University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/Specialization: OFFSHORE TECHNOLOGY – Risk Management	Spring semester, 2016 Open access
Writer: GOWTHAM BABU RAJENDRAN	…… (Writer's signature)

Faculty supervisor:
Professor EIRIK BJORHEIM ABRAHAMSEN, University of Stavanger
External supervisor(s):

Thesis title:

A Resilience Engineering Approach For Preventing Accidents due to Human Factors

Credits (ECTS): 30

Key words: Accidents, Incidents, Human Factors, Risk Assessment, Safety, Resilience Engineering, FRAM	Pages: 56 Stavanger, 14.06.2016 Date/year

A Resilience Engineering Approach For Preventing Accidents due to Human Factors

Gowtham Babu Rajendran

June 14, 2016

Acknowledgement

This Master thesis is the final step of my two years Master Program in Offshore Technology Specialization Risk Management at University of Stavanger. This report is prepared based on an idea that the people from risk and safety management will be able to understand the content and the purpose of my work.

I would like to start by thanking the Norwegian Government and the University of Stavanger for providing me free education with higher quality.

I would like to thank my supervisor, Professor Eirik Bjorheim Abrahamsen at University of Stavanger for his wonderful guidance and help throughout my work.

And last but not least, i am very grateful and heartfelt thanks for all my friends and family who were always with me during my hard times.

Gowtham Babu Rajendran,

Stavanger,
June, 2016

Abstract

Human factors are emerging as the main concern for the oil and gas industry. All the major accidents in the offshore industry will have a direct cause or some way or the other linked to the human factors. The main aim of this thesis is to reduce the incidents due to human factors.

In this thesis the commonly used methods Human Reliability Analysis and Barrier and Operational Risk Analysis are studied and their limitations are reviewed.

A new approach Functional Resonance and Analysis Method (FRAM) is used to overcome all the limitations and manage the human factors based on the principle of Resilience engineering.

FRAM is a risk assessment method used widely in the field of Aviation and air traffic management where high degree of precision and safety is required.

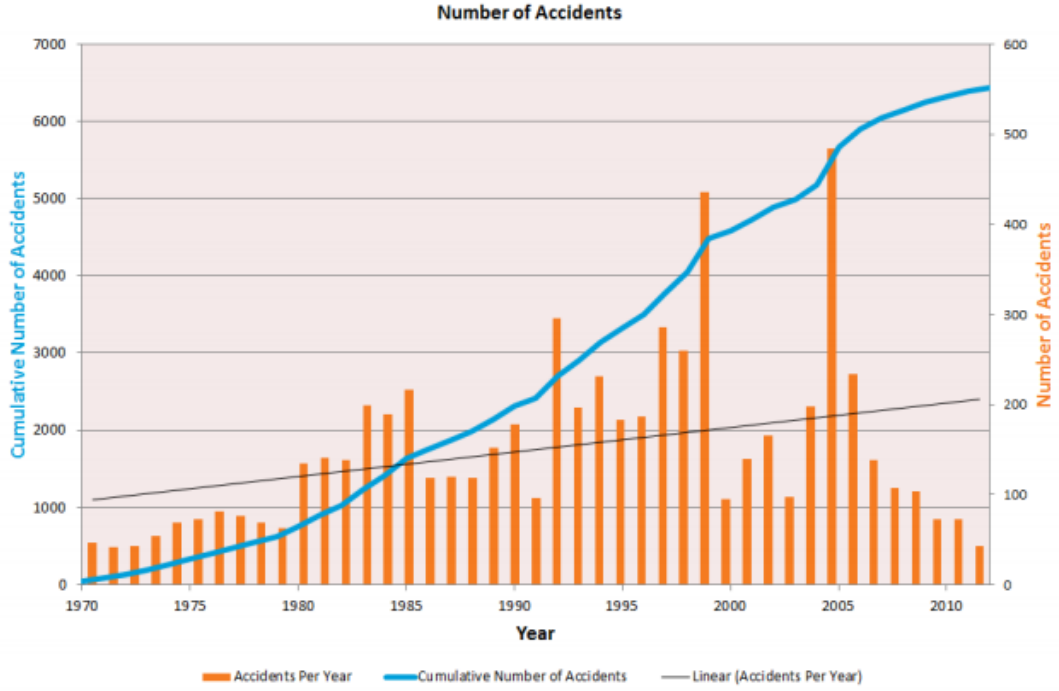
A case study on Macondo Blowout is performed using the FRAM method to illustrate its functionality and also to explain how the accident could have been predicted and prevented from the disaster.

TABLE OF CONTENTS

1. Introduction

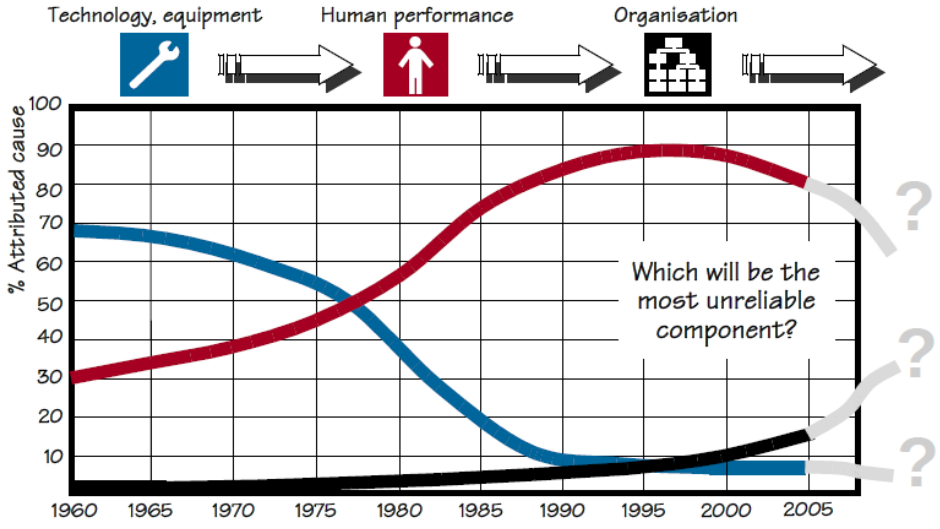
1.1. Background

In the recent years offshore activates are increasing. More rigs are being built and in parallel life extension of older asserts also takes place. Exploration of new geographies and operations are carried out in deeper and colder water regions. Hence, we can also expect more incidents and accidents in the industry. Are the new technologies and modern operations and safety management systems becoming safer? According to WOAD (World Offshore Accident Database) the number of incidents and accidents is increasing every year. The following figure shows the recent trends of accidents.



Number of Accidents (DNV.GL, 2014)

On the further look into the accidents it is clear that the Human Factors are one of the major causes of the accidents. According to (Hollnagel, 2008),



Attributed cause of accidents (Hollnagel, 2008)

In the past lack of technological development was the main cause of the accidents as the technology became powerful and precise then came the organizational and human factors. in the recent year's accidents due to technological defects are very less when compared to the incidents due to Human Factors as shown in the graph above.

Human error is the major source of risk in the existing offshore systems. The international maritime organization and the U.S coast guard have estimated that human factors are the direct cause of nearly 80% of ship incidents and accidents. Chadwell et al (1999) investigated the role of human factors in the petroleum industry incidents which resulted to be 47% are due to these factors. Human factors are not only the main causes of incidents but also play a major role in financial losses due to production downtime, environmental damage or lost drilling time etc. Hence in the recent years Human factors are consider as an important topic in risk reduction in the organization. Several new methods are being developed and adapted by the organizations to reduce the risk due to Human factors. This motivated me to start working on the topic human factors.

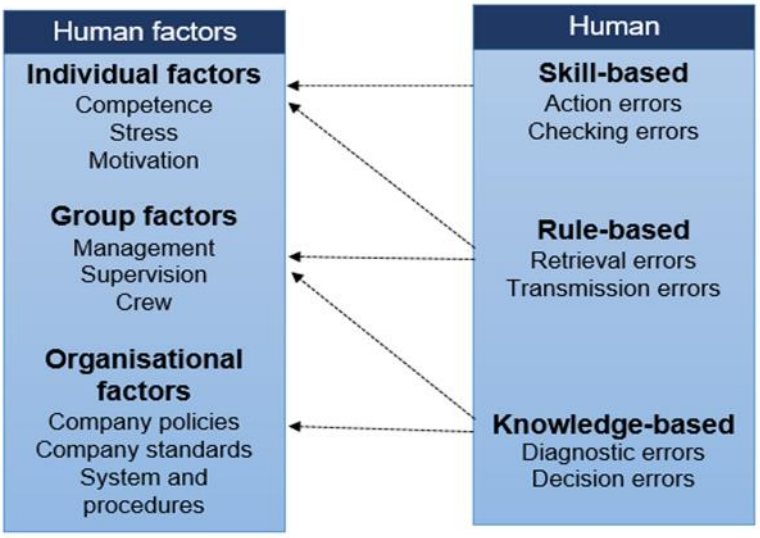
1.2. Scope

The main purpose of this thesis is to recommend a new approach for managing the risk due to human factors. we will be studying the current approaches used for risk assessment of human factors, review them based on their limitations and their respective consequences. In the later part of the report we will be using a new method FRAM (Functional Resonance and Analysis Method) adapted from Aviation industry for overcoming the consequences of the current approaches of the oil and gas industry. A case study is carried on the Macondo Blowout accident and will be illustrating, how the key issues of the accident can be avoided or prevented using the FRAM method.

2. UNDERSTANDING HUMAN FACTORS AND HUMAN ERRORS

Earlier in offshore industry, we often used these terms 'Human Factors' and 'Human Errors' without the proper understanding of what these terms actually mean. They were just used as general terms referring as a cause of accidents which occurred due to people other than technical faults. Traditionally Human Factors were defined as the scientific study of human and machine interactions. In the recent years the definition of these terms were extended to encompass the effects on safety by an individual, group or by an organizational factor.

Both Human factors and the Human errors are studied separately and then if any relationship between them are overlooked, this might be due to no agreement between them on precise nature and definition. The following figure shows an illustration on the relationships between the human factors (underlying causes) and human errors (their immediate causes).



Relationships between human factors and human errors (Gordon, 1998)

3. HUMAN ERROR

Many industrial psychologists like Reason, Rasmussen Kontogiannis and Embrey studied in detail on human error whose findings plays a major role in understanding the human error. Reason categorized human errors based on theory of human performance by Rasmussen, in terms of

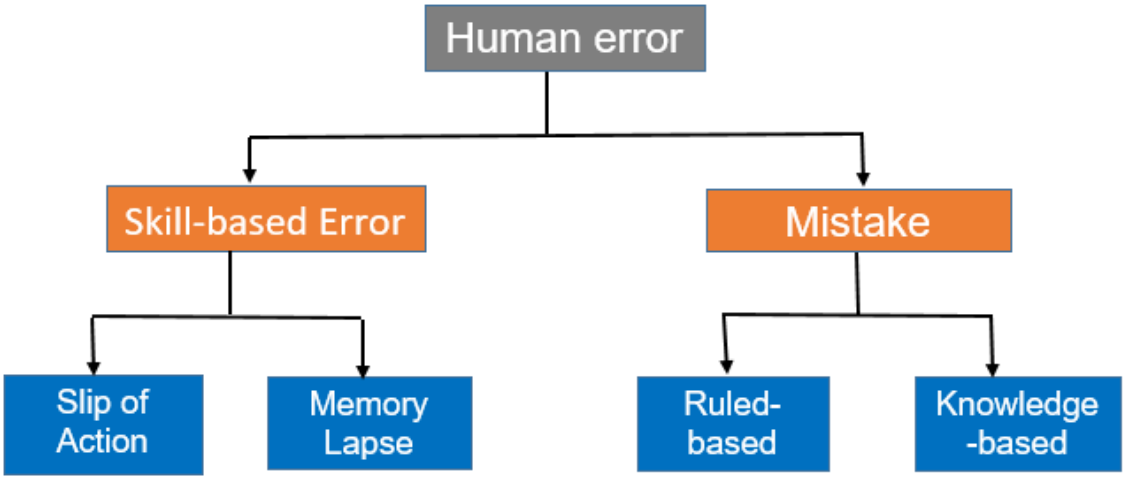
- Skill based slips and lapses
- Rule based mistakes
- Knowledge based mistakes

According to R.P.E Gordon reason's error types are complex and in order to understand and use it on a regular basis we are in need of considerable training.

