Global Journal of Management and Business Studies.
ISSN 2248-9878 Volume 3, Number 2 (2013), pp. 171-184

http://www.ripublication.com/gjmbs.htm

What Extent is Risk Reduction Required?

[1]Elahe Taheri, [2]Reyhaneh Taheri and [3]Alireza Arsalan

[1]Business Management Department, Higher Education Institute (Yazd ACECR), Yazd, Iran.
Iran, Yazd, St.Valiasr, alley 38, Plaque 24
[2]Electrical Engineering Department, Islamic Azad University, Yazd, Iran.
[3]Management Department, Higher Education Institute (Yazd ACECR), Yazd, Iran.

Abstract

Risk assessment is a step in a risk management procedure. Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat .
Operations in the oil, gas and petrochemicals industries involve hazards that can expose employees and members of the public to significant health and safety risks and lead to significant environmental impacts. Effective consideration of risk management issues has always been a concern to those responsible for managing businesses in this industry.
In this paper, we examine the issues facing business leaders who need to consider what they should be doing to risk management in a strategic manner.
We explore the following questions:

- What is Risk Assessment?
- How Management Systems Reduce Risk?
- What extent is risk reduction required?

Keywords: Risk, Risk Assessment, risk Management, safety.

1. Introduction

Businesses cannot afford to ignore the risks to their operations. The impact on the bottom line performance can be significant, and lasting damage can be made to the public perception of the business.

The challenge for business leaders is to know how to manage the business risks in a way, which is optimal for their business.

All businesses differ in their scope and nature of operations; therefore each business is presented with a unique set of risks to manage.

The level of management applied by a particular business should reflect its level of business risk. If a business does not apply sufficient controls, it may be exposing its business unnecessarily. If a business applies overly complex controls it will be wasting its resources.

Overly complex risk management control may result in confusion and misunderstanding and may lead to deliberate bypassing of the system.

Keeping the risk management process simple, and appropriate to the level of risk, will aid success.

2. Safety

Practical certainty that adverse effects will not result from exposure to an agent under defined corporal of risk.[2]

3. Risk Management

The total process of identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.[1]

Risk management: decision making process involving considerations of political, social, economic, and technical factors with relevant risk assessment information relating to a hazard so as to develop, and compare regulatory and non-regulatory option and to select and implement appropriate regulatory response to that hazard. [2]

Managers should therefore assess their current risk management methods and determine how appropriate they are for the business. The decisions relating to any further action can then be taken.

There are two simple measures that are often used in assessing current performance:

- The number of accidents or incidents relating to risk .
- The cost of risk.

3.1 The Number of Accidents or Incidents Relating to Risk

Measurement of the number of accidents and risk related incidents reported during a year gives an indication as to an organization's risk performance. Trends can be identified.

However, this approach is slow and mainly reactive and one may have to wait until the accidents or incidents have already happened. Often an accident or incident is the event that exposes a risk management problem.

Accident and incident data must be readily available and can provide a starting point for assessing historic risk performance and any trends.

However care must be exercised in their interpretation.

So, as a starting point, an organization should ensure it adequately reports accidents and incidents. Recognizing this will only lead to a slow rate of improvement in performance, the organization should develop proactive measures which focus on managing underlying issues which can lead to an accident.

4.2 The Cost of Risk

How much do you currently spend on managing risk? Is this too much or too little? There are techniques available for evaluating the true costs associated with risk issues. Many organizations fail to measure the true cost of risk effectively. The result is an ineffective use of resources and failure to identify where to focus management efforts.

Accidents can result in direct and indirect costs to an organization, but certain cost will not be recovered from insurance.(Fig.1)

Figure 1: Direct and Indirect Costs.

Organizations generally believe that the majority of costs are covered by their insurance contracts, however significant costs are often absorbed by other budgets (e.g. maintenance budget, sick pay, increased insurance premiums).

The point of lowest cost is not always obvious, however failure to consider the business implications of risk can lead to unacceptable burdens being placed on the organization as a whole. (Fig. 2).

