

PRINCIPLES OF RISK MANAGEMENT

Introduction

The term "Risk" has been used in many different applications. It can be applied to safety and it can also be applied to business investment (business risk, project risk etc.). Risk normally refers to something that is "uncertain" and that uncertainty normally carries a loss or adverse effect. However, in the context of health and safety management, the meaning of "risk" mainly refers to *risk of having accident, risk of having harms*.

The term "risk management" in the context of safety is often used interchangeably with the term "safety management" by many people. Although they may mean the same thing to many people, there are in fact conceptual differences between the two. The major difference is that the terms "hazard" and "risk" are put into perspective in the "risk management" concept.

Risk Management should be integrated with other elements of the management system to form a **comprehensive health and safety management system**. In such a system, "Risk Management" can be regarded as the "**Process Safety Management**", since it is regarded as the part of the management system that deals with the actual control of risks in the processes or activities of an organization.

The risk management concept emphasizes on the systematic identification, analysis and assessment of all hazards inherent in an activity so that effective measures can be established to control the risks. Without an understanding of what needs to be control, it will be difficult for the management to take the right actions to combat with the health and safety problems.

Legal Requirements on Risk Assessment

There is no explicit requirement on adopting risk management in the local legislation. However, the "General Duties" Clauses in the Factories and Industrial Undertakings Ordinance do in fact imply such a system. The Hong Kong Government is in the process of reviewing the existing occupational health and safety system in Hong Kong and it is foreseeable that such a system will be more explicitly enforced.

In the UK, "Risk Assessment" has been explicitly required in the "Management of Health and Safety at Work Regulation" as well as the "Control of Substances Hazardous to Health Regulations (COSHH)". "Risk management" is also widely promulgated by the Occupational Safety and Health Administration (OSHA) of the US in its "Guidelines on Workplace Safety and Health Programme Management". It is evident that the principles of "Risk Management" will become the guiding principles in the legislation of most advanced industrialized countries.

Some Definitions

The principles of Risk Management can be better understood by defining the following terms within the context of Risk Management:

Safety Defined

The word "*safety*" in fact does not give too much meaning in safety management and sometimes it can be quite misleading. The dictionary defines "safety" as: "*the quality of being safe; freedom from danger or injury*". However, in reality, attaining the state that is qualified by this definition seems impracticable. There is no such thing as an absolute safe environment. It can be imagined that even if every known safety concept, standard, or regulation was applied in a given situation, there would still be the probability, however remote, of an injurious or damaging event occurring.

Therefore, the dictionary definition is not applicable and should not be used in the context of safety management. The word "safety" should be defined with such a meaning that reflects the reality. There are a number of such definitions by various academics and authorities. Some of these definitions are quoted on below :

- U.S. National Safety Council --

"Safety" is the control of hazards to attain an acceptable level of risk.

- Gloss and Wardle in *Introduction to Safety Engineering* --

"Safety" is the measure of the relative freedom from risks of dangers. Safety is the degree of freedom from risks and hazards in any environment.

- Willie Hammer in *Occupational Safety Management and Engineering* --

Safety is a matter of relative protection from exposure to hazards; the antonym to danger.

- Lowrance in *Of Acceptable Risk : Science and the Determination of Safety* --

Safety is a judgment of the acceptability of risk A thing is safe if its risks are judged to be acceptable.

From the definitions quoted above, it is apparent that the word "safety" should only be define as a "relative and acceptable state" for which the risks are judged to be acceptable. The terms "*risk*" and "*hazards*" are commonly used in the above quoted definition and they are in fact the key words in the context of risk management.

Hazards Defined

Hazards are defined as the "*potential for harm or damage to people, property, or the environment*" and are the "*source of risk*".

Hazards include the characteristics of things and the "actions" or "inactions" of people. They are the "base" of all safety concerns, whether it is occupational safety, product safety, environmental affairs, fire etc. In all of those fields of safety endeavor, virtually all activities are to deal with the possible actions or inactions of people and the characteristics of properties, equipment, machinery, or materials that present the potential for harm or damage.

