REFERENCES

Aksel, K.H. (2002), Organising a Financial Institution to Deliver Enterprise-Wide Risk Management, PricewaterhuoseCoopers Working Paper, 14 pages

Barton, T.L.; Shenkir, W.G. and Walker, P.L. (2002), Making Enterprise Risk Management Pay Off: How Leading Companies Implement Risk Management, Financial Times/Prentice Hall PTR

Bielski, L. (2002), The great risk debate, Journal of American bankers association banking, Vol.94 No.2, pp.58-64

Carey, A. (2000), The boardroom imperative on internal control, Financial Times, Mastering risk supplement, 25 April 2000

Cobbold, I. and Lawrie, G. (2002), The development of the Balanced Scorecard as strategic management tool, PMA2002, Boston.

EIU (1995), Managing Business Risks, Economist Intelligence Unit, pp. 25-33

Elms, D. G. (1992), Risk assessment in D J Blockley, Engineering Safety, McGraw-Hill, New York.

Fatemi, A. and Glaum, M. (2000), Risk management practices of German Firms, Journal of Managerial Finance, Vol.26 No.3, pp. 1-17

Galloway, D. and Funston, R. (2000), The challenges of enterprise risk management, Journal of Balance Sheet, Vol.8 No.6, pp. 22-25

HEFCE (2003), Risk management in the higher education sector [online], Higher Education Funding Council for England, http://www.hefce.ac.uk/GoodPrac/risk/ [24 Nov 03]

Hoffman, D.G. (2002), Managing operational risk: 20 firm wide best practice strategies, John Wiley & Sons: New York

Keey, R. B. (2000), Management of Engineering Risk, Centre for Advance Engineering, University of Canterbury: New Zealand

Kippenberger, T. (1999), Internal audit and governance: the shift from control to risk, Journal of the Antidote, Vol. 4 No.3, pp. 6-7

Kletz, T. A. (1999), Hazop and Hazan, 4th Edition, IChemE Rugby, UK

Lawrence, W. W. (1976), Of Acceptable Risk, W Kaufman, Los Atos, CA.

Lawrie, G. J.; Kalff, D. C. and Andersen, H. V. (2003), Integrating Risk Management with existing methods of Strategic Control: Avoiding duplication with in the corporate governance agenda, 2GC Working Paper, 2GC Ltd: UK, 17 pages

Lawrie, G. J.; Kalff, D. C. and Andersen, H. V. (2003), Risk Management and Performance Management: a way to avoid duplication of effort by combining both tools, 2GC Working Paper, 2GC Ltd: UK, 24 pages

McCraig, K. (1999), Deloitte & Touche Finance Director Risk Benchmarking Results, Deloitte & Touche Working Paper, 14 pages

Molak, V. (1997), Fundamentals of Risk Analysis and Risk Management, Lewis Publishers,

Pidgeon, N.; Hood, C.; Jones, D.; Turner, B. and Gibson, R. (1992), Risk perception in Risk Analysis and Management, Royal Society, London

Ridley, J. and Channing, J. (1999), Risk Management, Butterworth-Heinemann

Simon, R. (1995), Control in an age of empowerment, Harvard Business Reviews, Vol.73 No.2, 8 pages

Simon, R. (2000), Performance measurement and control systems for implementing strategy, Prentice Hall: New Jersey.

Smallman, C. (1996), Risk and organisational behaviors: a research model, Journal of Disaster Prevention and Management, Vol.5 No.2, pp. 12 - 26

Stamatis, D. H. (1995), Failure Mode and Effects Analysis: FMEA from theory to execution, Quality Press, ASQC: USA

Standard Australian and Standard New Zealand (1999), Risk Management AS/NZS 4360: 1999, NSW. ISBN 0 7337 2647 X

Tchankova, L. (2002), Risk identification - basic stage in risk management, Journal of Environmental Management and Health, Vol.13 No.3, pp. 290-297

Vose, D. (2000), Risk Analysis: A Quantitative Guide to Monte Carlo Simulation Modeling, 2nd Edition, John Wiley & Sons: Europe

Wells, G. (1997), Major hazard and their management, IchemE, Rugby, UK

APPENDICES

APPENDIX A

ENTERPRISE RISK MANAGEMENT INTERVIEW QUESTIONS

1. General

1.1. What risks are of the most concern at the present?

1.2. What possible future risks are of concern?

1.3. What actions have you taken with respect to those current and future risks?

1.4. Do you allocate capital requirements or resources based on your assessment of risks?

2. Company Background, History, and Environment

2.1. How did you become aware of the potential advantages of adopting an enterprise risk management approach?

2.2. Why did you decide to initiate an enterprise risk management approach? Were you motivated by a single event or circumstance?

2.3. What are the goals for the enterprise risk management system?

2.4. What document relating to the enterprise risk management system could be made available to the researcher?

3. Organisational Structure

3.1. Describe the organisation structure for your enterprise risk management.

3.2. Do you have a risk officer? To whom does he/she report? What is the risk officer's job description?

3.3. Do you have appropriate resource, human and technological for managing risk?

4. Assess Risk (identify, source, prioritise)

4.1. How do you identify risk? Describe the process you followed to identify the comprehensive risk language, and describe any risk frameworks you use. (for example risk might be classified as strategic, operating or information risk)

4.2. Do you have an agreed upon set of objectives and have you identified the risk related to each objective?

4.3. With respect to the identification of risk, is it responsibility of one overall group or of each division?

4.4. With respect to the identification of risk, is it done for every department, division, and product?

4.5. Do you use a risk checklist or questionnaire to assist in identify risk? If so, describe.

4.6. Have you considered risk for each step in your value chain? The value chain is the sequence of business functions in which utility of usefulness is added to the products or services of an organisation.

4.7. For each significant process in the organisation, have you determined the risk level and the level of controls in that process?

4.8. Are your risks communicated throughout the company? If so, how?

4.9. After identify the given risk, have you sourced and measured it?

4.10. Is your risk measurement quantitative or qualitative?

4.11. Do you assess the significance of the risk? If so, how do you perform the assessment? Who is responsible for the assessment?

4.12. Do you assess the cost impact of the risk? If so, how do you perform the assessment? Who is responsible for the assessment?

4.13. Do you assess the likelihood of the risk? If so, how do you perform the assessment? Who is responsible for the assessment?

5. Develop Risk Strategies

5.1. Have you evaluated how effectively you are managing the risks? Are you managing or controlling? For any risks that you are under-managing, what changes have you made?

