University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/specialization: **Offshore Technology / Risk management**	Spring semester 2012
Writer: **Nwokocha Chigozie Cyril**	………………………………… Signature of writer
INSTRUCTOR/SUPERVISOR **Terje Aven UiS**	
Title of Master's Thesis: **COMPARISON OF THE SAFETY FACTOR APPROACH AND THE RISK-BASED APPROACH**	
Credit (ECTS) :	
Key Words: *safety factor approach, risk-based approach, probability, risk assessment, uncertainties, inherent safety, risk analysis, safety reserve*	Pages : 54 + Attachments/others ……………………. Stavanger, June , 2012

COMPARISON OF THE SAFETY FACTOR APPROACH AND THE RISK-BASED APPROACH

Master Thesis by

Nwokocha Chigozie Cyril

Thesis submitted in partial fulfillment of
the requirements for the degree of
Master of Engineering

Faculty of Science and Technology
Department of Mechanical and Structural Engineering and Materials Science
University of Stavanger
15.06.2012

ACKNOWLEDGEMENTS

This thesis is submitted in partial fulfillment of the requirements for the Master of Science degree at the University of Stavanger (UiS), Norway.

I wish to express my sincere thanks to my supervisor Professor Terje Aven for helping me develop an idea/topic that interests me and for his support and guidance throughout the period of this thesis.

I also wish to express my gratitude to all who helped me with the suggestions that has contributed to making my thesis a good job.
My sincere gratitude also goes to the members of staff at the UIS library for their help during this thesis.

I also wish to express my gratitude to all my family members especially my wife and my kids, as well as my friends, for their support.

Finally, I wish to thank God for seeing me through during the period of this master thesis.

ABSTRACT

Safety is at the Centre of most human endeavor. The safer a system, process, technology, or service is the easier and faster it gets embraced by the people. In order to ensure the safety of people, environment and the asset of stakeholders, different experts have adopted various approaches or measures which will reduce risk and maintain high safety level.

The aim of this thesis is to compare two of these approaches, the so-called safety factor approach and the risk-based approach, and also to present and discuss some integrated approaches in which the safety factor and risk-based approach are combined.

There are many advantages of using the safety factor and/or the risk-based approach in engineering design and many researchers have tried to combine both approaches with a view to harnessing the benefits inherent in using the approaches separately. These different measures which have been used by some experts to combine the benefit of the two approaches will be discussed but the detailed discussion with applications and computations will be subject for future work. The basic idea behind the integration of the approaches will be presented with simple example and recommendation will be given on which approach to adopt.

Keywords: *safety factor approach, risk-based approach, probability, risk assessment, uncertainties, inherent safety, risk analysis, safety reserve etc.*

Table of Contents

ABBREVIATIONS

ASET - Available safe egress time

RSET - Required safe egress time

SLS - Serviceability Limit State

ULS - Ultimate Limit State

FLS - Fatigue Limit State

PLS - Progressive collapse Limit State

WSD – Working Stress Design

ASD – Allowable Stress Design

LRFD - Load Resistance Factor Design

HAZID- Hazard identification studies

HAZOP- Hazard operability studies

QRA – Quantitative risk assessment

JHA – Job hazard analysis

FMEA – Failure mode and effect analysis

FMECA – Failure mode, effect and criticality analysis

FAR- Fatal accident rate

AIR – Average individual risk

ALARP – As low as reasonably practicable

RBD – Risk Based Design

RBT – Risk based testing

RBI – Risk based Inspection

PSF – Probabilistic Sufficiency factor

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

1 INTRODUCTION

This chapter is aimed to introduce the background and the aim of this thesis, as well as an outline of the contents.

1.1 Background

Due to global financial meltdown, most companies are trying to implement or adopt measures to reduce their expenses while maintaining the integrity of their plant and operations. In different fields of engineering, there is an increased use of the probabilistic risk assessment approach as a means of proposing the safety measures that has to be in place to reduce or eliminate potential hazards although most experts have argued on a different approach where probability is replaced by uncertainty.

Because probabilities are rarely known with certainties, the use of probability risk assessment approach has some uncertainties inherent in it. It suffers from the tuxedo fallacy because it does not consider uncertainties that lack adequate probabilities.

Information from the probabilistic risk assessment can serve as input for decision or policy makers, so an understanding of the uncertainties in this approach is very crucial.

The safety factor (safety margin) approach is also used to provide safety and reduce the likelihood of accidents. The safety factors can be found in different standards or regulations and they can serve as the minimum (or maximum) requirement in any situation where they are used. The safety factor approach is progressively being replaced in many disciplines by the risk-based approach but it is still very important in structural engineering and in toxicology.

Irrespective of the approach adopted in achieving a desired or recommended safety level, the possibility of human error and hence uncertainty can never be underestimated.

1.2 Aim of the Thesis

The purpose of this master thesis is to compare the use of safety factor approach and the risk-based approach and also present/discuss an approach which combines both safety factor and risk-based methods. General overview of both approaches will be done with a view to understanding them better and also the potential benefits/shortcomings of using them will be analyzed.

Because the probabilistic risk assessment approach is used increasingly in different areas of engineering and safety factors are prescribed in different standards, a comparison of the two approaches is necessary although the aim of both approaches is to ensure safety and reduce the probability of accidents.

This master thesis will in addition to the above, present and discusses different frameworks for integrating the two approaches because they are both important in reducing hazard.

1.3 Thesis outline/content

The first chapter of this thesis shall contain introduction, background knowledge, and aim of the thesis and the outline of the contents.

In the second chapter, the safety factor approach will be discussed. This discussion shall include- an overview of the approach, categories of safety factor, applications of safety factor in various disciplines, rule-of-thumb for calculating the safety factor, safety factor in standards, safety factor and design methods and potential benefits of the safety factor approach.

In the third chapter, a discussion of the risk-based approach is done and it includes- an overview of the approach, basic concepts in risk analysis and risk management, applications of the approach, potential benefits of the risk-based approach etc.

In the last chapter, the safety factor and risk-based approaches are compared and different platform to integrate the two approaches are presented with discussions. Recommendation on which approach to use is done and this is followed by the conclusion.

CHAPTER 2

2.1 OVERVIEW OF THE SAFETY FACTOR APPROACH

Safety factors are used to prevent failures or limit the consequences of failure in various disciplines example- in toxicology, in engineering, in finance, etc.

There are different terminologies used for the safety factor in various disciplines but the philosophy behind their applications is the same and their major purpose is to prevent failure of a system.

Some of these terminologies which have been used and are still being used for safety factor in various disciplines or applications are- safety margin, factor of safety, uncertainty factor, safety reserves, uncertainty margin, etc.

Since the origin of human species, safety factors/margin has been in use and different professions apply it in various ways, for instance, builders usually add additional material to their construction works, the extra strength offered by the additional material helps to ensure that the construction work is safe irrespective of the loads that are applied to it.

In 1860s, the German rail road engineer, A. Wohler recommended a factor of two for tension. [Randall, 1976] When driving, drivers are told to keep a safe distance between them and the car in front of them. In air transport, safety factors are also used extensively in providing needed safety in the air and this is achieved by making use of minimal distance to keep the airplanes apart in the air.

In fire safety engineering, 'safety margin describes the time buffer between the necessary time to escape from a fire and the time to untenable condition is reached in the building, or if considered, a construction or a tunnel, all barriers and safety measures taken into account'.[Alf Reidar N, 2011]

In toxicology, safety factors are used in order to ensure that the drug provided for consumption are safe and would not have adverse effect on the person administered with it.

In medicine, surgeons make use of the idea of safety factor when performing surgical procedure on patient with cancerous tumor. Areas of the cells close to the tumors can be removed in order to prevent spreading of the cancerous cells.

Depending on the discipline where it is applied, safety Factor can be defined in different ways but their underlying ideas are the same. In most fields of its application, safety factors are usually constant values which are imposed by law, standard, custom, contracts or specification and structures or systems must conform or exceed the safety factors before they are approved for usage by the authorities. The safety factor can be viewed as a measure of reliability of the system or design where it is applied.

There are distinctions which can be made about the safety factor- first, when it is calculated, the calculated value can be viewed as the realized safety factor and secondly, when it is viewed as a requirement by law or the authority, it can be regarded as the required safety factor, also known as the design safety factor or the design factor.

Safety factor can be viewed as a functional approach where the use of a numerical constant is applied. Addition of a constant to our desired value or multiplication of our value by a constant can be used to modify technological or physiological variables in the direction of safety.

Because the variables which we apply as safety factor are used in order to cope with uncertainties, many authors have argued that it is more appropriate to use the term-uncertainty function or uncertainty factor because the safety factors do not necessary give rise to safety.

‘Most commonly, a safety factor is defined as the ratio between a measure of the maximum load not leading to failure and a corresponding measure of the applied load. In some cases, it may instead be defined as the ratio between the estimated design life and the actual service life. In addition to safety factor, the related concept of safety margin is used in several contexts. Safety margin are additive rather than multiplicative; typically a safety margin in structural engineering is then defined as capacity minus load’ [N. Doorn and S.O. Hansson, 2011]

Because it can be used as a measure of a system’s reliability and the lower limit is prescribed by the standards, codes or regulations, most engineers try as much as possible to apply this in their design and construction works. Safety factor is how much the designed material would actually be able to withstand but the design factor is what the material is required to be, in order to withstand. The safety factor should be chosen such that it meets or exceeds the design factor although this may result in additional cost or maybe excessive weight of some structures.

For ductile materials, safety factor is usually checked against yield and ultimate strengths. The use of safety factor does not mean that the structure is safe; rather there are other factors which determine the safety of the structure in any given situation.

Safety factors are meant to compensate for five major types of failures:

(1) Higher loads than those foreseen,

(2) Worse properties of the material than foreseen,

(3) Imperfect theory of the failure mechanism in question,

(4) Possibly unknown failure mechanisms, and

(5) Human error (e.g., in design) [Moses 1997]

The first two of the above failures can be assigned some probability, although this can be more or less uncertain. They refer to variability of empirical indicators of the likelihood for failure to occur. On the other hand, the last three failures are difficult to assign meaningful probabilities because they refer to eventualities or surprises and so they are highly uncertain.