Risk Defined

As mentioned above, risk means something uncertain and the uncertainty carries some adverse effects. In other words, risk is made up of *probability of occurrence* (uncertainty) and *severity of consequence* (adverse effects). Lowrance in *Of Acceptable Risk : Science and the Determination of Safety* defines **risk** as "**A measure of the probability and severity of adverse effects**". By this definition, when we talk about risk, we are actually talking about how likely will an adverse effect (harm) will be realized, and if it is realized, how serious (injuries, deaths etc.) will be the consequences. A classic example is the risk of an aeroplane crash. The probability of an aeroplane crash is extremely small (in terms of crash per total flying hours of all aeroplane). However, the consequence of the crash of an aeroplane will be catastrophic. The risk of traveling on aeroplanes can then be calculated by taking into account the two factors of probability and severity.

The Process of Risk Management

The risk management concept enables a systematic and realistic framework to be established for accident prevention. It refers to the whole process of:

- hazards identification,
- risk estimation,
- risks evaluation,
- control measures establishment, and
- implementation of control measures.

This risk management process can be further divided into two distinct stages. The first stage concerns with the understanding of the "problems" (fact finding) while the second stage concerns with the "solutions" to the problems. The first stage encompasses the processes of hazards identification, and risk assessment.

□ Hazard Identification

Hazards Identification is a very important and distinct step preceding all other steps (hazards analysis, risk determination etc.) in risk management. This is in fact a **fact finding** exercise. The objective is to reveal all possible potentials for harm or damage that exist in a system or organization being analyzed. If this step is not conducted properly, the whole risk management scheme would be affected.

Many analytical methods have been developed for use in hazards identification. The appropriate method or mix of methods should be selected to enable the process be conducted "systematically" to achieve a better coverage of hazards.

□ Risk Estimation

After hazards have been identified, they will need to be further analysed to define their nature, the mechanism of harms, the groups of people that are particular at risk and the consequence of the hazards being realized. This will provide information on the relative severity of the various hazards and the groups of people to whom protections have to be provided.

As previously defined, risk is "a measure of the probability and severity of adverse effects". Therefore, in the "risk estimation process", the consequences as well as the probability of occurrence of those hazards identified are assessed.

□ Risk Evaluation (acceptability evaluation)

Risk Evaluation is the making of an overall judgement on the importance of a risk, to determine its acceptability.

On the basis of **risk estimation**, an **evaluation** is then made as to whether the risk is acceptable or additional safety measures are necessary to reduce the risk to an acceptable level. Risk assessment is very much a subjective judgement. However, by following certain principles, the subjectivity in risk assessment can be minimized.

□ Establishment of Control Measures

Risks can normally be reduced through one or several safety measures. The reduction can apply to either the consequences or the probability that they will occur. The control measures may be by ways of "engineering control" or "administrative" controls. "Engineering Controls" refer to hardwares such as guards, barriers, and other installations. "Administrative Controls" refer to software issues such as safe working procedures, safety systems etc. Measures stipulated in the legislation, national standards, code of practice etc. can be very useful sources of reference for establishing control measures.

□ Implementation of Control Measures

Appropriate control measures are put to work at this stage. It may take a long while to implement the measures because considerable time may be needed for training, equipment purchases, installation work, and often the need for overcoming resistance to change.

The process of risk management as mentioned above is a continuous process which is never ending. Some hazards may have been overlooked and need further identification and new hazards may be introduced in the course of time and the whole process will have to be performed again. Furthermore, the residual risk of certain hazards may also need to be assessed to evaluate their acceptability after appropriate control measures have been implemented.

METHODOLOGY FOR ASSESSMENT OF RISK

Quantitative Risk Measurement

For quantitative measurement, risk is normally expressed by the equation:

$$\text{Risk} = \text{Probability of occurrence} \times \text{Consequence of occurrence}$$

where probability is expressed as the event frequency per unit of time or activity, and consequence is expressed as loss in dollar value.