5.2. Do you use any form of risk scorecard or balanced scorecard?

5.3. What controls have you implemented to ensure you manage a given risk?

5.4. Once the given risks have been identified, how do you manage them?

5.5. Are there any tools that are used to manage risks? What are they?

6. Measure/Monitor Risk Processes

6.1. In general, are your risks increasing or decreasing?

6.2. How often do you update your identified risks?

6.3. How often do you update your risk assessment of risks?

6.4. How often do you review your controls and information gathering system based on your risks?

6.5. Do you have a summary metric or series of metrics that identify your risk level?

6.6. Is monitoring and measurement linked to your assessment and prioritisation o risks?

6.7. Describe key performance indicators you use and how they assist in managing risks?

Source: Barton et al. (2002) pp.225-229

APPENDIX B

PROPOSED ENTERPRISE RISK MANAGEMENT SYSTEM

This chapter intends to review the process to establish the enterprise risk management system for the case organisation, based on the process of AS/NZS 4360: 1999, Australian/New Zealand Risk Management Standard, which the Failure Mode and Effects Analysis is used as a risk assessment tool.

AUSTRALIAN/NEW ZEALAND RISK MANAGEMENT STANDARD

Australian and New Zealand Standard AS/NZS 4360: 1999 provides a generic guide for the establishment and implementation of the risk management process involving establishing the context and the identification, analysis, evaluation, treatment, communication and ongoing monitoring of risks. This standard will be exceptionally useful as it provides a thorough analysis of risk management generic to all industries.

An overview of the main element of the risk management system process as set out in AS/NSS 4360 is shown below:

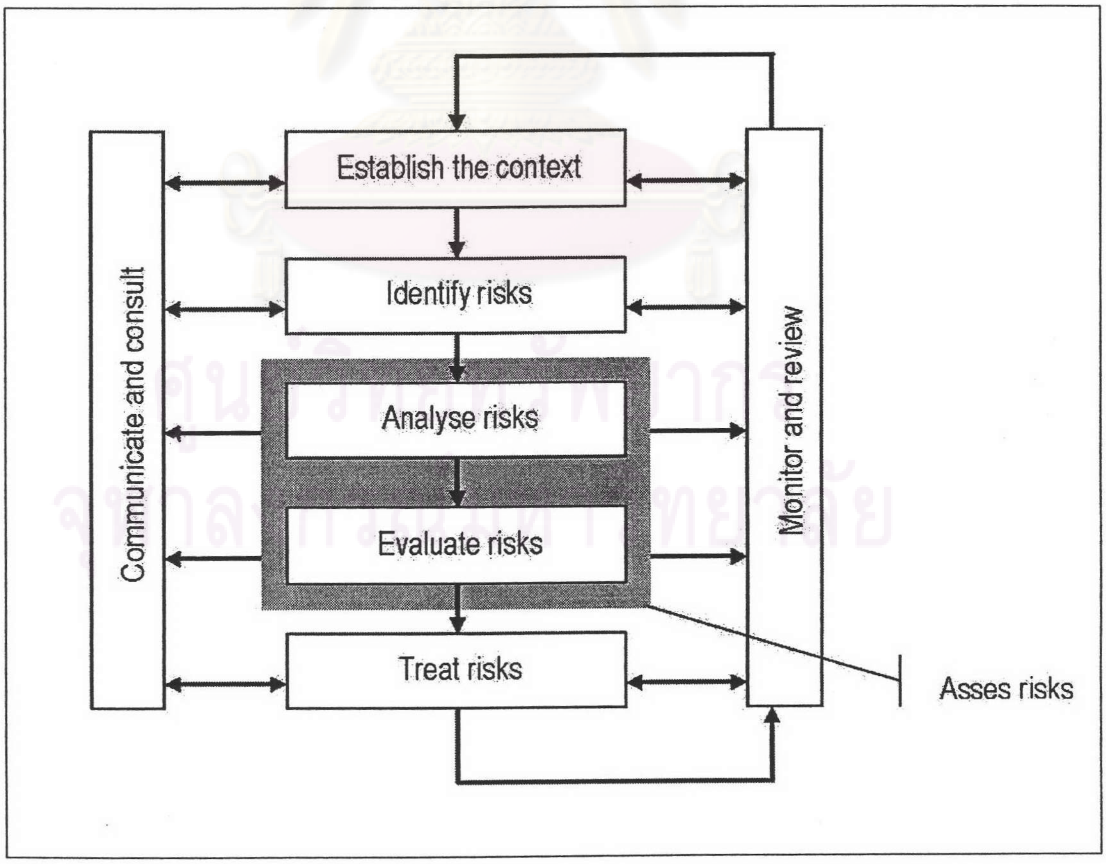

Figure B.1: Risk Management Overview
Source: AS/NSS 4360: 1999

Recall from the Theoretical Foundations, the risk management processes are:
Step 1: Establish the context
Step 2: Identify the risks
Step 3: Assess the risks
Step 4: Treat the risks
Step 5: Monitor and review
Step 6: Communicate and consult

This process can be applied at many levels in an organisation or levels of strategy as well as its operations, and can be tailored in detail in given organisational scale. It may be applied to specific organisations or in the management of recognised specific areas of risks.

The chart shows the risk management process which consists of establishing the context; identifying, analysing, evaluating and treating the risks; monitoring and reviewing the performance of management system and changes that may affect it.

According to the Standard, it is vital to communicate and consult with both internal and external stakeholder as well as concerning the process as a whole.

The Australian/New Zealand Standard suggests a six-step programme to implement a risk management programme as shown in the chart below.

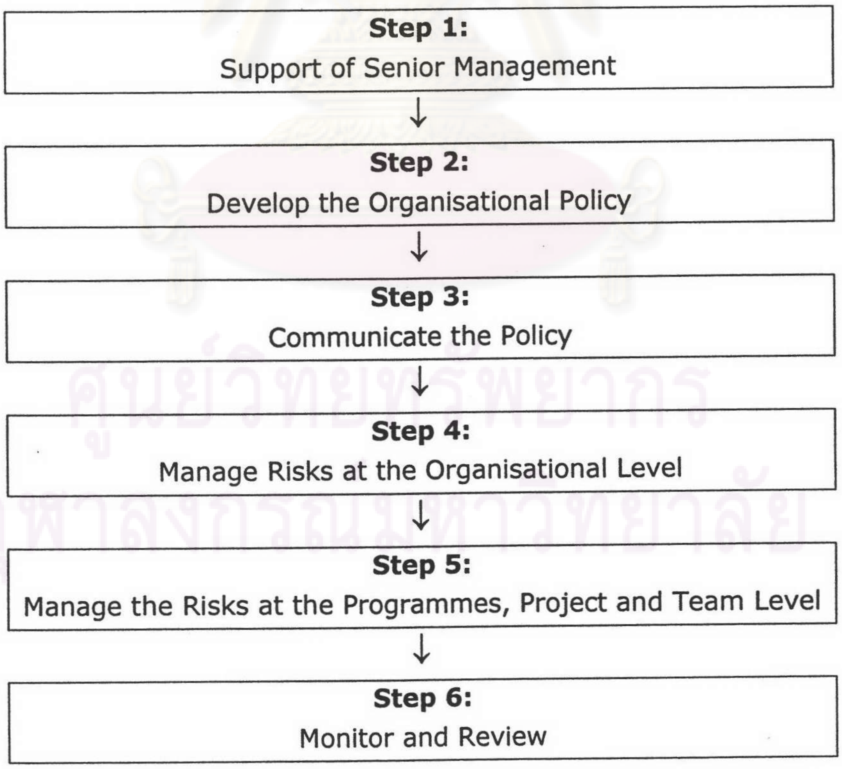
Step 1:
Support of Senior Management
Step 2:
Develop the Organisational Policy
Step 3:
Communicate the Policy
Step 4:
Manage Risks at the Organisational Level
Step 5:
Manage the Risks at the Programmes, Project and Team Level
Step 6:
Monitor and Review

