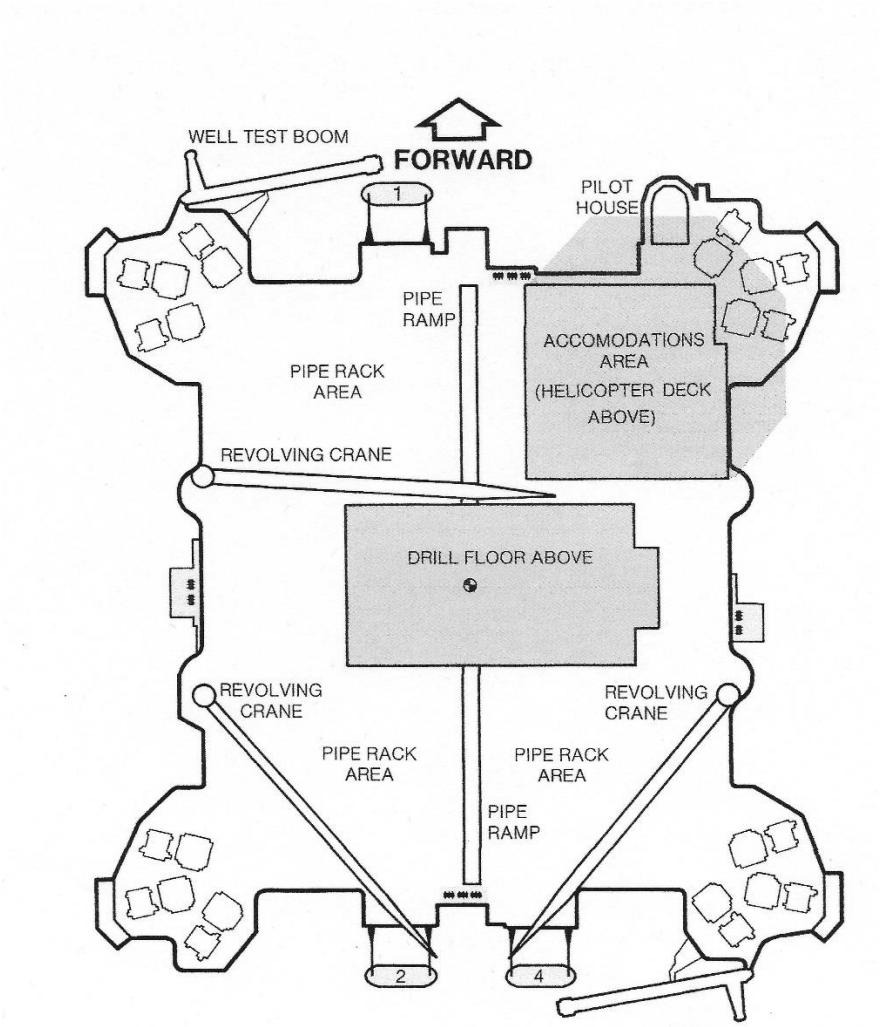


Figure 1-3 Ocean Ranger Weather deck layout (Hickman, 1984)

**1.4 What about training.**

The training policy and practice of ODECO reflected the general approach of the drilling contractors in the oil industry at that time; it emphasized on-the-job training, supplemented later with in-house courses for specific industrial duties. An inexperienced individual was hired as a roustabout, the general laborer in the oil industry. Through training on the job he could become familiar with the various activities on the drill floor and the general operation

of the rig. The *Ocean Ranger* had two ballast control operators each working a 12-hour shift. On paper they were supervised by the captain. ODECO did not require formal classroom training or testing for the ballast control operators. ODECO generally selected its ballast control operators from the drilling crew. If an individual showed the necessary interest and potential, he could train to become a ballast control operator. The stated training program of ODECO permitted a roustabout to train as a ballast control operator after 80 weeks' experience on the rig. After 24 weeks of training he could be placed in charge of the ballast control room. But policy and practice were at odds.

The actual practice was to identify prospective candidates by the interest they expressed in training for the position. After their regular 12-hour shift, the prospective candidate would be permitted to spend time in the ballast control room. No provision was generally made for them to work regular shifts as an understudy. When the candidate demonstrated to the experienced ballast control operator and to the captain that he had the necessary skills and understanding to operate the control console and to complete the daily calculations, his appointment as a full-time ballast control operator would be recommended to the senior rig manager. There were no courses nor tests to pass, either formal or informal, to determine their understanding of the system.

Three former ballast control operators gave evidence at the Commission. One testified that he responded to a newspaper advertisement and was appointed as a ballast control operator without any drilling or marine experience. After only several days of orientation he stood a normal 12-hour watch by himself in the ballast control room. Another had 28 weeks, and the third had 32 weeks, of roustabout experience before being appointed to the ballast

control room. The senior ballast control operator on the night of the disaster had 12 weeks roustabout experience and the junior operator had 40 weeks. This haphazard training appeared to be based on the assumption that the ballast system was fail-safe.

### 1.5 Early Warnings

We know from records, there was an incident with the ballast control system on February 6th, just a week before the disaster. The *Ocean Ranger* was taking on fuel oil and drill water. The ballast control operator was relieved by the captain so the operator could complete a routine inspection tour. Shortly after the loading of fuel oil had stopped, the operator was in the process of resetting the manually controlled fuel tank valves in the pump room. The rig developed a sudden 6-degree port heel.

The list occurred when the captain was at the ballast control console pumping out port ballast tank 14. The remotely controlled sea chest valve was also open causing a rapid ingress of sea water which the pumps couldn't counteract. The off-duty ballast control operator was called to correct the heel. The incident was considered serious enough that the crew prepared to go to lifeboat stations.

The toolpusher, the person in charge on the rig, severely criticized the captain for his actions. The captain agreed to not operate the ballast control console again. So the captain, the only person onboard who was trained in stability control and was formally qualified in stability control, did not understand the functioning of this ballast control system. Even his

knowledge of this ballast control system was incomplete. No effort was made to correct this deficiency.

As was common in the day, the incident review stopped with the blaming of a crew member. There was no review of the processes. No review of the procedures. No review of the manuals. No assessment of the orientation given the captain before he assumed responsibility for the ballast control system. The practice of blaming the employee would certainly lead to an incentive not to report incidents. The incident was not immediately reported to the Mobil office nor to the regulatory authorities. Evidence of a poor safety culture.

The *Ocean Ranger* did have an operating manual. It was referred to as the Booklet of Operating Conditions. However, the manual was not required reading for the ballast control operators prior to assuming their duties. Even if they had, the manual was deemed by the investigation to be difficult to read and lacking emergency control procedures. Testimony at the investigation by former crewmembers indicated that the manual had been produced for the purpose of fulfilling the regulatory requirement. If manuals are not produced with the needs and capabilities of the users in mind, their value is considerably diminished. Whatever the regulatory intent mandating the manual, it was seriously frustrated.

**1.6 What happened?**

On February 14th 1982, there were three drilling rigs operating on the Grand Banks of Newfoundland, but only the *Ocean Ranger* was lost. A fierce Atlantic storm was forecast for the area. The drilling rigs remained focused on drilling until conditions on the rigs reached operating limits for each rig. Environmental conditions intensified more quickly

and reached greater intensity than originally forecast. The crews prepared for the conditions as they had recalled from experience. The operations manual lacked guidance on how to prepare for extreme environmental conditions. No additional measures were taken to secure the ballast control room as it had never been damaged before.

The Commission determined the *Ocean Ranger* was still drilling at 4:30 p.m. on the afternoon of February 14th. The hang-off and disconnect process was started shortly after that time and was completed no later than 6:47 p.m. In a call at 6:47 p.m., the Mobil drilling foreman indicated they were having difficulty with compensator hoses that had become entangled in the derrick. He reported they were forced to shear the drill pipe in order to hang off. This would mean delays in getting back to drilling operations and would not be good news for a rig focused on drilling ahead. Developing plans on how to return to drilling as quickly as possible after the storm was likely the focus of attention of the leadership on-board the rig that evening.

The *Ocean Ranger* had disconnected due to weather conditions only once during its five-year operating history. That was just one month earlier, on January 16th. On that day, the maximum reported seas were 49 feet - the maximum swell 25 feet – the maximum reported pitch was 4.5 degrees – the maximum roll was 5.5 degrees with a heave of 22 feet. However, the *Ocean Ranger* did not deballast but maintained its 80-foot draft throughout that weather incident. Evidence indicated that the weather conditions and rig motions were not dissimilar on February 14th.

The *Ocean Ranger* had never previously de-ballasted because of storm conditions. There is no report that it did so that fateful night. So it was concluded that the rig had not de-ballasted from its 80-foot draft before a portlight broke in the ballast control room. It was the breaking of that portlight in the ballast control room that was the first link in the chain of events leading to the loss of the *Ocean Ranger* and all 84 people on board.

It was concluded that the portlight broke sometime between 7:45 and 8:00 p.m. Salt water soaked the public address and gas detection systems and spilled onto the ballast control console.

Testimony from former crew suggested that the failure of the portlight would not, of itself, be regarded of sufficient importance to report to shore. It would have been included as part of the next day's routine commentary on the equipment status. This may explain the complete absence of communication between the ODECO person in charge on the rig and shore-based ODECO personnel.

Similarly, when the shore based Mobil manager was first advised at 8:45 p.m. of the broken portlight he did not regard the event as significant, presumably because of the lack of concern expressed by the Mobil foreman onboard. During a later conversation at 10:00 p.m. he was again reassured that the *Ocean Ranger* was not in any difficulty as a result of the breakage. At no time was there any mention of damage resulting from the incident. This in spite of overheard VHF radio conversations that indicated damage to or malfunctioning of the public address system and gas detection panel, and issues with the ballast control panel itself.

In fact, when the toolpusher requested a status report shortly before 10:00 p.m., the ballast control operator replied that “everything was okay”. This was relayed by the Mobil foreman to the Mobil manager as “all systems are functioning normally.” The differences between the reported and actual conditions was attributed to an inaccurate assessment of the situation by the crew and to a lack of appreciation of the potential danger. The resulting lack of accurate and timely reports of the damage from those on board hampered the investigation of the loss. It also meant there was a great reliance on assumptions and deductions by investigators.

The conclusions regarding the effect of water on the equipment in the ballast control room were drawn from a number of sources. There were the VHF radio conversations overheard between 8:00 p.m. and 10:00 p.m. by personnel on the SEDCO 706, a nearby rig, as well as its standby vessel. There was the examination of the ballast control panel and switches recovered from the wreck. And there was the testing of new switches identical to those recovered. Of those people who overheard portions of the VHF radio conversations, no one sensed any degree of urgency or felt any concern. Indeed, nobody attempted to contact the rig to inquire about the problem. These conservations were all internal to the *Ocean Ranger.*

The susceptibility of the ballast control console and its components to sea water damage was a deficiency in its design. Had all the components been sealed and designed for a marine environment, the potential for water penetrating the switches would have been eliminated. The ballast control panel was designed to allow the operator to control the

valves and pumps by switches and to monitor their operation by the indicator lights. The damage to the panel affected the operation of both the monitoring and the control circuits. Had these functions been designed to operate separately, the potential for human error would have been significantly reduced.

The Commission concluded that if the crew had closed the deadlights, shut off the electrical and air supplies to the panel, cleaned up the sea water and glass, the *Ocean Ranger* and her crew would have survived the storm that night. However, the electrical supply to the panel was restored between 12:30 and 12:45 a.m. The reason for doing this will never be known with certainty. Whatever the reason behind the action, the restoration of power allowed short circuits in affected microswitches to open ballast valves in the port pontoon. Water flowed forward and the rig began to trim toward the bow.