The above equation gives a finite, numerical quantification of risk. In the analysis, calculated or estimated values of probabilities and consequences have to be obtained. On the basis of these values, an evaluation is then made as to whether the risk is acceptable or safety measures are necessary. The use of this equation presumes a knowledge of incident probability which is far more extensive and precise than seems to exist in reality. In reality, however, **subjective judgments** have to be used in many situations to determine the likelihood of the *occurrence* of a event as well as its *severity*. Therefore, **qualitative risk assessment** is used more often than not.

Qualitative Risk Estimation

However, there are also **systematic approaches** in estimating risk qualitatively by using appropriate decision making tools. One commonly used approach is the development of a "Risk Assessment Decision Matrix" which is adopted from the US Military Standard -- System Safety Program Requirements, known as MIL-Std-882-B. This type of "Matrix"

can be employed to measure and categorize risks on an informed judgment basis as to both probability and consequence and as to relative importance. An adaptation of the Matrix is illustrated on below:

Risk Matrix

| Severity of Consequence | Occurrence | | Probability | | |
|--|------------|----------|-------------|--------|------------|
| | Frequent | Probable | Occasional | Remote | Improbable |
| Catastrophic (Fatal) | | | | | |
| Critical (Major injury/ permanent disability) | | | | | |
| Marginal (Minor injury) | | | | | |
| Negligible (No injury) | | | | | |

Legend:

| | |
|--|-----------------------------------|
| | <i>1st rank action</i> |
| | <i>2nd rank action</i> |
| | <i>3rd rank action</i> |
| | <i>acceptable risk/ no action</i> |

By using this Matrix, risks can be roughly classified into different categories depending on the parameters on the two axes. The different categories of risks require different ranks of control action. Priority on control actions can be determined by adopting this kind of decision making tool.

SPECIFIC ANALYTICAL TECHNIQUES

Preliminary Hazards Analysis (PHA)

The PHA is also commonly used in System Safety Analysis. It is the initial effort in risk assessment during the system design phase of the system (project or operation) life cycle. Its purposes are to identify safety critical areas within the system, identify and roughly evaluate hazards, and begin to consider safety design criteria. PHA a very useful tool in analyzing the generic "hazard groups" present in a system, together with their evaluation and recommendation for control. It is a first and most important examination of the state of safety of the system. PHA is usually preceded by the use of a preliminary hazard list (PHL). The identification of hazards on a PHL can occur through the use of a variety of methods, such as checklists, hazard matrices, lessons learned, equipment descriptions, accident/incident report data, review of other historical records, and also with the aid of the ETBA.

In the PHA, a "risk assessment code" (RAC) is introduced. This RAC determines a risk level of a given hazard and is used to assess the scope of the system safety effort required. The RAC is generated based on the probability and consequence of occurrence of a hazard, which bases on the same principle of the "Risk Matrix" as described above.

Specific PHA and PHL worksheets are developed to facilitate the analysis. Column headings of these worksheets are shown on below. As can be evident from the format of the worksheets, the PHA is in fact an extension of the PHL.

Preliminary Hazard List

| Item | Hazardous Condition | Cause | Effects | RAC | Comments |
|------|---------------------|-------|---------|-----|----------|
| | | | | | |

Preliminary Hazard Analysis Worksheet

| Item | Hazardous Condition | Cause | Effects | RAC | Assessments | Recommendations |
|------|---------------------|-------|---------|-----|-------------|-----------------|
| | | | | | | |

Fault Tree Analysis

A fault tree is a graphical representation of *logical combinations* of causes that may lead to a defined undesired final (top) event or state. Examples of types of final events are an injury to a person, failure of equipment, the release of hazardous gases and an interruption to production.

A Fault Tree consists of a number of layers of events, the topmost layer is the final event mentioned in the previous paragraph. The occurrence of a event is caused by the input of a number of events at the next lower layer and so on. The events at the lower layer are controlled by "gates" which may be an "OR" gate or an "AND" gate. An "OR" gate denotes that the occurrence of any one of the events will lead to the occurrence of the next higher event. An "AND" gate denotes that the higher event will only occur when all the inputting events at the lower layer have occurred.