Figure B.2: Steps in developing and implementing a risk-management programme
Source: AS/NZS 4360: 1999

ESTABLISH STRATEGIC CONTEXTS

Risk management planning should begin during the earliest stages. Establishing the context provides an understanding of the environment and mode of operations in which the risk assessment is taking place. This step:

- Specify the main outcomes and objectives of the organisation;
- Identify and analyses the various stakeholders involved or affected by the organisation;
- Identify criteria for the success of the organisation against which the consequences of identified risks can be evaluated (e.g. Performance, cost , schedule);
- Defines key elements for structuring the risk identification and assessment process. A work breakdown structure may provide a good starting point but needs to be adapted to incorporate other elements.

IDENTIFY RISKS

Risk identification is typically addressed in two ways, one prescriptive and other creative. Checklists or questionnaires can be used, it should be for reviewing the identification process and ensuring that no known issues have been ignored. The preferred approach to identifying risks is brainstorming in a group workshop. This method may be more effective than the checklists. Brainstorming allows the identification process to draw on the creative capacity of the participants, reducing the danger that insufficient attention will be given to new issue, as usually happen with the checklists or questionnaires techniques.

Each of the key elements established in the previous step are systematically examined to identify what the risks are and how they may happen. Methods of identifying risk include:

- Brainstorming
- Using checklists
- Holding Focus group discussions
- Examining similar previous organisations
- Surveys and questionnaires

The Australian/New Zealand Risk Management Standard states that the identification of risks must take place within a given context. Defining this background and framework is the first step in any risk study, setting parameter for its scope. Previous generic study of risk and case histories may provide a guide for defining the scope.

ASSESS THE RISKS

Risk Assessment Tools:

After risks are identified by Brainstorming and Questionnaires, the next step is to assess the risks, which the assessment can be subdivided into two step, risk analysis and risk evaluation.

With the widespread use of risk analysis, a number of generic techniques and approaches have evolved. Some of the more common techniques, which look at very different aspects of system safety analysis, are:

- Failure mode and effect analysis;
- Hazard and operability study;
- Fault tree analysis
- Event tree analysis;
- Monte Carlo simulation;
- Probabilistic risk analysis;
- OSH Method of hazard identification; and
- Short cut risk-analysis method

Overviews of each method are discussed in the Appendix III.

Failure Mode and Effects Analysis (FMEA):

The Failure Mode and Effects Analysis (FMEA) is selected to be a risk assessment tool in this study. In order to facilitate documentation of the analysis of potential failure modes and their consequences a Process FMEA form was developed as shown next page:

Note: This FMEA Methodology is applied from the original text by the cooperation of Chrysler, Ford and General Motors.

FMEA
(Potential Failure Modes and Effects Analysis)

Item Name:		FMEA Team:	Prepared by:
			FMEA Date (Orig): (Rev.):

Process Step or Variable or Key Input	Potential Failure Mode	Potential Failure Effects	S E V	Potential Causes	O C C	Current Process Controls	D E T	R P N	Actions Recommended
What is the process step?	In what ways can the Process Step, Variable, or Key Input go wrong? (chance of not meeting requirements)	What is the impact on the Key Output Variables (customer requirements) or internal requirements?	How Severe is effect to the	What causes the Key Input to go wrong? (How could the failure mode occur?)	How frequent is cause likely to Occur?	What are the existing controls that either prevent the failure mode from occurring or detect it should it occur?	How probable is Detection of cause?	Risk Priority # to rank order concerns	What are the actions for reducing the Occurrence of the cause, or improving Detection? Should have actions on high RPN's or Severity of 9 or 10.
								######	
								######	

Applications of the FMEA form is describe below:

1. Item: Enter the name and number of the system, subsystem or component, for which the process is being analysed.

2. FMEA Team: List the names of the responsible individuals and departments which have the authority to identify and/or perform tasks. (It is recommended that all team members' names, departments, telephone numbers, addresses should be included on a distribution list.)

3. Prepared By: Enter name, telephone number and company of the engineer responsible for preparing the FMEA.

4. FMEA Date: Enter the date original FMEA was complied, and the latest revision date.

5. Process Step or Variable or Key Input: Enter simple description of the process or operation being analysed. Indicate as concisely as possible the purpose of the process or operation being analysed. Where the process involves numerous operations with different potential modes of failure, it may be desirable to list the operations as separate processes.

6. Potential Failure Mode: Potential failure mode is defined as the manner in which the process could potentially fail to meet the process requirements and/or design intent. It is a description of the non-conformance at that specific operation. It can be a cause associated with a potential failure mode in a subsequent (downstream) operation or an effect associated with a potential failure in a previous assumption should be made, in preparation of the FMEA, the assumption should be made that the incoming parts/materials are correct.

   List each potential failure mode for the particular operation in teams of a component, subsystem, system or process characteristic. The assumption is made that failure could occur, but may not necessarily occur.

7. Potential Failure Effect: Potential effects of failure are defined as the effects of the failure mode on the customer. The customer in this context could be the next operation.

8. Severity: Severity is an assessment of the seriousness of the effect of the potential failure mode to the customer. Severity applies to the effect only. If the customer affected by this failure mode, assessing the severity may lie outside the immediate team's field of experience or knowledge. Severity should be estimated on a "1" to "10" scale.