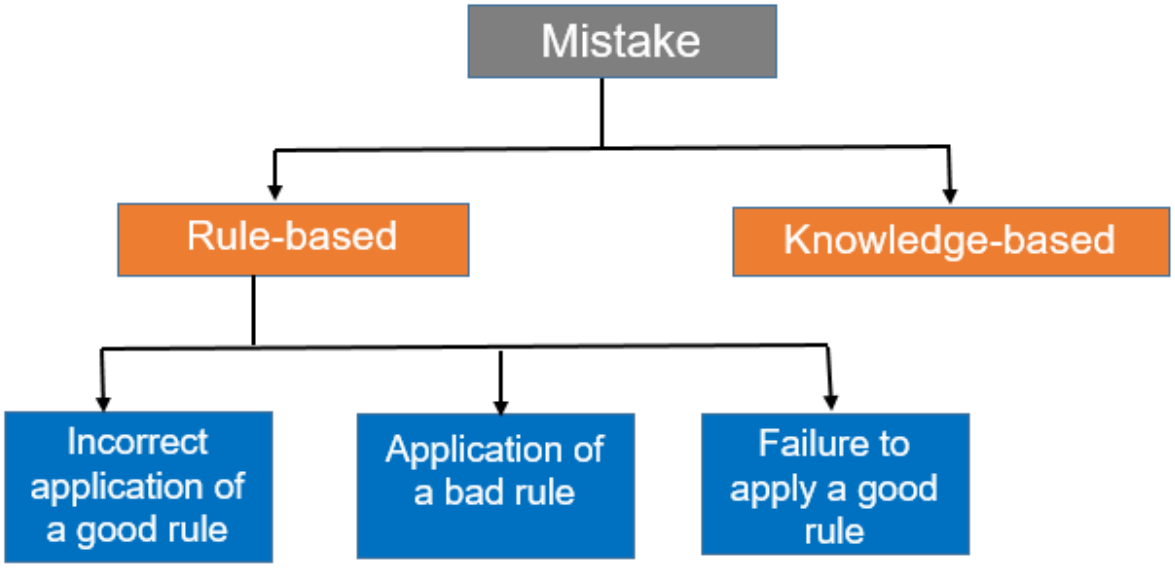
Kontogiannis and Embrey summarized human errors in a more simplistic approach into six categories (Gordon, 1998)

1. ***Action Errors*:** Errors when wrong or no action taken or when correct actions under wrong situations or object.
2. ***Checking Errors*:** The checks which are ignored or fault checks made or proper checks done on wrong objects or situation
3. ***Retrieval Errors*:** Receiving incorrect information or absence of required information.
4. ***Transmission Errors*:** Passing no information or incorrect information to the person. Or when the information is passed to a wrong personnel
5. ***Diagnostic errors*:** In the occurrence of an unusual or abnormal events, misinterpreting the actual situation.
6. ***Decision Errors*:** making wrong decisions considering the circumstances.

Reason's 'Skill based slips and lapses' relates to the first two categories Action and Checking errors, 'Rule based mistakes' relates to retrieval and transmission errors and the 'Knowledge based mistakes' relates to diagnostics and decision errors.



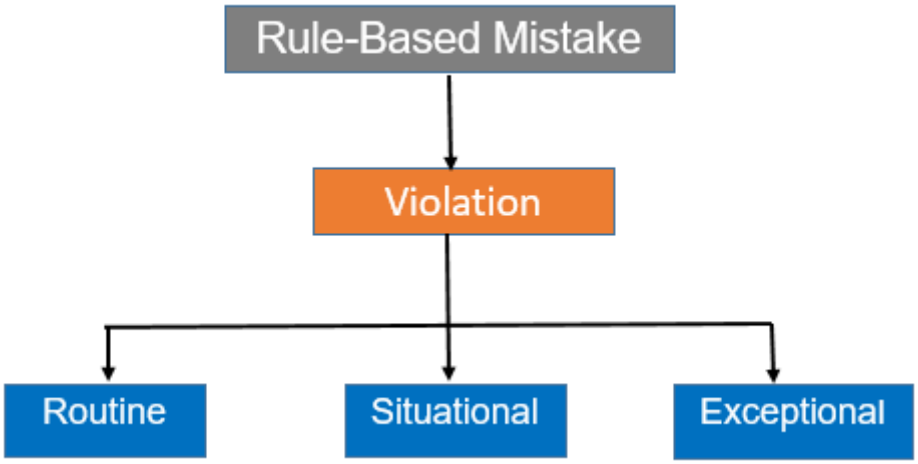
Human Error Typology (NOPSEMA,2016)



Mistakes (NOPSEMA,2016)

3.1. Violations

Violations refers to failure of applying a good rule. When an intentional action does not achieve desired outcome, then the violation is classified as human errors.



Rule-based mistakes (NOPSEMA, 2016)

There are several types of violation here we will discuss the major types,

- ***Routine*** – routine violations are very common and committed by most of the personnel's in the organization.
- ***Unintentional*** – breaking a rule as it was misunderstood or misinterpreted.
- ***Situational*** – as the name suggests it is not possible to get the job done in certain situations by following the rules
- ***Exceptional*** – deviation from the rules under unusual circumstances.

NOTE: When a violation achieves the desired outcome and does not cause any undesired outcomes it is not a human error.

For example: During the piper alpha incident, the personnel who followed the muster procedures could not access the life boats from the accommodation block. Personnel who survived the disaster was those who violated the rules and decided to jump in the ocean. In such cases it is advisable to review the rules and procedures.

Human errors are of two kinds in system disasters,

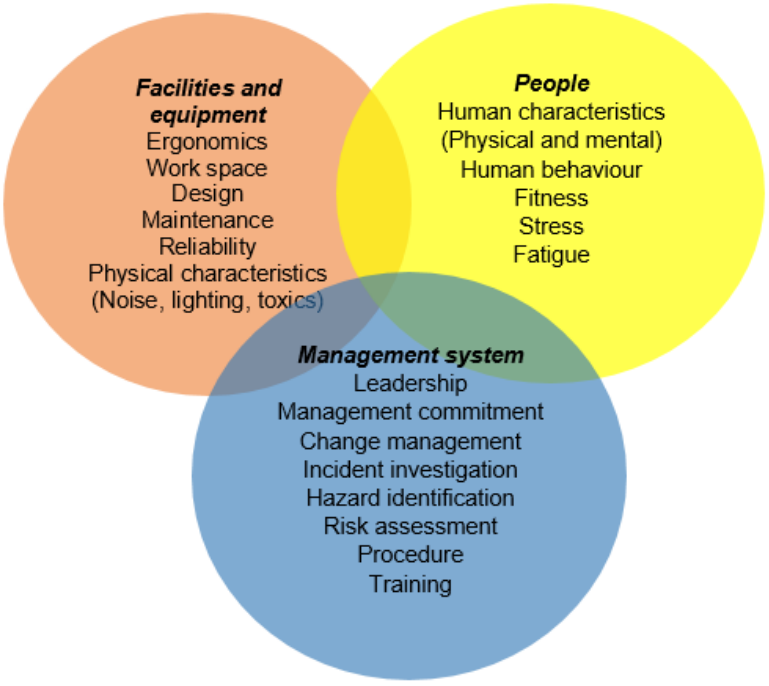
Active errors: Errors which have immediate effect on the system. These errors are mainly caused by frontline operators (like production operators, control room crews)

Latent errors*:* Errors whose consequences lie latent within the system, or comes into light only with the combination of other factors. These errors are caused mainly by the direct controlling personnel whose role has been already removed from the system (e.g. construction workers, designers, managers)

If both active and latent errors are identified at the work site, focusing on the actual problem will be made possible and therefore we can understand the basics of an error or accident.

4. HUMAN FACTORS

In general the Human factors is defined as the interaction between the humans, equipments and the management systems or organisations (IOGP, 2005).



Human factors interactions (IOGP, 2005)

NOPSEMA defined human factors into three basic categories as

- Organizational factors – includes the culture of the company, communication systems, decision making strategy, organizational priorities, availability of resources, leadership behavior, change management and relevant key performance indicators (KPI).

- Job factors - includes human-machine interface, physical working environment, availability and quality of procedures, workload, task requirements, equipment used and team member's behavior.

- Individual factors – includes personality, attitude, mood, mental ability, competence and skill, and individual health factors such as fatigue, alcohol and drugs, physical capability and psychological health

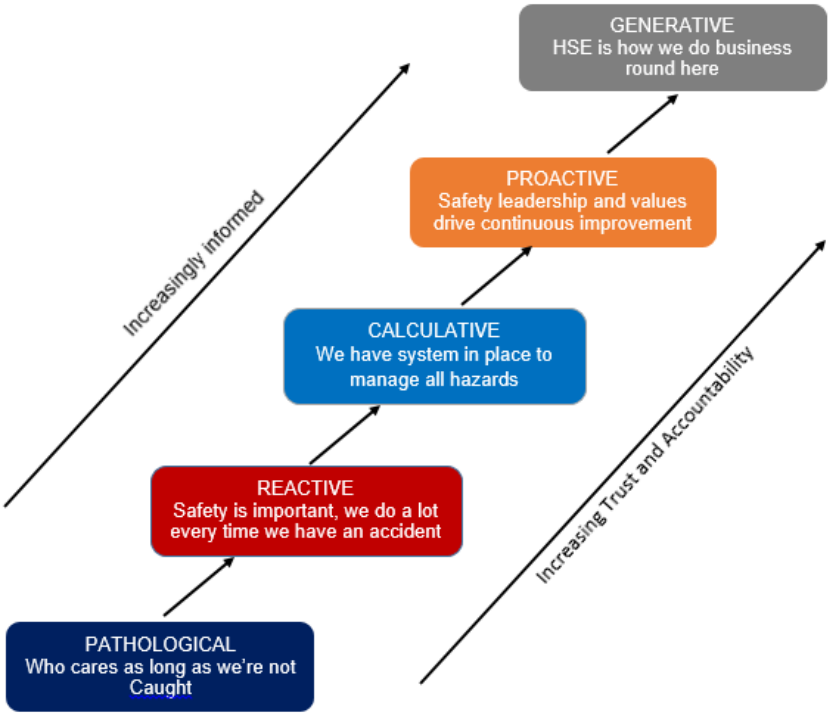
Some of the major human factor issues in the maritime and offshore industry are

- Leadership and safety culture
- Communications risks
- Perception of Risk and Decision-Making

- Fatigue
- Human Factors in Design
- Inadequate knowledge or training
- Poor maintenance
- Safety critical procedures
- Commercial and contractual environment
- Learning from incidents and accidents

4.1. Leadership and safety culture

Factors like attitude, shared values, beliefs and expectations which emphasize the critical importance of safety across any organization is highly influenced by the leadership and safety culture. The attitude towards the safety of an organization are determined by the factors like incentives and rewards implemented by leaders, behavior and interaction of the leaders with their personnel, decisions and actions taken by them to balance the safety against commercial imperatives. Safety culture cannot be changed abruptly but it is possible to have a gradual change by gauging its safety culture level and try to climb the ladder as shown below,



Culture ladder (Energy Institute, 2011)

4.2. Communication risks

Communications can be done in any form right from speaking, or by using sign language, or in pictorial form, or by any computer presentation. But the main motive is to transfer the complete information accurately and precisely. The person who

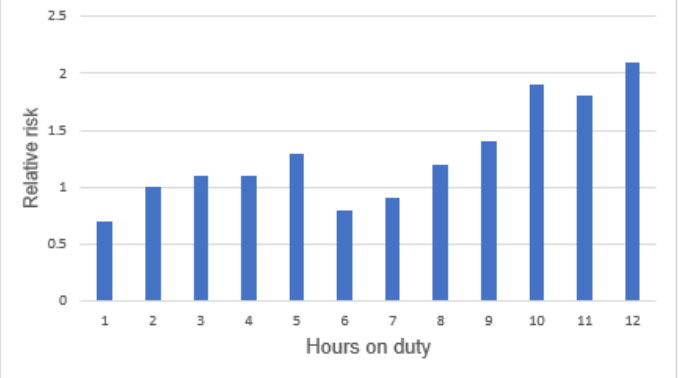
communicates should be responsible to make sure the message was received and understood by the person. Communication risk are high during the shit handover. Accidents like Piper Alpha are caused by poor communications during shift handover. Risk of communication also relies on the open door policy, standardization of terminologies used across an organization.

4.3. Perception of risk and decision making

During a critical situation proper understanding of the risk is very important. Incorrect decisions without proper understanding of the risk involved can lead to major accidents. An example for right decision during piper alpha accident only the personnel who decided to jump in the sea survived the incident. There might be situations where one should decide whether follow the standard procedures or decide outside the box for accidents. Hence poor judgement of the situations can lead to major accidents.

4.4. Fatigue

Fatigue is defined as feeling exhausted or tiredness and being ineffective in the work. Fatigue can be caused by excessive or prolonged exertion either by physical or mental exertion or by both. It is also a root cause for major incidents as a fatigued person is directly exposed to risk or making errors. Fatigue is mainly caused due to long shift hours, night working or frequent change of shifts. According to the energy institute briefing notes the risk are higher as the working hours increases. The average risks are nearly doubled when compared to working hours of 2-4 to 10-12.