Fault tree analysis can provide a very useful overview on how faults can lead to serious consequences. The various causes / faults leading to the final undesirable event can then be examined individually. The logical sequence in the fault tree also provides a useful insight for management for focusing efforts on critical issues. *Appropriate control measures* aiming at particular faults can be generated more readily. *Probabilistic estimates* for the

occurrence of an undesirable event can be more accurately worked out by this logical presentation of the precedent causes / faults.

Event Tree Analysis

An event tree can be regarded as the opposite of a fault tree. A fault tree is constructed by selecting a undesirable top event and then working downwards. An event tree starts with an initiating event and then describes the sequential consequences. For example, what happen when a fire breaks out? The break out of a fire is the *initiating event*. Subsequent events may be it is detected by the nearby fire detector, the fire alarm goes off, the fire station is alerted and firemen arrive and extinguish the fire. There may be a sprinkler system in place and the subsequent events will be different.

Every part of the sequential events contains the possibility of success or failure. Failure can be due to the malfunctioning of the detector or smoke not reaching the detector. An event tree provides opportunities for making probabilistic estimates. The initiate event is expressed as a frequency (event per year) and the other branch-off points are expressed as probabilities (the number of failures per trial or occasion of use)

Job Safety Analysis (JSA)

In this method, attention is concentrated on particular job tasks performed by a person or group. It is most appropriate for tasks which are well defined. The analysis is a direct examination of a job task to identify hazards inherent with the job task.

A JSA process consists of four mains stages, namely: *Structuring, Identifying hazards, Assessing risks and Proposing safety measures.*

Structuring

The first stage of JSA is to break down the job being analyzed into a number of suitably detailed steps or sub-tasks. This requires basic understanding of the job. Normally, the persons who are experienced in the job should be involved. Besides the normal standard job procedure, it is also important to take account of unusual tasks and those that are only seldom undertaken.

Identifying hazards

The next stage is to go through the sub-tasks one by one. The particular hazards will become more apparent in a sub-task suitably broken down. A number of relevant questions may be asked to aid identifying hazards:

- Which types of injuries can occur? -- A checklist of injuries / hazards may be prepared for use.
- Are hazardous materials, equipment, machinery etc. involved?
- Can special problems or deviations arise in the course of the work?
- Is the job task difficult?
- Can other ways of doing the work arise?

Assessing the risks

Each identified hazard or problem is assessed with reference to the severity of consequence, the number of people exposed and the likelihood of occurrence etc.

Proposing safety measures

One of the major advantages of JSA is appropriate control measures can be generate quite readily. An attempt can be made in this stage to propose ways of reducing the risks when going through the hazards / risks shown on the *record sheet*. The measures can apply to:

- equipment and task aids.
- materials to be used.
- work routines and methods (employ alternative methods if practicable).
- elimination of the need for a certain job task.
- improvements to job instructions, training, etc.
- planning how to handle difficult situations.
- install safety devices such as guards, barriers, detectors etc.
- use of personal protective equipment.

A typical Record Sheet is show on below:

| Job task | Hazards | Evaluation | Proposed measures | Remarks |
|-----------------|----------------|-------------------|--------------------------|----------------|
| | | | | |

Energy Analysis

The idea that lies behind this method is that for an injury to occur, a person must be exposed to an injurious or harmful energy. An injury occurs when a person's body is exposed to an energy that exceeds the injury threshold of the body. In relation to this "energy concept", an accident is sometimes defined as "*an unwanted energy flow of energy resulting from inadequate barriers that results in adverse consequences.*"

Harmful energies can take on many different forms and they can damage a person physically or chemically. The various forms of energies are listed in the checklist below. In fact, most hazards are the result or effect of energy of one form or the other. Therefore, the acceptance and use of this energy concept provides a comprehensive framework which encompasses virtually all possible kinds of hazards. The "energy checklist" developed can actually be used as a "hazards checklist" for conducting hazards identification.