Observing the trim, the ballast control operator probably removed power from the panel, thus closing any open valves. Before the removal of power, even if only minutes had passed, sufficient water would have entered the port pontoon to cause a port heel and probably a 4 or 5 degree trim to the bow. That trim combined with the pitch and roll in excess of 4 degrees caused by the prevailing sea and wind conditions gave a maximum forward inclination of 8 to 10 degrees.

Those are the figures reported by the Mobil drilling foreman at 1:00 a.m. However, the call was an alerting call only, with no reference to a Mayday or evacuation at that time. Another indication that whatever the problem, the crew still believed it could be isolated and rectified. The likely thought being that once power had been removed, any valves which

had been open would close, and the rig would appear to stabilize. Steps would then be taken to restore the rig to an even keel.

The obvious remedy would be to try to pump out the port bow tank or tanks, but the pumps were positioned all the way aft. Simply put, this was no longer possible as the height required to lift the water from the forward tanks exceeded the capacity of the pumps. The crew began threading the rods into the console. As crew members threaded rods into the console, they inadvertently opened more pontoon valves. It is likely that in an attempt to close the sea chest valve and other ballast tank valves was made, but that attempt would have actually opened the valve. Sea water would enter the manifold and into the forward ballast tanks. As the forward portion of the upper deck became lower, the chain locker openings would come within range of the largest waves. At this point, chain locker flooding would occur, accelerating the rate of forward trim.

At or before 1:09 a.m., the crew would have observed that despite pumping, closing both manual sea chest valves and "closing" the majority of ballast tank valves, the condition was worsening. At this point with no indication of what the pontoon valves were actually doing or notification of chain locker flooding, the crew would be at a loss to explain the increasing trim. They did finally realize that their efforts were not working.

The commission concluded that the key personnel on board the rig were unaware, up to the last hour, that a serious problem existed, and, when they became aware, they thought they could remedy it as they remedied the severe list on February 6th. When they began to realize, around 1:00 a.m., that the problem was beyond their ability to solve, they were

minutes away from abandoning the rig and unable to give adequate warning to those who might have helped them.

It was at 1:05 a.m. that their standby vessel, *Seaforth Highlander,* was finally called into close standby. It would be more than an hour before she would arrive because of the severe sea conditions. Whatever happened thereafter, happened quickly. At approximately 1:10 a.m. on February 15th, the *Ocean Ranger* began sending mayday signals. At approximately 1:20 a.m., the standby vessels from the other two rigs in the area were dispatched to the *Ocean Ranger*. At 1:30 a.m. the *Ocean Ranger*'s radio operator sent his final transmission. The crew was boarding the lifeboats.

Not all of the lifesaving equipment on board the rig was available to the crew at 1:30 a.m. The rig had by then developed a trim in excess of 15 degrees, with waves crashing over its bow, and the lifeboat located there would have been inaccessible. The only lifeboats accessible were the two located on the stern. The open truss construction of semisubmersible drilling rigs like the *Ocean Ranger* does not have a lee similar to conventional vessels. Under storm conditions the air gap between the surface of the sea and the deck of the rig made lowering of the lifeboats subject to violent swinging and possible impact damage from the rig's structure. We know that at least one lifeboat did manage to launch but was severely damaged and flooded. The *Alexander L. Kielland* another semisubmersible was lost two years earlier and had experienced similar lifeboat launching problems. Another design deficiency – the location and positioning of the lifeboats for static not dynamic conditions.

When the M/V *Seaforth Highlander* arrived at the location of the *Ocean Ranger* a flare alerted them to the location of a lifeboat. In addition to the lifeboat, the crewmembers also saw at least 20 men floating in the water. The M/V *Seaforth Highlander* came alongside and upwind of the lifeboat that held survivors. After the crew secured lines to the lifeboat, the lifeboat capsized with the loss of all on board. The efforts of the crewmembers of the M/V *Seaforth Highlander* to rescue the crewmen from lifeboat was considered to be all that was humanly possible under the circumstances. Notwithstanding their best efforts, the standby vessel crew was just not properly equipped for the job they were being asked to perform in the conditions that prevailed. Another deficiency – poorly equipped stand-by vessels and lack of training for their emergency response role.

The progressive flooding of the rig would have created an unstable situation and with the wave motion, the *Ocean Ranger* capsized and sank at approximately 3:15 a.m., February 15th 1982.

### 1.7 Conclusion

The story of the *Ocean Ranger* highlights a number of deficiencies in the operation of the *Ocean Ranger* and indeed drilling operations on the Grand Banks of Newfoundland and Labrador during the 1980s. Those deficiencies are commonly identified as design errors, lack of training, lack of adequate operating manuals and poor emergency response preparedness. These deficiencies don't however tell the whole story.

So re-examining this disaster in today's light with another 38 years of offshore experience provides further lessons. The story that begins to emerge as we review the investigation reports and listen to former workers of the *Ocean Ranger* disaster reveals the root causes related primarily to cultural issues, not just technical problems. While helpful in improving outcomes, regulations themselves do not ensure safety and may be counterproductive in their consequences. A complacent acceptance of rules and regulations may develop, and evolving technology that is applied may be only as good as the rule and the rule formulators. Those who argue for greater regulatory control ignore the ever-present human element. Human action is fundamental for interrupting the chain of events or minimizing their consequences. For effective human action, the actor must possess thorough knowledge of the process and emergency procedures and must apply that knowledge-based behavior. Cognitive science tells us the most natural mode of human discourse, storytelling, depends on causal knowledge and that in turn allows thinking to produce more effective action.

That major accidents are still happening, even in companies that have good safety standards, reveals the complexity of accident scenarios, which is difficult to fully explain even after investigations. It is a combination of rather low probability events that are facilitated by a series of technical, human, organizational, and societal factors. Thus, prevention of major accidents can only be effectively carried out through a holistic approach to the risk control issues including those technical, human, organizational, and societal factors. By integrating the holistic risk-focused approach into the management framework we can begin to stop learning safety by accident.

# Chapter 2 Precautionary Principle (PP) versus As Low As Reasonably Practicable (ALARP): Which One to Use and When

"The formulation of a problem is often more essential than its solution, which may be merely a matter of mathematical or experimental skills. To raise new questions, new possibilities, to regard old problems from a new angle requires creative imagination and marks real advances in science.", (Einstein & Infeld, 1938)

**Precautionary Principle (PP) versus As Low As Reasonably Practicable (ALARP): Which One to Use and When**

**Howard Pike[1], Faisal Khan[1]*, and Paul Amyotte[2]**

**[1]Centre for Risk, Integrity, and Safety Engineering (C-RISE)**

**Faculty of Engineering & Applied Science, Memorial University**

**St. John's, Newfoundland and Labrador, Canada, A1B 3X5.**

**[2]Department of Process Engineering & Applied Science**

**Dalhousie University, Halifax, Nova Scotia, Canada, B3H 4R2**

*** corresponding author: fikhan@mun.ca**

**Preamble**. This chapter has been published in the Journal of Process Safety and Environmental Protection, volume 137 (May 2020), pages 158 - 168. As primary author, I led the development of the framework, its implementation, and analysis of the results with the help of co-authors, Dr. Faisal Khan and Dr. Paul Amyotte. I have drafted the initial manuscript, which was reviewed and commented by co-authors.

## 2.0 Abstract

Safety and environmental risk go hand in hand with industrial development. However, it is unclear whether there is a linear or nonlinear relationship between risk and industrial development. Perhaps, it is case dependent. Some industrial endeavors such as offshore development, activities in a harsher environment, or development requiring new technologies (untested and untrusted technologies) may pose a higher risk (nonlinear) than

more conventional industrial development activities (e.g., petroleum refineries, petrochemical plants, pipeline transportation, and the like). Public perception plays a critical role in defining the risk versus development relationship. The public perception of risk is dependent on awareness and understanding of potential hazards and their likelihood of occurrence, and most importantly, effective communication of these along with the associated uncertainty. Public awareness can have a profound effect on the development of public policy, which in many cases is driven more by perception rather than by sound science. This paper sheds light on this crucial issue. It investigates two commonly used concepts of policy and decision-making, the Precautionary Principle (PP) and As Low As Reasonably Practicable (ALARP). The paper provides a clearer understanding of both approaches with an illustrative example. It proposes a process to help readers understand where and when PP versus ALARP would be most applicable.

The opinions and data presented here are based on the current study and relevant experience of the authors. The paper does not necessarily reflect the opinions of the authors' past or present employers nor correlate directly with previous projects on which the authors have worked.

**Keywords:** As Low As Reasonably Practicable (ALARP), Precautionary Principle (PP), Safety Decisions,

## 2.1 Introduction

The importance of the precautionary principle (PP) in the public review process cannot be ignored. Three public reviews of hydraulic fracturing in Atlantic Canada have used the principle in recommending, if not a moratorium, then a suspension of further development.

These recommendations resulted from elements of uncertainty of a range of issues related to the risk of unconventional oil and gas development. While the risk of suffering harm is an inescapable aspect of all human activity, loss of life, serious illness, and degradation of the environment are no longer acceptable consequences from any industrial development. Increased levels of awareness of environmental and development issues and greater engagement on the part of the public have led to a much keener interest in industrial risk management practices, policies, and effectiveness. Regulatory interventions and risk management use two widely recognized principles for risk reduction approaches: the "Precautionary Principle" (PP) and the "As Low As Reasonably Practicable" (ALARP) principle (TRB, 2018).

The public interest derives principally from notable public policy conflicts over industrial development believed to be hazardous or environmentally unfriendly and the implicit promise that we can keep technological risks thoroughly under control. This promise has driven an increased expectation for a society free of involuntary risks. However, risk as a concept perceived by the general public appears to be rather poorly understood. The word risk has become an emotionally charged word, used and abused repeatedly in the media and on the internet in ways that polarize discussions and create antagonism. The communication of risk to the public is a challenging task, made more so when trying to balance risks in one domain with benefits in another. All the progress and benefits that technology has brought in social development would not have been achieved if society were indeed to stop development at the first suggestion of any problem. The challenge is how to recognize the problem as an impending threat, to analyze the signs to identify the hazard, and then to manage the potential risk.

The management of risks associated with potentially hazardous industrial activities has been and continues to be the subject of considerable development in the range and extent of regulatory activity associated with the authorization of industrial activity (Melchers, 2001). If regulatory activity is to employ rational decision-making, it requires a clear and quantitative way of presenting risk so that it can be adequately weighed, along with all other costs and benefits. Risk analysis seeks to quantify risk as much as possible in terms not only of the probability of an event in time and space, but also the probability of a particular level of consequences. The scientist or professional engineer will readily admit that risks of a technical nature cannot be reduced to zero, but they can be reduced to very low values, from either or both aspects of probability and consequence, for almost all industrial activities. While risk assessment techniques help to measure the safety and environmental threat of a particular activity, evaluation methods use risk assessment techniques to assess the adequacy of the layers of protection provided for an activity. New approaches aim to reduce uncertainty over time through system monitoring that is iterative, structured, and systematic.

The definition of risk used in this paper incorporates the likelihood that a hazard will cause adverse effects, together with the measure of those effects. For this paper, two approaches to risk management are considered: the “Precautionary Principle” (PP) and the “As Low As Reasonably Practicable” (ALARP) principle. The paper explores the relationship between them with respect to risk management of industrial activity and how they can be better utilized. The primary objective is to encourage transparency and accountability in the application of risk management as embodied by the PP and ALARP to industrial activity to promote greater confidence in the risk management process.