Average risks for working hours (Energy Institute, 2011)

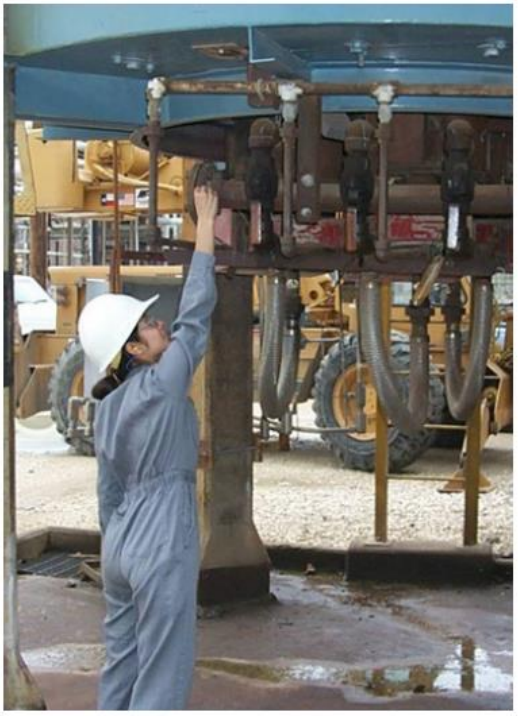
4.5. Human factors in design

Design deficiencies or lack of interface between the people and the technology reduces the human performances. These factors are often referred as “design induced human error”. It more important for an organization to include human factors during the design process to ensure easy accessibility and suitable for local work conditions. Oil and gas industry have to improve lots in the field of human factors engineering design by learning from industries like aviation, defense and nuclear power. Oil and

gas industries are continuously working on developing standards and processes to customize the needs. Some of the design errors are

Spacing congestion (IOGP, 2011)

The above image shows the design error by poor spacing which intern makes it difficult to operate the valve.



Difficulties in accessibility (IOGP, 2011)

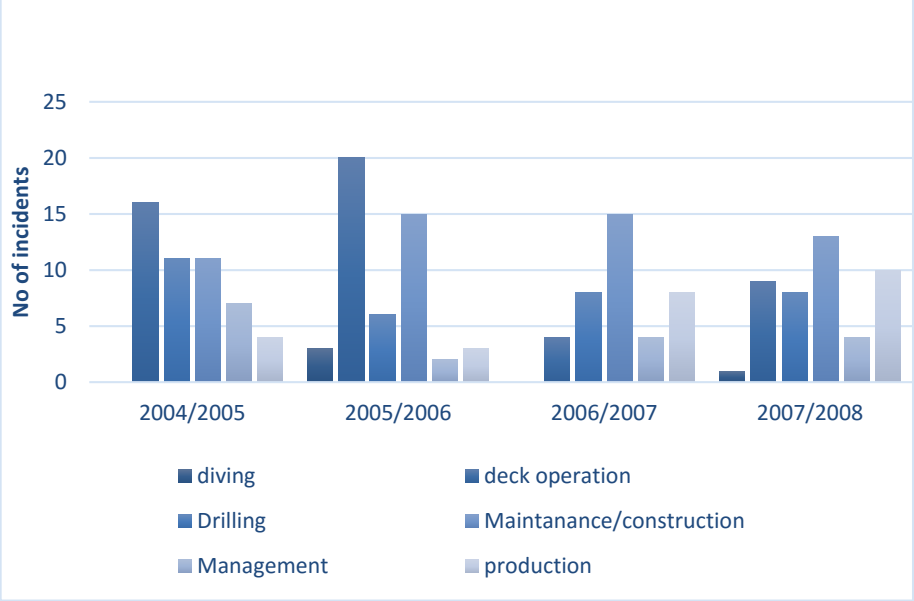
Followed international standards but failed to consider local work forces.

4.6. Inadequate knowledge or training

An employee's knowledge, skill and experience are measured by his competency. The skills, knowledge and attitude can be acquired through proper training. For a safe operation it is important to have a competent personnel. It is always advisable to have suitably qualified and experienced person (SQEP) for risk prone operations.

4.7. Poor maintenance

Poor maintenance is a major cause for fire and explosions. It may also result in hazardous work environment, lack of back-up systems required for emergency replacements. Maintenance tasks also includes the assurance of adequate supply of spare parts. According to the energy institute maintenance factors plays a major role in the root cause of many incidents. Cost cuttings in the organization is one of the main reason for poor maintenance.



Number of reported injuries in offshore 2004-2008 (Energy Institute, 2011)

4.8. Safety critical procedures

Safety critical procedures are instructions on how to carry out a job. It may be in any form on a paper or on a computer screen. If safety critical procedures are carried out incorrectly may lead to serious accidents or fatality. Providing clear and accurate procedures for operating is the most effective measure to mitigate such events. Operators should also make sure that the safety critical procedures are followed during an emergency.

Operator ignoring the safety critical procedure during an emergency situation.

4.9. Commercial and contractual environment

Operations in oil and gas industries are carried out in a complex environment which involves various stakeholders with different requirements, priorities and legal responsibilities. Decision making and communication is largely affected by these factors which may lead to serious consequences. The stakeholders must be aware of their responsibilities and contribution towards the safety of the oil and gas industry.

4.10. Learning incidents and accidents

Incidents and accidents occurs in spite of an organization having various preventive measures, tools and techniques to reduce failures. So it is mandatory that the organizations conduct's routine investigation of incidents for better understanding of the human error and human factor failures.

When these human factors are not managed effectively there are called ***Error-inducing factors***. The interaction between and within these categories can be ***complex*** and difficult to manage. Management of human factors should not be delegated to managers or individual supervisors or to any safety personal. An integrated organizational approach is required to ensure that high level decisions do not create error inducing factors. In the upcoming sections we will be discussing the present approaches and their limitations. We will also be using a suitable method for managing safety during these complex situations.

5. Integrating human factors with Risk Analysis – Currently used methods.

5.1. Risk Analysis

Risk analysis is the central part of risk management. Risk analysis process can be presented by several ways, but all the structures includes the three main key elements i.e.

1. Planning
   - Problem definition, information gathering and organization of work
   - Selection of analysis method
2. Risk assessment
   - Identification of initiating events (hazards, threats and opportunities)
   - Cause and consequences analysis
   - Risk picture
3. Risk treatment
   - Comparing alternatives, identification and assessment of measures
   - Management review and judgement. Decision making.

There are several methods available for integrating human factors with risk analysis in this report we will be discussing the commonly used ***Human Reliability Analysis (HRA)*** and newly developed ***Barrier and Operational Risk Analysis (BORA)***. The draw backs and limitations of these methods will be discussed for the need for a new alternate approach.

5.2. Human Reliability analysis

Human reliability analysis (HRA) can be defined as the method to assess the impact of potential human errors on the proper functioning of a system composed of equipment and people.

The primary functions of an HRA is

- Human error identification
- Human error quantification
- Human error reduction

Human reliability analysis integrates Human factors into risk analysis. The basic relations between the human factors and risk analysis process is mapped below.

Human factor	Risk assessment
Task analysis	System analysis
Human error identification	Hazard identification
Error representation	Risk modelling
Human error quantification	Risk assessment
Human error reduction	Risk reduction

Mapping Human factors with Risk Assessment

The principal components of HRA are briefly explained below,

i. Problem definition

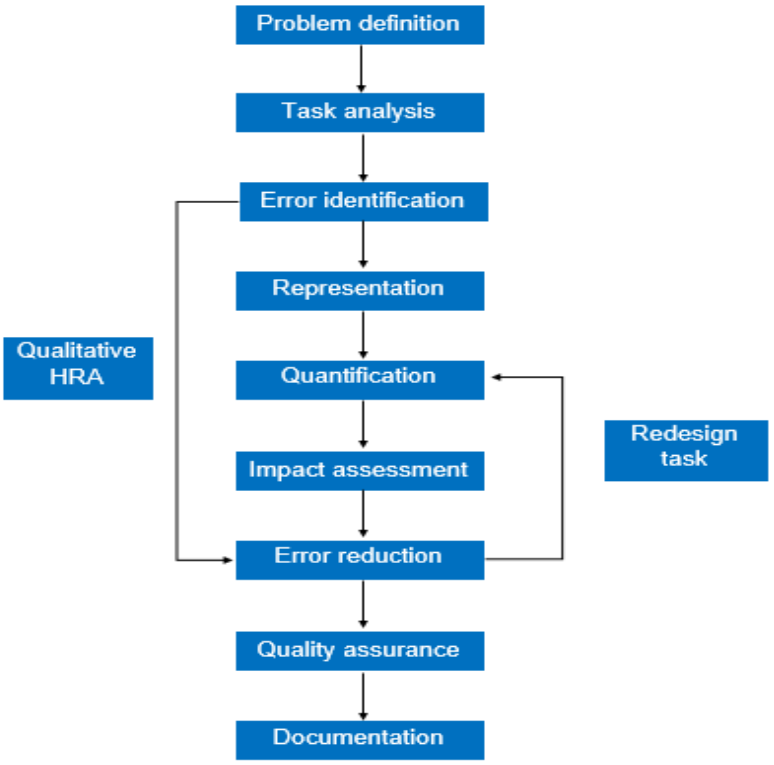
In problem definition the scope of HRA is to be determined, in general a set of key questions has to be answered in order to define the exact scope of HRA

- Is HRA a part of PSA (Probabilistic Safety Assessment) or is it a standalone assessment?
- Will the maintenance errors, misdiagnoses, rule violations errors be considered?
- If a quantified estimate of reliability is required?
- Whether relative or absolute quantification is required?
- What is the stage of system development?
- What are the risk assessment criteria?
- How extensive are the resources available?
- Are there any existing HRA for this system?
- Vulnerability of the system towards human error.

As the HRA proceeds, the problem definition may shift with respect to the above questions.

ii. Task Analysis

Task analysis refers to formally describing and analyzing human-system interactions. It defines the roles of the operators within the system in detail. A formal task analysis is a critical part in the problem definition stage as proper understanding the definition is more important for an analyst to predict the possible errors. task analysis is used to structure the operator's further analysis similar to engineering flow diagrams, pipping and instrument diagrams which are used to define the various states of and operations involved by the engineers. Therefore, without the task analysis further HRA may not be reliable.



HRA process

iii. Human error identification

After completing the task analysis, in human error identification we consider what can go wrong. In this error identification process at the least the following types of error should be considered (Kirwan, 1994)

- Error of omission – failing to carry out a required act
- Error of commission - act performed without precision or act performed in wrong sequence or act performed at wrong time
- Extraneous act – unnecessary act performed instead or in addition to the required act
- Error recovery opportunities- acts which can recover previous errors

iv. Representation

Once the operators task is defined and the error is identified the very next step is to represent this information in a format which helps in the quantitative evaluation of the human error. Usually it is used to see the impact of the human error in the context of other potential contributions to system risk such as hardware and software failures. Recoveries and human errors are usually embedded within the logical systems like fault tree and event tree analysis to carry out the risk assessment.

v. Human error quantification

The next step is to quantify the errors and to determine the overall effect of the human errors on the system reliability or system safety. There are several techniques to quantify the human error probabilities.

$$Human\ Error\ Probability = \frac{number\ of\ times\ an\ error\ has\ occured}{number\ of\ opurtunities\ for\ an\ error\ to\ occur}$$

vi. Impact assessment

The overall system risk level can be calculated once the errors have been quantified and represented in the risk assessment logic trees. Then we have to determine whether the system has an acceptable level of risk or not. If the level of risk is unacceptably high, then either the system must be discontinued or the risk level must be reduced.

vii. Error reduction analysis

Error reduction measures are derived in several ways

- Identifying and changing the root causes of the error (from the error identification stage)
- By altering the defined factors i.e. performance shaping factors
- Or by using ergonomics or engineering judgement to assess the task again in its system context and redesigning it to reduce its likelihood or its impact on the system.

If an error reduction measure is necessary to reduce the risk to an acceptable level, then the error reduction measure should be implemented and the system risk level have to be recalculated. In some cases, several iterations of error reduction methods may occur until acceptable risk factors are achieved.

viii. Documentation and quality assurance

Following the error reduction stage, the results will be documented. Quality assurance team should ensure that the required error reduction measure is effectively implemented and also if any assumptions are made during the analysis should ensure its validity throughout the life time of the system or the life time of HRA.

A detailed procedure for HRA is explained by Barry Kirwan (1994).

5.3. Main Issues in HRA

Human factors helps in the identification of the human performance issues and HRA helps to prioritize human factors issues based on risk. In many cases, Human Reliability Analysis is not matured enough to provide robust prioritization of issues. For example, in Oil and gas industry there are extensive list of human factors issues but in HRA there are no attempts to explain which of these issues is the most important in terms of risk.

Other Important factors like fatigue and safety culture are not adequately addressed by HRA methods.

Significant difference in quantitative results from different methods of HRA or by different analyst using same method.

More reliance on the expert judgement, due to scarcity of empirical human performance data particularly for serious accident situations.

No explicit account for the impact of organization and management aspects.

Limiting accounts for dependencies among actions. These uncertainties may lead to serious consequences.

The main issue is that the events are individually considered and the analysis is carried out separately for every individual events. Then the individual risk level is checked for the acceptance level and if it is lower than the acceptable level the risk is ignored. But in complex systems or complex situations risk of several events may couple and have serious effect on the system. HRA fails to show the dependencies of every events on the other events and their respective relationships. Hence the linear methods like HRA are not suitable for complex situation or complex systems.

5.4. BORA

Offshore Quantitative risk analysis was traditionally a crude analysis of barrier performance stressing technical aspects on consequence reducing systems. PSA (Petroleum Safety Authority) on the road to more detailed analysis reflecting operating factors, initiated a new technique Barrier and Operational Risk Analysis.