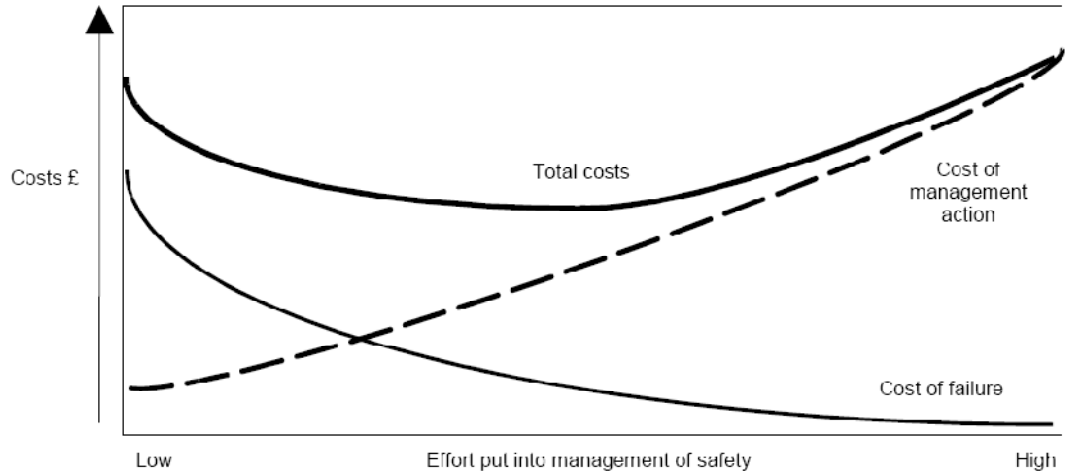

Figure 2: Costs vs. Effort.

4. Accidents or Incidents Relating to risk

As a consequence, organizations can perceive they have good levels of performance as they have low accident and incident frequencies. However, this may be by good fortune rather than good management.

So, as a starting point, an organization should ensure it adequately reports accidents and incidents. Recognizing this will only lead to a slow rate of improvement in management performance, the organization should develop proactive measures which focus on managing underlying issues which can lead to an accident.

Attention to risk is not merely an altruistic Endeavour. If managed properly, it can provide sustained business advantage. The costs of accidents can place a severe, but unrecognized, burden on the ability of an organization to operate profitably.

For example, an organization operates with a profit margin of about 5%. (Fig. 3).

Thus, knowing the cost of an accident or incident, the income required to overcome the cost of that accident or incident can be calculated.

$$\frac{\text{Cost of Accident}}{\text{Profit Margin}} = \text{Required Revenue}$$

If we consider an accident which results in a cost of £50,000 and the organization has a profit margin of 5%, the revenue required to overcome the cost of the accident is:

$$\frac{£50{,}000}{0.05} = £1{,}000{,}000$$

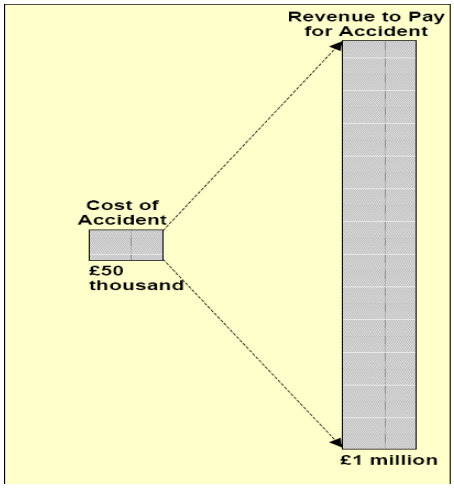

Figure 3: Revenues.

The true cost to the business of the accident is not the uninsured losses of £50,000 but is in fact the increased burden of having to generate an additional £1,000,000 of revenue.

The failure by management to recognize this direct relationship between risk incidents and the profitability of the business can lead to inappropriate cost reduction initiatives and missed opportunities for the implementation of effective strategies.

These strategies will incur costs of their own (salaries, diversion of resources, increased training and supervision). Therefore the challenge is to find the point at which the losses to the organization are balanced by the cost of an appropriate control programmed.[13]

Below is a summary of this six-part management system model (Fig. 4)

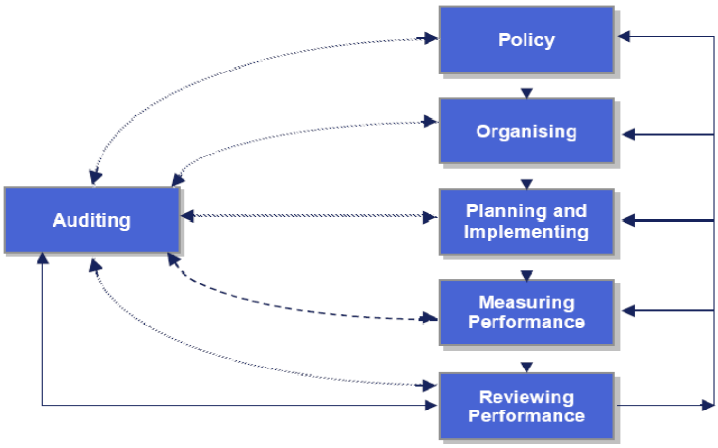

Figure 4: HSE Management System.