## 2.2 Background of the Precautionary Principle (PP)

We have for generations been using the folk wisdom that "it is better to be safe than sorry" and "an ounce of prevention is worth a pound of cure", which embodies the precautionary approach or principle. The environmental debates of the 1970s and 1980s began expressing a precautionary approach to industrial development. In the early 1980s, the precautionary principle started to emerge in international law, most notably in the World Charter for Nature (UN, 1982), but it was not until after it was incorporated as "Principle 15" in the RIO Declaration (UNCED, 1992) that it achieved international prominence and acceptance. It has become a feature of close to one hundred international agreements and has been incorporated into scores of domestic environmental and public health laws worldwide (Tollefson & Thornback, 2008). However, different views exist of what precaution is, and the precautionary principle has different interpretations. The criticism that is most commonly raised is that the PP is unclear. It should be remembered that the precautionary principle is not a scientific hypothesis, theory, or methodology rule; rather, it is a principle for making practical decisions under conditions of scientific uncertainty (Resnik, 2003).

Sandin (1999) has analyzed the various definitions of the precautionary principle along four key dimensions: threat, uncertainty, action, and command. Under Sandin's analysis, threat refers to the nature of the imminent harm, particularly its seriousness and irreversibility, while uncertainty indicates our lack of knowledge as to whether and how this threat might materialize. Under most definitions of the principle, where both the threat

and uncertainty meet defined thresholds, an action obligation is triggered to consider cost-effective measures to prevent degradation of health or the environment. The command dimension designates the legal status of the action obligation to be taken, which may be framed in either mandatory or permissive language.

According to Sandin, a challenge to utilizing the precautionary principle lies in the imprecision with which the dimensions of threat, uncertainty, action, and command are typically framed (Sandin, 1999).

The UNESCO World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), has developed a working definition of the Precautionary Principle (PP), or Precautionary Approach, which goes some way to clarifying the imprecision and defining boundaries for its applicability (COMEST, 2005):

"When human activities may lead to morally unacceptable harm that is scientifically plausible but uncertain, actions shall be taken to avoid or diminish that harm. Morally unacceptable harm refers to harm to humans or the environment that is:

- threatening to human life or health, or
- serious and effectively irreversible, or
- inequitable to present or future generations, or
- imposed without adequate consideration of the human rights of those affected.

The judgement of plausibility should be grounded in scientific analysis. Analysis should be ongoing so that chosen actions are subject to review. Uncertainty may apply to, but need not be limited to, causality or the bounds of the possible harm.

Actions are interventions that are undertaken before harm occurs that seek to avoid or

diminish the harm. Actions should be chosen that are proportional to the seriousness of the potential harm, with consideration of their positive and negative consequences, and with an assessment of the moral implications of both action and inaction. The choice of action should be the result of a participatory process."

The precautionary principle can be a rational procedural vehicle for decision-making in the face of uncertainty, provided that it instructs us to take reasonable precautions to deal with plausible threats. Traditionally, where the principle has not been considered as part of a decision-making process, regulators have only taken risk into account when it rises to a relatively high standard of certainty (Tollefson & Thornback, 2008).

Where the principle is part of the regulatory process, a regulator is empowered and, in some instances obliged, to take it into account. Their response must be proportional to the risk and must adapt as knowledge of the risk becomes more certain. The Supreme Court of Canada's decision (2SCR241, 2001) in Spraytech is an illustration of how the precautionary principle can be applied, and established the case law for the use of the precautionary principle. In that decision, the Court decided that a by-law that severely restricted the use of pesticides was a valid exercise of the Town of Hudson's authority to adopt by-laws to secure the health and general welfare of the people. The ruling by the majority of the Court used the principle as a means to provide justification and context for the Town's concerns with respect to pesticides rather than providing the legal basis for the validity of the by-law.

The most common way the principle finds its way into regulatory process is through its implicit or explicit adoption in statutes. In Canada, the principle is found, in the preambles to Species At Risk Act (SARA), the Oceans Act, and the Canadian Environmental

Protection Act (CEPA), in the purposes section of the old Canadian Environmental Assessment Act (CEAA) (s. 4), in the mandate section of the new Impact Assessment Act Bill C-69 (s.6 (2)), and as a mandatory strategic management principle under the Oceans Act (s. 30). It is expressed as a relevant consideration in the exercise of administrative duties vested in the Government of Canada and its agencies under CEPA and CEAA. It is also slowly finding its way into provincial legislation.

Where the argument is that the principle should be used as an interpretive aid where the statute may be silent, it is not entirely clear which version of the principle should apply. This is an uncertainty that appears to cause significant regulatory discomfort. When the principle is viewed as little more than "common sense," at best it provides little decisional guidance and at worst promotes uncertainty and subjectivity. The principle needs to respect the discretion of elected decision-makers to make judgments about the public good (Tollefson and Thornback, 2008).

From early Canadian case law, some themes begin to emerge. Courts and tribunals have not concurred with claims that compliance with the PP requires regulators to defer approval for industrial activities wherever any scientific uncertainty about the nature or extent of the potential harm exists. The level of scientific uncertainty and the forms of scientific evidence to be relied on in the approval assessment, however, are unclear. Where there are diverging opinions among regulators and especially among government's scientific advisors as to the nature or extent of the harm, it would appear that the test is met. Regulators seem clearly to want compelling evidence that a proposed activity poses a serious risk to human health or the environment before concluding that the principle applies. Moreover, what level of that risk is necessary is unclear (Tollefson & Thornback,

2008).

The Health and Safety Executive in the United Kingdom has noted in their guidance that the quantum of risk can be evaluated by creating and evaluating credible scenarios (UKHSE, 2001):

"Uncertainty is overcome by constructing credible scenarios on how the hazards could be realised and thereby making assumptions about consequences and likelihood. The credible scenarios can range from a 'most likely' worst case to a 'worst case possible' depending on the degree of uncertainty. For example, by assuming that exposure to a putative carcinogenic chemical will cause cancer, the chemical becomes subject to a very stringent control regime".

If there is considerable uncertainty about the nature of the hazards and the likelihood of them causing harm, then successful management of risk in any industrial activity must satisfy the premise that anything present in an activity which 'presents the possibility of danger' is regarded as a 'hazard.' When that hazard may have consequences that may be irreversible and harmful, there is an overriding need to introduce control measures to address the hazards (UKHSE, 2001).

The credible scenarios developed would form the basis for a risk assessment. The response that is required by the precautionary principle will depend on the outcome of the risk assessment. The overarching goal of the response is proportionality - the more significant and likely the threat, the greater the degree of precaution required. Where uncertainty exists, a margin of error should be left so that serious or irreversible harm is less likely to occur (Tollefson & Thornback, 2008). The importance of continuing to monitor and analyze the chosen action based on operating experience, new evidence, and lessons

learned should not be forgotten. The Precautionary Approach has the objective of achieving lower and more acceptable levels of risks but "is not based on 'zero risks'," a risk scenario that is not reflective of human activity (COMEST, 2005).

### 2.3 Fundamentals of Risk Assessment

All industrial activities carry an array of benefits and risks. Risk assessment has evolved from major accidents associated with industrial activities - the same industrial activities that are created for our benefit to supply energy, food, and commodities. Risk assessment involves formal and systematic analysis of the sources of harm or hazards, the consequences of exposure to such hazards, and barriers that prevent or mitigate exposure of such hazards. Such assessments attempt to forecast how the future will turn out if a particular course of action or inaction is undertaken. Risk assessment provides a basis for making informed decisions related to health and safety and the environment. It should be recognized that risk cannot be completely eliminated, but it can be managed in such a way as to mitigate or reduce harm to the greatest extent practical. Risk reduction strategies are employed to reduce the risk to a tolerable level.

There are four generally accepted categories of risk reduction strategies, in order of preference: inherent, passive, active, and procedural (Crowl & Louvar, 2011). Inherent strategies identify and implement ways to eliminate or significantly reduce hazards, rather than to develop add-on protective systems and procedures. Inherent strategies can reduce risk but cannot eliminate risk. It is widely accepted that inherent strategies achieve their best effect when considered early in the life cycle of industrial activity. However, the strategy can be applied to reduce the risk of existing activities (Amyotte et al., 2018). There

are four actions recognized as describing inherent strategies; Minimize (intensification); Substitute (substitution); Moderate (attenuation and limitation of effects); and Simplify (simplification and error tolerance).

Passive strategies add barriers that do not require activation of any device. They will only perform as intended if they are not isolated from the activity they are designed to protect. They can be rendered ineffective by a lack of proper attention and care. Active strategies add shutdown systems to prevent accidents. Active strategies require event detection and device actuation to accomplish their intended function. Because they have moving parts that can fail when called upon to act, they must, therefore, be inspected, maintained, and tested regularly. Procedural strategies are the least effective way to deal with hazards in an activity. Nevertheless, procedures for tasks such as operations and maintenance are essential and are usually a regulatory requirement. It is therefore critical that procedures are correct, easy-to-understand, follow, and enforce.

The application of these strategies is often described as a series of layers of protection surrounding an activity (Crowl & Louvar, 2011). Layers of protection are necessary because it is unlikely that a single strategy alone will effectively reduce the risk from the hazards. Each layer adds further defenses from the danger, thus reducing the risk from the activity. Inherently safer designs make these layers of protection more reliable and robust. Active and procedural layers of protection require constant maintenance and management to ensure that they continue to function as designed. If they are not managed correctly, the protection systems will degrade and increase the risks to an unacceptable level. These

strategies are judged “acceptable” in the sense that there is no “undue risk.” What “undue risk” means remains unquantified, which brings us back to risk assessment.

Kaplan & Garrick, (1981) summarized the essence of a risk assessment as answering three questions; what can go wrong, how likely is it, and what are the losses or consequences? By answering those questions, they proposed a set of triplets which begins to define risk in terms of: an identified scenario, the probability of that scenario, and the consequence or damage of that scenario. The development of credible scenarios is a critical step in the risk assessment. Ruling out what is physically possible too soon could lead to erroneous conclusions. In the 1990s, the choice of a worst-case scenario versus a maximum-credible one was the subject of numerous studies (Khan & Abbasi, 2002). Scenarios can be developed by starting with the harm or undesired end state and proceeding as follows:

1. We answer the third question first by defining a set of harms or undesirable end states (adverse consequences), e.g., in terms of loss of life, serious illness, degradation of the environment, or loss of property.
2. For each end state, a set of events can be developed that are disturbances to normal operations which, if a barrier fails, can lead to the end state. These are called initiating events (IEs).
3. We answer the first question by generating accident scenarios using logic diagrams such as either Event or Fault Trees, or Bowties which identify sequences of events that start with an IE and end at an end state. These scenarios can consist of hardware failures, human error, process properties, and natural phenomena. They can include a characterization of the harm through qualitative or quantitative evaluation of the

nature of any adverse effects associated with biological, chemical, and physical agents that may be present.

4. We answer the second question by estimating the probabilities of these scenarios using engineering and mathematical techniques with all available evidence, primarily experience and expert judgment.
5. The accident scenarios can be ranked according to their risk characterization

If we are to judge how closely the estimated value relates or represents reality, we must identify, quantify, and characterize uncertainties in the risk characterization. Uncertainty is a measure of the 'goodness' of that estimate of risk, which is more than statistical error or inexactness of numbers. It is increasingly understood as a multidimensional concept stemming from the limitations of the assessment methods used, scarcity of data, ignorance, the use of assumptions, and limited social robustness of findings and methods. Uncertainty can manifest itself in different parts of the risk assessments such as context, system boundaries, indicator choice, model structure, parameters, and data. Uncertainty plays a critical role in the assessment of risk and its use in decision-making. Berner and Flage ( 2016) stated that assumptions are part of the foundation of a risk assessment. They argue that judgment of the assumptions and conservatism embodied due to uncertainty should be performed by the decision maker.

