Assessing risk and prevent accidents in complex system

Student: Baiyu Teng
Supervisors: Jørn Vatn
Bodil Mostue

June, 2010, Trondheim, Norway

Preface

This report presents the results of the master thesis by Baiyu Teng, completed at the department of production and quality engineering, at the Norwegian university of science and technology.

I would like to thank my supervisors Jørn Vatn and Bodil Mostue for valuable comments and guidance to this thesis. I am grateful for the contributions of the people who volunteered personal time to add their knowledge to this project: Marvin Rausand from my department, he was kindly suggest me the topics which seem interesting and encouraged me to start as soon as possible ; Eivind Okstad from SINTEF, he provided with me the mass information I needed and made me to trust my point of view. Eirik Albrechtsen from SINTEF, he provided me with the case. All these people contributed with valuable information, and made me able to write this project.

Trondheim, May 2nd, 2010

Baiyu Teng

Abstract

The article intends to identify relevant risk analysis methods that include human and organizational factor, BORA and ORIM, and compare the two methods in the field of risk analysis. Discuss and define the term complexity as well as complex system in relationship to risk analysis, here Chinese traditional medical way of thinking is introduced due to the similarity of risk analysis and diagnosing people. Interaction and coupling are reviewed in order to better understanding the complex system. Integrated operation (IO) case was introduced, it was claimed to be a complex system according to the definition discussed before. BORA and ORIM are claimed to be not suitable to analysis the complex system like IO. Other approaches were introduced to analysis IO, STAMP and why-because analysis (WBA). At last some suggestions concerning the IO were presented to prevent accidents and reduce risk.

Contents

1. Introduction

1.1Background

As the development of the technology, people are possible to do more things more efficiency by various functions combined in a system, then the system become more complex, however, how to assess the risk in a complex system have been a problem being exploring these decades.

Someone would argue if there is no complex system, we do not need to bother, to think about the risk. Like the appearance of anti-radiation product due to the widely use of computers. But we need computers, we need complex systems to solve problems, we need to assess the risk of complex system, so we have to face this risk.

Integrated Operations (IO) is among other things contributing to new ways for organizing work, new work processes and increased automation, e.g. closer collaboration offshore-onshore, cooperation across organizational and geographical borders and use of integrated contractors (Grøtan et.al, 2008). It is one of the popular working modes that being discussing in the Petroleum industry. It uses the high-tech ICT to improve the production, like the e-drilling to make it more efficiency, the real time date in all the control places. It includes the foreign experts and contractors to develop plan and solve problems, even to control during the night in Norway because of the time zones, including more cross-discipline cooperation. What is more, it allows reducing the people offshore in order to reduce cost.

If we want to assess the risk of the IO; we need, first, to know whether it is a complex system.

Some people believe that human and organizational factors which included in quantitative risk analysis are considered to one way to assess risk in complex system, like BORA and ORIM. We also need to know whether these two methods are suitable to handle complex systems.

In this report, chapter 2 will introduce two methods –BORA and ORIM, which are considered by some experts that can assess risk in complex system. Chapter 3 gave some definitions of the complexity and what is complex system when we talk about risk analysis, whether the Integrated Operation (IO) is a complex system. Chapter 4 argues that BORA and ORIM are not suitable to analysis complex system. Chapter 5 introduces STAMP, WHA，which can be a way to handle complex system, and in addition, some key points are mentioned to help IO system reduce risk.

1.2 Objective and methods

Identify relevant risk analysis methods that include human and organizational factors-ORIM, the BORA, and the STAMP methodology. Discuss and define the term complexity with basis in the word complexity used in relation to risk analysis. with an example from so-called Integrated Operations, discuss in what manner methods may handle complexity and present the result from the case study, where one or more of the identified methods are applied.

The methods are mainly literature reviews and learning from expert seminars in SINTEF.

1.3 Shortenings

RIF: Risk Influence Factor
MTO: Man, Technology, Organization
CCR: Central Control Room
ORIM: Organizational Risk Influence Model
BORA: Barrier and Operational Risk Analysis
STAMP: Systems-Theoretic Accident Model and Processes
WBA: Why-Because Analysis
IO: Integrated Operation
RIO: Risk assessments of Integrated Operation

2. BORA and ORIM

2.1 BORA

Bora (barrier and operational risk analysis) is a relatively new method both for qualitative and quantities analysis of the risk from the scenarios. It introduces barriers and how technical human operational and organizational RIFs influences the barrier performance (Aven et al, 2006), A barrier was defined as ‘equipment, constructions, or rules that can Stop the development of an accident’ (Taylor, R. J. 1988). It is mainly a tool for the offshore installation in the operational phase to estimate the changes on the risk of hydrocarbon leakages due to the activities.

The steps are:
1) System identification.
This is often done by task analysis.

2) Identify barriers and develop Barrier block diagram, this should cover a representative scenarios, and it usually consists of initiating event, barriers and outcomes. This barrier block diagram can also be converted into event tree.

An example is show in figure 1:

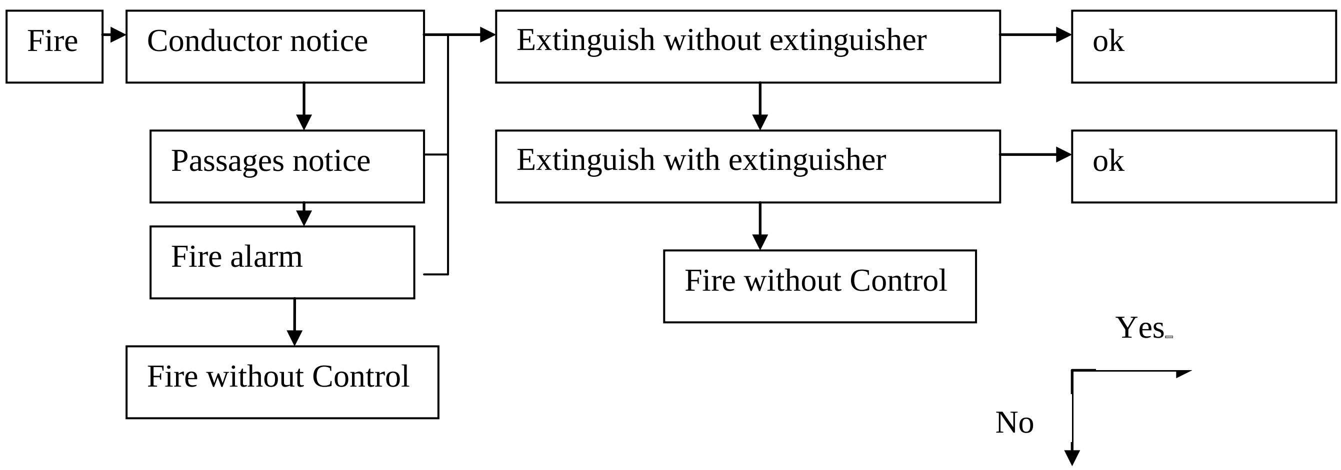


Figure 1 the barrier block diagram example

3) Establish fault tree. This is used for analysis of barrier performance (Aven et al, 2006) all of basic events should be analyzed

Example:

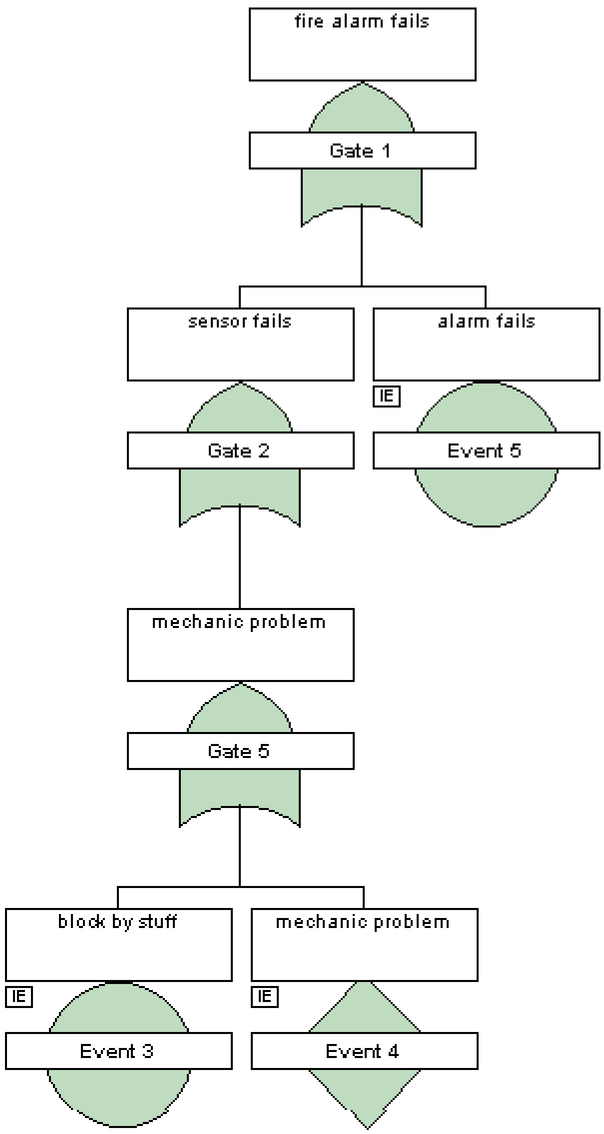


Figure 2 the fault tree example

4) Indentify the risk influence factors

According to Haugen (2005), risk influencing factors are factors that may influence the frequency/probability of an event occurring, they are not barriers, but factors that influences the performance of barriers.