The key elements are:

4.1 Set Your Policy

Prepare a written statement of your risk Management policy that states how the policy will be implemented and monitored. The policy should:

- Influence company activities such as the selection of people, equipment and materials, the way work is conducted, and the design of goods and services.
- Communicate to staff that hazards have been identified and risks assessed, eliminated or controlled.

4.2 Organize Your Staff

Involve your staff to ensure that the risk Management policy is most effective. The four elements of successful involvement are: ***Competence***, ***Control***, ***Co –operation***, ***Communication***

4.3 Plan and Set Standards

Ensure that your risk Management efforts will be successful through effective planning. There are several facets to planning: (Fig.5).

Figure 5: Planning.

Specifically, planning should include at least the following:

- Identifying hazards and assessing risks, and deciding how they can be eliminated or controlled
- Complying with the safety laws that apply to your business
- Agreeing to risk Management targets with managers and supervisors
- Setting a purchasing and supply policy which takes risk Management into account
- Designing of tasks, processes, equipment, products and services
- Setting risk Management systems of work
- Establishing emergency procedures to deal with serious and imminent danger
- Setting standards against which performance can be measured.

4.4 Measure Your Performance

Measure `risk Management` performance to discover if you are being successful. There are two types of monitoring: active monitoring (or sometimes referred to as a "proactive") and reactive monitoring.

4.5 Audit and Review

Learn from experience. Audits complement monitoring activities by looking to see if the `risk Management` policy, organization and systems are achieving the right results. While reviewing policies, attention should be given to:

- Compliance with `risk Management` performance standards
- Areas where standards are absent or inadequate
- Achievement of stated objectives
- Injury, illness and incident data.

Together this information will help you identify areas for improvement.

4.6 Level of risk Management

At what stage of evolution of risk management is your organization?..... and, at what stage do you and your stakeholders want it to be?

To help establish where an organization is and where it should be, its position on a management system matrix can be evaluated.

Having profiled your company's performance and gauged your position against others, you need to assess what level or risk management is most appropriate to your business; and in particular whether the current approach is still appropriate. To assist in this assessment an organization can conduct a "stakeholder needs analysis".

4.7 Organization Approaches to risk Management

Does it take a proactive approach or a reactive approach to risk management? For example, does the organization react to legislation and to accidents and incidents after they occur, or does it try to anticipate and take action before it has to?

Some organizations have no formal method of risk managing. The work is conducted without any rules or procedures being applied. Other organizations rely on large amounts of formal paperwork, guidelines and procedures to ensure operations comply with management requirements.

4.8 What is Risk Assessment?

Risk assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of risk management and synonymous with risk analysis.[1]

Risk assessment a process intended to calculate or estimate the risk to a given target organism, system, or (sub) population, including the identification of attendant uncertainties, following exposure to a particular agent, taking into account the inherent characteristics of the agent of concern as well as the characteristics of the specific target system.[2]

When evaluating the options a set of criteria should be used. Are risks acceptable to the regulators? Will the change help to communicate to staff that hazards have been identified and risks assessed, eliminated or controlled.

One simple yet powerful technique for prioritizing options is to use a qualitative (i.e. non quantified) risk assessment. This technique can be used to rank possible actions by assessing the comparative risks that the options aim to reduce.

Risk assessment represents an important component of a company's overall approach to Management planning. The planning process for addressing issues requires a three stage approach. (Fig. 6).