When discussing uncertainty, it is important to distinguish between aleatory (stochastic) and epistemic (knowledge related) uncertainty. Aleatory uncertainty refers to variation in populations, is typically measured using frequentist probabilities. Aleatory uncertainty is linked with the data, which can be improved by collecting more data or evidence to support

the data. Most engineering projects often suffer from aleatory uncertainty. Epistemic uncertainty refers to lack of knowledge about phenomena, usually translating into uncertainty about the parameters of a model used to describe some phenomenon or phenomena, is typically measured using subjective probability. Epistemic uncertainty is often challenging to address in the risk assessment. It requires deepening the knowledge and understanding of scientific or engineering principles. Although in many cases uncertainties can easily be distinguished, the two can occur combined due to inherent randomness. The uncertainty associated with analyzing the frequency of scenarios in probabilistic risk assessment increases with the challenging problem of data scarcity.

Paté-Cornell (1996) proposed six levels of treatment of both aleatory and epistemic types of uncertainty for risk analyses. Level 0 simply involves the detection of a potential hazard or of the different ways in which a system can fail, without attempting to assess the risk in any quantitative way, a zero risk approach. Level 1 does not involve any notion of probability and is based on the accumulation of worst-case assumptions and yields. Level 2 represents an attempt to obtain an evaluation of the worst possible conditions that can be reasonably expected (1) when there is some uncertainty as to what the worst case might be, or (2) when the worst case is so unlikely or infrequent that it is meaningless. Level 3 is characterized by a single point estimate which relies on a best estimate or on a central value, the mean, the median or the mode of the outcome distribution. While the mean is influenced by the dispersion of the distributions, it does not provide a sufficient description of the effects of uncertainties on the results. Level 4 relies on the probabilistic risk analysis process to obtain a distribution of the probabilities of different system states based on best

estimates of the models and parameter values. Level 5 allows the display of uncertainties about fundamental hypotheses by a family of curves. Since a full analysis and propagation of uncertainties is often a difficult and costly exercise, it should be done only if it is relevant to the risk management issue. Level 0, Level 1 or Level 2 are sufficient for decision making where there are no cost constraints when setting priorities. Aven and Zio ( 2011) have reviewed various methods to represent uncertainty along five main categories: the probabilistic analysis, probability bound analysis (combining probability analysis and interval analysis), imprecise probability (the robust Bayes statistics area), random sets (Dempster-Shafer belief functions), and possibility theory (a special case of the imprecise probability and random sets theories). They argue that a full risk uncertainty description is more than subjective probabilities and extends beyond the Bayesian approach. The Bayesian approach is discussed in the next paragraph.

Over the years, much has been learned on risk assessment and how to treat uncertainty, but relatively little of the new learning has become common practice. Kaplan & Garrick (1981) recognized early-on the uncertainty problem and launched the probability density of frequency concept. If data are collected on the failure frequency of a piece of equipment, one can build a distribution, $p(\lambda)$, and find a mean, median, mode, and variance. Data can be scarce, especially when it concerns a particular brand and type of equipment. One can also apply this reasoning on scenario and consequence. Kaplan & Garrick (1981), therefore, proposed the Bayes theorem stating that a prior probability distribution in which all existing background knowledge can be embodied, multiplied or intersected by a likelihood distribution of new evidence while normalizing the prior and likelihood co-

occurrence to a maximum probability of unity, yields an updated posterior distribution. The multi-stage use of Bayes theorem, formally called Hierarchical Bayesian Analysis (HBA) has more recently been applied to risk assessment as demonstrated in a few papers (El-Gheriani et al., 2017; Kelly & Smith, 2009; Khakzad et al., 2014; Yang et al., 2013, 2015), which outline further possibilities and applications.

For determining the probability of an event given data, classical statistics has the restriction that data shall be from the same population. Bayes' theorem allows the inclusion of data from similar equipment and plants and it merges and propagates aleatory and epistemic uncertainties. The uncertainty the Bayes model aggregates from prior and likelihood will be expressed through the variance and shape of the posterior. Because underlying background knowledge may contain uncertainty that cannot be expressed mathematically in one prior distribution, a type of prior sensitivity analysis, Robust Bayesian Analysis, applies systematic variations to determine the ranges of outcomes. The same could hold for the likelihood distribution. The principle of Bayes theorem is well known, but its use in the actual practice of risk assessment is still not common. Yet it is critically needed to deal with uncertainty (Pasman & Rogers, 2018).

A considerable number of major accidents have occurred according to scenarios that had been excluded as improbable. Risk assessments have an additional problem when dealing with low probability - high consequence events. Morally and practically, these events do not allow the luxury of a trial and error learning process. Then it is appropriate to invoke the `precautionary principle.' So, how can we make good decisions in risk management, or rather how can we make optimum decisions under uncertainty? Much has been written

about the topic and methods have been proposed in relation to economics and investment decisions. As previously mentioned, in the 1990s the choice of a worst-case scenario versus a maximum-credible one was discussed at length (Khan, 2001). However, what is physically possible should not be ruled out too soon. Analysis and lowering of the uncertainty will support decision making. A more credible threat may also stimulate resilience boosting measures (Kelly & Smith, 2009; Pasman & Rogers, 2018).

The scope of the assessment, which among other things defines the system boundaries, becomes very important. If we narrow the scope too far, we may ignore or introduce other hazards which could have the effect of decreasing overall safety and environmental protection. A wide view screen, rather than a narrow one, is indispensable for overall safety and protection of the environment (Kletz, 2005).

Important industrial activity decisions will always have proponents and opponents. Risk assessment results are afflicted with uncertainty and parties with opposing interests will fight in many forums to get a project accepted or not. Often when that fight gets into the public arena, such a project becomes a political bone of contention. Although the work procedure for a risk assessment sounds straightforward, the execution is usually somewhat problematic. We depend on assessments to support optimum decision making under uncertainty and must weigh the effort against the cost of the assessment. We want to look into the future, but predictive tools are fallible, and the prediction results are helpful but uncertain. All assumptions, data, models, model parameters, calculations, and statements in a risk assessment include uncertainties.

Uncertainty can arise from lack of or insufficient knowledge about events, system states, processes, and phenomena that factor into the estimation. Conventional risk models are not applicable to handle cases of high uncertainty because of their static character, insufficient knowledge base, and inadequate database. The integration of adaptive management and the ALARP principle produces a new generation of approaches called "Dynamic Risk Management." (Kalantarnia et al., 2009; Rathnayaka, 2015; Villa et al., 2016)

Adaptive management is a learning-based approach that involves the application of management in the spirit of experimental science to investigate how to manage more effectively (Williams et al., 2009). The underlying mechanism is to feed new information of outcomes back into the decision-making process so that engineering and environmental resources can be appropriately reallocated. Adaptive management is based on the recognition that there is a known high uncertainty about the system of interest and the necessity of using what is learned from the current management of resources to plan for future management.

Dynamic risk assessment and management is recognized as one of the new research trends of process safety and risk management development. Integration of Bayesian Network methods with many qualitative and quantitative risk assessment methodologies provides the capability to update and predict accident probabilities using new information or data collected during ongoing operation. Dynamic risk assessment methods can model the dynamic changes of hazardous conditions on highly complex technical and social systems, such as offshore drilling operations and production systems. The outcome of the assessment provides the real-time updated risk and better overall management of risk

through time. The use of dynamic risk assessment and management approaches helps to predict unusual situations and thus notify operators to take early actions to prevent accidents during operations. This way, rare events can be anticipated and avoided rather than relying on reactive safety measures.

### 2.4 ALARP (As Low As Reasonably Practicable)

The ALARP principle requires that those responsible for the industrial activity and, indeed, the public's safety, reduce risks to levels that are 'As Low as Reasonably Practicable.' As such, the principle involves effective recognition of the fact that, while in most circumstances risk can be reduced, beyond some point further risk-reduction is increasingly costly to implement (UKHSE, n.d.). The ALARP principle originated in the United Kingdom (UK). It is not a prescriptive risk management approach, but one that leaves considerable latitude to those responsible for the industrial activity to make effective decisions in deciding on the strategy to mitigate risks. The key element of the ALARP principle is the term "reasonably practicable." The first formal definition of 'so far as is reasonably practicable' was provided in the Court of Appeal judgment in Edwards v. National Coal Board, [1949] 1 All ER 743)(UKHSE, n.d.):

"'Reasonably practicable' is a narrower term than 'physically possible' … a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them."

The first introduction into UK law of the concept that industrial risks should be as low as reasonably practicable (ALARP) was in the 1961 Factories Act. The concept of "reasonably practicable" lies at the heart of the UK health and safety system. It is a key part of the general duties of the Health and Safety at Work Act 1974 and many sets of health and safety regulations and those of Local Authorities (UKHSE, n.d.).

Canadian Occupational Health and Safety legislation refers to the concept of a duty of care for stakeholders of industrial activity. All stakeholders are required to take every precaution reasonable in their circumstance to avoid harm. Their circumstances include their position, authority, knowledge, and understanding of the risk. The general concept is of having exercised reasonable care or Due Diligence in their actions, which is very similar in concept to that of the UK ALARP. The harm has to be reduced to as low as reasonably practicable.

The ALARP principle has been advocated as a fundamental approach to the setting of tolerable risk levels, particularly suitable for regulatory purposes. The approach sets an upper limit above which the risk must be reduced or the activity must stop, and a lower limit below which resources expended produce negligible risk reduction. The strategy is to reduce the risk as low as reasonably practicably to or below the lower limit. The critical words in ALARP are `low,' `reasonably' and `practicable.' Unfortunately, these are all relative terms - standards are not defined. `Reasonably' is also an emotive word, implying goodness, care, consideration, etc. What may be reasonable in some situations can be seen as inappropriate in others (Melchers, 2001). However, if the risk is above the maximum tolerable level, then the risk should be reduced or the activity giving rise to it discontinued whatever the cost.

What is the maximum tolerable level beyond which it is morally intolerable to impose risk? Flüeler & Seiler, (2003) have identified four different categories:

Category 1: voluntary risk exposure to satisfy one's desires, e.g., dangerous sports

Category 2: high degree of self-determination, direct individual benefit, e.g., car driving

Category 3: low degree of self-determination, personal benefit, e.g., working conditions

Category 4: involuntary, imposed risk exposition, no direct benefit, e.g., local residence near a hazardous installation.

The categories differ in the extent to which the individual is responsible for their exposure: participants in dangerous sports such as rock climbing are entirely responsible for their own exposure; on the other hand, if approval is granted to locate a hazardous facility in our neighborhood, there is little we can do about the risk, short of moving away. Flüeler & Seiler (2003) identify limits based on rates which Swiss society already accepts ranging from $10^{-3}$ to $10^{-5}$ as being appropriate. For Category 4 risks, which are risks imposed and providing no direct benefit for the person exposed, the limit of tolerability is one death in 100,000 ($10^{-5}$); for Category 2 risks, such as driving a car, the limit of tolerability is one death in 1,000 ($10^{-3}$). For Category 1 risks, for people who voluntarily engage in dangerous sports, it may be inappropriate to specify any risk level as intolerable, it could be argued, that would be an unwarranted interference with freedom of choice.