'In order to provide adequate protection, a system of safety factors will have to consider all the integrity-threatening mechanisms that can occur. For instance, one safety factor may be required for resistance to plastic deformation and another one for fatigue resistance. Also different loading situations may be taken into account, such as permanent load ("dead load"; that is, the weight of the building) and variable load ("live load"; that is, the loads produced by the use and occupancy of the building); the safety factor of the latter being higher because of higher variabilities. Similarly, components with widely varying material properties (e.g., brittle materials such as glass) are subject to higher safety factors than components of less variable materials (e.g., steel and metallic materials). Geographic properties may be taken into account by applying additional wind and earthquake factors. Design criteria employing safety factors can be found in numerous engineering standards and building codes' [N. Doorn and S.O. Hansson, 2011] and these are written by engineers working with different professional bodies and the major aim is to provide an adequate safety level at an affordable or reasonable cost.

2.1.1 SIMPLE ILLUSTRATION OF THE SAFETY FACTOR

Because of their importance and usage in different disciplines like in structural engineering, toxicology, designs etc., an understanding of this concept can be illustrated by using the following:

1) In fire safety engineering, safety margins are defined as the time buffer between available safe egress time (ASET) and the required safe egress time (RSET).

SAFETY MARGIN = ASET – RSET

ASET is the time from when the fire starts to when we have untenable conditions in the escape routes occur. RSET is measured from when fire starts to all occupants are relocated or have been evacuated to a safe place [Alf Reidar N, 2011]. Both ASET and RSET are found in national codes and international standards.

Safety factor (called safety margin in this context), is basically the time we need to get to safety from the time we have a fire.

2) Safety factor is used to reduce the chance of failure of a structure by applying the needed safety factor to different members of the structure that are safety critical. If a beam for instance is designed to carry a load of at most 20N and a safety factor of 2 was prescribed, the beam must be made to have strength of at least 40N. Because the safety factor is given by:

$$safety\ factor = \frac{actual\ strength}{required\ strength}$$

Division of 40N by 20N will give us the needed safety factor of 2. However, if a heavier load is to be applied to the beam, say 60N, the safety factor criteria will not be fulfilled, the beam may break. In order to meet the criteria in this case, more materials (resources) will be needed to make the beam to have strength of at least 120N.

Because different materials have different failure modes, several safety factors may be required in designing different parts of a structure which contains different material.

‘An example of this is an elevator cable.

1. The cable might fail by elastically extending too far, or fail due to metal fatigue.

2. The failure criterion for extension might be related to modulus of elasticity and a factor of safety less than 2.0 might be appropriate.
3. For metal fatigue, a factor of safety of 40 might be required based on a fatigue strength failure criterion.'

[http://www.mech.utah.edu/ergo/pages/Educational/safety_modules/Safey_Factor/safety_factor_ns.pdf]

2.2 CATEGORIES OF SAFETY FACTOR

The safety factors can be divided into three categories and these are discussed below:

Explicit safety factor- these are the safety factors that are usually used in various disciplines and most of them can be found in various standards or regulations. The explicit safety Factors are used for instance by an engineer when they divide or multiply the load on a structure by a standard known value, and the new value, which may be larger is used in the construction. Similarly, the regulatory toxicologist applies an explicitly chosen safety factor when she divides the dose believed to be harmless in animals by a previously decided constant such as 100, and uses the obtained value as a regulatory limit [J. Clausen et al, 2005]. Other disciplines where explicit safety factors are used are ecotoxicology, fusion research, radiotherapy, medical surgery, geotechnical engineering, and in air traffic safety.

Implicit safety factor – these are safety factors that are not explicitly chose but they are rather based on human choice. This involves choices that are not made in terms of uncertainty function. These safety factors are not usually standardized. For example in traffic safety research, the behavior of drivers can be described as if they applied a certain safety margin to the distance between their car and the car nearest ahead [J. Clausen et al, 2005].

Naturally occurring safety factor/reserves – these are safety reserves that have not been chosen by human beings rather, they are means of describing the features that have developed through evolution. They can be calculated by comparing structural or physiological capacity to the actually occurring loads. Safety reserves can be found in different parts of a living organism and it is these reserves that guarantee the survival of the organism in an environment. For instance, some trees have better safety reserve to withstand storm and strong wind. Although the physiological features of animals and plants have been adapted to loads that will be encountered, it is still logical to describe them in terms of safety reserves.

2.3 APPLICATIONS OF SAFETY FACTOR

Safety factor is used in numerous disciplines but only two applications will be considered here. These are:

1. Safety factor in Toxicology
2. Safety factor in structural engineering

2.3.1 Safety factor in Toxicology

According to Ballantyne et al in Basic elements of toxicology, Toxicology is a study of the interaction between chemical, biological and physical agents in biological organisms in order to quantitatively determine the potential for these agents to produce morphological and/or functional injury that results in adverse effects in living organisms, and to investigate the nature, incidence, mechanism of production, factors influencing their development, and reversibility of such adverse effects. [Ballantyne, B et al, 2009] In simple terms, it can be defined as the study of the adverse effects of substances (biological or chemical) on a living organism.

Toxicology is one of the disciplines in which the use of safety factor dates back to the origin of human species, although the use of an explicit safety factor is just recent.

In toxicology, safety factor is defined as the ration between an experimentally determined dose and a dose that is accepted in humans in a particular regulatory context. They are used as compensation for data deficiencies or for extrapolation from experimental animals to humans- or more general- they are used as compensation for different variabilities. The use of an inverse safety factor (now called application factor) of 0.3 to be applied to acute toxicity data was proposed in 1945 by Hart and co-workers. [Chapman PM et al, 1998]

The first proposal of safety factor for toxicity was in 1954 by Lehman and Fitzhugh [Dourson ML and Stara JF, 1983]. They proposed that the acceptable daily intake (ADI) be obtained for food additives by dividing chronic animal NEL's (No effect level) in mg/kg of diet by 100.

This value of 100 is still widely used today, although higher factors such as 1000, 2000, etc. are also used especially for the regulation of substances which induce severe toxic effects in human. [Dourson ML and Stara JF, 1983].

Toxicological safety factors are usually accounted for as products of subfactors, each of which relates to a given extrapolation; so a factor of 100 could be seen as comprising two factors of 10, one for the extrapolation from animals to humans and the other for extrapolation from the average human to the most sensitive parts of the human population [Weil CS, 1972]. For environmental studies (ecotoxicity), factors below 100, such as 10, 20, 50, are widely in use. [Chapman PM et al, 1998]

2.3.2 Safety Factor in Structural Engineering

Structural engineering is one of the disciplines where the use of safety factors has been well established and many different systems are in use- for instance partial safety factor method, limit states etc.

With respect to Structural engineering, Safety factor can be defined as the ratio of maximum load not leading to failure, to the measure of applied load.

Safety factors are major parts of design criteria which could be found in numerous regulations, laws, customs, contracts, and standards like NORSOK, DNV, ISO standards etc. Before the safety factors could be enshrined in the design criteria in any of the standards whether national or international standard, all possible integrity-threatening mechanisms or situations must be considered usually by a team of experts in the specific field and related disciplines.

The method of design that is used in any project also determines the definition of safety factor in that context. For example, different safety factors may be used for different properties of the material. The safety factors used in WSD (also called ASD) and LRFD may also be different.

By applying safety factors, engineers try to reduce the allowable stress, strain, or displacement below their actual values that can result in failure. The use of safety factors by engineers is normally due to variability in material property, dimensional variation, assumptions made during the design, degradation of the materials over time, higher cost of prototype testing and higher cost of unexpected failures.

According to David G. Ullman, safety factor can be used in one of the following three ways:-

1. It can be used to reduce the allowable strength, such as yield or ultimate strength of the material, to a lower level for comparison with the applied allowable stress.
2. It can be used to increase the applied stress for comparison with the allowable stress.
3. It can also be used as a comparison for the ratio of the allowable strength to the applied stress. [David G. Ullman, 1997]

Based on the above, the safety factor can be represented by using the formula –

$$SF = S_{al}/\sigma_{ap}$$

Where S_{al} is the allowable stress, σ_{ap} is the applied stress and SF is the safety factor. If the material properties are known precisely and there is no variation in them – and the same holds for the load and geometry – then the part can be designed with a factor of safety of 1 [David G. Ullman, 1997].

2.4 CLASSICAL RULE-OF-THUMB SAFETY FACTOR

The safety factor can easily be estimated based on the estimated variations of the following five measures – material properties, stress, geometry, failure analysis and desired reliability. The better known the material properties and stress, the tighter the tolerances, the more accurate and applicable the failure theory, and the lower the required reliability, the closer the safety factor should be to 1. The less known about material, stress, failure analysis, and geometry and the higher the required reliability, the larger the safety factor [David G. Ullman, 1997].

According to David G. Ullman, the simplest way to present the factor of safety (safety factor) is to associate a value greater than 1 with each of the measures and then define the factor of safety as the product of the five values [David G. Ullman, 1997]

$$FS = FS_{material} . FS_{stress} . FS_{geometry} . FS_{fairlure\ analysis} . FS_{reliability}$$

The contributions by the five measures towards the safety factor could be estimated as follows:

Estimating contribution for the material

$FS_{material}$ = 1.0 if the properties of the material are well known, if they have been experimentally obtained from tests on a specimen known to be identical to the component being designed and from tests representing the loading to be applied

$FS_{material}$ = 1.1 if the material properties are known from a hand book or are manufacturer's values

$FS_{material}$ = 1.2 – 1.4 if the material properties are not well known.

Estimating the contribution for the load stress

FS_{stress} = 1.0 – 1.1 if the load is well defined as static or fluctuating, if there are no anticipated overloads or shock loads, and if an accurate method of analyzing the stress has been used.

FS_{stress} = 1.2 – 1.3 if the nature of the load is defined in an accurate manner, with overloads of 20 – 50 percent, and the stress analysis method may result in errors less than 50 percent

FS_{stress} = 1.4 – 1.7 if the load is not well known or the stress analysis method is of doubtful accuracy.