The main aim of the project is to create a detailed and quantitative model of barrier performance, including the barriers for preventing the occurrence of initiating events as well as the barriers for reducing the consequences. The work was carried out to create a basic structure for barriers and barrier elements, considering the following barriers as the starting point,

- Prevent loss of containment
- Prevent ignition
- Reduce cloud/emissions
- Prevent escalation
- Prevent fatalities

5.4.1. BORA methodology

BORA an approach for incorporating organizational, Operational and human factors in QRA consists of six steps:

i. Developing a basic risk model
ii. Assigning average industrial frequency or probabilities of basic events and initiating events.
iii. Identification of RIFs (Risk Influential factors) and developing a risk influence diagrams.
iv. Assessing the status of RIFs
v. Calculating average industrial frequencies or probabilities of basic events and initiating events.
vi. Calculating installation specific risk by incorporating the effect of various factors like technical systems, technical conditions, operating conditions, human factors and organizational factors.

i. Development of a basic risk model

The building blocks of BORA model are barrier block diagrams, fault trees and influence diagrams. Barrier block diagram consist of initiating events, barriers to influence the sequence of events in desired direction and possible outcomes of sequential events. It is used to illustrate events scenario and the effects of the barrier systems. Quantitative analysis of the scenario is performed with the help of event tree analysis. Fault tree is used to analyze the performance of safety barriers. And the influence diagram is used to analyze the effect of RIFs in initiating events of event tree and basic events in fault tree.

ii. Assignment of average frequencies or probabilities

The basic step in quantification is to assign industry average frequencies for all initiating events and basic events in the event tree and fault tree respectively. These data can be found in generic databases or internal company databases. These probabilities can also be established by using an expert judgement.

iii. *Qualitative risk influence modeling*

The main moto of the RIF analysis is assigning each initiating events and barrier system with platform specific failure probabilities based on the different status of RIFs. Due to its complexity a combined approach is preferred to develop RIFs

- Top down approach - generic list of Risk Influencing factors is used as a basis
- Bottom up approach – events are chosen as a starting point

According to (Vinnem, Aven, Hauge, Seljelid, & Veire, 2004) following groups of RIFs are considered

- Personal characteristics
- Task characteristics
- Characteristics of the technical system
- Administrative control
- Organizational factors

RIF examples

RIFs for each initiating events and basic events in the event tree and fault tree should be identified. The number of RIFs should be limited to a maximum of 6 or lower for every event. During this process input from operational personnel is important to identify the important RIFs.

Influence diagrams are used to analyze the effect of RIFs on both the initiating and basic events.

An example of various RIFs in different groups are shown in the following table,

RIF group	Generic risk influence factors
Personal characteristics	Competence
	Working load/stress
	Fatigue
	Work environment
Task characteristics	Methodology
	Task complexity
	Time pressure
	Tools
	Spares
Characteristics of the technical system	Equipment design
	Material properties
	Process complexity
	HMI (labels, alarms, ergonomic factors)
	Maintainability / accessibility
	System feedback
	Technical conditions
Administrative control	Procedures
	Disposable work description
Organizational factors / operational philosophy	Programs
	Work practice
	Supervision
	Communication
	Acceptance criteria
	Management of changes

RIFs within different groups (Vinnem, Aven, Hauge, Seljelid, & Veire, 2004)

iv. Scoring of RIFs

Regarding the scoring of RIFs two options are proposed in BORA

- By using the results from existing projects like MTO investigation of incidents, TTS (Technical condition Safety). TTS project is a method to map and monitor the safety levels based on the status of various safety barriers and safety critical elements, and scores are given to each system according to predefined performance standards.

- Scoring scheme will be developed for each status of RIF on the basis of expert judgement on a specific platform.

Rating	Description of safety level
A	Condition is significantly better than the reference level
B	Condition is in accordance with the reference level
C	Condition satisfactory, but does not fully comply with the reference level
D	Condition is acceptable and within the statutory regulation' minimum intended safety level, but deviates significantly from the reference level
E	Condition with significant deficiencies as compared with "D"
F	Condition is unacceptable

Definition of grades in TTS project (Vinnem, Aven, Hauge, Seljelid, & Veire, 2004)

Score	Grade characteristics for the RIF procedures
A	Almost perfect procedures, with checklists, highlighting of important information, illustration, etc.,
B	Procedure better than industry average
C	Industry average procedures
D	Poorly written procedure and no highlighting
E	Procedure incomplete, out-of-date, inaccurate much cross-referencing etc.,
F	No procedures, even though the task demands them

Scoring scale for RIF procedures (Vinnem, Aven, Hauge, Seljelid, & Veire, 2004)

During practical assessments both these approaches may be combined.

v. Calculation of installation specific frequencies or probabilities

The main purpose of this task is to adjust the average industrial probability based on the scoring of the RIFs. Here the three main aspects are discussed

- Formulas for calculating installation specific probability or frequencies
- Assigning appropriate values for Q_is
- Weighting of RIFs

Let A be the failure event, $P_{rev}(A)$ be the installation specific probability of event A

Probability P_{rev} is determined by

$$P_{rev} = P_{ave} \sum_{i=1}^{n} Wi \ . Q_i$$

Where,

P_{ave} = industry average probability
W_i = weight / importance of RIF_i for the event
Q_i = measure of status of RIF_i
N = number of RIFs

Here

$$\sum_{i=1}^{n} W_i = 1$$

Therefor the main challenge is to determine the appropriate values of Q_i and W_i

Determining appropriate values of Q_i

To determine the values of Q_is we need to associate specific numbers to each score A-F.

P_{low} is the lower limit for P_{rev}, determined by expert judgement
P_{high} is the upper limit for P_{rev} determined by expert judgement

Then subsitute i = 1,2,….n in the following

$$Q_i = \begin{cases} \frac{P_{low}}{P_{ave}} \ \ if \ \ S_i = A \\ 1 \ if \ S_i = C \\ \frac{P_{high}}{P_{ave}} \ if \ S_i = F \end{cases}$$

Where S_i denotes the score of RIF_i

To determine the weight of W_i generally it is started by assigning weightage 10 to the most important RIF_i and relative weights are assigned for the remaining RIFs.

vi. Recalculating the installation specific risk

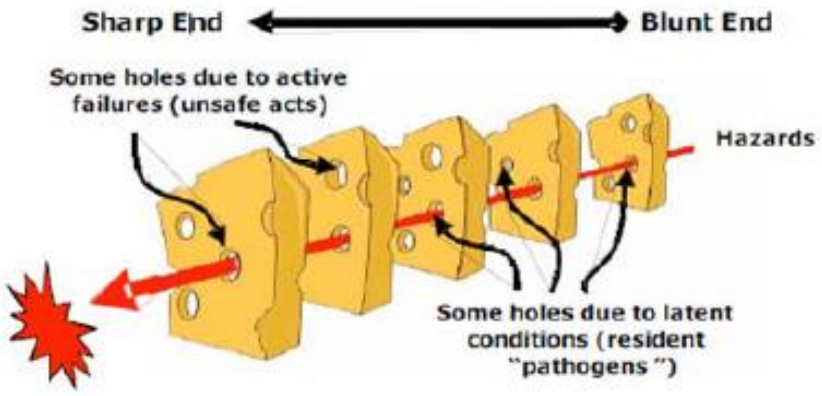
By using the platform specific data P_{rev} as a input we calculate the revised value for the installation specific risk using the risk model. We also consider the organizational factors, human factors, operational conditions, technical conditions and the technical systems on the platform during the revised risk values.

5.5. Limitations of BORA – Need for an resilient approach

Risk Influencing Factors (RIFs) are not independent always they will influence each other, hence it is better to have a clear picture of the relationships of RIFs.

RIFs are not clearly defined. RIFs are the factors that may influence the probability of an event occuring. RIFs are not barriers but they the factors which influences the performances of the barriers and other external factors. According to this, it is difficult to distinguish between the RIFs and barriers.

According to Hollnagel apidemiological models are still following the principles of sequential model as the direction of causality are in a linear fasion eg swiss cheese model. The barrier block diagrams are similar to the swiss cheese model which shows the direction of causality in linear fasion. But for complex situation or systems the defects are often transienteg the holes in the swiss cheese are moving continuously.



Swiss Cheese model (Reason, 1997)

Similar to RIFs the barriers are not independent to each other. For example in a gas leakage incident the barriers are pressure detection, alarm detection, human inspection etc. the barrier human inspection cen influence the other barriers. If the human inspection is carried earlier than the other barriers then it influences the probability of the leakage.

BORA seems simple in theory but it is complicated in operation. The block diagram is drawn for every possible initial events, for instatnce in a drilling process the are several intial events and each event can be drawn a barrier. Hence for the entire operations the number of block diagrams are not imaginable. Hence in complex systems drawing the clear picture of the barrier block diagram is not easy and it is diffucult to incoperate non-linear relationship.

Need for a Resilient approach

As dicussed explained above, both the HRA and BORA doesnot establish a relationship model of the events or functions for better understanding of the problem. These approaches cosiders asingle event at a time and if the risk level are moderate and acceptable the event is considered to be safe. But when this events with low probability couples with various other events it leads to an incident or accident.

As we all know accident are not because of a single cause or incident eg piper alpha, Macondo blowout etc., it is a combinations of various causes. Hence understanding the relationship of the functions and their dependencies place a major role in preventing of accidents.

In order to over come these difficulties I have a recommended an approach for risk assessment using the concept of **resilience engineering**.

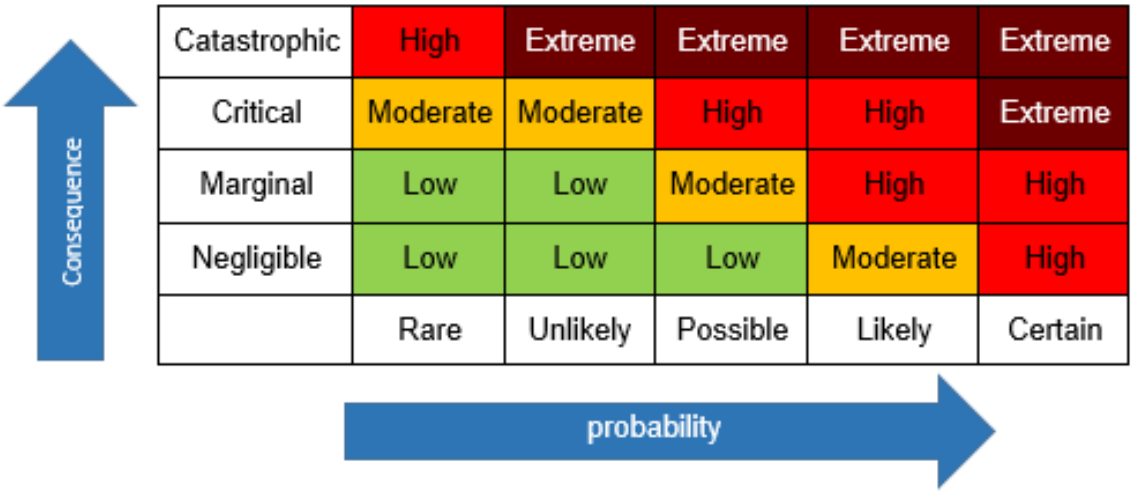
6. Resilience engineering

6.1. What is resilience engineering?

"Resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel, 2008)

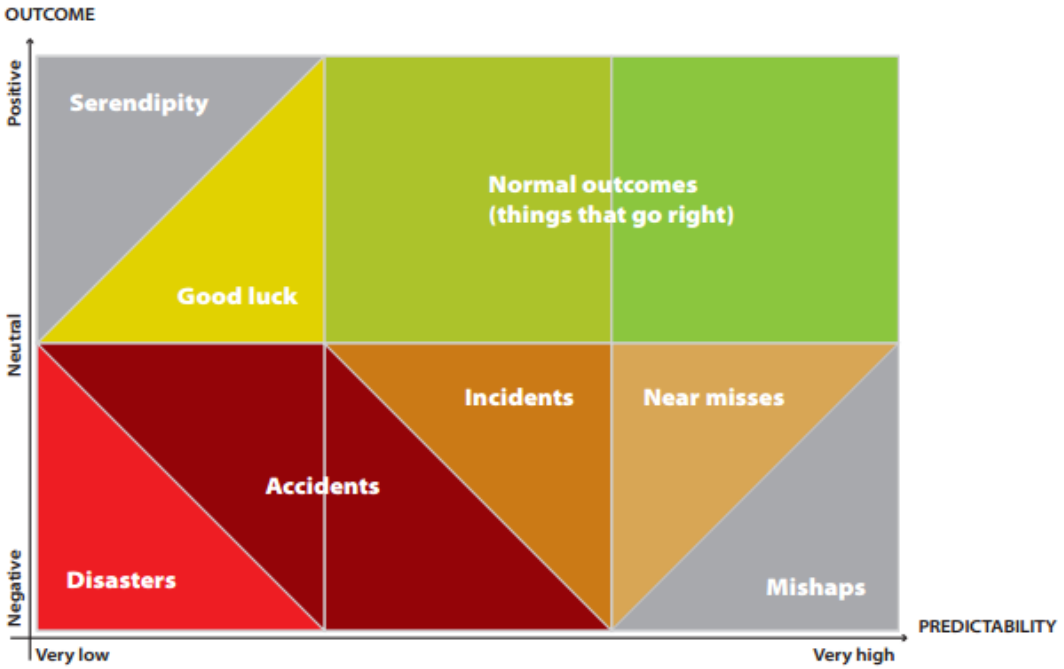
6.2. Scope of resilience

Traditionally safety was the focus on what could go wrong, or what went wrong. This was sensible because an enterprise has to understand what went wrong as well as what may go wrong in order to develop preventive measures against the event or its outcomes. The traditional risk matrix illustrates the above line of thinking. The example of a risk matrix is shown below,



Risk matrix

The risk matrix is generally based on the risk level of the possible outcomes with their probability of occurrence and their severity of the consequences. The risk matrix looks only at things that might go wrong but when considering the possible outcomes of an event it can go right as well as wrong. It therefore reasonable to expect the things which normally go positive can also be expected to go wrong in an unusual way. In this perspective it is advisable to include both the positive and negative outcome of the consequences i.e. all possible outcomes as shown in the figure (possible outcomes).