This is the key point that we can incorporate human organizational and operational RIFs into the barriers and then into the initiating events. Example:

- Personal characteristics: the experience of using the extinguisher .the work load of the conductor
- Task characteristics: time pressure
- Characteristics of technical system: maintenance of the fire alarm
- Administrative control: the shift of conductors
- Organizational factors: the position of extinguisher and fire alarm, the communication between driver and conductor.

It is better to use both bottom-up and top-down approach in order to cover each event. So every type of events can be considered in case of complexity and variation. If it is possible, write a detailed taxonomy of RIFs based on the MTO factors and experience from the case study (Aven et al, 2006)

5) Scoring risk influencing factors (Aven et al, 2006), each RIF is given a score from A to F, where:
A: status corresponds to the best standard in the industry: status corresponds to the industry average F: status corresponds to the worst practice in industry. And following the order, B, D, and E are in between.

We assume Q is the measure of the status, s denotes the score or status of RIF no i. Determine p_{low} as the lower limit for p_{ave} by expert judgment, p_{high} as the upper limit for p_{ave} by expert judgment(Aven et al, 2006).

$Q_{i(s)}=p_{low}/p_{ave}$ if s=A
$Q_{i(s)}=1$ if s=C
$Q_{i(s)}=p_{high}/p_{low}$ if s=F

According to the numeral analysis method, we can get $Q_i(B)$, $Q_i(D)$, $Q_i(E)$,
For the P_{ave}, we can establish it similar to the QRA, based on best available source (Aven et al, 2006).

6) Weighing the risk influence factors

We give the important of the RIFs; this is always done by expert judgment

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

The prob1ability of occurrence of event A –P_{rev}(A) is determined(Haugen,2007):

$$P_{rev} = P_{ave} \sum_{i=1}^{n} w_i \cdot Q_i$$

Here, P_{rev} could be the occurrence of event (after revising). P_{ave} is the industry average probability of occurrence, w_i is the weight (importance) of RIF no.i, Q_i is a measure of the status of RIF no. i, and n is the number of RIFs.

2.2. ORIM

ORIM stands for ‘Organizational Risk Influence Model’. In this method, organizational factors can be estimated by risk indicators and then we can find out how it influences on the failure modes. Risk indictors are proposed as a tool for risk control during operation of offshore installation (Øien, 2001), the starting point for ORIM is a QRA for installation.

The main steps are (Øien, 2001)

(1) the organization model development
The purpose of the framework is to control risk during operation, not for risk assessment. The model can be based on one specific event instead of general accident data.

The example organization model is:

.

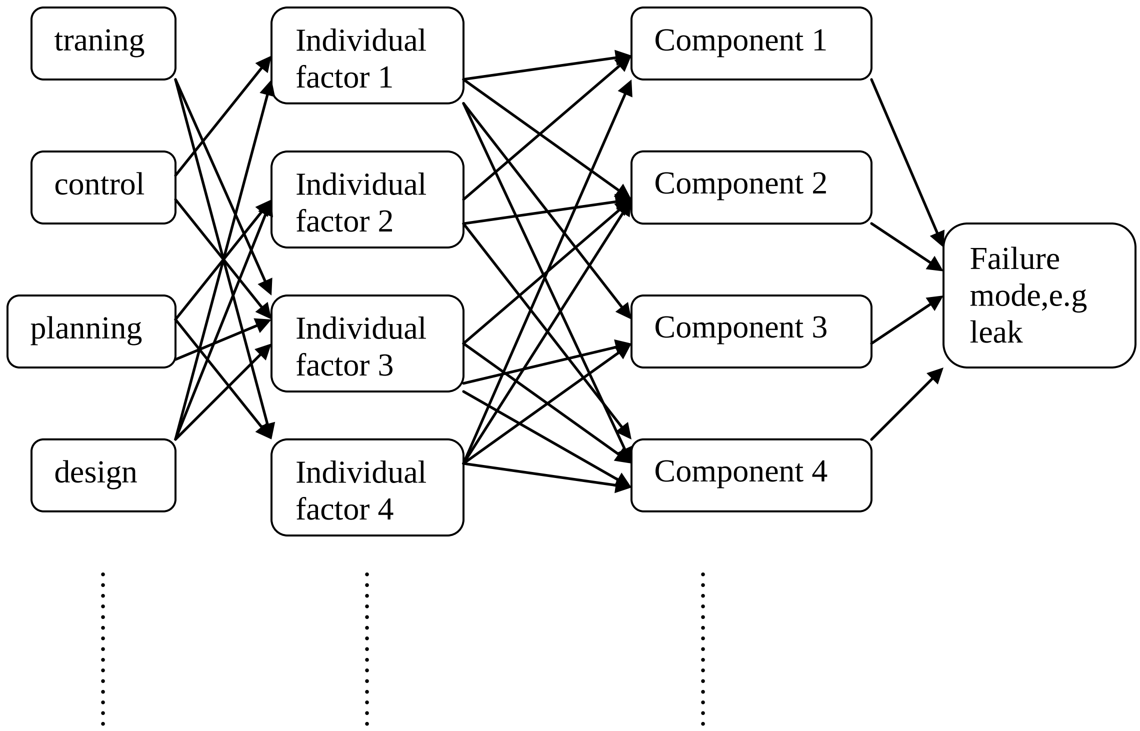


Figure 3 the organizational model example

In figure 3, from right to left:

- For the failure mode (parameter), we can get more information of these categories from Synergy which records specific accident and incident report
- For the second category, these can be some component/or equipment
- For the third, there can be some human factors, e.g. the main functions performed by the front-line personnel.
- For the last category, organizational factors, e.g. individual training, competence, and design.

(2) evaluation of the quality of the factors
This is rating of the organizational factors, in ORIM, we use risk indicators instead of expert judgment and something similar to safety audit tools.

(3) Quantitative method for assessing the effect on risk, we can use influence diagram or Bayesian network to model. Individual factors are not included as organizational factors in quantitative model because it has no influence on the quantification.

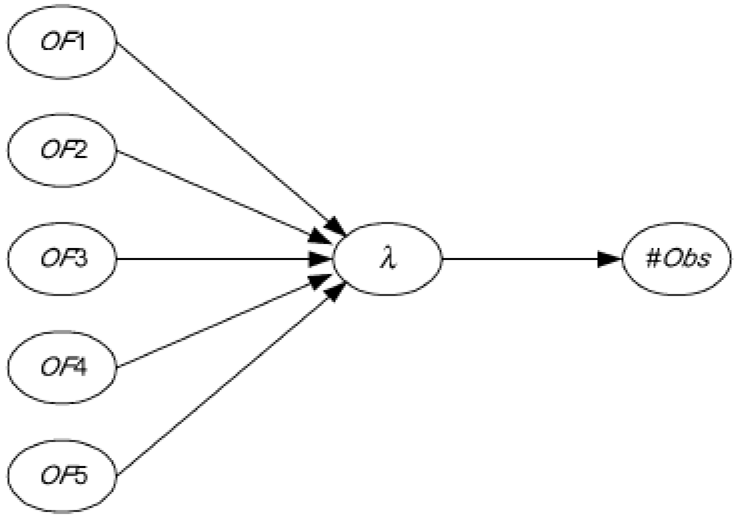


Figure 4 Quantitative model (Øien ,2001)

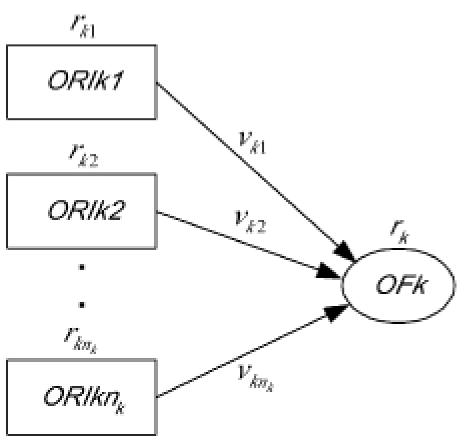


Figure 5 rating process (Øien ,2001)

- Rating process. By the rating process will know the present status.
  r_k is the rating value of OF_k

  $$r_k = \sum_{j=1}^{n_k} v_{kj} r_{kj}$$

  V_{kj} is the individual weights of the indictors assigned by expert judgment.

  $$\sum_{j=1}^{n_k} v_{kj} = 1$$

- Weighting process. By weighing process, we can know the impact of organizational factors on the failure mode. The organization factors (OF) will influence the leakage frequency λ, that will lead to the observed leakage.