Check list for Energy Analysis:

POTENTIAL ENERGY

- Person at a height*
- Object at a height*
- Collapse of structure*
- etc.*

EXTREME TEMPERATURES

- *Hot or cold object / surface*
- *Steam or gas*
- *Chemical reaction*
- *etc.*

CHEMICAL INFLUENCE

- *Toxic*
- *Corrosive*
- *Contagious*
- *etc*

KINETIC ENERGY

- *Flying objects*
- *Vehicle impact*
- *Moving machine parts*
- *etc.*

FIRE AND EXPLOSION

- *Flammable substance*
- *Explosive substance*
- *Dust*
- *Chemical reaction*
- *Pressure*
- *etc.*

RADIATION

- *Ionizing*
- *Laser*
- *UV, IR*
- *Sound*
- *etc.*

STORED PRESSURE

- *Compressed gases*
- *Compressed liquids*
- *Materials under tension*
- *Steam boiler*
- *Coiled spring*
- *etc.*

ELECTRICAL

- *Voltage*
- *Current (also in association with heating)*
- *Battery*
- *Static electricity*
- *Capacitors*
- *Magnetic field*

ROTATIONAL MOVEMENT

- *Movement machine parts*
- *Rollers*
- *etc.*

MISCELLANEOUS

- *Slips*
- *Sharp edge*
- *etc.*

Energy Analysis is not merely a tool for identifying harmful energies or hazards. It also provides a very useful conceptual framework for deciding on appropriate safety measures, barriers as the term used, to prevent harm from being caused to persons by the energies. In fact, when using Energy Analysis, a model of systems containing the following components should be looked at:

1. That which can be harmed, usually a human being, but possibly an object, a piece of equipment or a plant.
2. Energies, which can cause harm.
3. Barriers, which prevent harm from being caused, such as safety guards for machinery.

Energy Trace and Barrier Analysis (ETBA)

ETBA may be regarded as an extension of Energy Analysis employing the same energy concept. However, ETBA is frequently used in association with "System Safety Analysis". The ETBA has been designed as an investigative tool with which to focus specifically upon the following primary areas of concern:

1. Energy sources(s) within a given system;
2. The adequacy of any barriers or controls within the energy path;
3. The human factors interface; and
4. The eventual target(s) of unwanted or uncontrolled energy flow.

Failure Mode and Effects Analysis (FMEA)

This method is utilized for analysis of technical systems. It can be used at different system levels. In simple terms, it is designed to answer the questions: "How can the unit fail?" and "What happens then?". There are variations in the application of the method and the complexity of the systems analyzed. However, the analysis normally consists of the following main stages:

1. The system is divided up into different units in the form of a block diagram.
2. Failure modes are identified for the various units.
3. Conceivable causes, consequences and the significance of failure are assessed for each failure mode.
4. An investigation is made into how the failure can be detected.
5. Recommendations for suitable control measures are made.

A special record sheet is normally used to facilitate the analysis. The major column headings of the record sheet is shown in the table below.

FMEA Record Sheet

| Identification -- <i>component designation, function, etc.</i> | Failure Mode | Failure Cause | Failure Effect | Failure Detection | Possible Action | Probability and/or Criticality level. |
|---|--------------|---------------|----------------|-------------------|-----------------|---------------------------------------|
| | | | | | | |

Management Oversight and Risks Tree (MORT)

MORT was originally developed for conducting in-depth accident investigation and is a method that focuses on the safety work of organizations. Its area of application has since been extended. MORT emphasizes that when an accident reveals errors, it is the system which fails. People operating a system cannot do the things expected of them because directives and criteria are "less than adequate" (LTA), which is the phrase used throughout the analysis.

The MORT tree us a general problem description. It is rather like a fault tree and the same symbols are used. The tree contains around 200 basic problems. But, if it is applied in different areas, the number of potential causes it describes can raise to 1500.