Estimating the contribution for geometry

$FS_{geometry}$ = 1.0 if the manufacturing tolerances are tight and held well

$FS_{geometry}$ = 1.0 if the manufacturing tolerances are average

$FS_{geometry}$ = 1.1 – 1.2 if the dimensions are not closely held

Estimating the contribution for failure analysis

$FS_{fairlure\ analysis}$ = 1.0 – 1.1 if the failure analysis to be used is derived for the state of stress, as for uniaxial or multiaxial static stresses, or fully reversed uniaxial fatigue stresses.

$FS_{fairlure\ analysis}$ = 1.2 if the failure analysis to be used is a simple extension of the above theories, such as for multiaxial, fully reversed fatigue stresses or uniaxial nonzero mean fatigue stresses.

$FS_{fairlure\ analysis}$ = 1.3 – 1.5 if the failure analysis is not well developed, as with cumulative damage or multiaxial nonzero mean fatigue stresses.

Estimating the contribution for reliability

$FS_{reliability}$ = 1.1 if the reliability of the component need not be high, for instance, less than 90 percent

$FS_{reliability}$ = 1.2 – 1.3 if the reliability is an average of 92 – 98 percent.

$FS_{reliability}$ = 1.4 – 1.6 if the reliability must be high, say, more than 99 percent.

[David G. Ullman, 1997].

According to David G. Ullman, the above values are estimates based on experience with how these factors affect the design [David G. Ullman, 1997]. By choosing the needed value, the safety factor can easily be calculated. The use of this approach is viewed to be very conservative because it can result if large safety factors and over-designed components.

Another approach which is much better is the statistical approach which gives more precise values for the safety factor because it uses the normal distribution for the different material features.

2.5 SAFETY FACTOR IN STANDARDS

With respect to the ISO and the NORSOK standards, the safety factors are incorporated in the design criteria through the use of partial action factors. The action factors could be found in ISO 19900, NORSOK N-001, and DNV OS-101 etc.

For integrity of offshore structures, the following limit states are usually checked according to NORSOK and their definition according to the Norwegian Oil directorate are as follows:

Serviceability Limit State (SLS) is given by criteria of functional ability, i.e. non-acceptable displacements, deflections and vibrations.

Ultimate Limit State (ULS) is given by the risk of fraction, large inelastic displacements or strains which can be compared to a fraction.

Fatigue Limit State (FLS) is the defined life length given by the risk of fraction due to the effect of a repeated load (fatigue)

Progressive collapse Limit State (PLS) is given by the risk of a severe collapse after an abnormal or “freak” event such as explosion, fire, collision, earthquake or other accident which leads to fracture of an element.

In Norwegian standard NS 3479 the last limit state, PLS, is called Accidental Limit State (ALS)

The principal standard for the calculation of the action and action effects could be found in NORSOK N-003 and the principles for the combination of actions are given in ISO 19900.

The action factors may vary depending on the prevailing condition or some special consideration. In NORSOK N-001, the following has been taken into consideration when determining the action factors:

1. The possibility that the action may deviate from the characteristic actions;
2. The reduced possibility that different actions contributing to the action effect analyzed, will reach their characteristic value at the same time;
3. Possible inaccurate calculation of action effects, to the extent that such inaccuracies may be assumed to be independent of the construction material.

The action factor should be adjusted accordingly if conditions other than the ones mentioned above take effect. [NORSOK N-001, 2010]

For offshore structures, when checking the ULS, SLS, ALS, and FLS, the action factors that should be used are summarized in the table below

Table 1- Partial action factor for the limit states [NORSOK N-001, 2010]

Limit States	**Action Combinations**	Permanent Actions (G)	Variable Actions (Q)	Environmental Actions (E)[d]	Deformation actions (D)[e]
ULS	a[a]	1.3	1.3	0.7	1.0

ULS	b	1.0	1.0	1.3	1.0
SLS		1.0	1.0	1.0	1.0
ALS	Abnormal Effect[b]	1.0	1.0	1.0	1.0
ALS	Damaged Condition[c]	1.0	1.0	1.0	1.0
FLS		1.0	1.0	1.0	1.0

a
For permanent actions and/or variable actions, an action factor of 1,0 shall be used where this gives the most unfavourable action effect
b
Actions with annual probability of exceedance = 10^{-4}
c
Environmental actions with annual probability of exceedance = 10^{-2}
d
Earthquake shall be handled as environmental action within the limit state design for ULS and ALS (abnormal effect)
e
Applicable for concrete structures

2.6 SAFETY FACTORS AND DESIGN METHOD

There are basically two design principles or methodologies which can be adopted for designing structures in engineering. These are –

i. Allowable stress design method (ASD) also known as Working stress Design(WSD)
ii. Load Resistance factor Design method(LRFD)

These design methods can be used for different materials such as steel, concrete, timber, aluminum etc.

Allowable stress design (ASD) - this design method is also known as the permissible stress design or working stress design (WSD) and it is mainly used by the civil engineers. The safety factor is used by the engineer in the design to ensure that the stress developed in a structure due to service loads do not exceed the elastic limit.

In ASD, the capacity is usually divided by a global safety factor to find the allowable load. This means that in ASD, the same safety factor is used for different load conditions. The load and resistance factors are lumped into one safety factor.

Load and Resistance factor design (LRFD) – This design method was developed to replace the Allowable stress design method, though the ASD is still used by some designers in some cases. The LRFD is also called the Limit state design and it involves the following limit states-

Serviceability Limit State (SLS)

Ultimate Limit State (ULS)

Fatigue Limit State (FLS)

Progressive collapse Limit State (PLS) also known as Accidental Limit state (ALS)

In LRFD, different factors of safety are used for different loads and by so doing, this can result in safer or lighter structures depending on the type of load being used.

In standard practice, only one of this design methods are applied, so both methods cannot be together is a single project and there should be no interchanging of the methods in the middle of a project.

2.7 POTENTIAL BENEFITS OF SAFETY FACTOR APPROACH

Reduced cost- the use of the safety factor approach is cost effective because it is very easy to implement and it doesn’t involve costs that may arise from data acquisition and computation. There is a considerable decrease in the input variables involved in safety factor approach; hence the computational cost is very low. Because the numerical values used in this approach can easily be obtained from standards like NORSOK and ISO standards, it reduces the cost of hiring an expert for analysis related to safety of the design or system.

In the construction industry, the efficiency of the projects is usually more important than the amount of material used, so the use of the safety factor approach reduces the construction time, which from the cost-benefit perspective, may be preferable over saving the material.

Simplicity – Safety factor is a simple approach which helps to guarantee safety of the system or design. Because of its simplicity, it is less likely to make mistake in the use of safety factor approach. ”Plants inherently safer technologies tend to be simple in design, easier to operate, and more tolerant to errors” [Overton and King 2006]. If the calculations are simple, it is less likely that mistakes will be made, and thus, the likelihood of error in the construction is drastically reduced.

Ability to capture residual uncertainty – safety factor can be used as a means of compensating for unquantifiable uncertainties such as the possibility of errors in our calculations or unknown failure mode.

Safety factor is one way of introducing some degree of redundancy in our design, and it is an effective means of offering protection against dangers whose probabilities are not easily available. Although, in some cases, the safety factor may not be justified from the cost-benefit perspective but it can, however, be justified from the perspective of offering protection against uncertainties or surprises, for instance, uncertainties against unknown risks or failure modes.

Security - safety factor approach is a vital way of dealing with security threats. Many incidents have shown that engineering structures are not only threatened by unintended harm (acts of nature) rather, the integrity of engineering structures can also be threatened by intended acts such as acts of terrorism. Recent terrorist attacks have shown that it is very difficult to assign probabilities to such actions, however, the use of safety factors may be an effective means of reducing the consequence of such attacks when they happen.

CHAPTER 3

3.1 Overview of the risk-based approach

The risk-based approach is increasingly used in many disciplines and its ability to consistently identify potential risks and provide information for taking required action has made it an indispensable tool in many fields of its application. The risk-based approach has the advantage of addressing the vital purpose of safety engineering, which is the reduction of accidents or the reduction of the potential consequence when an accident happens.

The risk-based approach involves the use of probabilities which in most cases are based on prior knowledge of similar events. According to Bedford and Cooke 2001, probabilistic risk assessment is now increasingly used as a tool for dimensioning safety measures [Bedford and Cooke 2001]. Some proponents of this approach have even argued that safety of building construction, structures and some engineering systems is a matter of calculating probabilities of their failure or reliabilities and also, that probability theory gives a better representation of engineering when compared to reality.

The use of the probabilistic risk assessment was developed in the nuclear industry in 1950s, though the engineers that designed the nuclear reactors aimed at reducing the likelihood of accidents but they did not have the means of estimating the probabilities. The first probabilistic risk assessment of a nuclear reactor was the Rasmussen report (WASH-1400) and it was published in 1975 [Michal 2000]. The fundamental methods used in the report are increasingly used in many other industries, although some improvements have been done. Although use of the risk-based approach has gained popularity in many disciplines, its use of probability also fails to give an objective picture of risk because of the uncertainties associated with the probability. A better understanding of this approach starts with understanding the concept of risk and other related concepts and below is a comprehensive discussion of the aforementioned issues.

3.1.1 What is Risk Analysis?

This is the means through which risk can be described. This is one of the major steps carried out in risk-based approach. It is usually carried out in order to establish a risk picture, compare alternatives in terms of risk, identify critical factors with respect to risk and also demonstrates the effect of various measures on risk [Aven T., 2008]

Risk analysis can be performed at different phases in the life cycle of a system. These phases include planning or early phase, detailed planning phase, construction phase, transportation, installation, operation and decommissioning phases.

In majority of the cases, companies perform risk analysis in order to satisfy regulatory requirements but this should not be the main reason for such analysis. The main purpose of conducting risk analysis should be to support decision-making in the face of uncertainties. Risk analysis helps companies in finding the right balance between safety and the cost of safety.