Table B.1: Suggested Evaluation Criteria

Effect	Criteria: Severity of Effect	Ranking
Hazardous-without warning	Very high severity ranking when a potential failure mode affects safe operation and/or involve non-compliance with government regulation. Failure will occur without warning.	10
Hazardous with warning	Very high severity ranking when a potential failure mode affects safe operation and/or involve non-compliance with government regulation. However failure will occur with warning.	9
Very High	Major disruption to the maintenance operation. 100% of work-outputs may be regarded as non-value adding activity. Item inoperable, loss of primary function. Customer very dissatisfies.	8
High	Minor disruption to the maintenance operation. Nearly 100% of the work-outputs are non-value adding activity. Item operable, but at a reduced level of performance. Customer dissatisfied.	7
Moderate	Minor disruption to the maintenance operation. Portions (less than 100%) of the work-outputs are non-value adding activity. Item operable, but some comfort/convenience items inoperable. Customer experience discomfort.	6
Low	Minor disruption to maintenance operation. Nearly 100% of the work-outputs may have to be re-worked. Item operable, but some comfort/convenience item operable at reduced level of performance. Customers experience some dissatisfaction.	5
Very Low	Minor disruption to maintenance operation. The work-output may have to be sorted and a portion (less than 100%) reworked. Defects noticed by most customers.	4
Minor	Minor disruption to maintenance operation. A portion (less then 75%) of the work-output may have to be reworked online but out-of-station. Defects noticed by average customers.	3
Very Minor	Minor disruption to maintenance operation. A portion (less than 50%) of the work-output may have to be reworked online but out-of-station. Defects noticed by discriminating customers.	2
None	No Effect.	1

Note: The team should agree on an evaluation criteria and ranking system, which is consistent, even if modified for individual process analysis.

9. Potential Cause: Potential cause of failure is defined as how the failure could occur, described in terms of something that can be corrected or can be controlled.

10. Occurrence: Occurrence is how frequently the specific failure cause/mechanism is projected to occur in the failure in the failure mode should be considered for this ranking. The failure detecting measures are not considered here.

Table B.2: Suggested Evaluation Criteria

Probability of Failure	Possible Failure Rates	Cpk	Ranking
Very High: Failure is almost inevitable	1 in 2	≤0.33	10
	1 in 3	≥0.33	9
High: Generally associated with processes similar to previous processes that have often failed.	1 in 8	≥0.51	8
	1 in 20	≥0.67	7
Moderate: Generally associated with processes similar to previous processes which have experienced occasional failures, but not in major proportions.	1 in 80	≥0.83	6
	1 in 400	≥01.00	5
	1 in 2,000	≥1.17	4
Low: Isolated failures associated with similar processes	1 in 15,000	≥1.33	3
Very Low: Isolated failure associated with almost identical processes	1 in 150,000	≥1.50	2
Remote: Failure is unlikely. No failure ever associated with almost identical processes.	≤1 in 1,500,000	≥1.67	1

11. Current Process Controls: Current process controls are descriptions of the controls that either prevent to extent possible the failure mode from occurring or detect the failure mode should it occur. These controls can be statistical process control (SPC) or can be post-process evaluation. The evaluation may occur at the subject operation or at subsequent operations. There are three types of process controls/features to consider:
    - prevent the cause/mechanism or failure mode/effect from occurring, or reducing their rate of occurrences;
    - detect the cause/mechanism and lead to corrective actions;
    - Detect the failure mode.

12. Detection: Detection is an assessment of the probability that the proposed current process controls will detect a potential cause/mechanism.

Table B.3: Suggested Evaluation Criteria:

Detection	Criteria	Ranking
Almost Impossible	No known controls available to detect failure mode	10
Very remote	Very remote likelihood current controls will detect failure mode	9
Remote	Remote likelihood current controls will detect failure mode	8
Very low	Very low likelihood current controls will detect failure mode	7
Low	Low likelihood current controls will detect failure mode	6
Moderate	Moderate likelihood current controls will detect failure mode	5
Moderately high	Moderately high likelihood current controls will detect failure mode	4
High	High likelihood current controls will detect failure mode	3
Very high	Very high likelihood current controls will detect failure mode	2
Almost certain	Currents controls almost certain to detect the failure mode. Reliable detection controls are known with similar processes.	1

13. Risk Priority Number: The risk priority number is the product of Severity (S), Occurrence (O) and Detection (D) ranking

$$RPN = S \times O \times D$$

This value should be used to rank order the concerns in the process. The RPN will be between 1 to 1,000. For higher RPN's the team must undertake efforts to reduce this calculated risk through corrective actions. In general practice, regardless of the resultant RPN, special attention should be given when severity is high.

14. Actions Recommended: When the failure modes have been rank ordered by RPN, corrective action should be first directed at the highest ranked concerns and critical items. The need for taking specific, positive corrective actions with quantifiable benefits, recommending actions to other activities and following up all recommendations cannot be overemphasised. Actions such as the following should be considered:

- To reduce the probability of occurrence. An action-oriented study of the process using statistical methods could be implemented with an ongoing feedback of information to appropriate operations for continuous improvement and defect prevention.
- To increase the probability of detection. Generally, improving detection controls is costly and ineffective for quality improvements. Increasing quality controls inspection frequency is not positive corrective action and should only be utilised as a temporary measure, permanent action is required.

To conduct the Process FMEA effectively, one must follow a systematic approach. The recommended approach is an eight-step method that facilitates the Process FMEA:

1. Select the team and brainstorm: Make sure the appropriate individuals are going to participate. The team must be cross functional and multidiscipline and the team members must be willing to contribute.

2. Process flowchart: For Process and Service FMEA, the process flowchart is applicable.

3. Prioritise: After the team understands the problems, the actual analysis begins in order to know where the team should begin and what part is important.

4. Data Collection: To collect the data of the failures and categorise them.

5. Analysis: Utilise data for a resolution. The analysis may be qualitative or quantitative. The method may be brainstorming, cause-effect analysis, mathematical modelling, etc.

6. Results: Use the information to quantify the severity, occurrence, detection and RPN.

7. Confirm/Evaluation/Measure: To confirm, evaluate and measure the success or failure. The information from this step will be used to recommend actions to see the results of actions.

8. Do it all over again: To improve all over again which is continual improvement.

Risk Analysis:

Risk analysis determines how often identified risks are likely to occur and the magnitude of their consequences. The significance of risk is expressed as a combination of its consequence or impact on the objectives of the organisation and the likelihood of those consequences occurring. Consequence and likelihood may be accounted for using a qualitative, semi-qualitative or quantitative approach. The qualitative approach is most common and is briefly described below. The likelihood criteria are expressed as a probability of the annual occurrence on a descriptive scale from Rare to Almost certain. Consequences are rated in terms of the potential impact on the key criteria, such as Performance, cost, schedule, identified during the context step. The impact is then also described on a scale from insignificant to catastrophic.