- Effect on the risk.
  For the detailed method description, please read the report written by Øien(2001).

2.3. Comparison

Bora divides the system into small components, and for each basic event there are fault tree, it adds the risk influence factors into consideration, then the risk can be revised.

Comparing to ORIM, the advantages of BORA:

It is simple, both the qualitative part and the quantitative part. It combines the basic knowledge of risk analysis methods, like fault tree analysis, event tree analysis, in the end; the risk can be improved by using the risk influence factors. In Quantitative part, W_i (weight of RIF no.i) and Q_i (measurement of the status of RIF no. i) are not difficult to get.

The disadvantages of BORA are:

1. RIFs are not independent all the time, they will influence each other. E.g. take railway system as an example again. The time pressure can influence both the maintenance of fire alarm and the shift of conductors. Even though, when deciding the weight of the RIFs, the expert judgments will give the time pressure higher weight, it is still not precise, it is better to draw a clear picture of the relationships of RIFs.

2. RIFs are not clearly defined, according to Haugen (2005). Risk influencing factors are factors that may influence the frequency/probability of an event occurring, they are not barriers, but factors that influences the performance of barriers, other external factors etc. It is a bit difficult to distinguish them with barriers.

ORIM do not focus on the technical part, it considers the accident rate, organizational factors and risk indicators, and the calculation seems precise.

Comparing to BORA, the advantages and disadvantages of ORIM:

1. Viewing the accident rate from a relatively higher level, considering the case as a whole rather than decomposing it. It is better to analysis the complex system which has a lot of interactions.

2. The key point is quite clear, to establish the risk indictors in order to know how the organizational factors be influenced in order to know how the risk be influenced. It skips a lot of technical issues which we might spend a lot of time on in other models.

Disadvantages of ORIM:

1. Thought the whole way of thinking is quite logical; it is not easy to establish the risk indictors. There are literatures which are discussing the establishment of risk indictors alone.

2. For the different cases, BORA is easier because it has fewer differences between cases, it means that it is more like a ‘model’, but for ORIM, the workload and knowledge requirement of establishing risk indicators are much higher, and for different cases, risk indicators are much different.

3 .Complexity theory

Complexity theory is the science of investigating complex system and complexity. It is generally believed that it is come out in 1980th with the knowledge of system science, it is the new period of development of system science (Feng, 2003): The word ‘complexity’ is quite wide, algorithm complexity, computing complexity, grammar complexity, economic complexity, there is no strict definition of complexity.

3.1. Some definitions of complex system

There is no one general definition of complex system (Xu, 2000)
Some definition of the complex system:

(1) Complex system is chaotic systems.

A chaotic system is a deterministic (predictable) system, but it is difficult to predict, because the future state of chaotic systems are very sensitive to the current state of the system (Ian P et al.2000)

According to Cilliers(1998), generally speaking, complex system is formed with amount of elements, but it does mean that only huge amount of elements can form a complex system. There are various interactions, every element can both influence others and be influenced, and these interactions are non-linear.

(2) A Self-adaptive evolving system.

If the change is in response to achieving a certain goal or objective, or in response to an environmental Change, then systems that adapt themselves, are known as complex adaptive systems (Kauffman, S. and MacReady, W. 1995).

Complex system is an open system, the elements inside will have interaction with the environment, continuous energy is necessary to keep the system running. The complex system will be evolved as the time flies, the action in the past will has influence now, and the action now will influence the change of the future.

(3) Non-deterministic behavior (Le Coze,2005)

The determinism was quite popular in the 17th and 18th century, scientist believed that every cause has its effect and the movements of everything are determined by a law.

(4) Non-linear cause and effect relationship(Le Coze,2005)

The concept of linear relationship suggests that two quantities are proportional to each other: doubling one causes the other to double as well (Bar-Yam, 2000). For example: the volume of the medical depends on the weight of the children; doctors give more medical to the children who are heavier. Here we assume that they have the same situation of the disease. Non- linear means that the doubling the one will not cause the other to double, we can say it is random with tendency, but this tendency is changing all the time, it is quite difficult to foresee.

The cause –effect in complexity system is non linear. It is circular and difficult to expect, different causes can lead to the same effect, same cause leads to different effects, small cause can lead to large effect, and large cause can lead to small effects.

(5) Interdisciplinary (Le Coze, 2005), a hierarchical system including many action agents.

Complex system cut through the scientific disciplines and make us to study it articulated, this is interdisciplinary approach, like ecology and earth science, and these include and combine lots of science so that specialized science can not function alone

(6) Non decomposition(Le Coze,2005)

For the word decomposition here, it means the same as the 'analysis method'. Because of interdisciplinatity, the complexity system is non decomposition, we cannot treat it like the simply system.

3.2. Diagnosing people and risk analysis

Personally speaking, I believed risk analysis is like diagnosing a person.

When the patient is ill, we diagnose him and find out the cause the then give treatment plan—a gas leakage, we analysis it and find the cause and give remedial measure.

When the result of diagnose is wrong, the patient is dead---the analysis of the cause did not work---the gas leakage leaded to a huge accident.

After the patient died, sometime we anatomized him or use other methods to find the 'real cause' ---we do in-deep accident investigation of the accident.

Nowadays, people are focus more on the health protection than 'waiting' for the disease—preventing of an accident is quite important.

We do the health check every year—the industry does the safety check on a fixed-period.

The doctor use the 'health card' to record the history—the accident database recording every accident & incident, E.g. Synergy.

3.3. The Chinese medical way to see the complexity:

The Chinese medical system believes that the human body is a complexity system, and it is open to the environment, lots of interactions, lots of relationships.

It is believed that if you find some part of your body is not feeling well, they not only focus on this part, they consider the whole body as a whole, unlike the western way of treating the illness, for example, the yellow colour in your eyes can be the problem of the liver, and massage of the special point of foot will make the head feel better.

For the cause-effect relationship, Chinese medical doctors will give different people with different prescriptions. The same illness in different people can use different prescription, the some prescription can use for different illness. The Chinese medicine will influence the whole body, and the body will influence the medicine. So the amount of the medicine depends on the constitution of the patient. The history of health and usage of medicine will influence the next prescription; the following prescriptions will be influenced by the previous ones. So the system is changing all the time.

3.4. Complexity and risk analysis

According to Perrow(1984), the complex system have these features:

- proximity
- Common-mode connections
- Interconnected subsystems
- Limited substitutions
- Feedback loops
- Multiple and interacting controls
- Indirect information
- Limited understanding

3.4.1 Interaction and coupling

Tight coupling is a mechanical term meaning there is no slack or buffer or give between two items, what happens in one directly affects what happens in the other. (Perrow, 1984)

Loosely coupled system tend to have ambiguous or perhaps flexible performance standards (Perrow 1984).