According to Aven, T. 2008, there are three main categories of risk analysis methods: simplified risk analysis, standard risk analysis and model-based risk analysis. These are described in the table below -

Table 2 – Main categories of risk analysis methods [Aven, T., 2008]

Main category	Type of Analysis	Description
Simplified risk Analysis	Qualitative	Simplified risk analysis is an informal procedure that establishes the risk picture using Brainstorming sessions and group discussions. The risk might be presented on a coarse scale e.g. low, moderate or large, making no use of formalised risk analysis methods.
Standard risk Analysis	Qualitative or quantitative	Standard risk analysis is a more formalised procedure in which recognised risk analysis methods are used, Such as HAZOP and coarse risk analysis, to name a few. Risk matrices are often used to present the results.
Model-based risk Analysis	Primarily quantitative	Model-based risk analysis makes use of techniques such as event tree analysis and fault tree analysis to Calculate risk

3.1.2 Dimensions of risk

This refers to various aspects of a system that can be affected by an accident or exposed to risk. The consequences of an accident maybe related to personnel, the environment, assets as well as production capacity. The above aspects are regarded as the dimensions of risk because they can be affected when we have an accident. The different dimensions and their categories are as follows:

- Personnel risk
  Fatality
  Impairment risk
- Environmental risk
- Asset risk
  Material damage risk

  Production delay risk [Vinnem J.E., 1999].

3.1.3 Risk Management

In order to have an effective risk-based approach, a good risk management system must be in place. Risk management refers to all measures that are carved out to manage risk. Risk management deal with balancing the conflicts inherent in exploring opportunities on the one hand and avoiding losses, accidents and disasters on the other [Aven T. & Vinnem J.E., 2007].

According to Aven, T., 2008: Risk management is divided into three (3) main categories, which are –

1) Strategic risk
2) Financial risk
3) Operational risk

(1) Strategic risk comprises factors that are related to long –term strategy of the company.
(2) Financial risk relates to the company financial situation and it may be outside the company´s control.
(3) Operational risk relates to the normal operating situation in the company.

3.1.4 Methodologies for risk analysis

There are different methods used in risk analysis and the method that is chosen for a particular situation depends on the reason why the risk analysis is being carried out. Risk analysis methodology/technique chosen can be qualitative or quantitative. Some of the methodologies for risk analysis are as follows:

a) ***Coarse Risk Analysis***

This is also known as preliminary risk analysis. This analysis is usually by dividing the analysis subject into units and then performing the risk analysis for each of the units. This analysis is usually done by a team of 3 – 10 persons. The main aim of the preliminary risk analysis is to establish a crude risk analysis. Because the Preliminary risk analysis identifies the casual picture, other methods can be used to assess the situation in detail.

b) ***Job Safety Analysis (JSA)***

This is also known as Job Hazard Analysis (JHA) or Job Risk Assessment (JRA). It is a risk analysis methodology which is used in identifying hazards that are associated with a task/job that is to be performed. JSA is a qualitative risk analysis method and it is check-list based.

A sample of the JHA is presented later in the project and in Appendix A.

c) ***FMEA/FMECA – Failure Mode and effect (Critical) Analysis***

This is a risk analysis method developed in the 1950s and it's a simple method which shows you possible failures that can happen to a unit of a system and it predicts the failure effect on the entire system.

FMEA shows how significant the failure of a component can be, to the overall performance of the system. It is used in analyzing the failure of a technical system. If the critical nature of the failures is described the method is known as FMECA – Failure modes effect and critical analysis. This method systematically reveals the important failure of a system and so it can be used in evaluating how reliable the system is. It can also be used as precursor for more detailed quantitative analysis. In FMEA, technical failures are analyzed while the human failures are overlooked and this method is not suitable for a system that has much redundancy.

d) ***HAZOP – Hazard Operability***

This is a qualitative risk analysis method which is used in identifying the possible hazards in a processing unit. HAZOP can be used in many industries although it was originally developed for chemical processing industries. This method analyses the risk potentials of a possible deviation from original/design specifications of a system. This method is carried out by a group of personnel with a HAZOP leader. The method makes use of the work sheet to document deviations, causes of the deviations, consequences and recommendations/decisions.

e) SWIFT

Structured What-if technique (SWIFT) is a risk analysis method in which there is systematic use of "what-if" in order to identify deviations from normal condition. This method makes use of a checklist like HAZOP but it is a bit more flexible and can easily be adapted to the application. This is carried out by a team and it helps in identifying possible problems so that risk-reducing measures can be implemented accordingly.

f) Fault Tree Analysis

This is one of the most used risk analysis method and it has found application in many industries. Fault tree is a logical diagram which shows the relation between system failure and failure of the individual component of the system.

The unwanted event constitutes the top event of the tree while the various component failures constitute the basic events of the tree.

The fault tree comprises of graphical symbols showing the basic events of the system and the relation between them and the state of the system. A fault tree can also be represented by a reliability block diagram if consists only "And" and "Or" gates.

A simple fault tree is shown in the figure below by using the braking system of a car:

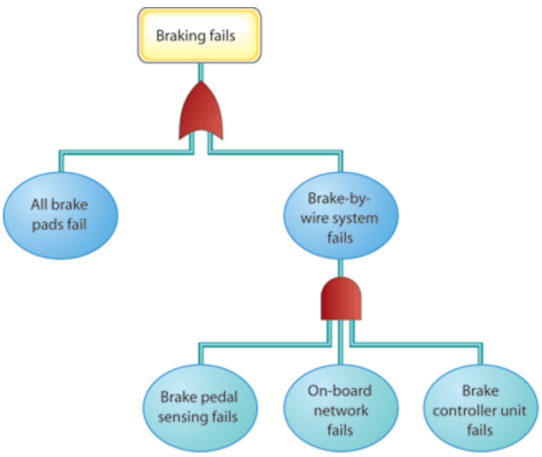

FIGURE 1 – FAULT TREE DIAGRAM FOR FAILURE OF BRAKING SYSTEM [David Kalinsky, 2005]

g) SAFOP

This is a modified version of HAZOP technique and it is used to analyze work processes and procedures in order to identify and evaluate risk factors. SAFOP is a powerful tool for risk assessment of new (planned) or changed operations and is applicable for all activities where a procedure will be used, such as process interventions, material handling, crane operations, maintenance, marine activities. [Vinnem J.E., 1999]

h) Event Tree Analysis (ETA)

This analysis is used in studying the different scenarios which initiating events can produce. If used qualitatively, ETA provides a picture of the possible scenarios but if used quantitatively, probabilities are assigned to various events and their consequences.

A simple event tree is shown below:

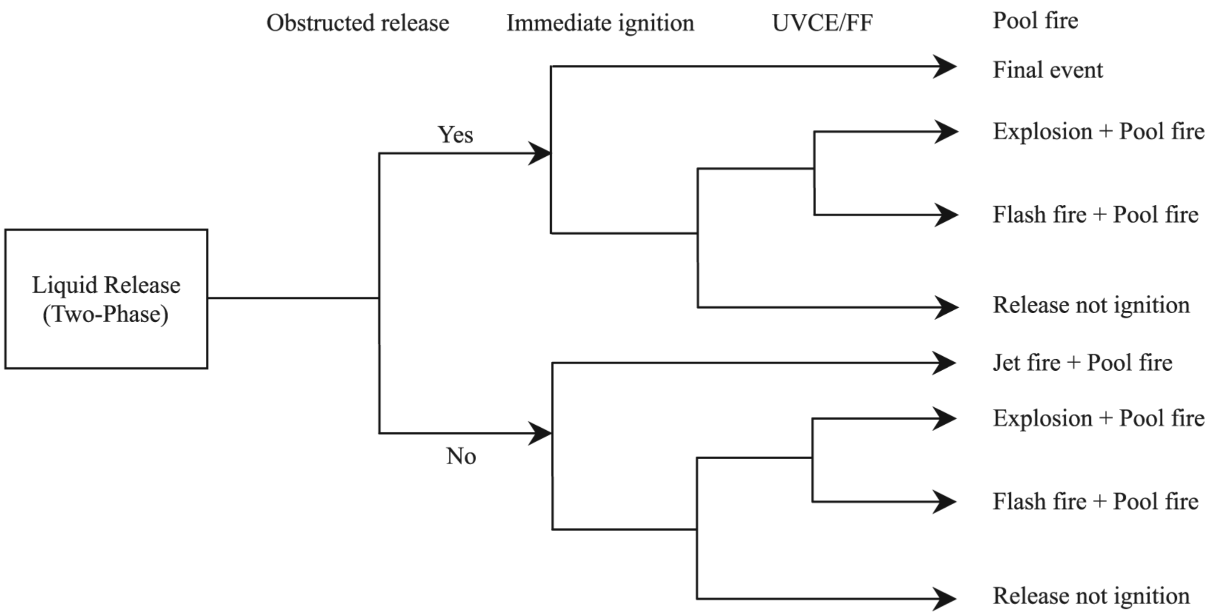

FIGURE 2- EVENT TREE DIAGRAM [Mohanad El-Harbawi et al ,2004]

Other risk analysis methods are Bayesian network, Monte Carlo Simulation, Bow-tie analysis, etc.

3.1.5 Qualitative and Quantitative Risk Analysis

There are two broad categories to which most of the risk analysis methods fall – qualitative risk analysis or quantitative risk analysis. Either of these two categories can be applied in the risk-based approach and the choice depends on the details needed and the reason for the analysis.

"Quantitative risk analysis is designed so that the security measures can be implemented, and this will allow the cost envelope to be implemented as well. There is yet a third method for risk analysis which is used and this is referred to as being the hybrid method, since it borrows characteristics from both the quantitative and qualitative risk analysis methods. Of the three approaches, the qualitative analysis is the most simple to use, and is therefore used the most often.

Qualitative analysis is useful because it allows one to quickly identify potential risks, as well as assets and resources which are vulnerable to these risks. Not only does qualitative analysis showcase the safety measures that have already been utilized, it will show those which could be useful if they are implemented.

The goal of qualitative risk analysis is to gain a level of risk protection which is acceptable, and one which will increase awareness among the necessary members of the organization. This analysis will often make use of calculations which are fairly basic, and it is often not necessary to know the value of all the assets in question.

While quantitative analysis does many of the same things which can be found with qualitative analysis, it is also capable of identifying the envelopes for which both safeguards and losses can be found. It is based on a process which is highly subjective, and it uses metrics which require it to have a high level of effort put into it.

At the same time, quantitative analysis is capable of presenting data in a manner which is friendly for management, and which expresses percentages, values, as well as probabilities.