There are obvious financial/economic implications "`reasonable practicability' is not defined in legislation but has been interpreted in legal cases to mean that the degree of risk can be balanced against time, trouble, cost and physical difficulty of its risk reduction measures. Risks have to be reduced to the level at which the benefits arising from further risk reduction are disproportionate to the time, trouble, cost and physical difficulty of

implementing further risk reduction measures" (Melchers, 2001). Baybutt ( 2014) concludes that the ALARP principle provides a useful framework within which to establish risk tolerance criteria. That Cost-Benefit analysis is useful in deciding what risk reduction measures are warranted for the costs involved. With the use of a disproportionate factor in the analysis the concept of reasonably practicable is formalized and provides justification and transparency for decisions made. In another paper it is argued that the ALARP principle should be interpreted in a dynamic way, meaning that the interpretation of the grossly disproportionate criterion ranges from one extreme, where decisions are made with reference to expected values, to another extreme, in which the cautionary principle is given special weight with no reference to cost-benefit (cost-effectiveness) analyses (Abrahamsen et al., 2018).

The implementation of ALARP in risk management also requires the continuous analysis of the benefits gained from risk reduction versus the resource to be consumed to ensure that risk is lessened to the lowest level. It is clear that financial implications are recognized in pursuing any safety or environmental improvement to demonstrate ALARP. It is possible, in principle, to apply formal cost-benefit techniques to assist in making a judgment(s) of this kind. This assumes that all factors involved can be converted to monetary values. Unfortunately, there are considerable difficulties and implied value judgments in evaluating monetary values for both benefits and costs. This problem is particularly acute for the analysis of hazardous facilities where the value of human life, the cost of suffering and deterioration of the quality of life and deterioration of the environment may play a significant role in the analysis (Melchers, 2001).

Risk tolerability cannot be divorced from broader issues in the community. It is intertwined

in matters such as risk perception, fear of consequences, and their uncertainty, as well as various other factors that influence and change society with time. Societal risk tolerability can change very quickly when there is a major industrial accident. The implication for the ALARP approach might well be what was considered sufficiently `low' for a particular type of industrial activity before an `accident' might not be regarded as sufficient for another similar industrial activity after an accident. There will be very considerable societal and political pressures for changing the acceptance criteria (Melchers, 2001).

In most situations, deciding whether the risks are ALARP involves a comparison between the barriers those responsible for the industrial activity have in place, or are proposing, and the measures that would typically be expected in such circumstances, i.e., recognized standards or relevant good practice. "Good practice" is defined in the general UK ALARP guidance (UKHSE, n.d.) as "those standards for controlling risk that are judged and recognised as satisfying the law, when applied to a particularly relevant case appropriately." In the United States, the Occupational Safety and Health Administration, OSHA, requires Recognized and Generally Accepted Good Engineering Practice (RAGAGEP).

Where the situation is complex, it may be difficult to decide based on good practice alone. More analysis of the situation and processes will be required. There may also be some cases, for example, a new technology, where there is no relevant good practice. In such cases, good practice should be followed as far as it can be, and then consideration given to whether there is any more that can be done to reduce the risk. If there is more that can be done, then the presumption is that those responsible for the industrial activity will implement these further measures, but this needs to be confirmed by going back to first

principles to compare the risk with the sacrifice involved in further reducing it (UKHSE, n.d.).

But there are some instances, often in high hazard industries or where there is a new technology with potentially serious consequences, where the situation is less clear-cut. In such cases, a more detailed comparison would need to be undertaken. The trouble is that risk and sacrifice are not usually measured in the same units. In these instances, a more formal Cost-Benefit Analysis (CBA) may provide additional insight to help come to a judgment (UKHSE, n.d.).

ALARP does not represent zero risks. We have to expect the risk arising from a hazard to be realized sometimes and for harm to occur, even though the risk is ALARP. This is an uncomfortable thought for many people, but it is inescapable. Of course, we should strive to make sure that those responsible for the industrial activity reduce and maintain the risks ALARP, and we should never be complacent. Nevertheless, we have to accept that risk from an activity can never be eliminated unless the activity is stopped. This also goes some way to explaining why risk assessments feed into contingency planning.

### 2.5 Summary and Illustrative Example

We have seen that the Precautionary Principle can be expressed in terms of four dimensions: threat, uncertainty, action, and command. If an activity presents a plausible threat yet there is scientific uncertainty about the threat, this should not preclude taking reasonable action before harm occurs to avoid or diminish the threat. We have also seen that threats can be evaluated by creating and evaluating credible scenarios. The credible scenario can be analyzed using risk assessment techniques.

Risk assessment is a model of decision-making used in making choices about environmental hazards and public health and safety. Risk assessment can be expressed in terms of answering three questions; what can go wrong, how likely is it, and what are the losses or consequences? Answering these questions identifies the hazard, consequences, and risk of an activity. Risk assessment classifies and describes those various risks and looks at the implementation of barriers to reduce the probability of occurrence. Any additional response to a threat can be identified. In figure 2-1 the dimensions of the Precautionary Principle: threat, uncertainty, action, and command have been aligned with the elements of risk management: hazard, risk, barrier, and response. Control measures are also shown in figure 2-1 as interventions in the process with prevention principles applied to the identified threat or hazard, prevention principles applied to the risk and response principles after realization of a scenario to minimize the consequences.

If there is considerable uncertainty about the nature of the hazards and the likelihood of them causing harm, then successful management of risk in an industrial activity must satisfy the premise that anything present in an activity which ‘presents the possibility of harm’ is regarded as a ‘hazard.’ The use of risk assessment to determine the required control measures, ensures that for hazards surmised to have consequences that may be irreversible and harmful, there is an overriding need to introduce control measures to address the hazards. Figure 2-2 illustrates how control measures may be included in a credible scenario.