The top event of the "Tree" may be an accident that has occurred. This can be due to an "oversight or omission", or an "assumed" hazard, or both. These are the two main branches of the "Tree". The branch "Oversight and Omission" has two subsidiary branches, one is called "Specific control factors" and the other called "Management system factors". The "Specific control factors" focuses on what occurred during the accident. This is further divided into the "accident" itself and how its consequences are reduced, e.g. through fire fighting, provision of medical treatment, etc. The "Management system factors" focuses on the question "Why". It is further divided into three further elements: policy, implementation, and risk assessment systems. The various elements in the tree are numbered, These numbers refer to a list of specific questions for each element which is provided as a complement to the tree.

The analysis involves going through the elements in the tree and making an assessment of each. There are two assessment levels: "Satisfactory" and "Less Than Adequate (LTA)". The assessments are in part subjective, but by asking specific questions for each element, the degree subjectivity can be reduced. Colour coding is used during the assessment process. Green mean OK, red means LTA, and blue means no answer to the question has been obtained. Irrelevant questions are crossed out. The analysis is complete when all elements have been covered.

Hazard and Operability Studies (HAZOP)

HAZOP is normally used by the Chemicals processing industry. HAZOP is applied on hardware systems, i.e. chemical plant and set up in chemical industry. However, this method may also be used for smaller scale operations which may exist in HKUST.

The basic idea behind HAZOP is similar to that of Deviation Analysis. A systematic search is made for deviations in a system model that may have harmful (often hazardous) consequences.

Guide Words

Guide words are established for use in HAZOP for identifying deviations, these guide words are summarized in the table below:

| Guide Word | Meaning |
|-------------------|---|
| NO or NOT | No part of the intention is achieved. Nothing else happens. |
| MORE | Quantitative increase, e.g. in flow rate or temperature. |
| LESS | Quantitative decrease. |
| AS WELL AS | Qualitative increase. The intention is fully achieved, plus some additional activity takes place, e.g. the transfer of additional material. |
| PART OF | Qualitative decrease. Only a part of the intention is achieved. |
| REVERSE | Logical opposite of intention, e.g. reverse direction of flow. |
| OTHER THAN | Complete substitution. No part of the original intention is achieved. Something quite different happens. |

Procedure

The procedure of HAZOP also consists of several main stages, they are: Structuring, Specifying intention, Identifying deviations, Specifying causes, and Proposing safety measures.

Structuring

The installation being analyzed is normally divided into different sections. In the case of a continuous process, the division is into tanks, connecting pipes, etc. The analysis will be repeated for each section, one at a time.

Specifying intention

The intention of each part to be analyzed has to be defined. This specifies how it is thought that the part will function.

Identifying deviations

Using the guide words one at a time, the deviations from the specified intention are identified. The consequence of each of the deviation is also determined.

Specifying causes

The conceivable causes or reasons for each of the deviations are then determined.

Proposing safety measures

For deviations that may have serious consequences, an effort is made to find control measures. The persons responsible for the measures are also specified in the record sheet.

HAZOP Record Sheet

| Guide Word | Deviation | Possible Cause | Consequence | Proposed Measures |
|------------|-----------|----------------|-------------|-------------------|
| | | | | |

REFERENCES:

1. *Lars Harms-Ringdahl. Safety Analysis -- Principles and Practice in Occupational Safety.*
2. *Fred A. Manuele. On the Practice of Safety.*
3. *Institution of Occupational Safety & Health. Risk Assessment -- A Practical Guide.*
4. *Ted S. Ferry. Modern Accident Investigation and Analysis, second edition.*
5. *UK Health & Safety Commission. Approved Code of Practice -- Management of Health and Safety at Work Regulations 1992.*
6. *UK Health & Safety Commission. Approved Code of Practice -- Control of substances hazardous to health Regulations 1988.*
7. *UK Health & Safety Executive. Successful Health & Safety Management.*
8. *Jeffrey W. Vincoli, Basic Guide to System Safety*
9. *Harold E. Roland, System Safety Engineering and Management - 2nd Edition.*