3.1.6 PARAMETERS FOR RISK ACCEPTANCE CRITERIA

There are different risk acceptance criteria which are used in various industries. These criteria are used in the risk-based approach and they can form the basis for the risk-based decisions. The RAC that is chosen may also depend on the provision of the laws governing the industries. Some of the risk acceptance criteria which are used in the oil and gas are as follows:

a) PLL
b) AIR and FAR
c) F-N Curve
d) Risk Matrix
e) ALARP

a) PLL (Potential Loss of Life)

This is the number of fatalities experienced in a period, for instance in a year. In some situations, PLL can be used as a decision-making aid because it is not usually common to define an acceptance limit for it.

Because PLL expresses absolute level of Fatalities, it is easy for non-experts to understand.

It is not easy to express PLL in physical terms, because the values are usually less than 1.

"PLL =0.1 does not imply that 10% of a person is dead! Such a value may be illustrated by expressing it as 10% probability of one fatality, although this is slightly imprecise; because there is also a small probability of more than one fatality." [Vinnem, J.E., 1999]

The PLL value will often favor the development concept that has the lowest manning level resulting from the lower number of individual exposed to risk. This underlines the fact that one way to reduce societal risk is to limit the number of personnel exposed to risk.

b) FAR and AIR

FAR is known as fatal accident rate while AIR is the average individual risk.

FAR value is the number of fatalities in a group per 100 million exposed hours. 10^8

AIR value is the average number of fatalities per exposed individual. FAR and AIR can be expressed mathematically by the expression below:

$$FAR = PLL.\frac{10^8}{Exposed\ hours}$$

$$AIR = \frac{PLL}{Exposed\ individuals}$$

FAR and AIR values can be calculated as average values for entire personnel on an installation or personnel on specific area on the installation. The exposed hours can be hours on duty or total hours on the installations.

c) *F-N Curve*

This is used in expressing group risk. Since the most common measure of risk is risk to individuals, the society is interested on the effects of accidents on the society. Group risk is used to express the risk on society or affected members of a society.

Although acceptance criteria are usually expressed for individual risk, it is sometimes necessary to express an acceptance criterion for group risk.

The F-N curve expresses the frequency of accidents with N-fatalities or more and below is an example.

The frequency here is thus cumulative frequency.

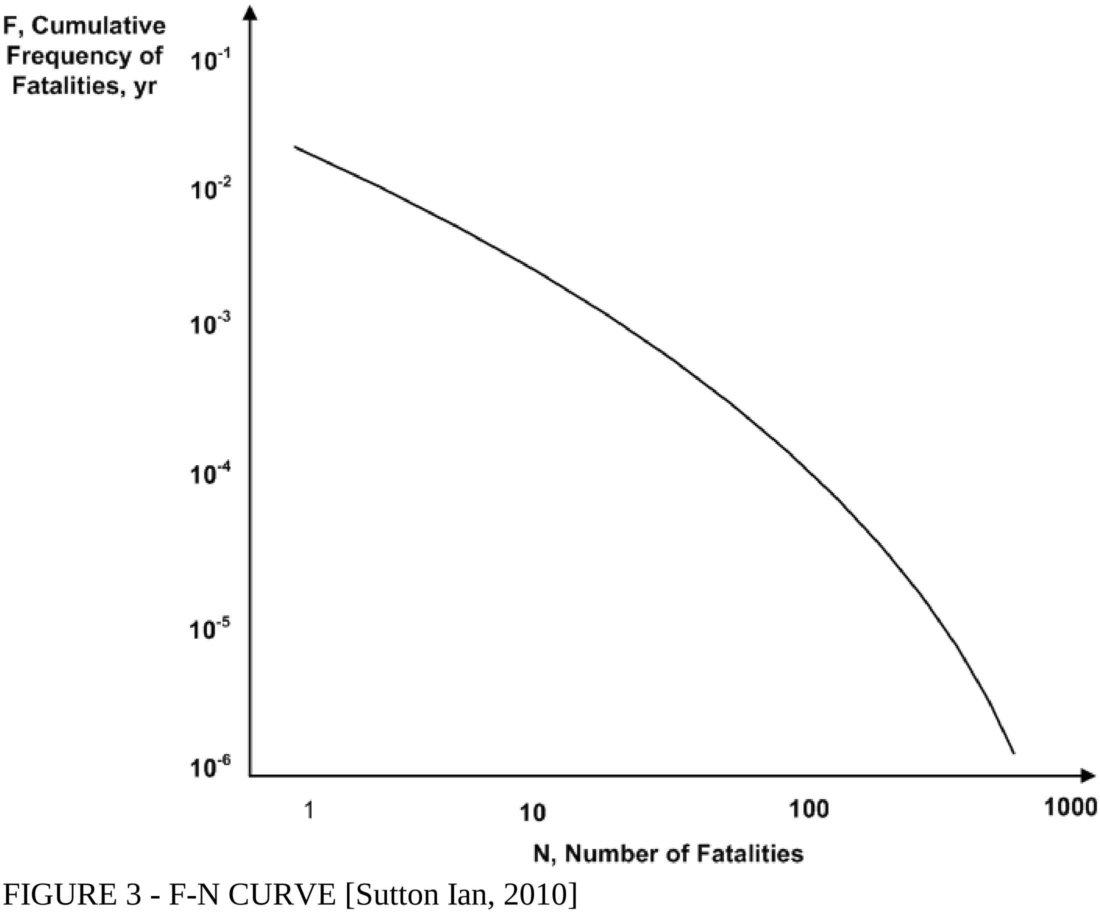

FIGURE 3 - F-N CURVE [Sutton Ian, 2010]

d) *Risk Matrix*

This is a qualitative risk evaluation tool which can be used to show consequences and probability of occurrence of an accident. It can be used to show risk level that is negligible, manageable or intolerable. It can be used to define the ALARP region where risk reducing measures are needed before an operation can take place. In order to capture all the risk aspects in a given situation, it is advisable to make use of 5 * 5 risk matrix. An example of this is shown in table 3 below with explanation of the risk levels shown in table 4.

Increasing consequences →	Consequence Categories				Increasing probability				
					1	2	3	4	5
	Severity	Safety	Environment	Cost (million Euro)	Failure is not expected $< 10^{5}$	Never heard of in the industry $10^{-5} - 10^{4}$	An accident has occurred in the industry $10^{-4} - 10^{3}$	Has been experienced by most operators $10^{-3} - 10^{2}$	Occurs several times per year $10^{-2} - 10^{1}$
	E	Multiple fatalities	Massive effect Large damage area, > 100 BBL	> 10	M	H	VH	VH	VH
	D	Single fatality or permanent disability	Major effect Significant spill response, < 100 BBL	1 - 10	L	M	H	VH	VH
	C	Major injury, long term absence	Localized effect Spill response < 50 BBL	0.1 - 1	VL	L	M	H	VH
	B	Slightly injury, a few lost work days	Minor effect Non-compliance, < 5 BBL	0.01- 0.1	VL	VL	L	M	H
	A	No or superficial injuries	Slightly effect on the environment, < 1BBL	< 0.01	VL	VL	VL	L	M

<u>Table 3- 5*5 Risk matrix</u> [DNV-RP-F116, 2009]

Risk	Description
VH	Unacceptable risk – immediate action to be taken
H	Unacceptable risk– action to be taken
M	Acceptable risk – action to reduce the risk may be evaluated
L	Acceptable risk - Low
VL	Acceptable risk - Insignificant

<u>Table 4- Risk categories</u> [DNV-RP-F116, 2009]

e) ALARP

This is a concept which stipulates that risk should be reduced to a level that is “As low as reasonably practicable”. This concept provides the framework for finding a balance between safety and the level of investment needed for the actualization of the safety goals. It is not easy to specify an acceptable level of risk due to the subjective nature of risk which makes it hard to do so; however, this concept of ALARP can be used for setting a value for acceptable risk. ALARP principle also stipulates that the cost, effort and time needed to reduce risk should not be grossly disproportionate when compared to the safety level that is being achieved.

“When a risk is not well understood it should be analysed and assessed in detail before making the ALARP judgment. If the risks are still not well understood a more precautionary approach should be adopted when judging what risk reduction measures are reasonably practicable. The lack of evidence about the effects of a hazard is not a justification for taking no action to reduce risk. In general, hazards which have a high consequence should be scrutinized more carefully than those that have a low consequence”. [Sutton Ian, 2011]

ALARP can be used as a qualitative measure of risk and the guidance below can be used in this regard -

“Use of best available technology capable of being installed, operated and maintained in the work environment by the people prepared to work in that environment;

Use of the best operations and maintenance management systems relevant to safety;

Maintenance of the equipment and management systems to a high standard;

Exposure of employees to a low level of risk”. [Sutton Ian, 2011]

The figure below shows the different aspects in the ALARP principle.

“Intolerable Region

Adverse risks are intolerable whatever benefits the activity may bring and risk reduction measures are essential whatever the cost.

ALARP or Tolerable Region

Risks are "As Low As Reasonable Practicable", i.e. while risks may be significant, they are tolerable in light of the potential benefits

Broadly Acceptable Region

Positive or negative risks are negligible, or so small that no risk treatment measures are needed". [Modulus pty, 2009]