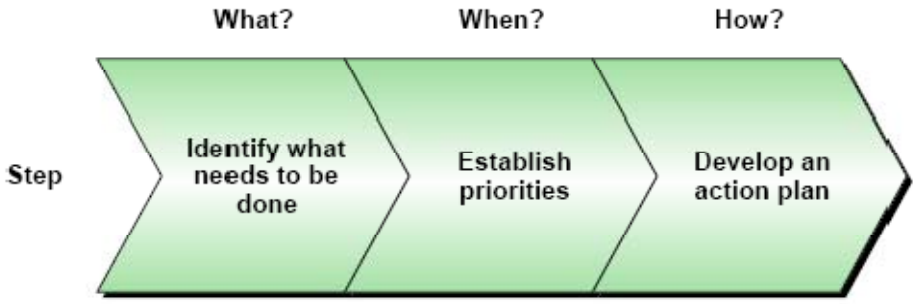

Figure 6: Planning.

Use	*Technique*	*Basis*
Typical for work places (used by Supervisors, Engineers or Managers) Less thorough more straightforward to apply	Inspections	Observation and recording of hazards by inspecting a workplace, work process or piece of completed work. Checklist of important points may be used as a guide.
	Hazard Survey	Observation and recording of hazards by conducting a topic specific inspection
	Sampling	Observation of how a sample or people are working
	Job Analysis	Three step approach for identifying hazards in work process
Typical for detailed risk analysis (usually by Engineers or Managers) More thorough Complex to apply	Hazard and Operability Studies (HAZOP)	Very thorough technique for identifying hazards in systems – usually used for detailed risk analysis of a system design or process
	Failure Modes and Effects Analysis (FMEA)	Very thorough technique for identifying hazards in sub-systems or components – usually used for detailed risk analysis of component design or process
	What If?	Identifying hazards which might occur if certain things go wrong – based on experience

The what? and when? aspects are often addressed using the technique of Risk Assessment. In particular, risk assessment allows prioritization of action to address hazards.

The process of risk assessment comprises two main steps: hazard identification and risk evaluation. Hazard identification seeks to identify what can lead to a loss, risk evaluation then determines the chance and severity of such a loss. There are a wide range of techniques which can be used to identify hazards

When there is an ever increasing awareness of hazardous risks that need to be managed by the industrial community, the risks need to be analyzed. This includes Hazard Identification, Risk Assessment and Risk Management. Risk cannot be evaluated without first identifying the hazards involved Many of the hazards will be identified by conducting a PHA (Process Hazard Analysis), such as HAZOP (Hazard and Operability Analysis), What If/Checklist or FMEA. The hazards may arise from a wide range of sources. [3]

FMEA is used to analyze specific systems or items of equipment that are best handled as objects rather than by the use of parameters or operations. FMEA is also used for analyzing pumps, compressors, fans and items of equipment having interactive mechanical and/or electrical components. Many authors, believe that FMEA is very good for analyzing complex equipment items where the failure of a component may have a major consequences. Some authors believe that FMEA does not relate to specific failures that have common causes. In such cases, it needs to be used with Fault Tree Analysis to broaden the scope.[3]

Management Systems provide the controls to reduce the potential risks associated with hazards. These controls reduce “Potential Risks” to “Residual Risks” (Fig.7).

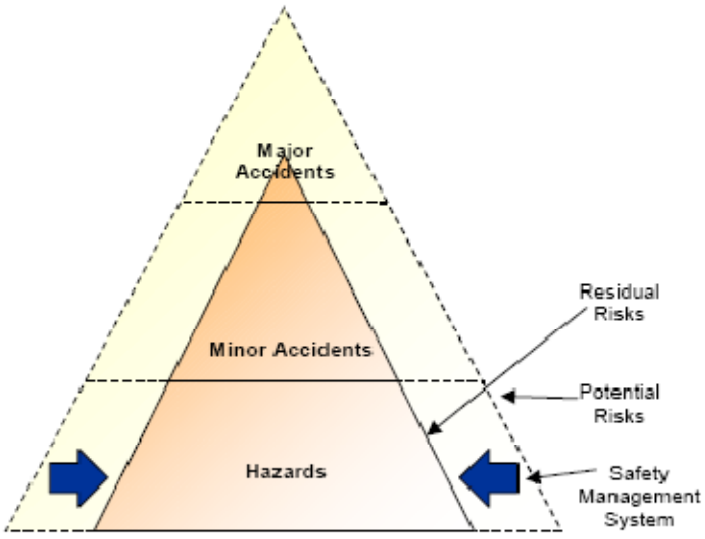

Figure 7: How Management Systems Reduce Risk?