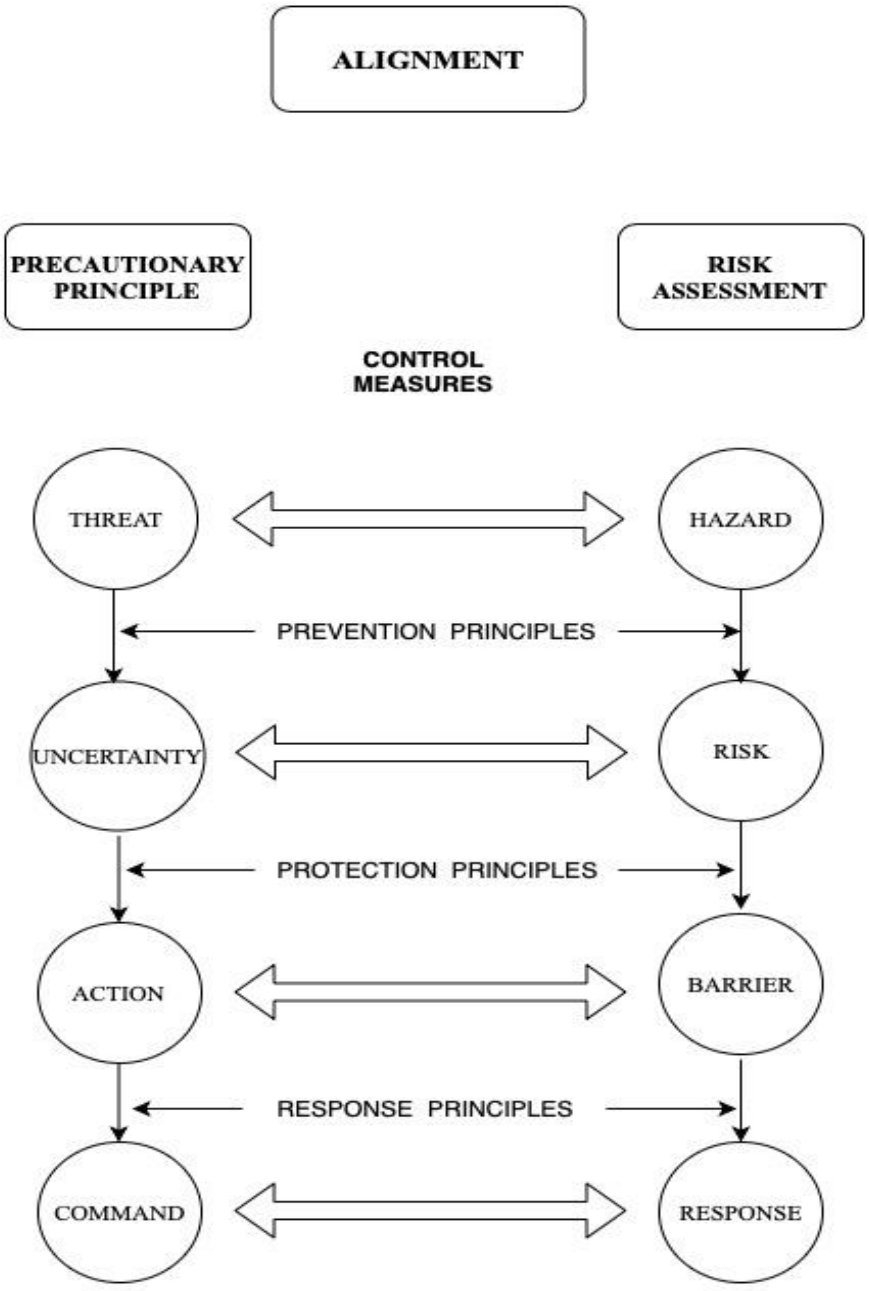


Figure 2-1 Alignment of precautionary principle and the risk assessment process

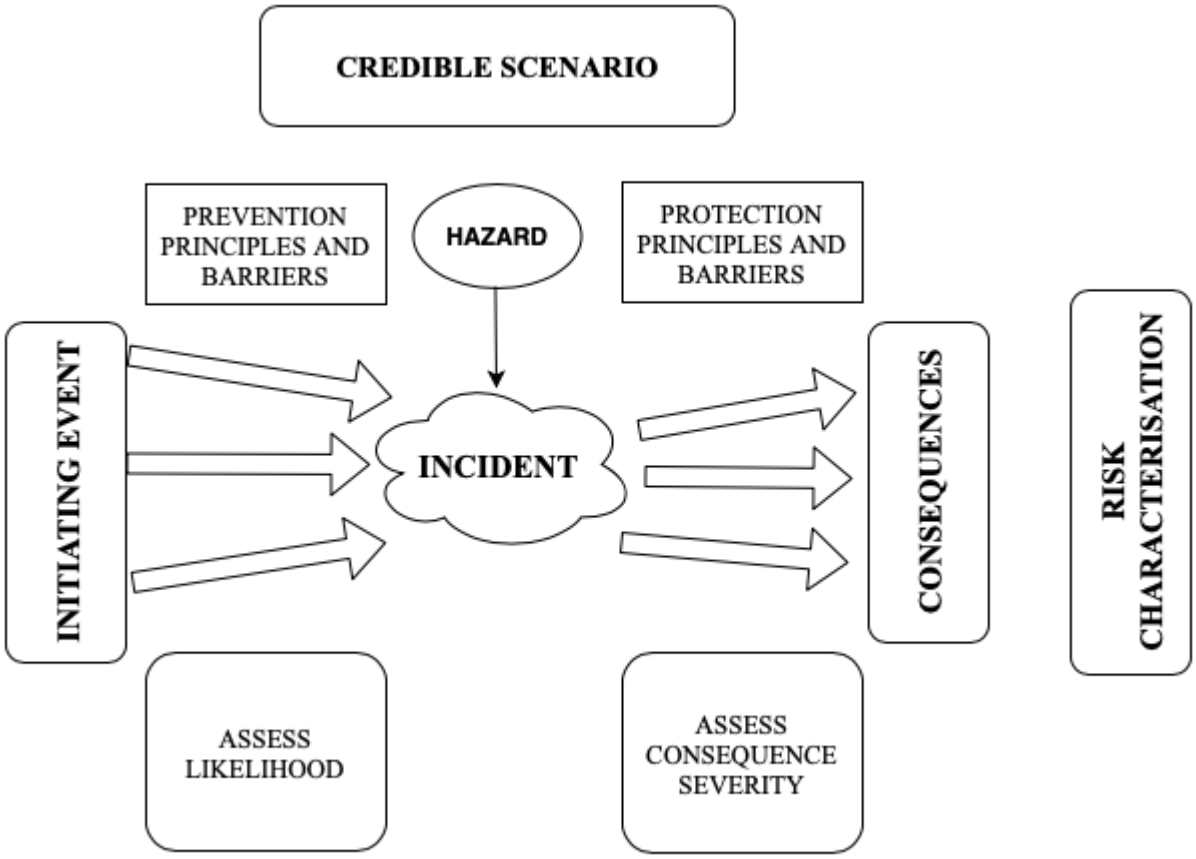


Figure 2-2 Illustration of the credible scenario Bowtie

Once the risks have been characterized we can assess if the precautionary principle applies or we have enough information to apply the ALARP principle. The importance of continuing to monitor and analyze the chosen action based on operating experience, new evidence, and lessons learned should not be forgotten. If the risk is above the maximum tolerable level, then the risk should be reduced or the activity giving rise to it discontinued whatever the cost. This approach is illustrated in the decision flow diagram given in Figure 2-3.

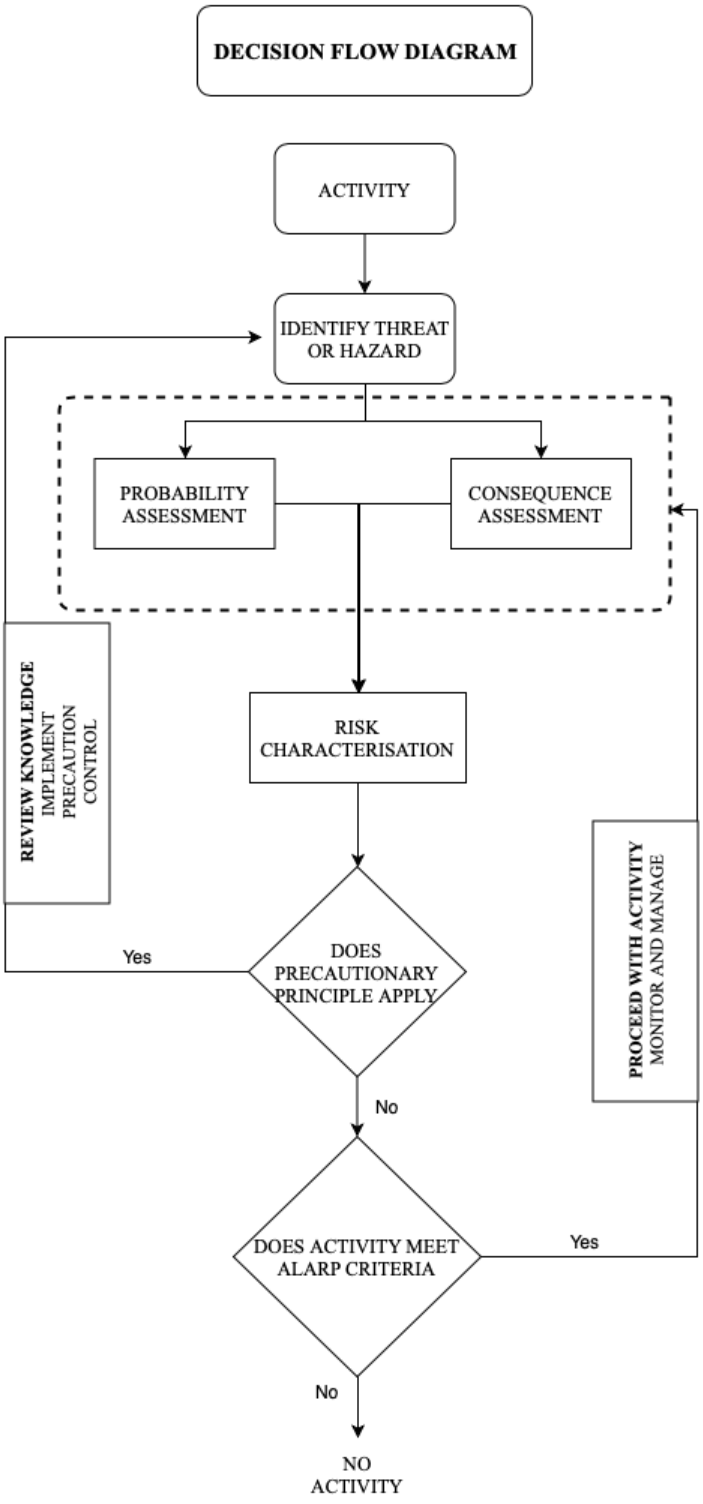


Figure 2-3 The decision-making flow diagram

Uncertainty is a measure of how well the risk has been estimated, which is more than statistical error or inexactness of numbers. It is understood as a multidimensional concept involving quantitative and qualitative dimensions stemming from the limitations of the assessment methods used, ignorance, the use of assumptions, and limited robustness of findings and methods. Uncertainty can manifest itself in different parts of risk assessment such as context, system boundaries, indicator choice, model structure, parameters, and data. Risk assessment is not a purely objective endeavor because it employs normative assumptions about the types of hazards we are concerned about, the level of risk that is acceptable, as well as the distribution of benefits and harm. One of the problems hampering our ability to implement the risk assessment model relates to a lack of agreement about the measurements used in the model and how to compare them. Should we measure in terms of dollars lost/saved, lives lost/saved, species lost/saved or some other measure of value? Even if we agree on some set of values to use in the model, we might still not agree on how to prioritize those values. In risk assessment, usually, the rare event comes with the most severe consequence and is therefore central in acceptability discussions.

It is clear that for the trustworthiness of a risk assessment we must learn to think in terms of uncertainty intervals to obtain bounds on estimated conditional randomness (aleatory) in probability and consequence. The effect of assumptions on results and the epistemic uncertainties in possible scenarios, models and data need to be identified. The latter can result in an unforeseen accident with consequences due to an unrecognized threat. On the positive side is the development of dynamic quantitative risk assessment methods, to

monitor changes in the risk and therefore safety level of the activity over time. Periodic reviews and site inspections assure the risk from an activity is ALARP.

As a simplified example, consider a scenario where one has a business opportunity in a city that is just under 200 km from home; under ideal conditions, it would be a two-hour drive. However, it is the middle of winter, the weather forecast is for snow flurries, and there is the possibility of ice patches on the highway. One has three basic options: take the trip, don't take the trip, or take reasonable precautions for the trip. There are a variety of different possible outcomes, but basically, they are arriving safely or not arriving safely. The worst possible outcome would be dying as the result of an accident or getting stranded in the snow. One does not know the probability of dying on this trip, but it is not zero. Basing the decision on the worst possible outcome (death), one would not likely make the journey. If death is treated to be just as probable as any other outcome, then that would negatively impact the assessment of the option of taking the trip. One would assume that it would not be rational to apply either of these principles to the decision because they deny both opportunities and benefits. All human activity requires individuals and society to assume some level of risk. So it is not unreasonable to think that to obtain opportunities in life, one must take some risk. The application of the precautionary principle to this scenario can offer sound advice and would counsel one to make the journey, but to take precautions to avoid threats that are plausible and irreversible but also preventable, such as death. Death can be regarded as a severe possibility even if one does not consider it as even minimally probable. One does not have to regard death as probable in order to take reasonable precautions to avoid a collision. What risk reduction strategies should be employed? Would risk assessment help with the analysis of this scenario.

The application and use of risk reduction strategies are meant to reduce the risk associated with a system. For example, seatbelts secure the vehicle occupants and reduce the risk of injuries in a collision. Defensive driving techniques are taught to introduce the skills necessary to minimize the risk for the task of driving a vehicle. Some risk reduction strategies for this scenario are summarized in Table 2-1.

Table 2-1 Risk Reduction Strategies

| | |
|---|---|
| Inherent strategies | Explore the possibility of video conferencing or teleconferencing |
| Passive strategies | Vehicle suitably sized for highway driving<br>Vehicle crumple zone<br>Use of winter tires<br>Wide shoulders on the road<br>Clear sight lines<br>Divided highway |
| Active strategies | Seatbelts<br>Airbags<br>Anti-lock brake system (ABS)<br>Electronic stability control (ESC)<br>Lane departure alert<br>Auto braking |
| Procedural strategies | Defensive driving techniques |

As a risk assessment method, the bowtie model and diagram is used to analyse and communicate risk scenarios. The essence of the bowtie consists of plausible risk scenarios

around a specific hazard and incorporates the risk reduction barriers. The interaction between the driver, the vehicle, and the road is a complex system that may be influenced by a multitude of factors in each of these components. Many of these risk factors are statistically associated with accident rates, but the relative significance of the various risk factors is difficult to assess and validate. Also, many of these risk factors can influence the accident outcome. The bowtie diagram can be used (Figure 2-4) to illustrate the complex reality of road transportation as simply as possible without losing the context.