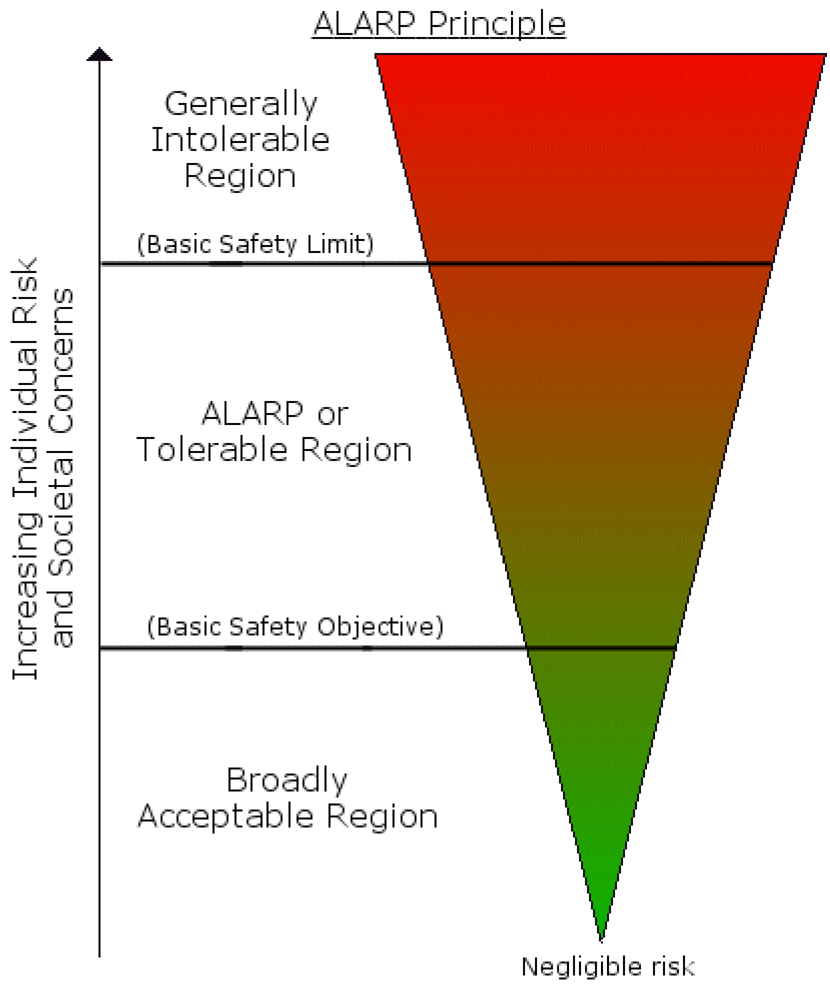

FIGURE 4 – ALARP DIAGRAM [Modulus pty, 2009]

3.2 APPLICATIONS OF RISK-BASED APPROACH

The risk-based approach has found increasing applications in various disciplines – financial, engineering, technical, legal etc. Many experts/proponents of this approach have argued that it is a cost effective method of achieving an organization's objectives. Some of the applications of this approach are-

- Risk-based design
- Risk-based testing
- Risk-based inspection/maintenance

3.2.1 Risk-based design

This is a method which provides a consistent, an effective and systematic framework for design and approval of new/novel structures or technology. The use of the risk-based design ensures that innovative technology and designs can be approved quickly. Risk-based design is used immensely in maritime, naval, and offshore industries.

According to DNV, modern risk-based method is used to ensure that:

- 'All key safety issues and other relevant aspects are covered
- Resources are not spent on unrealistic ideas
- The chance of success with daring new ideas is maximised
- Sound and cost-effective risk reducing measures are implemented
- Less daring technology can be taken into use as quickly and effortlessly as possible.' [DNV,2011]

The development of a new idea into a viable technology involves numerous challenges, but the use of the risk-based design, ensures that such challenges are identified and creative solutions are used to address them. The risk-based design method is employed in the design and construction of numerous large offshore structures and vessels that are very difficult to classify. This design approach has many milestones and according to DNV, it includes the following:

- Design review meeting

- Definition of approval basis
- Hazard identification
- Approval in Principal. Statement of feasibility issued by DNV affirming that the new technology is considered conceptually feasible and suited for further development and approval
- Risk and cost benefit assessment
- Concept improvements
- Selection of approval methods
- Analysis and testing
- Reliability assessment [DNV,2011]

3.2.2 Risk-based Testing

This is a type of testing which is used for software products. There are basically two types of risks associated with software products- project risk and product risk. Project risks include organizational issues, technical issues and third party issues. On the other hand, product risks are risks related to the functionality of the software product.

Risk-based testing for software products involves prioritizing the test functions or attributes based on the risk of failures. The main concern in risk-based testing is to identify the area that is most susceptible to failure and this is done by using state transition testing and boundary value analysis. The use of risk-based testing procedure ensures that the crucial and strategic features of the software are identified and this helps in giving the desired quality level for the product.

3.2.3 Risk-based Inspection/ Maintenance

The use of this methodology helps in the planning of inspection and maintenance of a plant and it makes use of risk analysis. Because most risks in the plant may be associated with small percentage of the machines/components, the use of the risk-based inspection/maintenance methodology ensures that better attention is given to high risk items without overlooking items that need less attention. The use of this methodology also ensures that the critical components that need attention are identified and maintained and this helps to reduce the downtime of the plant, which in turn eliminates the financial loss that comes with lost production time.

'Risk Based Inspection makes use of a broad range of technologies including consequence modeling, reliability and failure frequency analysis and limit- state approaches to provide industry with a risk-based method for evaluating and developing inspection plans. RBI is used in calculating both the consequences of possible failures and the likelihood with which those failures are expected to occur. The product of consequences and likelihood is used to identify which equipment poses the greatest risk and therefore warrants the most inspection attention in order to manage that risk' [http://www.dnv.com/services/software/products/safeti/SafetiRBI/]

The figure below compares the use of risk-based inspection and time-based inspection:

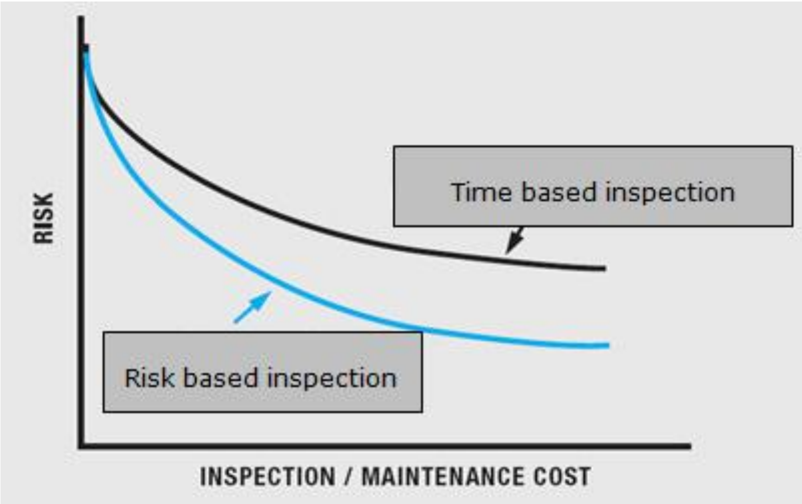

Figure 5 Risk-based inspection VS Time-based inspection
[Asset Integrity Engineering]

The technique adheres to international codes and standards, replacing time based inspection with a number of significant advantages;

- Reduced operational risk.
- Increased plant availability and reduced unplanned outages.
- Reduced inspection and maintenance costs without compromising safety or reliability.
- Flexible technique able to continuously improve and adapt to changing risk environment.

- Inspection techniques and methods clearly defined based on thorough understanding of potential failure modes. [Asset Integrity Engineering]
-

3.3 POTENTIAL BENEFITS OF RISK-BASED APPROACH

Economic optimization- this is one of the major reason why many companies favour the use of risk-based approach in design, testing, inspection, maintenance etc. Many experts argued that economic optimization of risk management measures is the main objective of probabilistic risk analysis [Guikema and Pate-Cornell 2002]. If for instance, the accident probability is found by analysis, it is possible to calculate the expected benefit from a safer design and this can aid in decision making.

There is huge financial gain in making use of risk-based approach in inspection, testing, design etc. because the resources are allocated to critical components and there is reduction in operational downtime. The result from a risk analysis can serve as an input into a cost-benefit analysis which could help in making risk-informed decision. The output of the probabilistic risk analysis can also be used as input into economic analysis of small and simple projects but in large projects, the use of output from probabilistic risk analysis is not accurate enough as direct input for economic analysis.

Better precision- the risk-based approach could be used to provide a more precise description of the design parameters. This is based on the presumed nature of risks and uncertainties and Savchuck (1992), for example, argues that contrary to traditional design approaches, the variables in probabilistic design methods are assumed to be random, which corresponds to the nature of the real states. [Savchuck, 1992]

Due to uncertainties associated with probability, there have been strong objections against the introduction of unreliable probabilities into probabilistic models. Quantitative introduction of uncertainties into the model may result in an increase in the failure probability of the system of the components. The use of sophisticated statistical methods in risk analysis and calculations can ensure that the probability of accident will be found with better precision.

Integrated system approach – Risk-based approach could be used to provide an integrated assessment of the safety of the whole system. Different risk analysis techniques can be used to evaluate the probability of failure of various components of a system and thus; the overall probability of failure of the system can easily be calculated. Any uncertainty in the probability of the components will result in making the estimated probability of the system uncertain.

Because of the integrated system approach of the risk-based methodology, it is easy to compare different components of a system and this will help in identifying the critical elements and thus, help in inspection and maintenance. The integrated nature of the risk-based method also ensures that failures as result of human factors are considered.

CHAPTER 4

COMPARISON AND INTEGRATION OF BOTH APPROACHES

4.1 COMPARISON

There are many differences between the safety factor approach and the risk-based approach and some of these differences have been highlighted in the previous sections of this thesis.

The Comparison between the discussed approaches can be done under the following:

APPROACH – risk-based approach addresses the crucial goal of safety engineering by reducing the probability of accidents or potential hazards. The use of risk-based approach ensures that risk analysis is carried out and probability of failure is well calculated. With information from the risk analysis, risk reducing measures can be employed in order to endure safety and reliability of the equipment or system.

On the other hand, safety factor addresses the goal of achieving safety indirectly and it does have a direct approach like the risk-based approach.

UNCERTAINTY- this is a situation for which there is lack of knowledge. Although it has been used interchangeably with risk, in various contexts, they are quite distinct and should not be used as such. Under uncertainty, probabilities are either unknown or they are known with insufficient precision.

In safety engineering, some of the probability estimates used in calculations may be uncertain so this should be taken into account when using output of risk analysis for decision- making purpose. This means that the use of the probability in risk-based approach takes into account, potential adverse effects only to the extent that probability can be quantified [Clausen et al, 2006]. The difficulty which may arise from trying to quantify some elements for instance, human factor, can lead analysts to focus only on events/components which can be assigned precise probability estimates. Probabilistic risk-based approach tends to neglect potential events for which probabilities cannot be obtained [Hansson, 1989].

Safety factor approach on the other hand, is intended to compensate for in practice unquantifiable uncertainties such as the possibility that there may be unknown failure mechanisms or errors in one's own calculations [N. Doorn and S.O. Hansson, 2011]. In most cases, safety factor may be set higher in order to compensate for uncertainties. This is done regularly in the field of toxicology [Fairbrother, 2002]. Other methods which take account of the uncertainties and are also used in safety engineering are inherent safety and use of multiple safety barriers.