But to what extent is risk reduction required? In the case of safety management risks should be reduced to a level that is '***As Low as Reasonably Practicable***' (ALARP).

There is a requirement to manage safety risks to a level as low as reasonably practicable. Therefore the implementation of risk control measures which bring risks into the ALARP region must be effectively monitored.

The ALARP principle became a legal requirement in the UK under the 1974 HASAW Act and the Tolerability of Risk (TOR) diagram (Fig. 8) was initially developed for the nuclear industry and has subsequently been widely adopted by other industries.

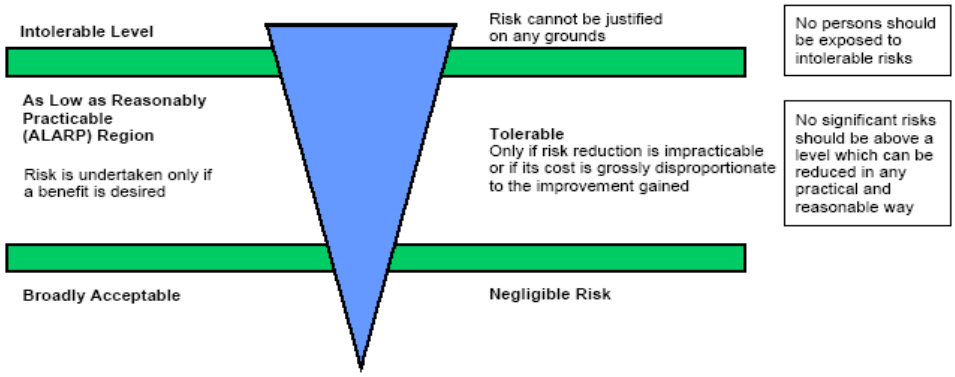

Figure 8: Tolerability of Risk (TOR).

Interpretation of the ALARP principle (Fig. 9) provides a framework for determining whether existing systems are "safe" – and also for "valuing" and controlling investments in management.

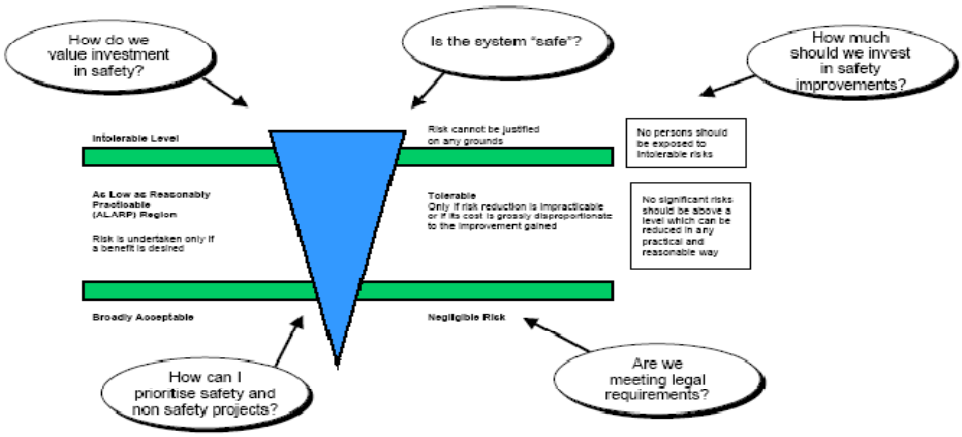

Figure 9: Interpretation of the TOR diagram.

Between the Intolerable and Broadly Acceptable Levels, risks must be reduced As Low As Reasonably Practicable (ALARP). Risks in this ALARP region are only acceptable if further risk reduction is impracticable or the costs of further risk reduction measures are grossly disproportionate to the safety benefits. In the ALARP region, all potential risk reduction options need to be assessed using costs / benefit analysis and managers need to assess whether the costs are grossly disproportionate to the benefits. (Fig. 10).

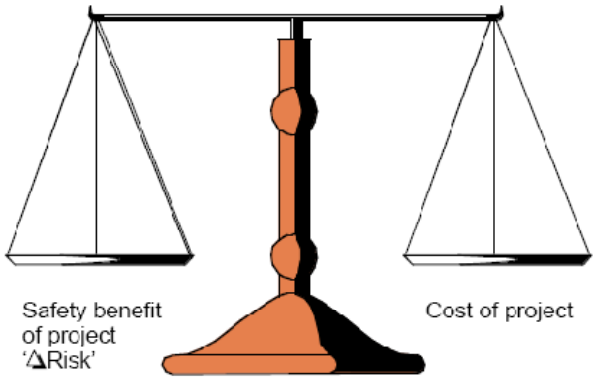

Figure 10: Cost benefit analysis in the ALARP region.