Possible outcomes

Traditionally safety was focusing on negative outcomes which has very low probabilities of occurrence such as accidents and incidents. The unwanted negative outcomes like mishaps are generally eliminated. While considering a simple relation between the event and their outcomes, it is possible to characterize several subsets of the outcome as,

- Positive outcomes with a high probability of occurrence. This subset consists of success or the events that not only turns positive but are also intended and expected to be positive. It is highly predictable that chances of something going wrong is very less.

- Positive outcomes with low probability of occurrence. This subset represents the positive things that can happen, but unexpectedly.

- Negative outcomes which have very low probability of occurrence i.e. things which go wrong unexpectedly but not unimaginable outcomes. This subset represents the outcomes that are serious and hard to predict. This includes the common category of incidents and accidents.

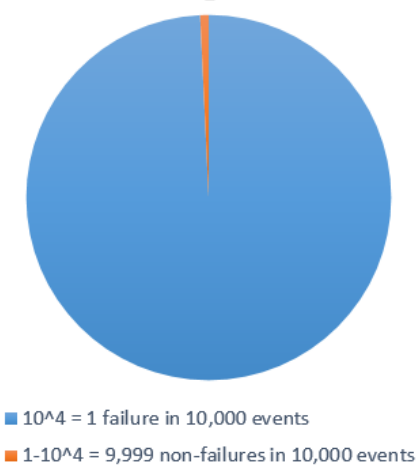
- Negative outcomes with a high probabilities of occurrence, these outcomes are expected to occur regularly. In practice these outcomes have a minor consequence as they would have been eliminated, for example using ALARP principle. These outcomes are commonly called as near misses or unsafe actions or almost accidents. The subset mishaps i.e. near misses with serious consequences which is predictable are normally assumed that it would have been eliminated.

In order to know about the traditional and current safety scenario we have a proper understanding of Safety I and Safety II

6.2.1. Safety I things that go wrong

Historically, the starting point of safety has been the occurrence of actual adverse outcomes (accidents) or potential adverse outcomes (recognized risks). Things that go wrong i.e. adverse outcomes are usually explained by the predictable cause and their Reponses to either contain them or to eliminate them. New types of accidents if any have been accounted similarly by introducing new causes such as human factors or technology defects. As this was effective in providing short term solutions, for centuries we have been explaining accidents in terms of cause effect relations. unfortunately, persistence of the deficiencies will not be explained by just seeing on the hindsight of the deficiencies.

Consequences of defining safety by adverse outcome (what can go wrong) is illustrated as follows, consider the following figure

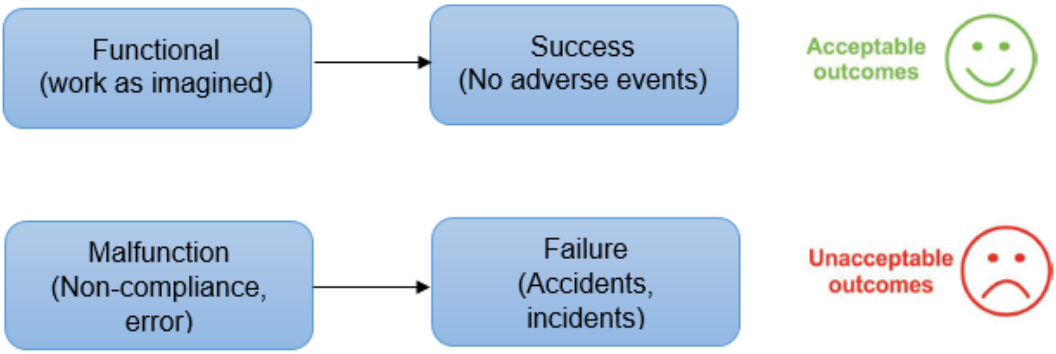


Imbalance of things can go right and things can go wrong (Hollnagel, Wears, & Braithwaite, 2015)

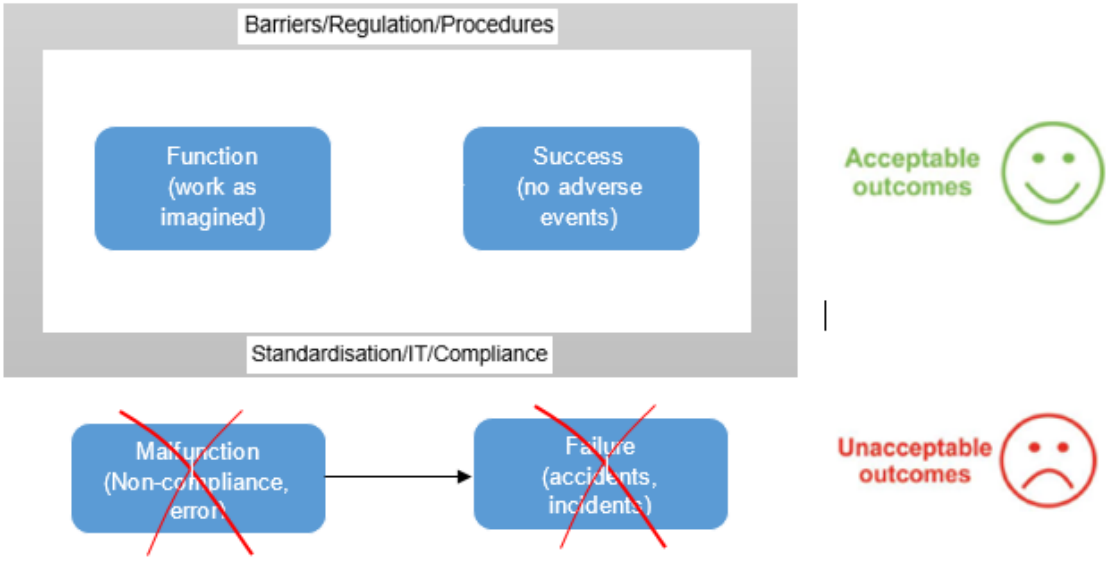
The probability of the things can go wrong is as thin line as shown in red colour is 1 out of 10000 events this indicates that the probability of things can go right is 9999 out of 10000 events.

Safety-I always focus on what went wrong, numerous methods explain what went wrong or methods to find the failure components are explained in numerous models. The general solution is look for malfunctions or failures and try to eliminate their causes or to introduce barriers or both, it is called as Find and Fix.

It is quite different situation for the events that go right, they are usually given very less attention in the safety management activities like risk assessment and safety assurance. There are no regulations from the authorities to monitor what goes right. It is assumed in Safety-I that the things that go right and things go wrong have different causes and happens in different ways.



Failures and success according to Safety-I

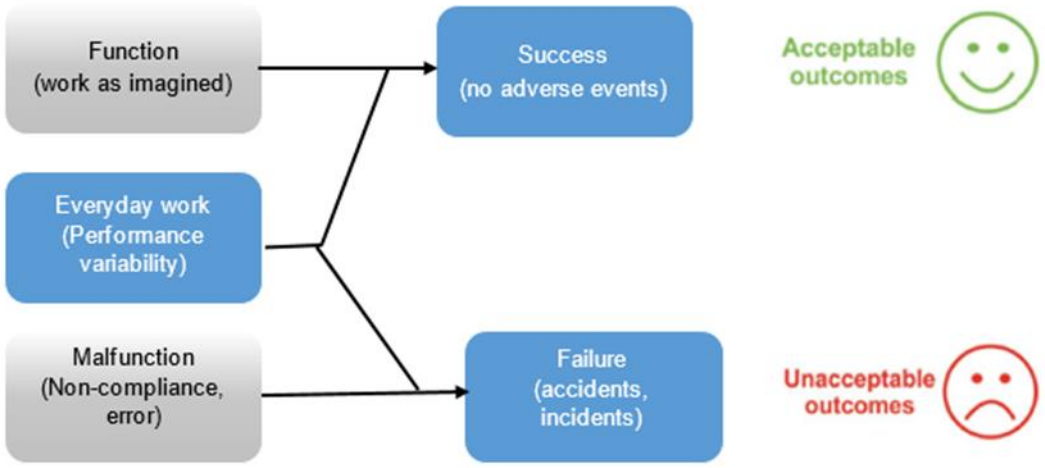


Safety by eliminating and preventing

Safety is by eliminating the way of malfunctions and preventing the way of going right with the help of barriers is shown above Safety-I. It also assumes that the components of the system are bimodal in functioning i.e. it has two modes of functioning either performing correctly or malfunctioning.

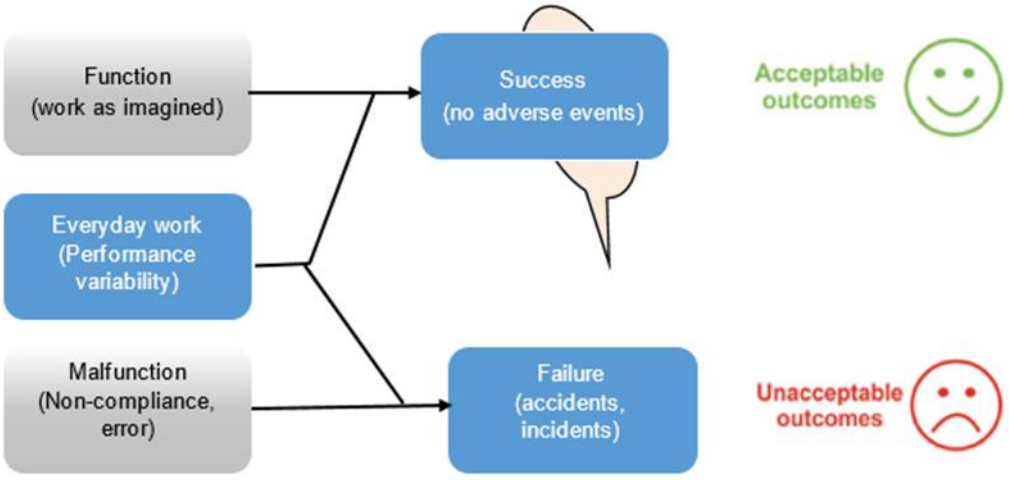
6.2.2. Safety-II things go right

Unlike Safety-I, in resilience engineering instead of looking only at things which go wrong, things which go right should also be considered and understand how it happens. It is acknowledged that things go right because the workers are able to adjust to the conditions and work accordingly rather than work as imagined. It also acknowledges that both the outcomes (acceptable and not acceptable) have a common basis as shown below



Basics of safety -II

According to resilience engineering failures are not treated as a unique individual events, it is seen as an expression of everyday variability in performance. It is a safe consideration as the things that goes wrong has been right several times before and will also go right in the future.



Understanding variability of everyday performance

Safety-II is ability to function as required in varying conditions, to bring the number of acceptable outcomes as high as possible. Therefore, proper understanding of everyday activities is very much necessary to understand why things go right. Proactive approach of safety management is required so to intervene before something goes wrong.

6.3. Four corner stones of resilience

The main goal of resilience engineering is to achieve resilience in a system. For an organization to be resilient it has to possess four essential abilities[11]

- Ability to respond

  A resilient organization should be able to respond i.e. know what to do during regular and irregular disruptions either by responding with prepared set of responses or by adjusting the normal functionality. It is the ability to respond or knowing what to do. This ability to address is called as actual.