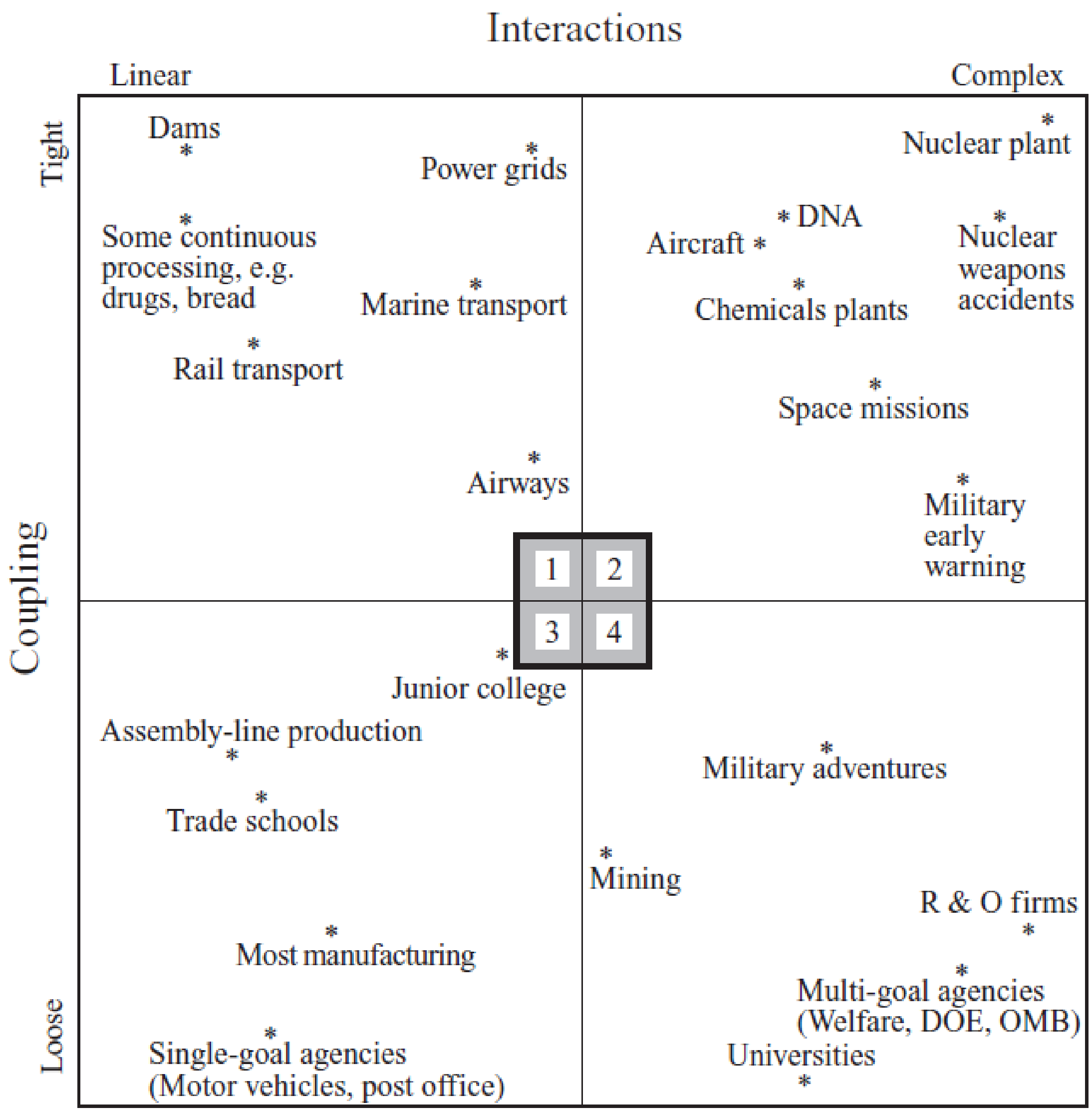


Figure 6 Relationships between interaction and coupling (Perrow 1984)

In the figure 6, Dams, power grids and nuclear plant, they are almost in the same line, that means, they are in the same level of tight coupling, but nuclear plant are much more complex, there are much more unexpected interactions in nuclear plant than in Dams and Power grids.

Let us look across the bottom, post office and university are loose coupling, if there is something goes wrong, they have more ’response time’ to deal with it, in post office, mails can be piled up without emergency alarm. students can have crazy actions with tolerance from residents .however, for post office, they are almost linear production sequence without lots of branch paths and feedback loops, university have teaching, researcher, public service (Perrow, 1984), they can interactive with each other, For example, when teacher is absent from a lecture, some students will be happy for they have more free time, some students may become angry because they have to get up early without breakfast for this lecture, one or more of the student will lodge a complaint to the dean, the dean wants to protect the fame of the department, he will, in one hand, investigate this case, in other hand, pacify the students, for some reasons, the media know about this…it really has lots of interactions.

Tight coupled system have more time-dependent processes, IO system has limited response time to accident, the process has to be monitoring all the time, because when these is an accident, they have to take action quickly to avoid the serious consequence.

3.4.2 Complex system

After the literature review, if a system has these features, we can say it is a complex system:

- An open adaptive system that can evolve.
- Not determined by general law and linear cause-effect relation.
- Have complex human, organisation and social interaction.

Besides the points above, these are some characteristics

- Non-decomposition (Le Coze, 2005):

HAZOP or FMEA are the analysis method using decomposing the installation into parts and identifying what cause-effect relationship could lead to hazard. In this case(see appendix B), The onshore central control room (CCR) cannot be analysis alone because it has quite a lot interactions with various contractors, onshore support centre, onshore drilling centre and so on.

According to Richard I. Cook (2009), ‘Safety is a characteristic of system and not of their components’, safety can not be discussed when decomposing the system into components, and the state of safety is dynamic and changing all the time. He also claim that ‘post-accident attribution accident to a ‘root cause’ is fundamentally wrong’, failure required multiple faults, there are multiple contributor to accident, accidents are created by the linking of the causes together rather than the individual causes. So the root cause can not be viewed isolated, the evaluations should reflect that social cultural understanding of the nature of the failure rather than the technical.

- Organisations are difficult to predict through quantitative methods (Le Coze, 2005):

Complex system should not mainly include technical risk assessment. So data is not easy to get, what is more, because the system is updating quickly, the data is not less useful than the simply systems. Quantitative does not only include probabilistic way, but the exact data got from equations.

3.4.3 Is IO system complex?

According to the case, the CCR will move from offshore to onshore and eDrilling will be applied, several expert centres will support operation and continue to support onshore CCR, by using the ISD (Integrated Service Delivery) contracts, The company has integrated contractors for several years. More detailed information is in appendix B.

IO can be recognized as a complex system.

- An open adaptive system that can evolve.

There are several feedback loops in the IO system, telling us the adaptive characterise. Various workers shift their jobs, one worker who was doing the job for some times and then shifted his job to another worker from another contractor or company, the next worker will continue well, when there is something wrong with the previous job, the next worker will inform his as well as reporting it to the accident data base.

When planning IO, sometime People reconstructing the system in order to reduce exposure of vulnerable parts of failures, they also concentrate critical resource in the area of expected high demand, providing path way for retreat from fault (Richard I.Cook, 2009).

IO system also influence by the weather, the government's policy, the economic situation etc, it is an open system. One investigation at one time cannot reveal the future. It requires a lot of time because the huge and complex system, furthermore, in the end of the investigation, the situation may be much different from the beginning, that means; the result we got is 'out of fashion'.

- Not determined by general law and linear cause-effect relation.

There is only a few specialization of workers, workers in offshore platform are cross-trained, they tend to rotate, maintenance workers can operate equipment in an emergency, people can fill in and know something about other's job, interdependencies happens frequently. So it is impossible to use linear cause-effect analysis, in IO one cause can have several effects, on effect can be caused by several courses, removing a component or shutting down means temporarily severing numerous ties (Perrow, 2004).

In simple system, every worker has his clear response. It is easy to find the root cause of an accident and the response person, but in complex system, some accident happen during the shifts, in specific installations, people are cross-trained and not specialised, it is not easy to find someone to blame.

- Have complex human, organisation and social interaction.

In complex system, the safety culture, the strategies and the government policy interactive actively with each other. The support centre not only support the IO installation, but also other's installation, both at Norwegian continental shelf (7 installations) and partly in other countries. the interactions are among different society, they have to adjust and balance the job in other countries and IO, so a change in IO may raise a trouble, for example, the maintenance support centre has a tight schedule in IO and in other project in Mexico, if a emergency maintenance task is required, maintenance support centre has to rearrange the schedule, so sometime it is impossible to change because the tight schedule.

The edrilling, even it is real time data, this information is still indirect information, it still requires person to work on the installation, this is multiple and interacting control between control center staff and machines.

Organizational interactions.The offshore CCR, onshore CCR, contractors share the same real time information as the operator, the communication become quite important, decisions among these staff, staff and machines, machines and system, all the relationship becomes mix and not easy to make it clear.

Social interaction.Large numbers of offshore workers retiring between 2009-2013, recruitment is problem, a number of offshore engineers has been recruited from countries whose language and culture is different from that of the Norwegian workers (see appendix B)

4. BORA and ORIM are not suitable for complex system

BORA

According to Hollnagel(2004) epidemiological models still follow the principles of sequential model as they show the direction of causality in a linear fashion, one example of epidemiological models is the Swiss cheese model, figure 7, and the barrier block diagram is similar to the Swiss cheese model, which shows an accident emerging due to holes (failures) in barrier and safeguards, so barrier block diagram shows the direction of causality in a linear fashion, for the complex system, the defects are often transient e.g. the holes in the Swiss cheese are continually moving (Zahid H. Qureshi, 2007)

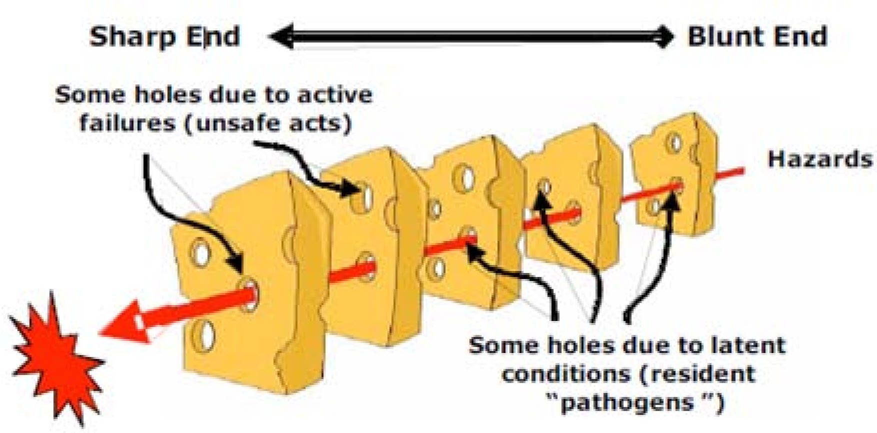


Figure 7 Swiss cheese model of accident causation (Reason 1997)

In addition, not only the RIFs are not independent of each other as we have mentioned above, the barriers are not independent of each other either. Take the gas leakage for instance, the barrier can be pressure detection, alarm detection, human detection (by inspection) etc. the human detection has influence on the activity of other barriers like pressure detection and alarm detection. Human detection can happen before the pressure and alarm detection, or after, or between, so it will influence the probability of gas leakage.