The Risk Management Standard, AS/NZS 4360:1999 details each analysis as follows:

Qualitative analysis uses descriptive scales to describe the magnitude of potential consequences and the likelihood that those consequences will occur. These scales can be adapted or adjusted to suit the circumstances, and different descriptions used for different risks. Quantitative analysis is used as an initial screening activity to identify risks which require more detailed analysis where the level of risk does not justify the time and effort required for a fuller analysis or where the numerical data are inadequate for a quantitative analysis.

Quantitative analysis uses numerical values (rather than the descriptive scales used in qualitative and semi-quantitative analysis) for both consequences and likelihood using data from a variety of sources. Consequences may be estimated by modelling the outcomes of an event or set of events, by extrapolation from experimental studies or past data. Consequences may be expressed in terms of monetary, technical or human criteria. In some cases more than one numerical value is required to specify consequences for different times, places, groups or situations.

Likelihood is expressed as a probability, a frequency, or a combination of exposure and probability. The way in which likelihood and consequence are expressed and the ways in which they are combined to provide a level of risk will vary according to the type of risk and the context in which the level of risk is to be used.

Risk Evaluation:

Risk evaluation is about deciding whether particular risks are acceptable or not to taking into account:

- The controls already in place;
- The cost consequences of managing risk or leaving them untreated;
- Benefits and opportunities presented by the risks;
- The risks borne by other stakeholders.

The outcome is a list of risks with agreed priorities ratings from which decisions can be made about acceptable levels of tolerance for particular risks and where greatest effort should be focused.

TREAT THE RISKS

The purpose of risk treatment is to determine what will be done, and who will be responsible for the risks that have been identified. Risk treatment converts the earlier analysis into actions to reduce risk.

Risk treatment options are evaluated in terms of feasibility, costs and benefits with the aim of choosing the most appropriate and practical way of reducing risk to a tolerable level. The option chosen should provide a Risk Action Plan to deal with risks before they arise and a Contingency Plan that provides for recovery if a risk eventuates. Risk Action Plans will manage different risks in different ways. They may seek to:

- Reduce the likelihood of occurrence;
- Minimise the consequences;
- Transfer/share risk;
- Retain risk.

A major part of the process for treating risks in an organisation will involve identifying the optimum level of risk transfer that is realistically achievable and obtains best VFM over the life of the organisation.

Once the range of unacceptable risks has been identified through foregoing steps, the various options for treating the remainder are considered. These include reducing the likelihood of the risk, or reducing its consequence or transferring it in fell or part. In engineering work, the opportunities for simple risk transference are limited. However the risk may often be avoided altogether by choosing a more prudent solution to the original problem (Keey, 2000).

MONITORING AND REVIEWS

Continuous monitoring and review of risks ensures that new risks are detected and managed, action plans are implemented and managers and stakeholders are kept informed. The availability of regular information on risks can assist in identifying trends, likely trouble spots or other changes that have arisen.

A risk register database is the main management tool for monitoring risk. It contains a ranked list of risks, references to associated Risk Action Plans and names of individuals responsible for each risk.

Risk Early Warning System:

Risk management needs to be actually embedded in the day to day operations of the business to be effective and sustainable. It needs to appeal to, and capture the attention of, operational line management by being unbureaucratic, focused on the areas of real risk to the business and help, rather than hinder, decision making.

Many organisations find effective embedding to be the trickiest part of risk management. Generic risk early warning system's objectives are (Deloitte, 2003):

- Be truly operational: driving risk aware behaviour and successful risk management into day to day operational activities;
- Enable pre-emptive action: minimising uncertainties and avoiding fire fighting;
- Bring the right information to the right time: using visually simple reporting, focused on problem areas, to get the heart of the matter quickly;
- Take bureaucratic out of the business facilitating sensible, quick decision making.

Hence risk early warning system can embed risk management which gives a linkage between risks and performance, driving risk management through specifically derived performance indicators, focused on the causes of key business risks. Risks are often monitored using traffic light reporting of these operational 'lead' indicators, focusing on measuring the cause and driver of key risks, rather than 'lag' indicator describing the symptoms or impact of those risks. This provides a framework for early warning of future problems so that timely management actions can be taken. Deloitte (2003) propose the procedures to establish the risk early warning system as follows:

1. Identify prioritise and analyse risks:
2. Map the cause of key risks and identify business improvements:
3. Determine 'lead' KPIs for the key driver of risk and measure performance improvement
4. Make risk early warning system an automatic operational activity

The benefits of embedding risk early warning system to the enterprise risk management system are Deloitte (2003):

1. Early Identification of Problems: a risk management process will add a great deal more value to the business if it is truly able to warn organisations about areas of underperformance, potential catastrophe and operational loss before they become a problem and give organisations the opportunity to pre-empt problems and address key concerns in advance. The risk early warning system uses 'lead' metric which are specially designed to do exactly this and avoid unexpected risks.

2. Reinforce Operational Management: managers can adopt the risk early warning system as their own performance reporting system. It is aligned with what they need to achieve.

3. Tool for change and improvement: The system involves the generation and monitoring of clear action plans to address areas of concern or underperformance before they become a problem. Additionally the mere of measuring the cause of risks drives behaviours to improve the management of them. What is measured really does get done.

COMMUNICATE THE RISKS

When the risk is established, the creditability of the chosen message-bearers is important, since all parties to the process bring their own biases. There are four conceptual approaches to risk communication (Pidgeon et al., 1992):

- The top-down transmission of expert opinion to a non-expert audience;
- An interactive exchange of information and opinion among individual, groups or organisations;
- An exchange of information within a wider cultural or institutional context;
- A political process of empowering risk bearing groups society.

Whether the view of risk communication, its effectiveness hinges on trust. Thrust is hard to gain, but easy to lose (Keey, 2000). If the source of communication is not trusted, perhaps because the present evidence contradicts past message, then it is unlikely that the new massage will be trusted.

Australian/New Zealand Risk Management Standard suggests the objectives of good communication are clarity, objectivity, timeliness, regularity. Although these objectives are sound in principle, but they are difficult to achieve in practice.

The basic rules of communication include:

- Write clearly and simple;
- Avoid hiding adverse information and be open;
- Take the initiative, especially when one has negative information;
- Avoid "killer words" such as perfectly safe, risk-free, which are never true;
- Quantify risks as far as possible;
- Acknowledge that there are no dumb question;
- Be frank when dealing with the media;
- Be aware of factors that inspire trust;
- Put data in context and choose risk comparison carefully;
- Remember that other will decide what is acceptable to them.