- Ability to monitor

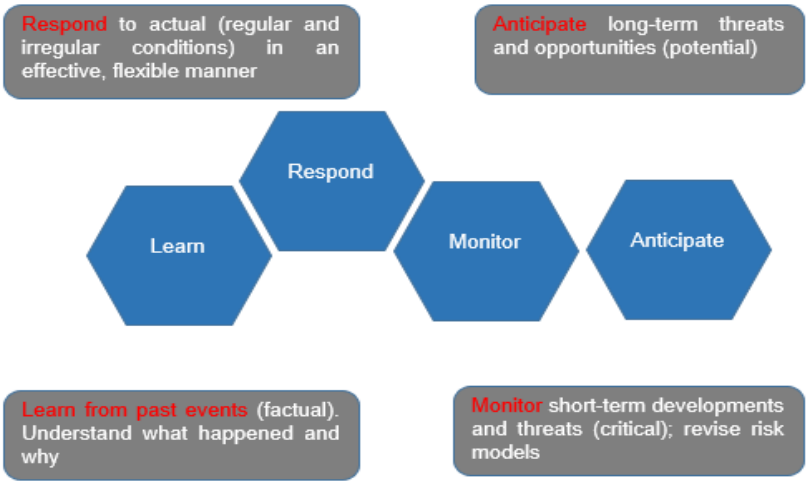
  A resilient organization should be able to monitor i.e. Knowing what to look for that can bring threats to the system. The act of monitoring should cover what is happening in the system, its environment and its own performance. This ability to address is called as critical.

- Ability to learn

  A resilient organization must be able to learn from its experience. In particular, it should know how to learn right lessons from right experiences including both success and failures. This ability to address is called as factual.

- Ability to anticipate

  A resilient organization should be able to anticipate i.e. to know what to expect like threats, developments and opportunities in the future. This ability to address is called as potential.



Abilities of resilience engineering

All the four abilities are essential for an organization to be resilient. Resilience engineering ensures that all the abilities cannot be considered individually or independently. Resilience engineering approach is currently used in fields like air traffic control systems where high safety standards are followed. The advantages of resilience engineering approach over safety management and safety culture based on some general categories and characteristics are shown by comparing the three approaches.

Approach / Indicators	Safety management	Safety culture	Resilience engineering
Commitment of top-level management	Defined goals on occupational safety and health issues as well as principles of prevention	Safety awareness on all levels of the organisation, safety philosophy described, allocation of necessary organisational structure	Clear instructions for safe decision making
Resources	Management of resources as a responsibility of top-level management, standards based on estimation of necessary resources	Provision of resources as a leadership task, conflicts between efficiency and safety are decided in favour of safety	Allocation of resources buffer for critical situations
Flexible scope of action/ compliance	Compliance with safety regulation, observation of compliance	Promotion of safety awareness on all levels	Definition of a room to manoeuvre when it comes to safety relevant decisions
Continuous process improvement	Audits, frequent revisions	Measuring and learning, culture to report failures and near misses	Proactive identification of possible failures, identification and promotion of safe and good practices

Comparison of Resilience Engineering with Safety Culture and Safety management

6.4. Resilience engineering risk perspective

Resilience engineering is an important field for understanding and managing safety in socio-technical systems. Various efforts have been made in the recent years to provide a suitable clarification and concepts for a resilient system. The key points to understand a resilient system are

- Unacceptable events cannot be attributed to malfunctioning of components or breakdown. They are understood as an unexpected combinations of normal performance variability.
- According to resilience engineering effective safety management is not based on hindsight or failure probability calculation nor on error tabulation. Safety management must be proactive not just reactive.
- In conventional view on safety management, performance variability is considered as a threat or something that should be avoided. They are constrained by means of barriers, rules, interlocks and procedures.
- Performance variability is normal and essential in resilience engineering. It is considered as the source of both negative and positive outcomes. Constraining performance variability cannot will not lead to safety, instead reinforce the performance variability leading to positive outcomes.

For an organization to be resilient it must have the following four abilities

- Ability to respond to regular and irregular threats.
- Ability to monitor, know what is going on
- Ability to anticipate risk and opportunities
- Ability to learn from experience

In order to formulate a risk perspective for resilience engineering we have to understand the basic risk perspective. Two main categories of risk perspective are

- Probability is considered as the main component of risk and it is interpreted as an objective probability of an activity. It is referred as the traditional risk perspective.
- Uncertainty is the main component of the risk and probability is a subjective tool (knowledge based) for expressing these uncertainties. This is referred to alternative perspective of risk.

In traditional risk perspective, risk is defined by probability distribution or by probabilities expressing stochastic uncertainties. Probability P is defined as the fraction of times the event A occurs. The probability distribution P_x is associated with X a random variable. Here the risk is defined by P and P_x, uncertainties are often neglected or as statistical variations reflected by simple confidence intervals.

In alternative risk perspective uncertainty is the main component not probability. According to Aven risk perspective it is two dimensional combination

i. An event A and its consequences C
ii. And the associated uncertainties U

It is commonly referred to (A, C, U) perspective, the risk associated with an activity is understood as

Uncertainty about and severity of the consequences of an activity (Steen & Aven, 2011)

The uncertainties are described using the subjective probabilities P based on knowledge K. If probability P is said to be 0.1 it means that according to his/her degree of belief the probability of an event A, drawing a random ball from an urn containing 10 balls is 1. This risk perspective includes the following elements (A, C, P, U, K). According to alternate perspective the probability is just a tool to express uncertainties.

Risk perspective for resilience engineering

The basics used here is (A, C, U) risk perspective explained above. In order to introduce define resilience we introduce a concept of vulnerability (Steen & Aven, 2011)

Vulnerability or robustness = (C, U|A)

The vulnerability is defined as a two dimensional combination of C consequences and its associated uncertainties U, given occurrence of event A. The uncertainties of various consequences C can also be defined by the probability K of occurrence of the event A. thus the vulnerability is also defined using the following elements (Steen & Aven, 2011)

Vulnerability = (C, P, U, K|A)

Where C is consequence, P probability, U uncertainty and K background knowledge given that the event A takes place. Vulnerability analysis is a part of risk analysis since vulnerability is considered as an aspect of risk.

Resilience is a closely related concept of robustness. The key difference is the event A, the consequences C and the Uncertainties are related to a fixed A in robustness and vulnerability. Where as in resilience engineering the event A is open to any type of event. Therefore, resilience can be defined as (Steen & Aven, 2011)

Resilience (C, U| any A, including new types of A)

Resilience description: (C, P, U, K| any A, including new types of A)

For all the above definitions, consequences C depends on the performances of barriers B, to show this explicitly we write C = (B, C) resulting in describing resilience as (B, C, P, U, K| any A, including new types of A)

The performances of the barriers are expressed by the capacity of the barrier. In general performance influencing factors (PIFs) influences the performances of the system and the barriers.

All the measures carried out to manage resilience is called as the resilience engineering. The risk assessment following the risk perspectives (C, P, U, K| Any A, including new types of A) is referred to as extended risk assessments.

The main elements of an extended risk Assessment are (Steen & Aven, 2011)

- Identifying initiating events, A
- Cause analysis
- Expressing vulnerability (C, P, U, K|A) i.e. Vulnerability analysis
- Resilience analysis expressing (C, P, U, K| Any A, including new types of A)
- Risk description and characterization

Here the term cause refers to the events and conditions leading to a specific outcome i.e. the occurrence of event A (Steen & Aven, 2011).

7. Resilience Engineering Approach to Risk Assessment (FRAM Method)

FRAM method describes the systems failure as result of a functional resonance from the variability of normal performance. This is a model or a representation of organizational and/or individual functions where the characteristics of every function provides the basis for describing its potential variability. It was first proposed by Hollnagel 2004, since then it is used in various domains such as aviation, Air Traffic Management, healthcare. FRAM method can be used as accident investigation model to find where these coincidences may have arisen, as well as in risk assessment to explain how coincidences may arise from the performance variability.

7.1. Principles of FRAM

The FRAM has a clear articulated theoretical basis, explained in the following four principles

- The principle of equivalence of success and failures
- The principle of approximate adjustments
- The principle of emergence
- The principle of functional resonance

Principle of equivalence of success and failures

Principle of equivalence of success and failures can be summarized into the following points

i. Both failures and normal performance are an emergent phenomena and are from a common source
ii. The outcomes or result of the actions may differ from that was required, intended or expected these differences can be either harmful or beneficial.
iii. The flexibility and adaptability of human work is the main reason for its efficiency.
iv. However, the adaptability and flexibility of the human can also be the reason for the failures that occur, although it is cause of rare occurrence of such failures.

The inevitability of approximate adjustments

The variability of a system's normal functioning in a systemic perspective is due to two basic facts

- Usually the operating conditions are underspecified rarely, if ever, as imagined or as prescribed. This is a consequence of intractability in socio-technical systems. This means that it is practically impossible to prepare in advance, a set of instructions that can be followed later. The best possible solution is to provide guidelines that can be used as a basis for concrete actions. Guidelines and procedure are generally supported by extensive professional training.

- Second, that the operating conditions more or less changes dynamically in an orderly manner. Hence it is impossible to prepare a precise procedure in advance. Therefore, the people who are supposed to act in the situation be managers or operators can plan for a short term. They must be always ready to revise their plans and adjust the plan implementation matching the current conditions.

Consequences are emergent

The variability of normal performance can rarely be large enough to be the cause of a malfunction or an accident itself. But the variability combines in an unexpected way from multiple functions leading to disproportionally large consequences, hence producing non-linear effects. Hence both normal performance and failures are considered to be emergent rather than resultant phenomena, since neither of them can be attributed to the malfunctioning's of a specific parts or components.

Functional resonance

FRAM method replaces the traditional cause-effect relationship with the principle of resonance. By focusing on the relationship between system functions FRAM overcomes the limitations of established methods. This principle means that the variability of number of functions can resonate every now and then, this means that there is a possibility of the variability of one function reinforce with other leading to exceed the normal limits. Of course the outcome can be advantageous as well as detrimental. This principle makes possible to capture the dynamics of the system functioning, therefore the emergent system properties that is hard to understand is decomposed into isolated components in order to identify it.

7.2. Description of the FRAM method

The method comprises of five steps

- The first step is to define the purpose of the analysis as the FRAM can be developed for both accident investigation and as well as safety assessment.

- The second step is to identify and describe the system functions. In FRAM terms, a function constitutes an activity which has necessary consequences for the state of another action.

- The third step is assessing and evaluating the potential variability of every singular function. The methodology uses a priori assessment of set of Common Conditions (CCs) that have an influence on the performance variability. The CCs are derived from Common Performance Conditions (CPC) described by Hollnagel. This evaluation must be integrated with retrospective information extracted from various accident database to the extent of available data.

- The fourth step Is to identify the functional resonance. The main aim is to determine all possible ways in which a variability of a single functions spreads in the system and how it combines with the variability of other systems

- The last step is to identify the effective counter measures to be introduced in the system. In FRAM perspective the main aim of the counter measure is damping the performance variability and maintain a safe state in the system. But it is also consistent with the principle of resilience engineering which considers to amplify the functional resonance that leads to the desired outcomes.

  The outline of how FRAM can be used in risk assessment of an organizational change is discussed in the following

  Step 1: purpose of the analysis

  The very first step is to identify the purpose of the analysis, as mentioned earlier FRAM can be used as a safety assessment method as well as an accident investigation method. Although major steps are same in both the methods, but some of the required details needed may vary in both the cases. For example, in accident investigation performance conditions are well known, where as in future conditions it has to estimated. In the present description the focus is on looking into possible future events i.e., focus is on risk assessment of an organizational change. Once this objective is achieved the following steps are to be followed in an orderly manner to identify and evaluate risks.

Step 2: Identification and Description of relevant system functions

System identification and description of the system functions takes place in the following sub steps.

Function Identification

Once the modelling level and its focus is determined, the next step is to identify the system functions. The principles that guide this is the need for achieving a description of normal activities performed by the socio technical system is being analyzed. Therefore, it is necessary to describe the functions without judging the possible quality or correctness of their outputs. The identification of functions is useful to start from task analysis or from the official documents of the organization. The function identification process is very essential in assuring the quality of resulting system modelling.

Once the initial function identification is done the next step is characterization of each functions. This does not prevent that the set of functions is modified at a later point. It is easy to make modifications in the FRAM modular approach.

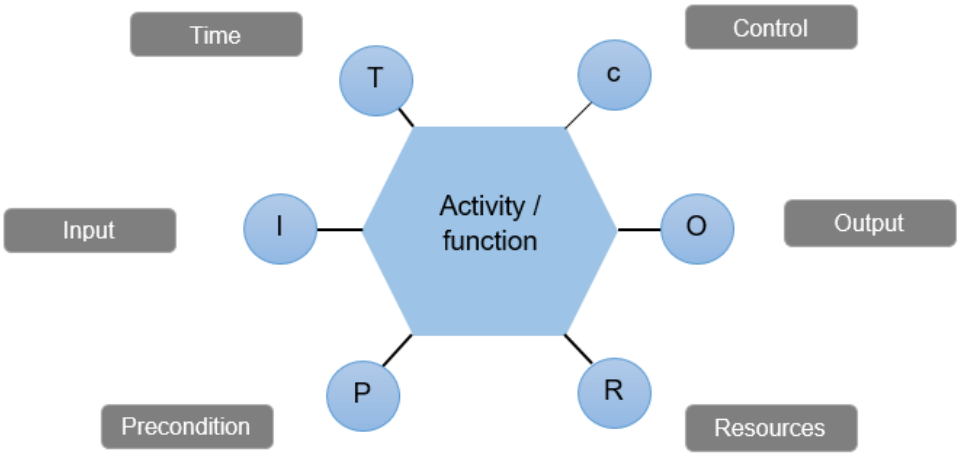
Function description

Following the function identification, it proceeds by characterization of each function in terms of six parameters,

1. Input (I): that which the function process starts the function or transformed to produce the output
2. Output (O): that which is the result of the function it can be either a product or specific output or a state change.
3. Preconditions (P): systems conditions that has to be fulfilled before a function can be carried out.
4. Resources (R): that which the function consumes or needs to produce the output.
5. Time(T): temporal constraints affecting the function (duration, starting time or finishing time)
6. Control (C): how the function is monitored or controlled.