The time sequence is also important on the result, if it is takes a long time before the response person detect the accident, even it is detect by the pressure detection at a early time, it still will have a serious consequence, if the response person has a short response time, there may be only a small incident.

The BORA seems simple in theory but complicated in operation. Just look at one barrier diagram, this is from the MTO project (see appendix A), and there are 27 initial events, every initial event can draw this barrier diagram, and this is only the drilling, there are other kinds of accidents.

What is more the probability of ignition is also dependent on the initial size of the leak, leak point and weather conditions, for the complex system, drawing a clear picture of the barrier block diagram is not easy. It is difficult to incorporate non-linear relationship, including feedback.

For the ORIM:

If there is a gas leakage, we may ask why it happened, according to ORIM, we need to find the organizational factors as well as the organizational risk indictors.

If the accident is in the manned installation, the offshore and onshore CCR can be the direct reason, we can see from the figure in appendix B, the onshore CCR have interaction with the other organizations and between these organizations, there are its interactions. So the number of organisational factors can be huge. And if for the organizational risk indicators, which can help us assess the organizational factors, the number can be even larger and difficult to find. Because it concerns about the details of the system, the smaller the components is, the more connection it will be, like the neuron in our body.

The time length is a problem, if you believe the huge number is not a problem, when you have found organization factors A, B, and their risk indicators, and you start to find other organizational factors, the situation of A or B or both may be different from the moment when you found A. So the quantitative answer will be much different. Even the computers can not be an assistant; computers can only run for the designed programme, until now it can not replace the brain of the human being. This is what complex system: an open adaptive system that can evolve.

5. Other approaches to assess risk related to IO

5.1. STAMP

A model for analysing human, organizational and technical (hardware and software) factors in complex socio-technical system was proposed by Leveson (2004), according to Leveson, it called STAMP(systems-theoretic accident model and processes). Accidents in complex system do not occur simply due to independent component failure, however they occur rather when external interaction among system components are not adequately handled by the control system (Zahid H. Qureshi, 2007).

This model are not resulting from a chain or sequence of event .it treats the system as whole :how they interact and fit together (Leveson 2004). Systems are viewed as interrelated components in a dynamic balance situation due to the feedback loop of information and control, and the system is adapting to achieve its ends and react to changes itself as well as the environment. The goal of the control structure is to enforce constraints on system development that result in safe behaviour (Leveson 2004)

Stamp do not decompose system and accident explanations into structural component a flow of event, instead, it uses the hierarchy control based on adaptive feedback mechanisms. Safety arises from the interaction of system components not the individual components (Leveson 2004).

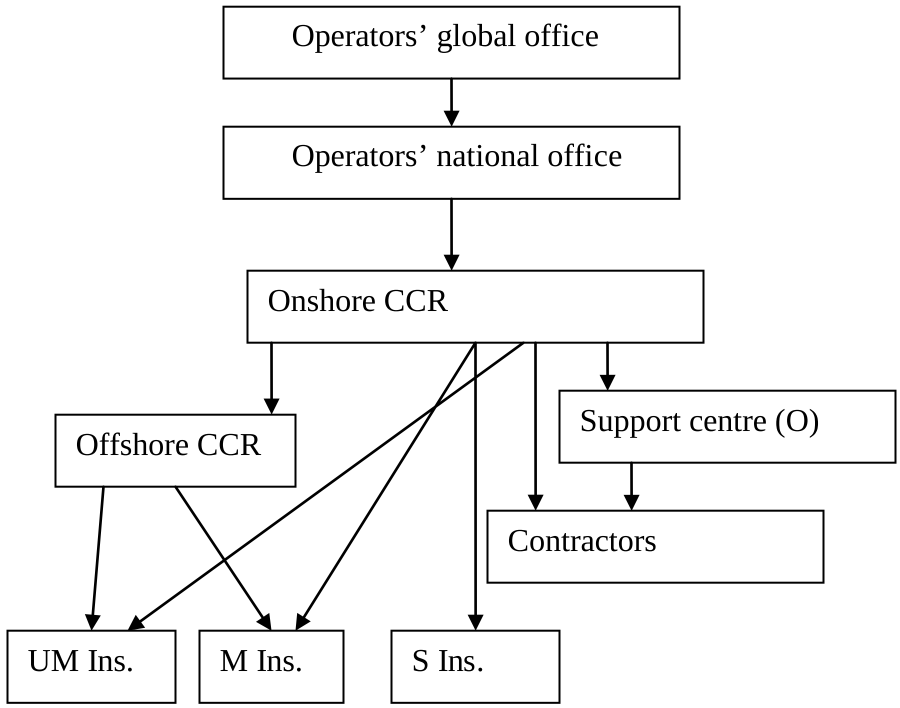


Figure 8 hierarchy chart of IO

UM Ins.:Un-manned installation
M Ins: manned installation
S Ins.: subsurface installation

Hierarchical control structure (Figure 8) is analysed to indentify the safety constraints at each level and the reasons for the flawed control(Zahid H. Qureshi, 2007). A classification of accident factors are list by Leveson (2004) in figure 9, by using this, hierarchical control is analysed.

Leveson attributes the organisational factors as a key accident factor which led to the failure at the lower technical and operational levels, organizational factors are at the highest levels of command for the lack of coordination and communication (Zahid H. Qureshi, 2007)

STAMP is useful not only in analyzing accidents that have occurred but in design period, hazard analysis can be thought of as investigating an accident before it occurs. unlike traditional hazard analysis, they focus on failure events and the role of component failures in accident, STAMP works well for the software and system design errors, includes organizational and management flaws and accounts for the complex role (Leveson, 2004).

1. Inadequate Enforcement of Constraints (Control Actions)

1.1 Unidentified hazards

1.2 Inappropriate, ineffective, or missing control actions for identified hazards

1.2.1 Design of control algorithm (process) does not enforce constraints

- Flaw(s) in creation process
- Process changes without appropriate change in control algorithm (asynchronous evolution)
- Incorrect modification or adaptation

1.2.2 Process models inconsistent, incomplete, or incorrect (lack of linkup)

- Flaw(s) in creation process
- Flaws(s) in updating process (asynchronous evolution)
- Time lags and measurement inaccuracies not accounted for

1.2.3 Inadequate coordination among controllers and decision makers (boundary and overlap areas)

2. Inadequate Execution of Control Action

2.1 Communication flaw

2.2 Inadequate actuator operation

2.3 Time lag

3. Inadequate or missing feedback

3.1 Not provided in system design

3.2 Communication flaw

3.3 Time lag

3.4 Inadequate sensor operation (incorrect or no information provided)

Figure 9: a classification of control flaws leading to hazards (Leveson, 2004)

5.2. Why-because analysis method

Why-because analysis (WBA) method is a rigorous technique for analysing the behaviour of complex system (23)

WBA models the sequence of events leading to an accident, according to the accident investigation report, we can keep the significant events and states in proper time order, each pair in the sequence is interactively analyzed to move towards a causal explanation using Lewis' counterfactual test (Zahid H .Qureshi, 2007).

Lewis (1973) developped a number of logics to capture counter-factual arguments which provide a formal semantics for causation, it states that, A is a causal factor of B, if and

only is: if A (causal factor) happens, B (effect)happens, and A did not happen, B either. In other word: A is the necessary causal factor of B. (Zahid H .Qureshi, 2007)
After the WBA, we get the”Why-Because Graph". It uses a visual way to present the cause-effect relationships between factors so that it can be easily understood by a non-expert, and it can help us understand the complexity of cases analyzed (24)

An example of the leakage accident:

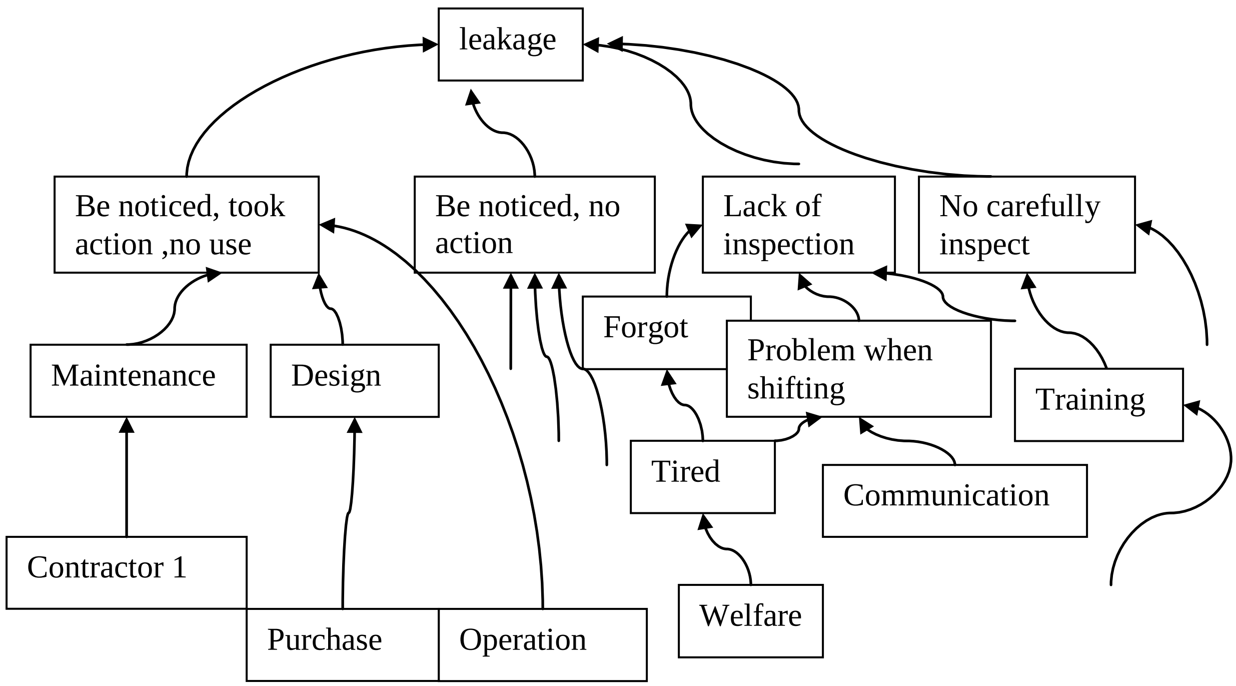


Figure 10 Why-Because Graph of the leakage (example)

5.3. Some other scattered thinking of the complex system

If we assume the accidents are the thieves who will steal your property in the flat, BORA and ORIM seems like to analysis the different thieves, for example, thief A is the gas leakage, thief B is the fire… different thieves have different barriers and indicators, but our goal is to keep our flat away from the thieves, we do not need to care so much about who are the thieves, how old are them, such like that, what we should do is, for example, remember to lock the door, like the safety management.

For the complex system, the incidents cannot be avoided, we can consider as the ‘energy release’ from the system, just like the volcano, our earth needs to release energy; or the acnes in our face, our body needs to release toxin. What is more, the incidents can be the indicator of the big accident.

5.3.1 It is difficult to use Reductionism

The western country would like to use reductionism to analysis our body, like anatomy, from the body to the organs, from organs to cells, from cells to DNAs, however the DNA is a complex system, there are millions of base-pairs, it is impossible to make all of the base-pairs clear. Another example is the atmosphere,Which includes gas molecule, like O_2, N_2, dust, etc, the weather depends on the irregular movements of the gas molecule; they believe if they know exactly the parameters like location, momentum, at any time, the weather forecast will come out. They put the admeasuring apparatus in a fixed distance. However, it is impossible to measure the gas molecule between the apparatus, it is also impossible to put the apparatus in different layer of atmosphere. What is more, in the end, the difference of the input parameters will be larger after using differential equation several times, so the weather forecast becomes uncertainty. Our body and atmosphere are complex system; they cannot use Reductionism (Zhu, 2005).

It is similar in the IO system, Reductionism is impossible to be applied here; there is plenty of interactions, non-linear, loops, etc. several contractors are doing one cooperated job, because they belongs to different companies, they may not know each other and they have their own 'way' of doing things, the 'way 'may be the same in one company but different from companies to companies, this may causes accidents, for example, there is no standard or common rule for the sequence of the maintenance job, workers from contractor Ⅰ use the sequence: step A, step B, step C, step D, workers from contractor Ⅱ use the sequence: step B, step A, step C, step D, step A and B can change the sequence. One day, after finishing step A, workers from contractor Ⅰ shift their job to contractor Ⅱ, the workers from contractor Ⅱ will miss the step B and continue to do step C.

5.3.2 It is difficult to use Positivism

Positivism, simply speaking, is to use the experiment to research; it is also not suitable for complex system.

There is an old story from Chinese philosopher called Zhuang Zi more than 2000 years ago: Zhuang Zi (we called Z) Hui Zi (we called H) are going through a bridge, Z is watching the river and said:'look at the fish swimming freely, they must be happy '. H said: 'you are not fish, how do you know fish is happy' Z said: 'you are not me, how do you know I know the fish is happy or not 'H said:' of course, I am not you, I don't know whether you know the fish, you are not the fish, you don't know the feeling of the fish, right？Z said:' back to the beginning, when you said that 'you are not fish, how do you know fish is happy? ', you have always know me (knew what things I knew)

Z felt ‘the fish is happy’ from the experience, but not be proved is Positivism, like the western way –everything should be proved by experiments and deduction.

The main stream of Chinese traditional way of thinking is ‘Intuition’; we would like to treat the case as a whole, like the classic conscious –‘harmony between man and nature’. This conscious has domain for a long time until Newtonian mechanics appeared, but now this conscious has become popular in western countries. So, thinking a system as case rather than decomposing it, the Chinese traditional way of thinking is ‘practice-get concept and method from experience-use this to solve problem—if it is right, repeat several time to prove it -- theory’(Zhu,2005).

We use the same way to look at the IO system, the accident database is quite important, after operating the system for several days, we can find out which parts is most vulnerable, find out the solution, then practice the solution, if it works after several time, we can write it into the standard or ruler.
What is more, recognizing hazard and successfully manipulating system operation to keep inside the tolerable performance boundaries require the contact with failure, system performance will be robust if operator can notice the ‘edge’ which the system performance begins to deteriorate, difficult to predict. In order to improve safety, operators must be provided with views of the hazards, the knowledge of how their action would influence the system performance (Richard I.Cook, 2009).

5.3.3 Organizing the element is more important than the elements themselves

In daily life, we have experienced several tiny things, which can result in a serious accident. For example, a soldier’s lost in a battle may run to the enemy, the enemy will know some secrets, a battle will lost just because a solider.

The French army is considered to be best when it comes to enjoying life, but they are not so good at fighting, when Napoleon reorganizes the army, it becomes one of the most powerful armies in the world. So the sequence influences the whole. The relationship between parts is quite important for the complex system (Zhu,2005).

For example, in IO, onshore CCR and offshore CCR have some similar functions, like the emergency shutting down system, when emergency happens, any of the CCR can take action to shut down the system, but did you think about why we should arrange it? If both the offshore CCR and offshore CCR should shut down the system, then the shut down action can be done, of course, we know the system will be more dangerous.
This obvious decision/arrangement (most of us take it for grant) tells us the importance of the relationship between parts.

For choosing the contractors, it is not so important concerning the high quality of their service, we know that every coin has two sides; you have to pay much more to get a better quality of the service. But if you notice the relationship of the contractors, you can spend less but get more. For example, if contractor Ⅰ has a close relationship with contractor Ⅱ, they have worked together for several projects, it is better to hire them rather than ‘strange ‘contractors.

5.3.4 Find out the key point of the complex system

Like the saddle point, or the fulcrum---‘give me a fulcrum, I can move the earth’, the stone in a mountain is different from the stone in the ground because the location.

One of the Chinese medical system is acupuncture, it analysis the channels and collaterals, acupuncture points, however we cannot find actually where they are, the channels and collaterals, acupuncture points are the relationship between the cells and organs, these key points are quite important for treatment.
In IO case, we can find that examples: onshore CCR is a key point, it connects to almost all the organizations, like the root of the plant, when we pull out the root, we get the whole plant, if we try to pull the branch, it is not easy to get the whole plant before the branch broken. Communication is also a key point; it acts like the bridge among the organizations.

6. Conclusion

BORA includes the barrier analysis, bringing the higher level consideration than the ordinary method, however, it is not suitable for complex system, even the barrier block diagram is simple, it can be a huge project to draw the whole picture including RIFs, for quantitative aspect, a small inexact can result in a big different in the final result. It is not necessary to spend so much time, energy and money to develop the model and calculate it.

In ORIM is not easy to establish the risk indictor, the time length to find the risk indictor is a problem, ORIM looks more like a monitor, but it is not applicable for every system. Complex system requires higher level of analyzing. In addition, both BORA and ORIM depends on the quantitative result, but quantitative analysis is not suitable for complex system, it does not mean that quantitative analysis is not useful at all for complex system, we still need calculation, but it is not practicable.

We have also discussed several definitions of complexity and complex system, for risk analysis, if a complex system is ‘An open adaptive system that can evolve’, ‘Not determined by general law and linear cause-effect relation’, ‘Have complex human, organisation and social interaction’, it is a complex system. Complex brings new causes of failure, e.g. the widely use of the ICT, but it does not bring in new event types, e.g. fire, explosion, gas leakage. So changeable is inside the unchangeable, likewise. Chinese thinking of medical can be brought to deal with it, because diagnosing people, in some extents, and it is similar to risk analysis.