APPENDIX C

RISK ASSESSMENT TOOLS

RISK ASSESSMENT TOOLS

A decision maker must be able to identify and have an understanding of the range of possible outcomes and consequences related to any given option. Furthermore, the decision maker should be able to ensure strategies are in place to minimise or maximise the effect risks have on a future situation. There are eight different methods that can be used in a risk management system to identify the risk. These common methods are:

- Failure mode and effect analysis;
- Hazard and operability study;
- Fault tree analysis
- Event tree analysis;
- Monte Carlo simulation;
- Probabilistic risk analysis;
- OSH Method of hazard identification; and
- Short cut risk-analysis method

Failure Mode and Effect Analysis:

The method aims to identify the nature of failures, by dividing a system into smaller subsystem or components that consider the full range of failure modes and sub consequences. The failure mode and effect analysis (FMEA) utilises a qualitative analysis, with capabilities to quantify the likelihood and severity and to assess the impact of different failure modes on a system.

The FMEA is most applicable when only one risk impact is considered at a time. The analysis takes these identified risks though from its initial identification to its final mitigation, the FMEA's typical applications are:

- A macro assessment, which identifies a specific impact scenario and determines the course of actions to be taken.
- A micro assessment, which focuses on the creation of a single risk activity from the interaction between a system and its surrounding environment. This takes a possible risk and assesses its potential outcomes and mitigation strategies.
- Changes in a system's overall risk profile because of a subsystem and component's modification. Modifications are result in possible variations in the interaction of the system and its surrounding environment, which need to be reassessed.
- The addition of rating risk likelihood and severity give a quantitative approach to the prioritising the risks.

The FMEA analyses the impact of risk factors in sequence. The failure mode is defined followed by an analysis of each subcomponent to determine if they contribute to the failure and the consequences of this contribution.

The analysis does not assign monetary values to the outcomes, which limits the justification of the appropriate mitigation strategies even if a ranking system is incorporated. Large scale significant risks require deterministic justifications because possible ramifications can have large monetary and social consequences.

The FMEA is a simplilistic method that does not require extensive training in statistical analyses or large quantities of historical data. It is subjective and depends on the user's perceptions and understanding of the risks being evaluated.

In summary, the FMEA is best utilised for simple to medium complexity of risk management application. In these cases, the lower complexity of risk does not justify and in-depth analysis, which includes statistical validation and additional time to produce the requirement detail.

The level of detail required by the FMEA is determined by the capacity of the analysis, such as analysis application. It is important to understand that this simplitictics analysis can become paralysed by excessive detail and the Pareto Principle whereby minority of the causes creates the majority of the problems.

The FMEA is best utilised for applications where only one form of impact is being considered, for example, reduction in quality and production. It can be applied in the design of maintenance plans.

Hazard and Operability Study (HAZOP)

This analysis is undertaken when the design is effectively complete. The purpose of a Hazard and Operability Study (HAZOP) analysis is to determine the manner different circumstances and/or faults could create serious safety issues and/or affect operational outputs. The HAZOP analysis is a qualitative method, which can be used to ensure the risks of an effectively complete design have been taken into account before final implementation.

A HAZOP analysis aims to reduce the risk of initial complications in the implementation of a design by aiming to eliminate negative consequences initiated through a poorly planned implementation.

The purpose of a HAZOP analysis is to ensure the implementation phase of a design is (Elms, 1998):

- Commissioned trouble free with an efficient subsequent operation;
- Implemented without last minute expensive modifications; and
- Communicated to all stakeholders to ensure they are well briefed on the implementation sequence.

A HAZOP analysis is conducted once a design is effectively complete with the aim of eliminating the need of troubleshooting in the implementation of a project.

The focus of a HAZOP formulates a thought process that examines the possible likelihood and consequences of the design not meeting the desired requirements. It can be utilised in the engineering design of a new project and modifications to existing resources, i.e. machinery, equipment and structures.

A team must be assembled, and the findings from a HAZOP will depend on the knowledge and experience of that team. It is important to ensure a competent team is used and they are partially or completely independent from the design to ensure an objective analysis.

The application of a HAZOP analysis is best suited to evaluating the risk of original designs and future modifications thereafter of systems.

Fault Tree Analysis (FTA)

The contributing factors influencing undesirable outcomes are not always immediately clear and may have many possible causes that in turn have many possible root sources. The Fault Tree Analysis (FTA) graphically displays in a logical structure the assessment of events and scenarios, which can lead to undesirable outcomes. This qualitative method starts with a large undesirable outcome being defined and the situations, which can lead to the outcome eventuating.

The FTA is a top-down analysis, which starts with the definition of an undesirable outcome, which is traced back in a chronologically progression to the root causes.
The chronological progression is achieved by diagrammatically linking situations with their causes via AND and OR contributors. For a situation to occur it could have many causes, which could be independent or co-dependant with each other (Ridley and Channing, 1999).

AND describes the logical operations whereby the co-existence of all input contributory factors are required to produce an output.
OR describes the logical operation whereby if any one of the input contributing factors is present the output will occur. Each situation branches off from the ultimate undesirable outcome and is traced through the different situations, which support the failure until the root causes are identified. The flow chart below demonstrates the process of the FTA.