5. Conclusion

The classic accident causation pyramid has demonstrated the relationship between potential hazards (unsafe acts or unsafe conditions) and serious accidents. Safety culture directly influences the occurrence of unsafe acts, especially those unsafe acts which are classified as violations as opposed to errors. It can also be reasonably argued that safety culture may often be a causal factor in circumstances that lead to the existence of unsafe conditions.

Risk Management culture is something an organization is (the beliefs, attitudes and values of its members regarding the pursuit of safety) and something that an organization has (the structures, practices, controls and policies designed to enhance safety). The latter is easier to manipulate than the former. It is hard to change the attitudes and beliefs of adults by direct methods of persuasion, but acting and doing, shaped by organization controls, can lead to thinking and believing.

In order to implement measures to control specific risks it may not be necessary to conduct a major change initiative. However, large scales of change may be required if an organization was, for example, trying to move from the compliance stage of evolution to risk management stage.

No matter what the nature of the change is, there is a common process of change which has to be followed.

In the case of large scale, organizational change, the process is very similar to that of personal change. For a significant improvement to happen, you have to first feel a real need to change. Then you need to have the desire to change and courage to proceed.

References

[1] Gary Stoneburner, Alice Goguen1, and Alexis Feringa, ,(2002), *Risk Management Guide for Information Technology Systems*

[2] World Health Organization, Geneva, 2004, "*IPCS(international programme on chemical safety) RISK ASSESSMENT TERMINOLOGY"*

[3] M J. Jafari et al, *Risk Assessment of a Tunneling Process Using Machinery Failure Mode and Effects Analysis (MFMEA)"*

[4] NIST Special Publication 800-12, (1995), *An Introduction to Computer Security: The NIST Handbook* .

[5] Jaworski, Lisa, (1993), *Tandem Threat Scenarios: A Risk Assessment Approach.* Proceedings of the 16th National Computer Security Conference, Baltimore, MD: Vol. 1, pp. 155-164.

[6] NIST Interagency Reports 4749.,(1991), *Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out*.

[7] Katzke, Stuart, (1992), *A Framework for Computer Security Risk Management*. 8th Asia Pacific Information Systems Control Conference Proceedings. EDP Auditors Association, Inc., Singapore, October 12-14.

[8] Proceedings,(1991), *4th International Computer Security Risk Management Model Builders Workshop*. University of Maryland, National Institute of Standards and Technology, College Park, MD

[9] NIST Special Publication 800-26,(2001), *Security Self-Assessment Guide for Information Technology Systems*

[10] NIST Special Publication 800-27, (2001), *Engineering Principles for IT Security*.

[11] OMB Circular A-130, (2000), *Management of Federal Information Resources.* Appendix III. November.

[12] The Costs of Accidents at Work, HSE 1996

[13] Successful Health and Safety Management' HSG65

[14] Meyer, C.H., and S. M. Matyas., (1982), *Cryptography: A New Dimension in Computer Data Security*. New York, NY: John Wiley & Sons.

[15] Nechvatal, James.,(1991), *Public-Key Cryptography.* Special Publication 800-2. Gaithersburg, MD: National Institute of Standards and Technology.

[16] National Bureau of Standards.,(1985), *"Computer Data Authentication"*. Federal Information Processing Standard Publication 113. May 30.

[17] National Institute of Standards and Technology.,(1991), *Advanced Authentication Technology.* Computer Systems Laboratory Bulletin.

[18] National Institute of Standards and Technology.,(1993), *Data Encryption Standard.* Federal Information Processing Standard Publication 46-2. December 30,.

[19] Eti, M.C., Ogaji, S.O.T., Probert, S.D., (2006), *Development and Implementation of Preventive Maintenance Practices in Nigerian Industries Applied Engergy*, 83, P.1163-1179

[20] Gharari, N., (2007), *Risk Assessment in Tunnelling with TBM Using FMEA Method And Temporary Ventilation Design*, MSc thesis, Shahid Beheshti University (MC).