According to Perrow, linear and complex is two dimensions of interaction, and coupling includes loose coupling and tight coupling. But not all complex system are tight coupling, like the universities, we cannot apply the same measure to prevent accident in tight coupling and loose coupling.

IO is a complex system, it fulfils the prerequisite and it has the characters of the complex system, so BORA and ORIM is not suitable to apply here. To assess the risk of IO, STAMP may be one of the approaches, in STAMP, the system is viewed as the interrelated components in a dynamic situation, decomposing system is not exist in STAMP, hierarchy control is used base on adaptive feedback mechanism. Another approach is why-because analysis, by investigating, it models the sequence of events which will lead to accidents, events and states are analyzed in proper time order.

Using STAMP and WBA, we may be not able to assess exactly the quantitative result of the risk, but we can better manage and operator the system, risk can be reduced due to the good performance and management, quantitative way of thinking is quite common is western, take the simple example in daily life, in the west, there is strict quantitative standard of in recipes, like 2dl water, 20g salt, put in the oven for 10 minutes with the temperature 250°C. But I Chinese recipes, you will always see they wrote like this: water in proper quantities, 2 spoon salts, some green onion. There are quite a lot of such examples, however, I admitted, use the number to illustrate is one way, not applicable for all of the problems. So, at last, some key point is mention which might be ignored, e.g. How to organize the element is more important than the elements themselves.

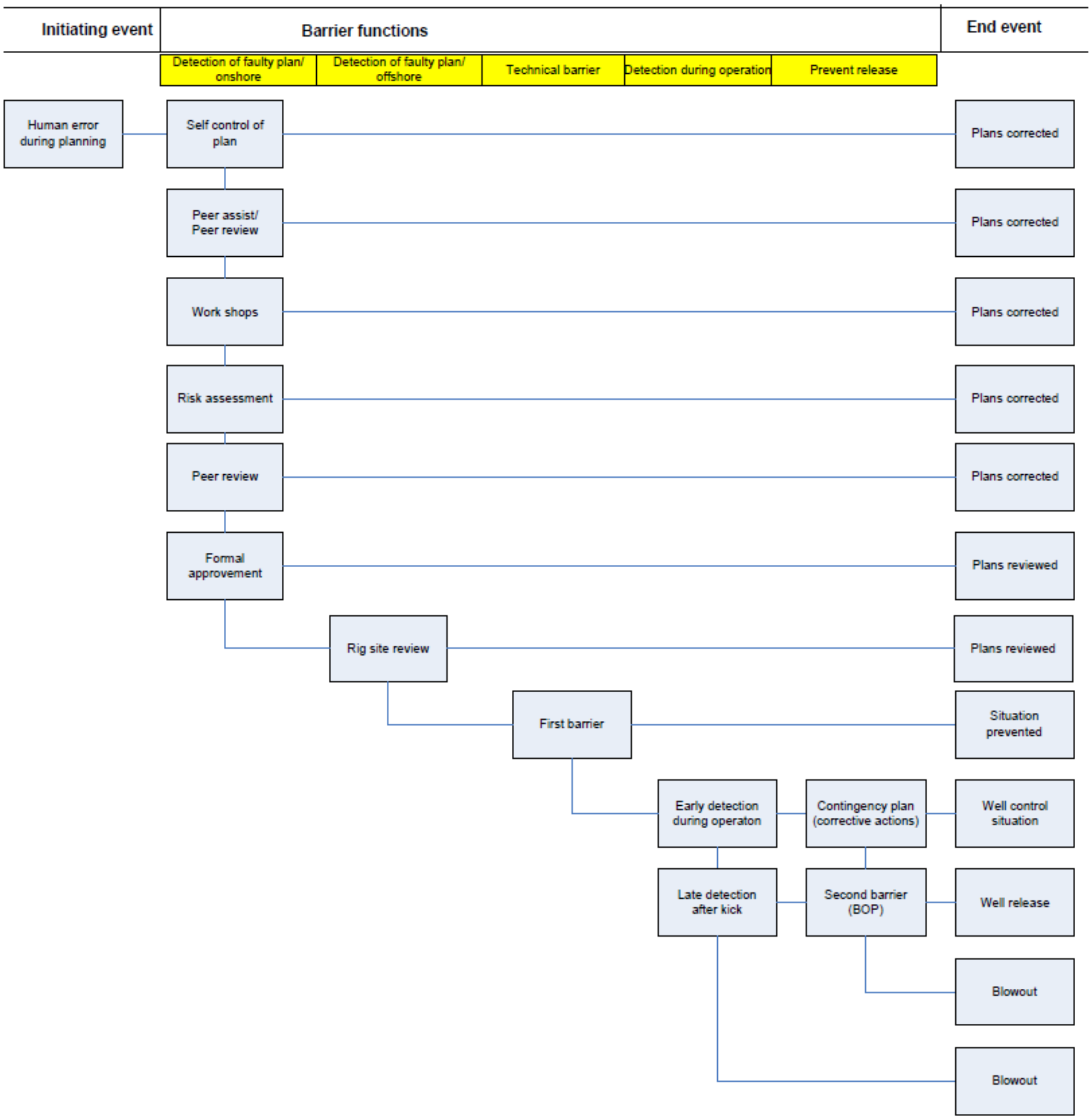
Reference

1) Grøtan Tor Olav, Albrechtsen Eirik, Rosness Ragnar, Bjerkebæk E (2008). The Influence on Organizational Accident Risk by Integrated Operations in the Petroleum Industry, Safety Science Monitor 14, 1, article 5.
2) Zhijun Feng. (2003). the outline of soft science, p34 - 35.
3) Guozhi Xu. (2000). System science, p299.
4) Ian P. McCarthy, Thierry Rakotobe-Joel& Gerry Frizelle. (2000). Complex systems theory: Implications and promises or manufacturing organizations. Vol. 2, Nos. 1–7.
5) Paul Cilliers. (1998). Complexity and Postmodernism, London.
6) Kauffman, S., Macready, W. (1995). Technological evolution and adaptive organizations, Santa Fe, NM: Santa Fe Institute Working Paper 95-02-008.
7) Jean -christophe Le Coze. (2005). Are organisations too complex to be integrated in technical risk assessment and current safety auditing? Safety Science, 43, 613-638, 2005.
8) Charles Perrow. (1984). Normal accidents. Basic Books, NY.
9) Yaneer Bar-Yam (2000). 'Linear and Nonlinear' in 'Concepts in Complex Systems', (New England Complex Systems Institute (NECSI), Cambridge, MA), URL: http://www.necsi.org/guide/concepts/linearnonlinear.html.
10) Leveson. (2004). A new accident model for engineering safer systems. Vol. 42, No. 4, April 2004.
11) Zahid H. Qureshi. (2007). A Review of Accident Modelling Approaches for Complex Critical Socio technical Systems. Conferences in Research and Practice in Information Technology Series; Vol. 336.
12) Lewis, D. (1973). Causation. Journal of Philosophy. Vol. 70, No. 17, Seventieth Annual Meeting of the American Philosophical Association Eastern Division (Oct. 11, 1973), pp. 556-567
13) Richard I. Cook. (2009). How complex systems fail. MD, Cognitive technologies Laboratory, University of Chicago.
14) Stein Haugen. (2005). Lecture materials on risk analysis in NTNU.Norway.
15) Erik Hollnagel. (2004). Barriers and accident prevention. Aldershot, UK: Ashgate
16) Terje Avenb, Snorre Skleta, and Jan Erik Vinnem. (2006). Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part I. Method description. Journal of Hazardous Materials, Volume 137, Issue 2, 21 September 2006, Pages 681-691.
17) Stein Haugen. (2007). Lecture materials.NTNU,Norway
18) K, Øien. (2001). A framework for the establishment of organizational risk indicators. Reliability Engineering and System Safety, 74 (2001) 147-168.
19) Taylor, R. J. (1988). Analysemetoder til vurdering af våbensikkerhed. Glumsø, DK: Institute for Technical Systems Analysis.
20) Okstad E., Sørli F., Wagnild B. R., Skogdalen J. E., Haugen S., Seljelid J., Sklet S., Vinnem J. E.(2009). Human and organizational factors effect on safety barriers in well operations. IADC Drilling HSE Europe Conference & Exhibition. Amsterdam.
21) Reason, J. (1997): Managing the Risks of Organizational Accidents. Ashgate Publishing Company, Burlington USA, 1997.