COMPLEXITY- the safety factor approach is a less complex approach to safety than the use of the risk-based approach. The safety factor approach makes use of already prescribed numbers from national or international standards or regulations. The simplicity of the safety factor approach makes errors less likely and this helps to increase the efficiency of the design. The use of risk-based approach on the other hand is more complex because the estimation of failure probability can depend on many input variables. The estimation of the probability may also involve the use of complex mathematical or statistical methods which in most cases can be difficult for some people. This can also make the simplification of the model a bit much difficult especially for the non-experts.

FINANCIAL BENEFIT- the financial gain from the use of risk-based approach has been argued by many proponents of this approach as the most important benefit from it. The use of the risk-based approach ensures that the designs are economically optimized. Outputs from the risk analysis can be used as input into the cost-benefit analysis. The financial benefit of the risk-based approach could also be seen from its various applications, for example, the use of risk-based inspection and risk-based maintenance which ensures that downtime are reduced because most failure-prone components of the plant are inspected and maintained first.

The use of safety factor approach can, in some cases, be conservative because it provides regulatory bounds on various design parameters. The safety factor approach to safety can result in 'over-engineering', which can lead to excessive use of materials and higher cost of design and construction. 'There is no way to translate the difference between using safety factor 2.0 and safety factor 3.0 in the design of a bridge into quantifiable effect on safety. Without a quantifiable effect (such as reduced expected number of fatalities) it is not possible to calculate the marginal cost of risk reduction and therefore, economic optimization of design, is not possible' [N. Doorn and S.O. Hansson, 2011].

Cost of analysis- this is another aspect of cost which can be considered when deciding on which of the approaches to adopt. The use of the risk-based approach can involve risk analysis and estimation of the failure probabilities, and these are dependent on different input variables. As the number of variables increases, the cost of data acquisition and computation also increases. In some cases, this may lead to delay in the project as a result of long time needed for the simplification of the model. The application of safety factor is very simple and because it does not utilize many input variables, it can be advantageous from the cost-benefit perspective.

INTEGRATION AND OPTIMIZATION- the use of the risk-based approach offers a more integrated assessment of the safety of the entire system than use of safety factors. Because most components in a system are cross-correlated, the use of risk-based approach gives a more integrated account of the whole system which in turn, provides higher safety level. The use of the risk-based approach also makes comparison of different components of a system easier and this helps to indicate which component to improve or maintain.

It can be used to compare different engineering components within some engineering system or as a tool for priority setting and for the effect evaluation of safety measures. It is in this context of local optimization that probabilistic analysis has its greatest value (Lee et al. 1985).

Safety factor on the other hand, cannot be used as a mean of comparing different components of a system, so it cannot provide an integrated assessment of safety of the whole system.

Compatibility with organizational arrangement- there has been lots of emphasis on the division of risk decision process into two distinct part- risk assessment and risk management. The use of the risk-based approach seems to be compatible with this risk assessment-risk management paradigm. This organizational distinction helps to limit the influence of the risk assessors on the management decisions.

'Compared to the safety factor approach, PRA seems more compatible with this organizational division between risk assessment and risk management. The selection of safety margins is a value-dependent exercise that forms part of the basis for scientific and technological work. In contrast, a PRA can be performed on the basis of scientific information alone. It is then up to the regulatory decision makers to set the acceptable probability of failure; however, in most fields of engineering, there is no separation in practice between risk assessment and risk management' [N. Doorn and S.O. Hansson, 2011].

4.2 INTEGRATION OF SAFETY FACTOR AND RISK-BASED APPROACH

Risk based approach may not be able to capture some uncertainties and the use of the safety factor alone has been argued to be conservative, any approach which combines both approaches should address their shortcomings.

Traditionally, safety factors are used to ensure the safety of the structures by compensating for uncertainties in load, material qualities, and errors in the theory that is used. The use of safety factor is a classical approach, which uses cheap deterministic optimization to prevent failure. During the design stage, the design engineers try to identify the failure modes, and they also identify design variables which will make the structure safe with respect to the identified failure modes.

The risk-based approach on the other hand, makes use of risk analysis methods in identifying different failure modes and also the probabilities of failure. Establishing the probabilities may be challenging is some cases especially if there is no historical data similar to the one assessed. If different failure modes are identified, it may be difficult to deal with if their distributions are irregular and have non-differentiable boundaries [Melchers, 1999]. Use of the risk-based approach ensures that any engineering design has a failure probability that is lower than a given or specified upper bound.

BASIC IDEA – Use of deterministic safety factors which are prescribed in standards has been argued as being conservative in some cases and use of risk-based approach also has its shortcomings. The basic idea of integrating the two approaches is to eliminate the shortcomings inherent in using the approaches separately and this is achieved by using risk-based methodology to identify that cost effective and minimum safety factor which would not lead to failure but rather maintain the integrity of the material or component where it is used.

For example, if a safety factor of 4 is used to produce a beam, it means that the strength of the beam is four times the load it can withstand. The cost of producing the beam also depends on the strength- the higher the strength, the more the material used and the higher the price of making the beam. Risk-based approach (risk analysis) can however be used to show if really the beam needs to be made with such a strength. The probabilities of failure of using different safety factors are evaluated and historical data can also be used to show that the chosen safety factor is in fact accurate. The integration is achieved by using risk-based approach to adopt a cost effective and reliable safety factor and this is discussed in the measures below.

4.2.1 PROPOSED APPROACH

In order to benefit from the advantages of using either of the approaches discussed earlier, integrated approaches are used.

Because safety factor does not give a clear indication of how far we are from failure and the use of probabilities is sensitive to statistical hypothesis especially tail assumptions[Castillo E.,1988],an approach which combines the safety factor approach and the risk based approach in order to benefit from both would be prefered. Many researchers have proposed different measures which combine the two approaches but three approaches which has combined the safety factor and the risk-based approach and which will be discussed in this thesis are:

- Inverse reliability measure
- Probability sufficiency factor
- Probability-safety factor method with sensitivity analysis

INVERSE RELIABILITY MEASURE

This measure was proposed by Birger (1970) and the safety factor *S* is defined as the ratio of the capacity of the system, G_c (e.g. allowable stress) to the response G_r. In order to account for uncertainties, the safety factor is greater than one, for instance in aircraft, a safety factor of 1.5 is used for the loads.

The combination of the risk-based and safety factor was done by addressing the probabilistic interpretation of safety factor. Birger's proposition was to consider the probability distribution function F_Q of the safety factor. This implies that, unlike the deterministic safety factor, $\frac{G_c}{G_r}$ in equation 1 below is a random function.

$$F_S(s) = prob\left(\frac{G_c}{G_r} \le s\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Given a target a target probability, $P_{ftarget}$, Birger suggested calculating s^*(known as Birger safety factor) by solving the equation :

$$F_s(s) = prob\left(\frac{G_c}{G_r} \leq s^*\right) = prob(S \leq s^*) = P_{ftarget} \quad \ldots\ldots\ldots\ldots\ldots\ldots.. (2)$$

The safety factor (known as Birger safety factor) can be found by setting the cumulative density function of the safety factor equal to the target probability and solving for the safety factor. This is shown in figure 6 below:

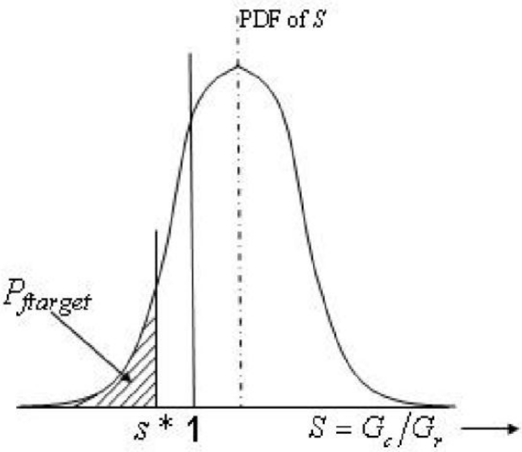

FIGURE 6 - Schematic probability density of the safety factor *S*. The PSF is the value of the safety factor corresponding to the target probability of failure

PROBABILITY SIFFICIENCY FACTOR

This is a measure developed by Qu and Haftka (2003). Initially, it was called probabilistic safety factor and it this measure is similar to the earlier inverse reliability measure proposed by Birger (1970). Birger safety factor combines the advantages of safety factor as well as that of probability of failure.

According to Qu and Haftka, failure occurs when the safety factor *S* is less than 1. The design condition which stipulates that the probability of failure should be smaller than the target probability for a safe design is written as

$$P_f = Prob(S \leq 1) = F_S(1) \leq P_{ftarget} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (3)$$

By making use of inverse transformation, equation (1) can be expressed as:

$$1 \leq F_S^{-1}(P_{ftarget}) = s^* \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. (4)$$

The probability sufficiency factor is shown in the figure 5 above. The design requirement $P_{ftarget}$ is known and the corresponding area under the probability density function of the safety factor is the shaded region in Figure 6. The upper bound of *s** is the value of the

Probability sufficiency factor (PSF). The region to the left of the vertical line $S = 1$ represents failure. To satisfy the basic design condition s^* should be larger than or equal to one. In order to ensure that the value of s^* is equal or greater than unity, we can manipulate the variables G_c or G_r by increasing or decreasing their value. The PSF s^*, represents the factor that has to multiply the response G_r divide the capacity G_c, so that the safety factor can be raised to 1.[P. Ramu et al, 2006]

For example, a PSF of 0.6 means that G_r should be multiplied by 0.6 or G_c be divided by 0.6 so that the safety factor ratio increases to one. In other words, this means that G_r has to be decreased by 40% (1−0.6) or G_c has to be increased by 66% ((1/0.6) −1) to achieve the target failure probability. It can be observed that PSF is a safety factor with respect to the target failure probability and is automatically normalized in the course of its formulation.