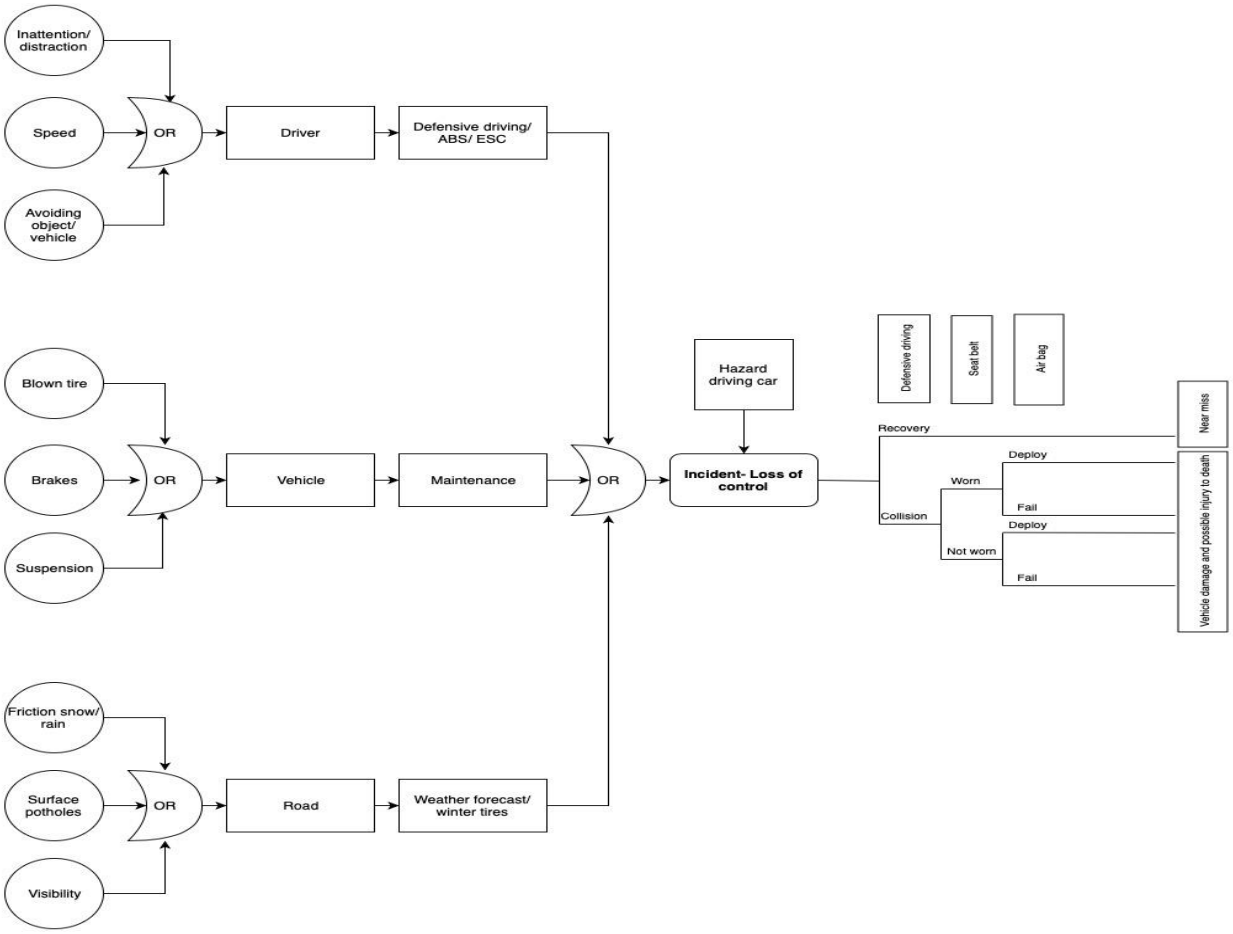


Figure 2-4 The Bowtie accident model for the road transportation scenario

The central hazard in the Bowtie diagram has been identified as driving a car. The occurrence of a road traffic accident can be seen as an unwanted event in the transportation system. Losing control over the vehicle has been defined as the undesired critical event that may be caused by either the driver, the vehicle, or the road or its environment or any combination of them. The consequence analysis involves the formation of the event tree model. Once control over the vehicle has been lost, there are two things that might happen – either regaining control over the vehicle, or being involved in a collision. To regain control of the car, the procedural risk reduction strategy of defensive driving techniques is

employed and the active risk reduction strategies could be employed: ABS (anti-lock braking system) and ESC (electronic stability control). If these fail, there would be a collision. To mitigate the effects of a crash, seatbelts are worn, and the headrest should be set to the correct height. Also, modern vehicles have airbags and are designed with crumple zones to dissipate the energy to lessen the impact on the occupants of the vehicle.

The number of people killed or injured in road traffic accidents depends primarily on the factors of exposure, accident rate and injury severity. Exposure to the risk of a road accident is usually referred to as the amount of travel, i.e., vehicle kilometers or the number of people exposed. The accident rate is the risk of a road accident per unit of exposure, and serves as an indicator for the probability of accident occurrence. The higher the accident rate, the higher the likelihood of an accident on a given trip of a given length. While statistics for the road in this scenario are not available, Transport Canada does publish Canadian motor vehicle traffic collision statistics; Table 2-2 shows the casualty rates for 2017, Table 2-3 shows the percentage of fatalities and serious injuries by road user class for 2017, and Table 2-4 the number of collisions by location for 2017. There is no reason to believe that these statistics would not be representative of the road in this scenario.

Table 2-2 Casualty rates – 2017 (Transport Canada, n.d.)

| | **Per 100,000 Population** | | **Per Billion Vehicle-Kilometres** | | **Per 100,000 Licensed Drivers** | |
|---|---|---|---|---|---|---|
| | **Fatalities** | **Injuries** | **Fatalities** | **Injuries** | **Fatalities** | **Injuries** |
| **Canada** | 5.0 | 421.9 | 4.8 | 404.9 | 7.1 | 595.6 |
| **NL** | 6.1 | 516.8 | 6.0 | 513.0 | 5.4 | 463.7 |
| **PE** | 9.2 | 406.5 | 9.1 | 403.7 | 12.7 | 561.0 |
| **NS** | 4.9 | 505.8 | 4.0 | 414.5 | 6.5 | 667.5 |
| **NB** | 6.6 | 353.3 | 5.7 | 307.6 | 9.0 | 484.3 |
| **QC** | 4.3 | 438.8 | 4.6 | 475.5 | 6.4 | 659.1 |
| **ON** | 4.1 | 362.2 | 4.0 | 357.1 | 5.8 | 513.9 |
| **MB** | 5.5 | 940.6 | 4.9 | 844.4 | 8.1 | 1,390.2 |
| **SK** | 8.6 | 390.7 | 6.8 | 311.1 | 12.5 | 566.8 |
| **AB** | 7.1 | 401.0 | 4.8 | 273.1 | 9.5 | 539.4 |
| **BC** | 5.7 | 437.4 | 6.9 | 523.5 | 7.9 | 605.3 |
| **YT** | 18.2 | 694.2 | 10.3 | 392.1 | 24.0 | 913.9 |
| **NT** | 6.7 | 224.6 | 7.2 | 241.0 | 11.5 | 382.3 |
| **NU** | 0.0 | 60.5 | 0.0 | 575.0 | 0.0 | 411.6 |

Table 2-3 Percentage of fatalities and serious injuries by road user class – 2017 (Transport Canada, n.d.)

| **Road User Class** | **Fatalities** | **Serious Injuries** |
|---|---|---|
| Drivers | 53.5 | 48.9 |
| Passengers | 16.9 | 17.6 |
| Pedestrians | 15.4 | 14.3 |
| Bicyclists | 2.0 | 4.6 |
| Motorcyclists | 10.4 | 12.4 |
| Not Stated/Other | 1.8 | 2.2 |
| **Total** | **100.0** | **100.0** |

Table 2-4 Number of collisions by location – 2017 (Transport Canada, n.d.)

| **Location** | **Fatal** | **Personal Injury** |
|---|---|---|
| Urban | 746 | 81,938 |
| Rural | 908 | 28,013 |
| Not stated | 25 | 2,528 |
| **Total** | **1,679** | **112,479** |

Urban includes:

1. Metropolitan roads and streets and other urban areas, or
2. A speed limit at the collision site of 60 km/h or less.

Rural includes:

1. Primary or secondary highways, as well as local roads, or
2. A speed limit at the collision site exceeding 60 km/h.

While these statistics are informative, they do not tell what the risk of making the 200 km road trip or 400 km return trip would be. We can use a random occurrence model to determine the probability; this would mean we consider road travel as a discrete random

variable with only two outcomes that can occur at any location along the road. The cumulative distribution function (CDF) denoted as $F_X(x)$ for a potential accident will be:

$$F_X(x) = P(X<=x) = 1- e^{- \lambda x} \quad (1)$$

Where P is probability and X is the distance traveled before the first occurrence of the event, a collision, which implies no occurrence or collision in distance *x*. The mean value of the distance to the first collision, X, can be shown to be $1/ \lambda$. The average rate of occurrence is denoted by $\lambda$. From Table 2-2 the Transport Canada data for the province of Newfoundland and Labrador, $\lambda$ is $6.0 * 10^{-9}$ vehicle-kilometers of being involved in a collision involving a fatality and $5.1 * 10^{-7}$ vehicle-kilometers of being involved in a collision involving an injury. Therefore, the probability of being involved in a collision with a fatality during a 400 km road trip would be $2.4 * 10^{-6}$, and the probability of being involved in a collision with an injury is $2.1 * 10^{-4}$. These probabilities are representative of the risk involved in this scenario but contain a number of uncertainties.

The data in Table 2-2 from Transport Canada is inclusive of fatalities from more than just the driver of the vehicle. From Table 2-3, we see that the fatalities and injuries are for those inside the vehicle and outside. So the driver would be a smaller population of the overall data statistic. Therefore, the probability of being injured or dying would be lower than has been calculated. From Table 2-4 we can see there is a greater chance of being killed in a rural location which includes highway driving rather than an urban area where speeds are lower.

If this journey is considered a Category 2 risk, where there is a high degree of self-determination and direct individual benefit, the limit of tolerability is one death in 1,000 ($10^{-3}$), and the risk is ALARP. If this journey is considered to be a Category 3 risk, where the trip is required for employment and there is implied low degree of self-determination but with personal benefit, the limit of tolerability is one death in 10,000 ($10^{-4}$) and is still acceptable. This does not mean that all reasonable risk reduction strategies should not be taken, such as those recommended by Transport Canada for winter driving:

1. Get vehicle ready in the fall for winter.
2. Install four matching winter tires.
3. Pack an emergency kit.
4. Learn and practice winter driving techniques before they are needed.
5. Plan trips and check road and weather conditions.
6. Remove all snow from vehicle before each trip.
7. Ensure extra travel time in bad weather.
8. Avoid using cruise control on slippery roads.
9. Travel with a fully charged cell phone.
10. Slow down and wear seatbelt at all times.

While we have not discussed the environmental footprint of a 200 km drive, it is safe to assume that the carbon footprint of one vehicle on a trip of 400 km return is hardly noticeable. However, the footprint of millions of vehicles and road trips representing billions of vehicle-kilometers is a significant contribution. Just like road fatalities, hardly

anybody notices the footprint of a single journey, and we have come to accept routine traffic as the cost of living in the modern world.

This example may seem straight forward but as we begin to assess the factors that lead to a safe journey we can see how uncertainty can creep into the assessment of the likelihood of a collision. The example has demonstrated that the PP and ALARP can be used as viable principles in the decision making process under conditions of uncertainty.

**2.6 Conclusion:**

All human activity requires individuals and society to assume some level of risk. The precautionary principle is seen principally as a way to deal with a lack of scientific certainty. Often, we find ourselves in a situation where the available scientific evidence allows for more than one tenable interpretation. Scientific consensus about many contemporary risks is unlikely to be achieved in a reasonable timeframe given the complexities and uncertainties faced. Consequently, science cannot be expected to provide ultimate authoritative answers about causality, nature, magnitude, and probability of many contemporary risks. The adoption of robust, transparent and accountable approaches towards the various aspects of risk and uncertainty can be identified as one crucial means of regaining public confidence in regulatory decision-making.

For any industrial activity that could have serious and harmful consequences and when there is significant scientific uncertainty about either the nature and magnitude of the consequences or likelihood of occurrence of these consequences or both, the Precautionary Principle would be the appropriate approach to be applied. If there is sufficient experience with operations and consequently known uncertainty, it is more suitable to use the ALARP

approach. The knowledge and scientific proofs can only be developed if we proceeded with the industrial activity with caution while utilizing a strong safety culture and proactively monitoring for risk. The ALARP approach provides the framework to understand the current state and to cautiously move forward monitoring and updating knowledge as it is being developed. Application of the ALARP approach through both cautious and preventive operations would help to better understand and minimize the likelihood of occurrence, or consequences of potential risks or both.

Dynamic risk management methods that provide for monitoring and updating the risk provide a practical approach that would help to enhance the inherent safety of industrial activity by providing better overall management of risk over time.

## Summary and Conclusions

The story of the *Ocean Ranger* highlights a number of deficiencies in the operation of the *Ocean Ranger* and indeed drilling operations on the Grand Banks of Newfoundland and Labrador during the 1980s. Those deficiencies are commonly identified as design errors, lack of training, lack of adequate operating manuals and poor emergency response preparedness. These deficiencies don't however tell the whole story.