22) Hollnagel, E. (2004): Barriers and Accident Prevention. Aldershot, United Kingdom: Ashgate Avebury; 2004.
23) Qingshi Zhu. (2005).Chinese medical system is a complex system.
24) http://www.rvs.uni-bielefeld.de/research/WBA/#what-is-wba. (Last visited 9.May)
25) http://www.causalis.com/about/methods/why-because-analysis.html(Last visited 9.May)

Appendix A

Figure 11 Barrier diagram showing failure scenarios in planning (Okstad E., et al, 2009)



Appendix B

RIO research activity:

Risk assessments of IO scenario

Future scenario: "Onshore CCR, eDrilling, support centers and integrated contractors"
The future scenario description is based on descriptions by Tveiten et al. (2008)

We find ourselves in year 2015. The field has been in operation since 1980 and has entered the tail production phase.

A global oil and gas company has decided to move the central control room (CCR) from offshore to onshore on an existing installation. At the same time, the company has decided to implement eDrilling. The company has already in place several expert centers which supports operations, which will continue to support the onshore CCR. The company has for some years integrated contractors closely to operation by use of ISD (Integrated Service Delivery) contracts.

After the implementation of onshore CCR and eDrilling, it is believed that the system will look as following:

Type of field: Gas/Oil

Wells: 100

Living quarters: 36 beds

Organization:

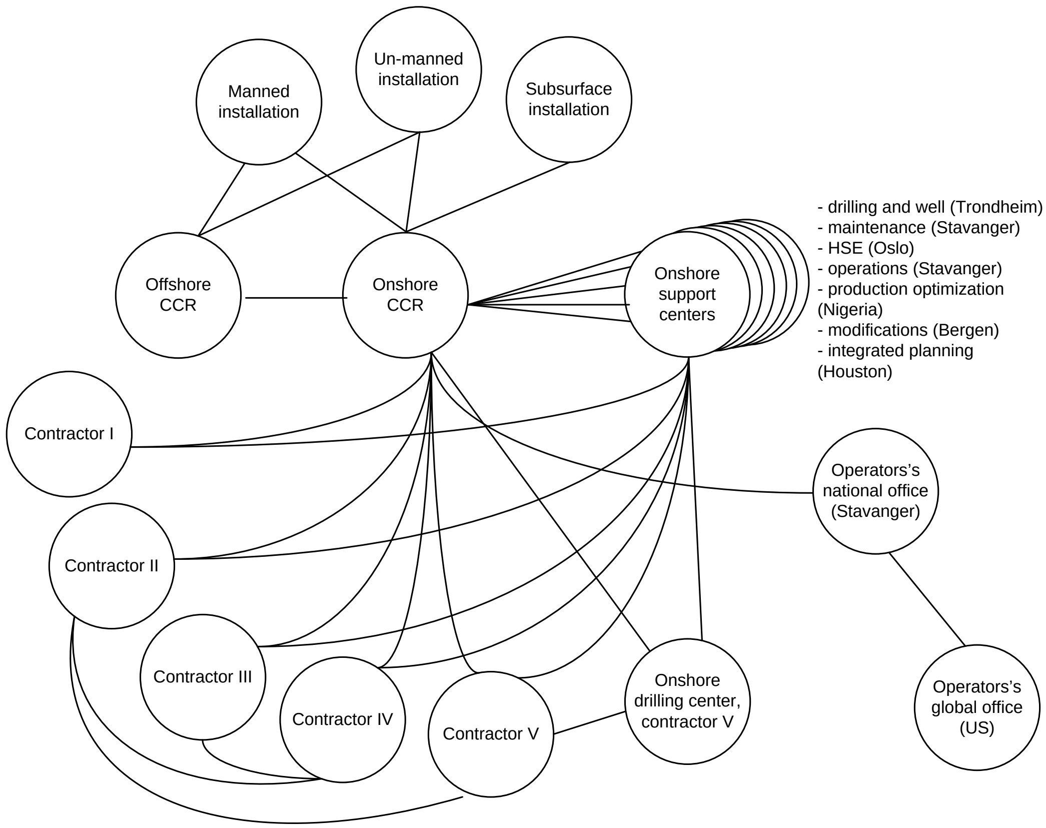
- Lean staffing levels; remotely operated production part of the time (night);
- One manned installation, one un-manned installation and one installation on ocean floor.
- The operator is a global company, its head office is in US and operates in several fields across the world. The operator has a Norwegian office located in Stavanger.

Onshore CCR:

- All control room functions rest with the onshore CCR.
- Complete onshore CCR in Norway;
- Three 8h-shifts per day, 7 days a week. Three operators in each shift.

Offshore CCR:

- Complete offshore control room; manned by one operator on 12-hour day shift.
- The offshore control room is closed during the night.
- There are four offshore process operators, one of whom is available to the onshore CCR at night if needed
- The offshore process operators work day and night shifts and are all cross-trained.



Working hours, shift arrangements and rotation system:

- Offshore: 12-hour dayshift; 14 days offshore followed by 4 weeks at home.
- Onshore: The CCR has three shifts, each lasting 8 hours. On-shore staff rotation every 9 months. The staff of the operations group and the planning group has standard 8-hour workdays.

Onshore support centres

- There are 7 different support centres located at different places in the world that assist the operation by expert knowledge and assess to real time information on the installation performance as well as information from the operator's other installations
- The centers support not only this installation, but also the operator's other installations, both at the Norwegian Continental Shelf (7 installations) and partly in other countries. For example, the maintenance support center, responsible for maintenance planning (opportunity based maintenance), also supports operations in Africa, the Caspian Sea and the Golf of Mexico.
- The support centers are manned 8-16 local times.
- Some experts, located in Nigeria, have been hired to help interpret the steadily increasing amounts of reservoir data. The communication between the CCR and the hired expertise takes place in collaboration rooms (broadband communication), and on a daily basis. These exchanges include consultation as needs arise in addition to

scheduled, regular meetings, and meetings by appointment. The experts in Nigeria offer well-service support at night.

Contractors

- 5 contractors are at current time involved in different operations of the field (e.g. drilling, maintenance).
- The collaboration is based on the concept integrated contractors. By use of collaboration technology, operators and suppliers are integrated, e.g. in morning meetings. The purpose of using an integrated supplier is, among other things, to maximize expertise and to reduce costs associated with the supplier and the operator/oil company having parallel organizations. Central elements in such cooperation are total planning, cross-trained personnel and moving contractor tasks onshore. The contractors share the same real time information as the operator, and has their own collaboration rooms used for daily communication with the operator, e.g. in morning meetings
- The drilling contractor is a sole supplier of drilling services in the sense that all areas of responsibility, such as directional drilling, drilling fluids, cementing or logging during drilling, are covered by one contract, which was signed as early as 2004. This type of contract is called an ISD (Integrated Service Delivery) contract, and among its central elements were factors such as total planning, cross-trained personnel and moving tasks onshore. The objective of the cross-disciplinary training across different job categories is to ensure that personnel are trained to carry out tasks in addition to their own field of expertise, even across company boundaries. It has emerged lately that there is a good deal of discontent with the many of the new arrivals' level of competence, and that there is concern that events may evolve because those on duty, whether offshore or onshore, will lack the resources to handle the situation.

The field has been in operation since 1980. According to studies, remote operation of the platform would improve both the efficiency and the safety of the platform; and furthermore extend the life of the field and the wells. For these and other reasons, a decision has been made to move the CCR onshore. New technology made this scenario possible. Three operators man the CCR. A control room still exists on the platform: it is manned by one operator during daytime. A subsea installation is also operated by the CCR, via remote control.

During the last years, oil and gas fields on the Norwegian shelf have been remotely operated by an onshore organization consisting of groups of experts within different areas.

The process related to the moving of the CCR onshore has been characterized by opposing views by the operating company and the labour organisations. The labour organisations opposed the decision of moving the CCR due to safety concerns. There are still some worries related to onshore CCR among operator and contractor workers, not least during night time when the offshore CCR is unmanned.

Due to the large numbers of offshore workers retiring in the period between 2009-2013 and recruitment problems in the years prior to this period, few people on the platform or in the CCR possess offshore experience of any duration. Recruitment problems at home is also the reason why a number of offshore engineers have been recruited from countries whose language and culture differ from that of the Norwegian workers. One fears that this development will result in lack of offshore experience at the onshore CCR. One also fears that the onshore operations centre will have problems persuading the staff to rotate to offshore jobs after they have experienced working onshore, resulting in the disintegration of the factory competence.

Some of the challenges so far have concerned differences with regard to culture and language, different offshore/onshore shift arrangement, and the handling of an increasing number of handovers. The fact that they are under constant pressure from different directions to increase production has also represented a challenge for the control room operators.

eDrilling (real time drilling simulation, 3D visualization and control from a remote drilling expert centre) will be implemented at an Onshore Drilling Center, located at the drilling contractor. The integrated drilling simulator serves as an important medium for real time communication and collaboration among different drilling actors (offshore and onshore personnel, drilling contractors and service providers). The eDrilling concept provides i.a. real-time supervision of the drilling process; early diagnosis of the drilling state and conditions; flow model calculations; and early warning of upcoming unwanted conditions and events.

The platform’s energy needs are supplied by onshore sources. There is an emergency generator on board for use in the event of power failure. Communication via satellite is also available as a backup in the event of the breakdown of ordinary lines of communication.