APPLICATION - Probability sufficiency factor (PSF) is very useful in estimating the resources needed to achieve the required target probability of failure. For example, in a stress-dominated linear problem, if the target probability of failure is $10^{-5}$and a current design yields a probability of failure of 10^{-3}, one cannot easily estimate the change in the weight required to achieve the target failure probability. Instead, if the failure probability corresponds to a PSF of 0.8, this indicates that maximum stresses must be lowered by 20% to meet the target. This permits the designers to readily estimate the weight required to reduce stresses to a given level. [P. Ramu et al, 2006]

The use of this measure helps to improve the response surface approximation, computational efficiency and it also allows easy estimate of resources needed to attain a required safety level. The PSF can also be found by use of the Monte Carlo simulation which involves generation of random samples points according to the statistical distribution of the variables. Detailed discussion on the use of the Monte Carlo simulation is not done here but is part of the future research on this thesis.

PROBABILITY-SAFETY-FACTOR METHOD WITH SENSITIVITY ANALYSIS

This method was proposed by Castillo et al. and because of the computational work involved in it; only its basic idea will be discussed. The method consists of a sequence of classical designs, based on given safety factors, which (a) minimize cost or optimize an alternative objective function, (b) calculate the different failure mode probabilities or their upper bounds, and (c) update the safety factors to satisfy both the safety factors and the failure probability requirements. The process is repeated until convergence [Castillo et al, 2004].

This method involves fixing bounds for the safety factor and the probabilities of failure for each failure mode. Estimated upper bound for the failure probability of the system is calculated from the failure modes. This method involves solving systems of equation (minimization problems) the scope of which is beyond this thesis. This method:

$$\underset{\bar{\mathbf{d}}}{\text{Minimizes}} \quad h\left(\bar{\mathbf{d}}, \bar{\boldsymbol{\eta}}\right)$$

subject to

$$g_i\left(\bar{\mathbf{d}}, \bar{\boldsymbol{\eta}}\right) \geqslant F_i^k; \quad i \in I_f,$$

and

$$\beta_{F_i}\left(\bar{\mathbf{d}}, \bar{\boldsymbol{\eta}}, \boldsymbol{\kappa}\right) \geqslant \beta_i^0; \quad i \in I_f.$$

where $\beta_{Fi}\,; i \in I_f$ are the reliability indices associated with all failure modes and κ is the vector of parameters defining the statistical variabilities.

‘In each step of the solution, exact values of the actual safety factors, and exact values or bounds for the probabilities of failure for the different modes are calculated, and the corresponding safety factors updated, until the resulting design satisfies both the required safety factors and failure probability bounds. As a result, the engineer is informed about the failure probabilities for the different modes, as required by modern analysis, and the corresponding safety factors, as in the classical analysis.
An advantage of this approach is that the optimization procedure and the reliability calculations are decoupled’ [Castillo et al, 2004].

A summary of the methodology is given in these basic steps:

Initialization – the safety factors are initiated to their lower bounds

Step 1 – the optimal classical design which minimizes the cost subject to the safety factor constraint is obtained (this is the master problem)

Step 2 – Exact values or upper bounds for the probabilities of failures or β-values for all failure modes are calculated, solving a minimization problem per failure mode
(This is a sub problem).

Step 3 – safety factors are updated through series of iterations to satisfy the needed probability of failure.

Step 4 – we check for convergence of the safety factor and probability of failure if there is no convergence, we have to start again from step 1, else we can go to step 5.

Step 5 – calculation of the actual safety factor associated with non-active constraints and return of design values, associated safety factor, failure probabilities for different failure modes.

The final stage of this approach is a Sensitivity analysis. This analysis helps the designer to know which data values have more influence on the design. The sensitivity analysis involves converting all the data to artificial variables and it allows us to determine how much a small change in any of the data values, such as the cost of the materials, the safety factors, etc., affects the total cost and the reliability indices of the engineering work. The method controls for safety against all failure modes by a double check: via safety factors and via reliability indices [Castillo et al, 2004]. This method is used in Structural engineering for example in the designing of the retaining wall.

4.3 RECOMMENDATION AND CONCLUSION

The safety factor approach and the risk-based approach have been presented with their benefits and applications. Although the two approaches are still in use today by some designers, they have shortcomings which the user has to be aware of- use of safety factor can be overly conservative and there are uncertainties associated with probabilities which are used in the risk-based approach especially with tail assumptions.

Using probabilities in the risk-based approach can lead to much emphasis on the dangers that could be assigned probabilities easily, however, the use of the risk-based approach is highly indispensable when optimization is important for example in prioritization of inspection and maintenance operations. Risk-based approach is therefore, a useful tool for setting priority and evaluation of safety measures.

On the other hand, the use of safety factors is very easy because the minimum factors of safety are specified in standards or codes which are written by experts and it is believed to provide adequate level of safety at reasonable cost. There are several groups that are interested in safety factors due to various reasons, they include- Engineers, Management, insurance companies, marketing/ sales personnel etc. Establishment of a safety factor should be viewed as a corporate decision because several groups are affected by this.

None of the aforementioned approaches should be viewed as the best; rather approaches which combine both methods can be adopted because benefits of both approaches will be combined. The approaches which were discussed includes- inverse reliability measures proposed by Birger, Probabilistic sufficiency factor proposed by Qu et al and the probability-safety-factor method with sensitivity analysis proposed by Castillo et al. The inverse reliability measures are very easy to apply and it is similar to the probability sufficiency factor. Its advantage is that it helps one to know the amount of resources required to attain a given safety level. The probability-safety-factor method is also a very good approach which combines risk-based and safety factor methodology with sensitivity analysis. It is more complex than the first two approaches due to the numerous computations that need to be done but the results are reliable.

Finally, I think that the use of any of the approaches depends on many factors like cost, nature of project, location etc. but whichever approach that is adopted, the safety of people, environment and the stakeholders should not be compromised.

REFERENCE

Asset Integrity Engineering, http://www.assetintegrityengineering.com/Asset-Integrity/Risk-Based-Inspection.html

Aven T and Vinnem J.E (2007), “Risk Management, with applications from offshore oil and gas industry”, Springer Verlag, New York

Aven, T. (2008) “Risk Analysis, Assessing uncertainties beyond expected values and probabilities”, Wiley

Ballantyne, B., Marrs, T. C. and Syversen (2009), T., Basic Elements of Toxicology. General, Applied and Systems Toxicology

Bedford, T., & Cooke, R. M. (2001). Probabilistic risk analysis: Foundations and methods. Cambridge: Cambridge University Press

Birger, I.A. (1970), Safety Factors and Diagnostics, Problems of Mechanics of Solid Bodies, Sudostroenve Publishers, Leningrad

Castillo E. (1988) Extreme Value theory in engineering, New York: Academic Press.

Castillo et al, (2004), Design and sensitivity analysis using the probability-safety-factor method. An application to retaining walls, Structural Safety 26 (2004) 159–179

Chapman PM et al (1998) A Critical evaluation of safety (uncertainty) factors for ecological risk assessment. Environmental Toxicology Chem; 17

Clausen Jonas et al (2006), Generalizing the Safety factor approach, Reliability Engineering & System Safety **,**Volume 91, Issue 8, August

DNV-RP-F116 -Integrity Management of Submarine Pipeline Systems, “Sec.4. Risk Assessment and Integrity Management (IM) Planning” October 2009

Doorn N. and Hansson S.O. (2011), Should Probability Design Replace Safety Factor? Philosophy and Technology; Volume 24, Number 2.

Dourson ML, Stara JF (1983), Regulatory History and experimental support of uncertainty (safety) factors. Regul Toxicol Pharmacol; 3 (3):228-38

El-Harbawi Mohanad et al (2004) "Using geographic information systems in assessment of major hazards of liquefied petroleum gas", Disaster Prevention and Management,Vol. 13 Iss: 2

Guikema, S. D., & Paté-Cornell, M. E. (2002). Component choice for managing risk in engineered systems with generalized risk/cost functions. Reliability Engineering & System Safety, 78(3), 227–238.

Hansson, S. O. (1989). Dimensions of risk. Risk Analysis, 9(1), 107–112.

http://www.dnv.com/industry/maritime/servicessolutions/consulting/technicalconsulting/asa/riskbaseddesign.asp assessed on 04.06.2012

http://www.dnv.com/services/software/products/safeti/SafetiRBI/
http://www.mech.utah.edu/ergo/pages/Educational/safety_modules/Safey_Factor/safety_factor_ns.pdf

http://www.modulus.com.au/cgi-bin/riskmanagement/riskmanagement_help.pl?action=EVALUATE assessed on 04-05-2012

Kalinsky David, http://www.eetimes.com/design/embedded/4006464/Architecture-of-safety-critical-systems assessed on 05-06-2012

Melchers R.E. (1999) Structural reliability analysis and prediction, New York: John Wiley

Michal, R. (2000). The nuclear news Interview. Apostolakis: On PRA. Nuclear News, 27-31(March)

Moses, F. (1997) Problems and Prospects of reliability-based optimization. Engineering Structures, 19(4)

NORSOK STANDARD, N-001 Edition 7, June 2010

Overton, T. & King, G.M. (2006). Inherently safer technology: an evolutionary approach. Process safety progress, 25(2)

Ramu P. et al (2006), Inverse reliability measures and reliability-based design optimization, Int. J. Reliability and Safety, Vol. 1, Nos. ½

Randall FA. (1976), The safety factor of structures in history. Professional Safety; January:12-28.

Reidar Nilsen Alf (2011), Contributions to Fire safety Design of Tunnels; PhD Thesis UiS no. 145.

Savchuk, V. P. (1992). Some applications of probabilistic methods in space structures design. Reliability Engineering & System Safety, 37(2)

Sutton Ian. (2010), Risk Analysis and Risk Matrices in the Process Industries: Understanding risk. Version 1. suttonbooks.

Sutton Ian. ALARP (As Low as Reasonably Practicable) Risk: Determining acceptable risk for industrial facilities [Internet]. Version 1. suttonbooks. 2011 Nov 20. Available from: http://suttonbooks.wordpress.com/article/alarp-as-low-as-reasonably-practicable-2vu500dgllb4m-10/. Assessed on 04-06-2012

Ullman David G. (1997), The Mechanical Design Process, 2nd edition McGraw-Hill

Vinnem Jan Erik (1999), “Offshore Risk Assessment, principles, modelling and applications of QRA studies”, Springer

Weil C.S. (1972), Statistics vs safety factor and scientific judgment in the evaluation of safety for man. Toxicol Appl Pharmacol; 21:454-63