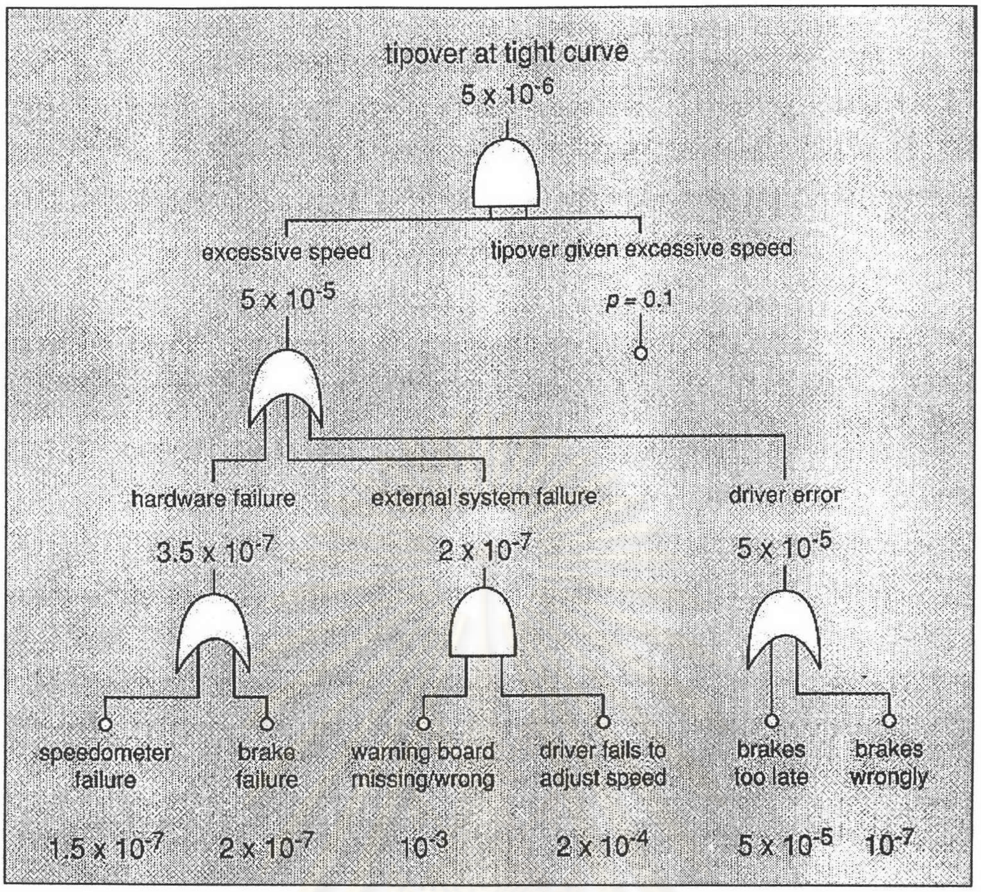

Figure C.1: Fault Tree Analysis
Source: Keey (2000)

The FTA is best utilised in the identification of underlying (root) causes of major problems (outcomes) and assists in the decision-making of mitigation strategies.

The FTA is best applied when the stakeholders are involved in developing the logic for identifying the root causes and essentially constructing the tree. This input creates greater credibility, especially in safety applications, because the people affected by the outcome are involved in the analysis. An outcome can have serious consequences, however the root causes can seem innocent in nature and initially not considered contributors to such a serious consequence. However, the FTA actively identifies these underlying causes and exposes them to ensure effective mitigation strategies are undertaken. The focus of identifying root causes leads the FTA being utilised in health and safety applications.

Event Tree Analysis (ETA)

The Event Tree Analysis (ETA) is a continuation on from the Fault Tree Analysis (FTA). The ETA utilises probabilities to estimate the likelihood of causes acting as catalysts for an unwanted outcome. The use of probabilities to assist in the quantification of possible root causes enables mitigation strategies to be prioritised in a deterministic manner.

The ETA has similar applications as the FTA but with the added feature of assigning probabilities to the possible contributing factors of the final outcome. The assignment of probabilities gives the added functionality of:

- Assigning priorities to the mitigation strategies of the identified root causes; and
- Estimating the severity of root causes and how they influence the final outcome.

The ETA is conducted in a similar manner as the FTA except with the addition of likelihood and consequences been assigned and estimating the outcome.

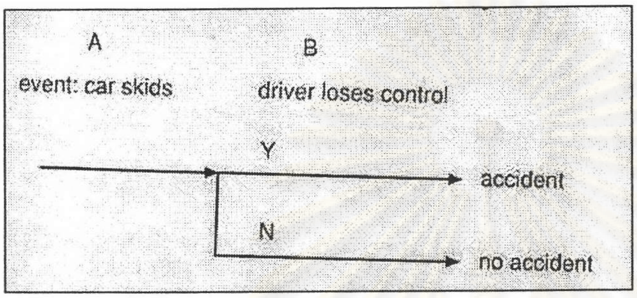

Figure C.2: Example of Event Tree Analysis
Source: Keey (2000)

Figure above shows a simplified event tree.

The ETA can be used in the same situations as FTA but has the added feature of probabilistic justification. Quantitative results give a priority structure to the mitigation of risk, and the level and complexity of safety features. The ETA can have an advantage over a FTA if the risks require prioritisation by the determination of the likelihood and the consequences of situation occurring.

Monte Carlo Simulation

A Monte Carlo simulation is a complex mathematical method that encompasses a range of techniques to describe the impact of risk and its consequences. The uncertainty or the unknown parameter within this risk analysis model is represented by a probability distribution. The range of values that the parameter may take and the probability depends on the size and shape of this distribution. With the aid of computer programmes this quantitative method has been simplified by the computer undertaking the tedious random sampling and iterations of the simulation. A Parameter is a numerical measure of a population. Because it is based on observations in the population, its value is almost never known.

The application of Monte Carlo simulation involves random sampling of each probability distribution within the model to produce a large number of scenarios. Each probability distribution is sampled in a manner that reproduces a distribution s shape that reflects the probability of the values that could occur. The characteristics of Monte Carlo simulation mean it can be applied in situations that require:

- The variables of the distribution model to be accurate;

- Correlation and inter-dependencies to be included in the model;
- Recognition of a justifiable method being used; and
- Ease and swiftness of modifying the analysis with the aid of a computer programme.

The steps of Monte Carlo Simulation are: (Molak, 1997) and (Vose, 2000):
1. Design the Structure of Risk. The analysis should provide the information that the decision-maker requires and be adaptable to different risk situations. The problem should be broken down into smaller parts to make the analysis more manageable, but it is important to take into account the Pareto effect.
2. Define distributions that describe the uncertainty of the problem. Probability distribution models can be placed into categories for modelling firstly, non-parametric and secondly, parametric. A Non-parametric distribution is more realistic and flexible because the parameters directly determine the range and shape of the distribution. A Parametric distribution is based on mathematical functions, which combined with one or more distribution parameters to determine the range and shape. There are a large number of distribution models, which can be used to describe the uncertainty of the problem and examples are; triangular, uniform, betaPERT, cumulative, discrete and general distributions.
3. Determine the input uncertainty of the model. The input data for the distribution model can come form various sources, which include: Historical statistics, Projections and extrapolations, Expert opinions and forecasts, The number of iterations conducted in the analysis can increase the level of precision. However, this is limited by the initial quantity and quality of input data, and the time taken to do the iterations. For operational risk the simulation involves running through thousands of iterations or hypothetical "years", with randomly generated inputs applied to the underlying risk distributions and the outcomes tabulated. The simulation is continued until the resulting empirical distributions and the targeted distribution become statistically stable enough to ensure the results are within the appropriate confidence level.
4. Presenting and interpreting the risk analysis results. The process data has be interpreted into usable information to assist in the management of risk. To aid the decision maker the processing of data should include its validity (i.e. the sources and limitations of the data) and the removal of the complex statistical noise.

The Monte Carlo technique tends to be computer intensive and requires a large amount of statistical data. Many problems and the generation of statistical data can be very time consuming even with the assistance of computers. For this reason, Monte Carlo simulation is avoided when other simpler analysis can be used effectively. Monte Carlo simulation, however, has the advantage that it will solve many problems for which no other solutions exist. Monte Carlo simulations are use in a broad variety of applications including NASA, the US nuclear weapons programme, important scientific endeavours throughout the world, and in finance where market risks are assessed. Because of the heavy reliance on computer programmes to undertake the iterations, specialised programmes have been developed specifically for Monte Carlo simulation.