So re-examining this disaster in today's light with another 38 years of offshore experience provides even further lessons. The story that begins to emerge as we review the investigation reports and listen to former workers of the *Ocean Ranger* disaster reveals the root causes related primarily to cultural issues, not just technical problems. While helpful in improving outcomes, regulations themselves do not ensure safety and may be counterproductive in their consequences. A complacent acceptance of rules and regulations may develop, and evolving technology that is applied may be only as good as the rule and the rule formulators. Those who argue for greater regulatory control ignore the ever-present human element. Human action is fundamental for interrupting the chain of events or minimizing their consequences. For effective human action, the actor must possess thorough knowledge of the process and emergency procedures and must apply that knowledge-based behavior. Cognitive science tells us the most natural mode of human discourse, storytelling, depends on causal knowledge and that in turn allows thinking to produce more effective action. When we tell stories about the past – we can learn. When we tell stories about the future – we can predict. And when we tell stories about the present

– we analyze the situation. All of this can help identify causes and foresee consequences to produce better risk assessments.

That major accidents are still happening, even in companies that have good safety standards, reveals the complexity of accident scenarios, which is difficult to fully explain even after investigations. It is a combination of rather low probability events that are facilitated by a series of technical, human, organizational, and societal factors. Thus, prevention of major accidents can only be effectively carried out through a holistic approach to the risk control issues including those technical, human, organizational, and societal factors. By integrating the holistic risk-focused approach into the management framework we can begin to stop learning safety by accident.

All human activity requires individuals and society to assume some level of risk. The precautionary principle is seen principally as a way to deal with a lack of scientific certainty. Often, we find ourselves in a situation where the available scientific evidence allows for more than one tenable interpretation. Scientific consensus about many contemporary risks is unlikely to be achieved in a reasonable timeframe given the complexities and uncertainties faced. Consequently, science cannot be expected to provide ultimate authoritative answers about causality, nature, magnitude, and probability of many contemporary risks. The adoption of robust, transparent and accountable approaches towards the various aspects of risk and uncertainty can be identified as one crucial means of regaining public confidence in regulatory decision-making.

For any industrial activity that could have serious and harmful consequences and when there is significant scientific uncertainty about either the nature and magnitude of the

consequences or likelihood of occurrence of these consequences or both, the Precautionary Principle would be the appropriate approach to be applied. If there is sufficient experience with operations and consequently known uncertainty, it is more suitable to use the ALARP approach. The knowledge and scientific proofs can only be developed if we proceeded with the industrial activity with caution while utilizing a strong safety culture and proactively monitoring for risk. The ALARP approach provides the framework to understand the current state and to cautiously move forward monitoring and updating knowledge as it is being developed. Application of the ALARP approach through both cautious and preventive operations would help to better understand and minimize the likelihood of occurrence, or consequences of potential risks or both.

Dynamic risk management methods that provide for monitoring and updating the risk provide a practical approach that would help to enhance the inherent safety of industrial activity by providing better overall management of risk over time.

**Recommendations**

This work can be further improved by focusing on;

- One of the challenges for risk assessment is data scarcity. Additional data maybe collected by re-examining investigations of significant offshore disasters, Alexander Kielland, Piper Alpha and Exxon Valdez. The upcoming fortieth anniversary of these disasters provides an opportunity to re-examine the lessons to be learnt from these disasters and re-tell their stories.

- With the upcoming fortieth anniversary of one of the worst industrial disasters, Bhopal, provides another opportunity to re-examine the lessons to be learnt from this tragedy and re-tell its story.
- Precautionary Principle and As Low As Reasonably Practicable are perceived to be two very different and unrelated principles. Further examples or stories can be developed to further demonstrate how these principles are related and when to use them.
- Major accidents keep occurring that seem preventable and that have similar systemic causes. By re-examining a series of accidents from one company the evolution of risk assessment, the challenges of learning from accidents, and additional insight to systemic factors can be demonstrated, for example Exxon with the *Exxon Valdez*, Esso Longford gas plant and the refinery in Torrence California.

# Bibliography and References

2SCR241. (2001). *114957 Canada Ltée (Spraytech, Société d'arrosage) v. Hudson (Town) - SCC Cases (Lexum)*. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1878/index.do

Abrahamsen, E. B., Abrahamsen, H. B., Milazzo, M. F., & Selvik, J. T. (2018). Using the ALARP principle for safety management in the energy production sector of chemical industry. *Reliability Engineering and System Safety*, *169*(January 2017), 160–165. https://doi.org/10.1016/j.ress.2017.08.014

Amyotte, P. (2014). An Editor's perspective on giants and disasters. *Journal of Loss Prevention in the Process Industries*, *32*, 466–467. https://doi.org/10.1016/j.jlp.2014.11.006

Amyotte, P., Irvine, Y., & Khan, F. (2018). Chemical safety board investigation reports and the hierarchy of controls: Round 2. *Process Safety Progress*, *37*(4), 459–466.

Baybutt, P. (2014). The ALARP Principle in Process Safety. *Process Safety Progress*, *33*(1), 36–40. https://doi.org/10.1002/prs.11599

Berner, C., & Flage, R. (2016). Strengthening quantitative risk assessments by systematic treatment of uncertain assumptions. *Reliability Engineering and System Safety*, *151*, 46–59. https://doi.org/10.1016/j.ress.2015.10.009

COMEST. (2005). *The Precautionary Principle*. https://unesdoc.unesco.org/ark:/48223/pf0000139578

Crowl, D., & Louvar, J. (2011). *Chemical Process safety - Fundamentals with Applications* (third). Pearson Education, Boston MA.

Einstein, A., & Infeld, L. (1938). *The Evolution of Physics*. Cambridge University Press, London UK.

El-Gheriani, M., Khan, F., Chen, D., & Abbassi, R. (2017). Major accident modelling using spare data. *Process Safety and Environmental Protection*, *106*, 52–59.

Flüeler, T., & Seiler, H. (2003). Risk-based regulation of technical risks: Lessons learnt from case studies in Switzerland. *Journal of Risk Research*, *6*(3), 213–231.

Hickman, T. A. (1984). *Royal Commission on the Ocean Ranger Marine Disaster; Report One: The Loss of the Semisubmersible Drill Rig Ocean Ranger and its crew*.

Hickman, T. A. (1985). *Royal Commission on the Ocean Ranger Marine Disaster; Report Two: Safety Offshore Eastern Canada*.

Hopkins, A. (2014). Issues in safety science. *Safety Science*, *67*, 6–14.

Kalantarnia, M., Khan, F., & Hawboldt, K. (2009). Dynamic risk assessment using failure assessment and Bayesian theory. *Journal of Loss Prevention in the Process Industries*, *22*(5), 600–606.

Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. *The Annals of Occupational Hygiene*, *1*(1), 11–27.

Kelly, D. L., & Smith, C. L. (2009). Bayesian inference in probabilistic risk assessment-The current state of the art. *Reliability Engineering and System Safety*, *94*(2), 628–

643.

Khakzad, N., Khan, F., & Paltrinieri, N. (2014). On the application of near accident data to risk analysis of major accidents. *Reliability Engineering and System Safety*, *126*, 116–125.

Khan, F. (2001). Use maximum-credible accident scenarios for realistic and reliable risk assessment. *Chemical Engineering Progress*, *97*(11), 56–64.

Khan, F., & Abbasi, S. (2002). A criterion for developing credible accident scenarios for risk assessment. *Journal of Loss Prevention in the Process Industries*, *15*(6), 467–475.

Kletz, T. A. (2005). Looking beyond ALARP - Overcoming its Limitations. *Process Safety and Environmental Protection*, *March*, 81–84.

Mannan, M. S., & Waldram, S. P. (2014). Learning lessons from incidents: A paradigm shift is overdue. *Process Safety and Environmental Protection*, *92*(6), 760–765. https://doi.org/10.1016/j.psep.2014.02.001

Melchers, R. E. (2001). On the ALARP approach to risk management. *Reliability Engineering and System Safety*, *71*(2), 201–208.

Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M., & Cozzani, V. (2012). Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management. *Risk Analysis*, *32*(8), 1404–1419. https://doi.org/10.1111/j.1539-6924.2011.01749.x

Pasman, H., & Rogers, W. (2018). How trustworthy are risk assessment results, and what can be done about the uncertainties they are plagued with? *Journal of Loss Prevention in the Process Industries*, *55*, 162–177.

Rathnayaka, A. K. F. (2015). Methods and models in process safety and risk management: Past, present and future. *Process Safety and Environmental Protection*, *98*, 116–147.

Resnik, D. B. (2003). Is the precautionary principle unscientific? *Studies in History and Philosophy of Science Part C :Studies in History and Philosophy of Biological and Biomedical Sciences*, *34*(2), 329–344.

Sandin, P. (1999). Dimensions of the precautionary principle. *Human and Ecological Risk Assessment (HERA)*, *5*(5), 889–907.

Silva, E. C. (2016). Why are major Accidents still occurring? *Process Safety Progress*, *35*(3), 253–257.

Sloman, S., & Fernback, P. (2017). *The knowledge illusion: why we never think alone*. Riverhead Books.

Throness, B. (2014). Some Safety Aspects on the Design of Sparger Systems for the. *Process Safety Progress*, *33*(2), 115–123. https://doi.org/10.1002/prs.11635

Tollefson, C., & Thornback, J. (2008). Litigating the Precautionary Principle in Domestic Courts. *Journal of Environmental Law and Practice*, *19*, 33–58.

Transport Canada. (n.d.). *Canadian Motor Vehicle Traffic Collision Statistics: 2017 -*

*Transport Canada*. Retrieved May 10, 2019, from http://www.tc.gc.ca/eng/motorvehiclesafety/canadian-motor-vehicle-traffic-collision-statistics-2017.html

TRB. (2018). Designing safety regulations for high-hazard industries. In *Transportation Research Board - Special Report* (Issue 324). National Academies Press. https://doi.org/10.17226/24907

UKHSE. (n.d.). *Risk management: ALARP at a glance*. Retrieved May 15, 2019, from http://www.hse.gov.uk/risk/theory/alarpglance.htm

UKHSE. (2001). *Reducing risks, protecting people*. https://www.hse.gov.uk/risk/theory/r2p2.pdf

UN, 1982. (1982). *A/RES/37/7. World Charter for Nature*. https://www.un.org/documents/ga/res/37/a37r007.htm

UNCED. (1992). *A/CONF.151/26 (Vol. I) REPORT OF THE UNITED NATIONS CONFERENCE ON ENVIRONMENT AND DEVELOPMENT*. https://www.un.org/documents/ga/conf151/aconf15126-1annex1.htm

USCG. (1983). *United States Coast Guard Marine Board of Investigation: MODU Ocean Ranger, Capsizing and sinking in the Atlantic Ocean on February 15, 1982 with multiple loss of life*.

Villa, V., Paltrinieri, N., Khan, F., & Cozzani, V. (2016). Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. *Safety Science*, *89*, 77–93.

Williams, B. K., Szaro, R. C., & Shaprio, C. D. (2009). *Adaptive Management: The U.S. Department of the Interior Technical Guide*.

Yang, M., Khan, F. I., & Lye, L. (2013). Precursor-based hierarchical Bayesian approach for rare event frequency estimation : A case of oil spill accidents. *Process Safety and Environmental Protection*, *91*(5), 333–342.

Yang, M., Khan, F., Lye, L., & Amyotte, P. (2015). Risk assessment of rare events. *Process Safety and Environmental Protection*, *98*, 102–108.