The basis for the further analysis is the description of each function that is made in a simple table format. The representation is a diagram showing functions in hexagons and the connections between them as lines. Unlike event tree and fault tree the analysis is made on the basis of descriptions of the functions rather than the basis of the diagram.

FRAM model



FRAM model

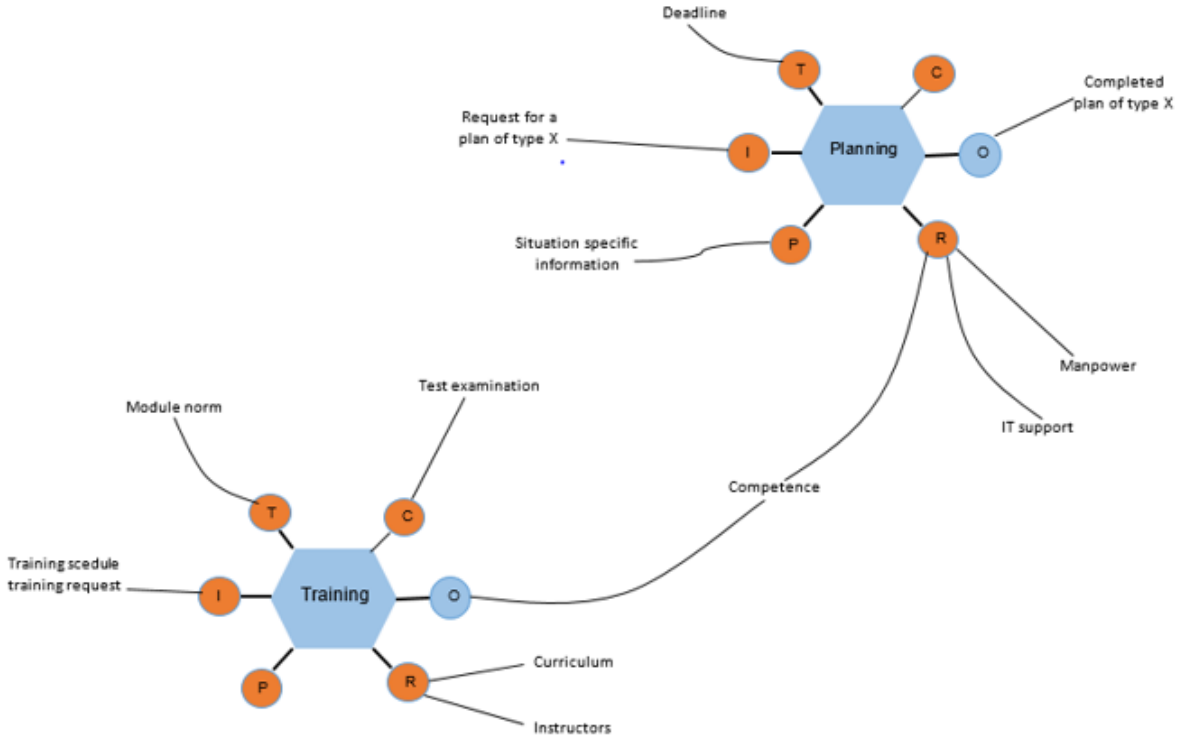
FRAM model differs from the classical models like event tree and fault tree by the fact that it is not a diagram or flowchart but the description of the functions in terms of the six characteristics or aspects. Classical models like event trees and fault analysis show only a single representation of a system, which focus on one set of possible cause effect relations. But in FRAM model no such constraints exists.

There will always be a straight forward description of the six aspects or parameters but in the spirit of the method it can always be refined at a later stage of the analysis. On completion the tabular description defines a set of potential couplings among other functions.

FRAM instantiation

Once the functions have been described the very next step is to identify the couplings among the functions. This can be achieved by linking the functions in accordance with the descriptions provided by the tables. The result constitutes the FRAM installation of a system and is often represented graphically.

In FRAM installation the link represents the dependencies among the functions defined by the six aspects rather than the causal flow or cause effect relations. Only for the purpose of the illustration an example of cause effect relation is shown below



Example of FRAM installation (Hollnagel, 2011)

Step 3: Assessment of potential performance variability

In FRAM the variability of function is affected by performance conditions, in the sense performance variability will be increased by adverse performance conditions whereas the advantageous performance conditions will reduce the performance variability. Therefore, it is necessary to understand the nature and origin of the performance for this change in perspective to be practically useful.

In addition to the variability from habitual or intentional performance adjustments, it also the result of a number of external and internal factors. The six main sources of organizational and human performance variability are.

1. Fundamental human psychological and/or physiological characteristics. Example – vigilance and attention, refractory periods, forgetting, fatigue etc.
2. Pervasive psychological phenomena of higher level like creativity, ingenuity and adaptability, for an example overcoming temporal constraints and under specification.
3. Organizational conditions and requirements
4. Social or team psychological factors, such as complying with group working standards, etc.
5. Ambient working conditions

6. Work environment variability induced by unpredictability of the domain.

The detail explanation of common conditions and performance variability as a function of performance conditions and also performance variability of specific functions are provided by (Hollnagel,2013).

Identification of functional resonance

In FRAM, the variability of a function can have two different ways of consequences. One is through the quality of a function's output. This is, analogous to various possible failure modes of an output. i.e. the in which output differs from what it was intended or expected. The failure modes can be characterized as shown below,

Timing	Too early / Too late / omission
Duration	Too long / Too short
Sequence	Reversal / Repetition / Commission / Intrusion
Object	Wrong action / Wrong object
Force	Too much / Too little
Direction	Wrong direction
speed	Too fast / Too slow
Distance	Too far / too short

Dimension of failure modes

The evaluation of downstream influence of the variability of a function is supported by the characterization of the outputs in terms of failure modes. For an example, if the output of a function comes too late, then it will be resulting in reduction of the time for the following functions to produce their output.

Other way is that the variability of a function can have consequences such that the performance variability may lead to change in one or more CCs. Increased variability may result in increased use of resources, may increase the number of goals or reduce the available time. This makes possible for accounting direct coupling among functions as well as the influence on common performance conditions (CPCs). In practice it can be too complex for this to be done manually and determining the propagation of variability, therefore it should be supported by some kind of software tool.

Identification of effective countermeasures

Once the possible range of performance variability and the potential risks are identified obviously the next and final step is to determine the countermeasures for either mitigating or eliminating those risks. Where there is a case in which the risk can be eliminated by changing something or any other means it should be done since prevention is the most effective solution. In the cases where the risk cannot be eliminated by changing something then other solutions should be considered.

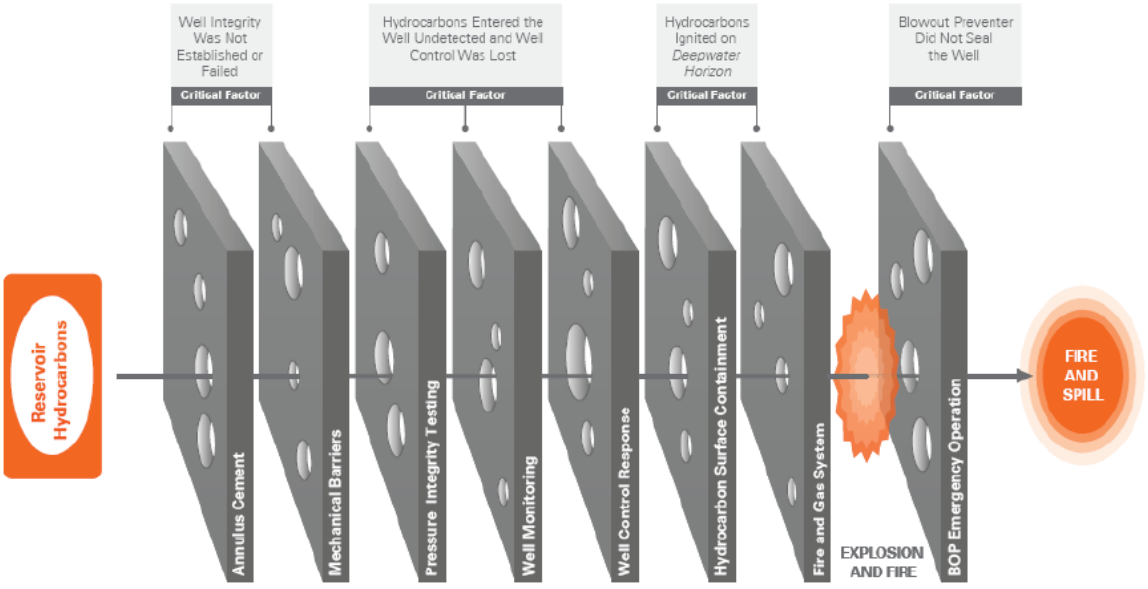
In functional perspective one should also consider solutions that directly address the dynamics of the system i.e. the way in which functions are carried out. If the risk is associated with the performance variability of either from a single function or through the couplings of various functions the logical solution is to dampen the variability. Dampening can be achieved in various ways it should be selected in a way such that it addresses the most likely source of the variability.

8. Case study

8.1. Deepwater Horizon - Macondo Blow Out

Deep water horizon a drilling rig which was stationed in the Gulf of Mexico for an exploratory drilling on the Macondo well. Deepwater Horizon is a mobile and temporary rig which drills the well and identifies if any viable reservoir of hydrocarbons and makes it ready and safe for a permanent production rig. This process involves drilling a deep bore hole in stages, inserting steel tubes and filling the casing with the cement. 20 April 2010, was an unforgettable day in the history of offshore oil and gas industry on which the world's largest offshore oil spill occurred with a total of 11 fatalities – The Macondo blowout. Complete accident report by BP (British Petroleum) can be found in the following site:
http://www.bp.com/content/dam/bp/pdf/sustainability/issue-reports/Deepwater_Horizon_Accident_Investigation_Report.pdf

The accident report concludes that the accident was not caused by a single action, it was result of a complex interaction of human judgements, mechanical failures, engineering design, team communication and operational implementation. The accident sequence is so complex where several barriers where breached. The illustration of barriers breached is shown below using Swiss cheese metaphor.



Swiss cheese metaphor – Macondo blowout (Hubbard & Embrey, 2010)

8.2. FRAM Safety Analysis – Macondo Blowout

A simple illustration of the FRAM model is explained by considering the Macondo blowout is discussed below.

Identification of essential system functions and characterization of each function based on six parameters

Exploration and production process involves a large number of companies working on the platforms according to their specialties. In deep water horizon the primary companies involved were Transocean (platform owner), Halliburton (supplier of cementing services) and British petroleum (operator). For a better focus on the analysis functions which are directly involved during the time of accident are studied. However, for deeper analysis we have to consider the entire exploration and production process. We have focused on the main functions Drilling, cement Placement Temporary Abandonment. Drilling is the function of drilling wells with the support of geological and geophysical studies. The drilling mud is used as a coolant during the drilling process. Monitoring the volume and density of the mud is necessary for avoiding problems in formation and removing the drilling waste. During this activity invasion of hydrocarbons can occur in the well hence control measures should be taken by controlling the mud pressure or by using safety valves.

Following the drilling activity comes cement placement, Here the drilling column is removed and a steel tube insulation is inserted. The gap between the steel tube and the formation is injected with a special cement.