A2.1. Probabilistic Risk Analysis (PRA)

The risks associated with complex engineering systems require appropriate calculations and analysis for determining frequencies of extremely rare events for which little or no data is available. Probabilistic Risk Analysis (PRA) is a quantitative method, which is hierarchical by nature because its structure accommodates large quantities of information that is utilised in the analysis. Many PRA s are based on fault trees to model the system, event trees to quantify the failure and Monte Carlo simulations to determine the likelihood of the failure.

PRA was developed to facilitate the quantification of risk associated with complex engineering systems that have significant consequences on the environment and society s well being. It is particularly appropriate for assessing extreme-event risk. The criterion for an extreme-event risk is it has low probability of occurrence with severe consequences.

PRA complements the engineering design of complex systems because it provides a holistic view. Examples of extreme-events are nuclear core meltdowns and large earthquakes, and examples of complex systems are large oil refineries, nuclear power plants and multi story buildings. Figure 6 is an example of high consequence and low likelihood event.

The steps of probabilistic risk assessment: (Molack, 1997)
1. Disturbance of complex systems: Identify project risk variables. These systems pose low risk when they are operating at steady state as designed.
2. Integrated model of system response: The design of complex systems is broken down into subsystems to make the risk analysis model more manageable. Beware of the weakest subsystem s boundary conditions can limit the overall risk exposure. The integration of risks is essential because subsystems can be dependant on one another and changes in one subsystem can result in boundary conditions changing in another.
3. Identify types and levels of severity: Using both qualitative and quantitative methods to establish a system s root causes and the likelihood and consequence of occurrence.
4. Assessment of current risk: Requires information on risk contributors and potential risk management strategies because without this information PRA will only provide: Accept status quo and continue operation; or Shut system down.

PRA is an in-depth analysis designed primarily for complex risks and systems. Therefore it is best utilised in similar situations as Monte Carlo simulations. A PRA requires a large amount of time and research to obtain data to use in the analysis therefore it is generally only used for complex risks and systems. PRA has the same limitations as Monte Carlo simulation because PRA uses Monte Carlo simulation in its analysis. It has had notable utilisation in the gas and oil exploration activities. Where seismic data, field size distributions, quantity and quality of the resource, and recovery per square kilometre are some of the critical risks that require assessment and PRA can be used to solve these complex unknowns. Other specific uses for PRA are:

- Nuclear reactor safety analysis.
- Battle strategy simulations.
- Large scale engineering projects such as, dams, motorways and structures.

OSH Method of Hazard Identification

Occupational Health and Safety (OSH), have set guidelines regarding the assessment of risks to provide a safe working environment in accordance with the Health and Safety in Employment Act 1992. The OSH Method of Hazard Identification sets a baseline for employers to establish their health and safety strategies and systems. This method relies on other assessment methods to evaluate risks. However, the OSH method focuses primarily on eliminating workplace deaths, injury, loss and damage.

The OSH Method of Hazard Identification is utilised to ensure conformance with the Health and Safety in Employment Act 1992 as stated in the Guide to the Health and Safety in Employment Act 1992.

- Employers and others are also expected to ensure that their actions at work do not result in harm to other people, including members of the public.
- Section 5 of the Act sets out the principal objective, it also lists three means contained in the Act to achieve it: The Act promotes excellence in health and safety management;
- It requires people in places of work to perform specific duties to ensure that people are not harmed as a result of work activities; and
- It provides for the making of regulations and approved codes of practice relating to specific hazards 6.

The OSH Method of Hazard Identification fundamental characteristics provide a basis application, which is a tool to conform to the Health and Safety in Employment Act 1992 specific sections 7-10. The characteristics are:

- Identifying all hazards and potential hazards
- The likelihood and consequence of a hazard occurrence
- Planning the introduction and continual monitoring of preventative measures of: Eliminate or Isolate and/or Minimise.

The fundamental components of the OSH assessment are:

- The identification of hazards in the work place;
- The evaluation of risks associated from these hazards;
- Evaluating and determining the control of the risks; and
- Implementing the control strategies.

The characteristics of the OSH method ensure it is utilised in the following situations:

- To meet responsibilities for identifying and controlling significant hazards as defined in the Health and Safety in Employment Act 1992.
- To consider the likelihood of harm actually occurring to anyone in particular circumstances, and the possible consequences which could result.

- To enable the planning, introduction and monitoring measures to ensure risks are adequately controlled at all times. Without effective assessment there can seldom be effective control.

Short Cut Risk-Analysis Method (SCRAM)

This method is devised as a short-cut method for estimating the significance of an identified risk. The Short Cut Risk Analysis Method (SCRAM) can be utilised in conjunction with other analysis to assist in the quantification of rating risk.

The SCRAM objective is to provide a quick analysis of the significance of a risk and can be done as part of an initial investigation or part of a detailed investigation at the end. The significance rating rates different risks on the same scale. This ranking of risk can be used to determine the appropriate level of mitigation strategies to be applied. The SCRAM can be applied:

- As a preliminary method for determining a decision whether a risk could be pursued or not; and
- As a tool to identify the significance of a risk and the required mitigation strategies.

The SCRAM method yields a risk rating which is an index of the risk potential. It provides a conceptual indicator identifying the significance of various risks on the same index scale. The results are only a quick way of determining the potential risk associated with an opportunity and interpretations should factor in the constraints of this method. The SCRAM should be used bearing in mind that the risk rating is a conceptual indicator and historical data would be required to determine the rating s justification.

The SCRAM could be best utilised in small to medium complex risks and in conjunction with other analysis methods to ensure a rigorous analysis is conducted if required. The SCRAM can be used as a preliminary analysis to determine priorities and if a more thorough analysis is required or finally to quantify the findings from a qualitative analysis.

BIOGRAPHY

The son of a civil engineer and housewife, Chonnanart Saikaew was born on 22 July 1979 in Uttaradit, Northern Thailand, but spent most of his childhood in Had-Yai and Bangkok as his father had to be relocated every four years. He is the eldest brother of Saikaew family together with the younger brother (born 1985).

Chonnanart was first educated at Payathai primary school and then in 1990 went to PhotisarnPittayakorn school completing junior high school (M3) qualification. Having been interested in engines and mechanics, he left school and studied the Vocational Qualification in Mechanical Engineering at King Mongkut's Institute of Technology North Bangkok and simultaneously studied the non-formal education programme, Ministry of Education, which he gained senior high school (M6) qualification in the following year.

At the age of 17, he attended the twinning engineering degree programme between Thammasat University and the University of Nottingham, majored in Mechanical Engineering. Having spent two-and-a-half years at Thammasat and another four years in Nottingham, he was eventually conferred the Bachelor's Degree in Mechanical Engineering in July 2002 and went on to become a postgraduate student at Chulalongkorn University.