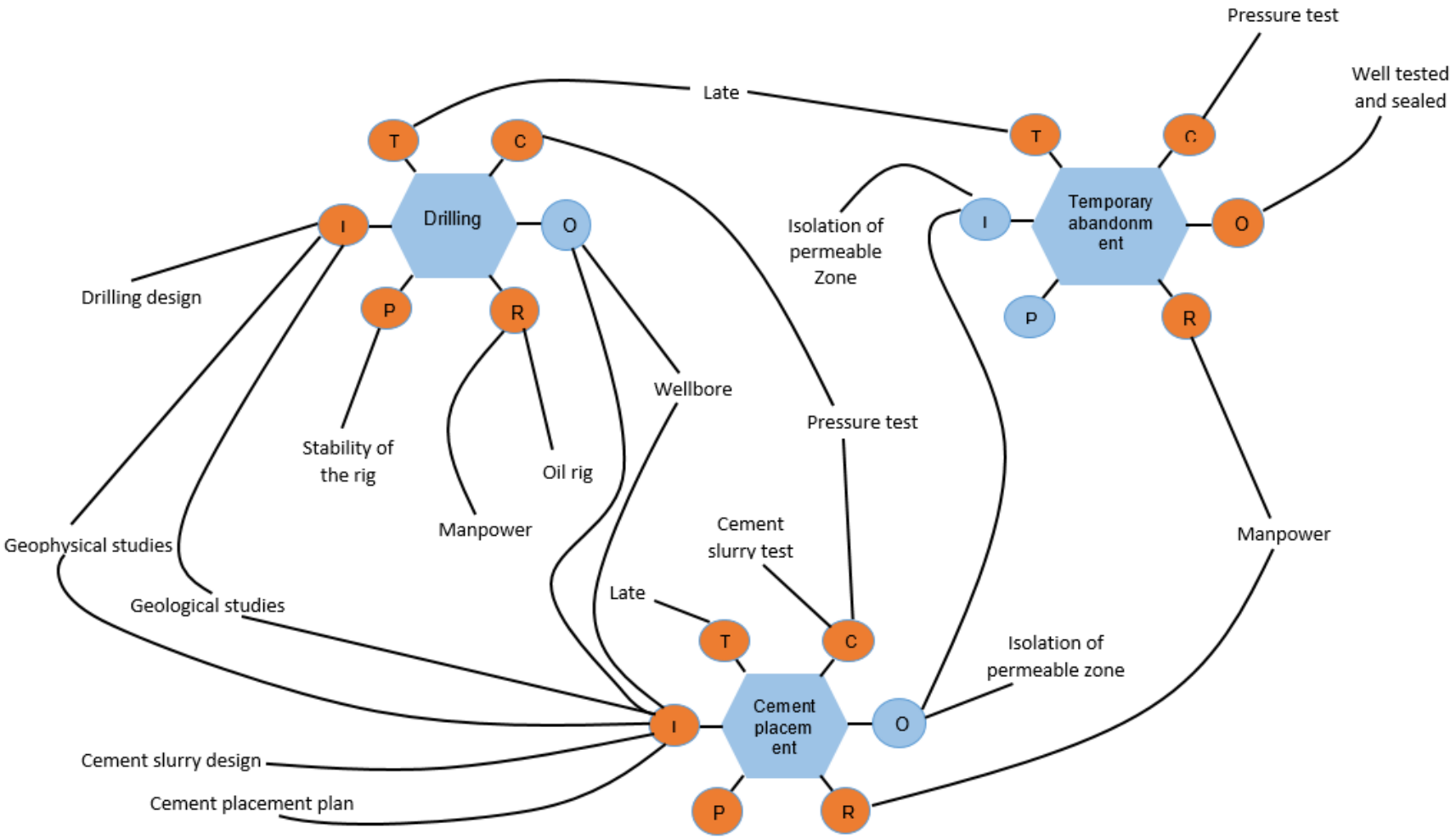
Temporary abandonment includes testing of the well, sealing ad safety devices and also disconnected from the platform so that the well, for future production from the well. In the case of deep water horizon disaster occurred before the temporary abandonment could be achieved.

Assessment and evaluation of the potential variability considering normal and worst case situations

Deepwater horizon has geological and geophysical studies as inputs for the drilling function. These studies might have variation, incompleteness and inaccuracy of the information. However, this can be eliminated or the process can be made resilient by continuous analysis of the drilling wastes that return from the well and make necessary corrections.

Time delays are another main source of performance variation, as organizations main goal is to achieve the target on time for better profits it pressurizes the workers to compromise on the performances including safety issues.

Pressure test results plays a major role in the performance variations as the fault readings and misinterpretation of data can have serious effect on the variations. The main aim of cement placement is to isolate the well from the invasion of hydrocarbons and ensure its safety on future operations.



FRAM model developed for Macondo Blowout Accident issues

Performance variations in the cement slurry may result in the weakening of the cement providing room for the invasion of hydrocarbons or fractures in the formation. Additional cement slurry test is performed to assess the formulation of the cement. These tests are carried out in a well-equipped laboratory located outside the platform and the results are stored in a database. These test are performed by a specialized company which have no contact with the platform. This test can play a major role in making the process more resilient by establishing a proper procedure for communication of the results to stakeholders and by predefining preventive and corrective measures with the team involved. Cementing correction is one of the main action to be taken in the case of detecting a performance variation.

Temporary abandonment activity is assessing the integrity of the well and seal it for the future exploration. The main objective is to isolate the well for safe operations. Performance variations can be detected during the well abandonment testing, providing preventive and corrective actions can make the process resilient. Generally, checklists and procedures are provided to review the results or the process to detect the variations. Operators must also be trained to notice the variations that are not included in the checklists.

Identification of functional resonance. The combinations of variability may result in undesirable outputs

The combination of the variations in the performance aspects of cement placement plan and cement slurry design can have a serious consequence in the process of cement placement. A fragile cement due to the performance variation of both the activities may lead to the consequences of invasion of the hydrocarbons possibly an uncontrollable situation. To prevent the oil spill we can use safety devices like Blowout Preventers. But it is clear that the performance Variations in blowout Preventers makes the process less resilient.

The FRAM approach as shown in the connection diagram represents all the relationships and dependencies of each function on the other, hence the effect on the function's performance by the performance variation of other functions can be easily identified and the consequences can be reduced.

Thus the proposed approach detects all the performance variations in the process and predicts the possibility of the accident in far advance situations. Hence an incident or accident like Macondo Blowout can be easily prevented.

9. Discussion and Conclusion

From various accident reports it is evident that the human factors are the main causes of an incident or system failures. In the recent years organizations consider human factors as one of the major issue and have started to implement various measures to reduce risk due to human factors, but still the industries finds it difficult to control the risk. There several methods available to reduce the risk due to human factors but still the industry need more effective and reliable techniques to manage these risks.

In the commonly used methods like HRA, BORA etc., the main aim is to detect the risk, perform a quantitative analysis and check whether the risk is at acceptable level or if it is of high risk level risk reduction methods are used. This procedure is repeated for several times until the risk is reduced to an acceptable level. But in practical reducing any risk to zero is nearly impossible. It is very important to understand that risk due to human factors and human error are inevitable.

It also clear that the common risk assessment methods like HRA etc., the risk assessment is made for each event separately and checked for risk levels and if the risk levels are low and acceptable the risk is considered to be safe. But when two or more risk gets coupled with each other then the resulting risk is high and may have serious consequences and lead to accident. These methods fail to predict these risk or establish the relationship between these events.

Humans are prone to make mistakes and will err in their judgement. They will also drift from the known procedures; these drifts are normal but if not managed properly it can have a cumulative negative effect on the overall process.

Resilience engineering is the best possible approach for overcoming all the above problems. Performance variability in resilience engineering view both normal and failure performances have a common source. The outcomes may sometime differ from what was required, expected or intended. This difference can be either beneficial or harmful. The adaptability and flexibility of the human performance is the reason for the efficiency, however they can also be the reason for its failures.

In order to be adaptable and flexible it is necessary to understand the process completely i.e., not only how it can fail but also how can it go right. When we focus on how it can go right we get to understand the near misses as well. Near miss is defined as a situation which was circumvented by the performance variance of the personnel. In this view the factors which contributed to the near misses can also be identified.

One of the main drawbacks of the oil and gas industry is that we fail to record how it went right. which makes it difficult in learning from the past. In Resilience engineering all the performances including near misses are recorded and monitored for detecting the performance variances.

In order to adopt these principles, we are in need of a model which can represent the variability of normal performance and that can provide more comprehensive explanations for the accidents to identify the possible risks.

When looking in to aviation industry where safety is their main concern and priority. They are in need of high precision of the data and learning from the past. It is one of the industries which includes human factors as its major contributor of the system's operation. The Air traffic management need to more accurate and also be ready for adaptability and flexibility at any point of time to avoid serious accidents. In the air traffic management system, they widely use Functional Resonance Analysis Method (FRAM). Which helps them to monitor and respond accordingly without affecting the entire system.

Functional Resonance Analysis Method (FRAM) over comes the intrinsic limitations of the commonly used methods by focusing on the relationship between the system functions. It also eliminates the traditional cause effect relation by the principle of resilience. FRAM can also be used as an accident model to find the root causes of the accident, which helps in better understanding of the system.

A practical implementation of the FRAM method is established in the case study on Macondo Blowout accident. The Safety assessment model for the accident situation of Macondo blowout is established. The model clearly represents the dependencies and the relationships between the system functions. which makes the path to understand the normal performance and the possible performance variability clearly visible and accessible.

In FRAM method the possible performance variabilities are identified and they are mapped with other functions to identify the dependencies and their effect on the system functions. Hence the accidents or incidents can be predicted and prevented far earlier than any other methods, as shown in the case study where the possibility of Blowout is predicted with the performance variations of the other functions.

The main reason for this method to be more successful in preventing the accidents is that it focuses on damping the variability instead of eliminating the failures i.e., by improving the conditions where Trade-offs are need to be made.

References

A White Paper on Resilience Engineering for ATM. (2009). Retrieved from https://www.eurocontrol.int/sites/default/files/article/content/documents/nm/safety/safety-a-white-paper-resilience-engineering-for-atm.pdf

Arezes, P., & Carvalho, P. (Eds.). (2014). *Advances in safety management and human factors edited by*. Retrieved from http://www.ahfe2016.org/files/books/2014SMHF.pdf

Aven, T. (2008). *Risk analysis: Assessing uncertainties beyond expected values and probabilities*. United Kingdom: Wiley-Blackwell (an imprint of John Wiley & Sons Ltd).

British Petroleum. (2010, September). *Deepwater horizon accident investigation report*. Retrieved from http://www.bp.com/content/dam/bp/pdf/sustainability/issue-reports/Deepwater_Horizon_Accident_Investigation_Report.pdf

DNV.GL. (2014). *THE WORLDWIDE OFFSHORE ACCIDENT DATABANK (WOAD) THE PURPOSE OF WOAD*. Retrieved from http://production.presstogo.com/fileroot7/gallery/DNVGL/files/original/79060cc678d242999f1cf41551f8ee5a.pdf

Energy Institute. (2011). *Human factors briefing notes - energy institute*. Retrieved from https://www.energyinst.org/technical/human-and-organisational-factors/human-factors-briefing-notes

Gordon, R. P. E. (1998). The contribution of human factors to accidents in the offshore oil industry. *Reliability Engineering & System Safety*, *61*(1-2), 95–108. doi:10.1016/s0951-8320(98)80003-3

Health and Safety Executive. (2012, January). *Managing human performance - Briefing notes*. Retrieved from http://www.hse.gov.uk/humanfactors/briefingnotes.htm

Hollnagel, E. (2013, September). *An application of the functional resonance analysis method (FRAM) to risk assessment of Organizational change*. Retrieved from http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/44/057/44057156.pdf

Hollnagel, E., Wears, R. L., & Braithwaite, J. (2015). From safety-i to Safety-II: A white paper. Retrieved from https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-whte-papr.pdf

Hubbard, A., & Embrey, D. (2010, September). *Deepwater horizon – summary of critical events, human factors issues and implications. R*etrieved from http://www.humanreliability.com/documents/DeepwaterHorizon-HumanFactorsIssuesOG.pdf

IOGP. (2005, June). *Human factors defined - a means of improving HSE performance*. Retrieved from http://www.ogp.org.uk/pubs/368.pdf

IOGP. (2010, March). *Risk assessment data directory human factors in QRA*. Retrieved from http://www.iogp.org/pubs/434-05.pdf

IOGP. (2011, August). *Human factors engineering in projects*. Retrieved from http://www.iogp.org/pubs/454.pdf

Kirwan, B. I. (1994). *A guide to practical human reliability assessment*. United Kingdom: Taylor & Francis.

NOPSEMA. (2016). *Human error*. Retrieved April 12, 2016, from https://www.nopsema.gov.au/resources/human-factors/human-error/

Paries, J., Wreathall, J., & Hollnagel, P. E. (2010). *Resilience engineering in practice (Ashgate studies in resilience engineering)*. United Kingdom: Ashgate Publishing.

Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot: Ashgate Publishing.

Society of Petroleum Engineering. (2014, March). *The human factor: Process safety and culture*. Retrieved from https://www.onepetro.org/general/SPE-170575-TR

Steen, R., & Aven, T. (2011). A risk perspective suitable for resilience engineering. *Safety Science*, *49*(2), 292–297. Retrieved from http://www.sciencedirect.com/science/article/pii/S0925753510002237

Vinnem, J. E., Aven, T., Hauge, S., Seljelid, J., & Veire, G. (2004). Integrated barrier analysis in operational risk assessment in offshore petroleum operations. *Probabilistic Safety Assessment and Management*. Retrieved from http://preventor.no/u/0201.pdf

Hollnagel, E. (2008). Resilience engineering and safety assessment. Retrieved from https://www.eurocontrol.int/eec/gallery/content/public/document/other/conference/2008/safety_r_and_d_Southampton/day_2/Erik_Hollnagel_Resilience_engineering.pdf

Pollock, R. A. (2014). Dispelling myths about human error. Retrieved from https://www.onepetro.org/conference-paper/ASSE-14-631?sort=&start=0&q=myths+of+human+error&from_year=&peer_reviewed=&published_between=&fromSearchResults=true&to_year=&rows=10#