Risk Analysis and Management: An Introduction

Article · January 2008

DOI: 10.1007/978-1-84800-131-2_41

1 author:

Krishna B. Misra
RAMS Consultants
130 PUBLICATIONS **2,890** CITATIONS

SEE PROFILE

41

Risk Analysis and Management: An Introduction

Krishna B. Misra

RAMS Consultants, Jaipur, India

Abstract: Risk is the possibility of a hazardous event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of consequence (or impact) and likelihood of the event. Qualitatively, risk is considered proportional to the expected losses which can be caused by an event and to the probability of this event. Quantatively, it is the product of probability of hazardous event and the consequences. General views about risk perception and risk communication are discussed that help decision making. Risk management anf Risk governance along with probabilistic risk assessment and alternative approaches to risk analysis are also discussed.

41.1 Introduction

From the time of emergence of *Homo-Sapiens* on this planet, man with his intellect, inventive nature, ingenuity, and skills has always been trying to improve his living conditions and create favourable conditions for his survival. In this process, man created man-made systems for his own benefit and comfort. The history of industrial development indicates that as man tried to use technology to improve his standard of living, but in doing so, several new problems not anticipated earlier cropped up. Technology became means to provide objects and conditions for sustenance and contentment and technology can be viewed as the changing environment of humanity. Ingenuity and innovation were required to overcome several practical problems associated with new inventions and technological improvisations. In fact right from the dawn of industrial revolution, safety and dependability have been very much on the mind of man and through innovative designs man has been resolving these safety and reliability problems very ably.

41.1.1 Preliminary Definitions

All technological advancements have *hazards* associated with them. A *hazard* is an implied threat or danger of possible harm. It is a potential condition to become a loss. A *stimulus* is required to cause the hazard to transfer from the potential state to a loss (or accident). This stimulus could be a component failure, a condition of system, an operator failure, a maintenance failure or a combination of other events and conditions. Thus a *stimulus* can be defined as a set of events or conditions that transforms a hazard from its potential state to one that causes harm to the system, property or personnel. An *accident* is usually considered as the loss of a system or part of a system, injury to or fatality of operators or

personnel in proximity and damage of property of equipment or hardware. Technically speaking, an accident can be defined as a dynamic mechanism that begins with the activation of a hazard and flows through the system as series of events in a logical sequence to produce a loss. Still simply put, an accident is an undesired and unplanned event. Now coming to the definition of *risk* in simple terms, it can be called as expected value of loss. Risk is associated with likelihood or possibility of harm. It will not be out of place to mention about safety here and to underline the difference with risk, which some people often misunderstand. Safety in simple terms is the condition of being free from undergoing or causing hurt, injury or loss. safety can be thought of as a characteristics of a system like, quality, reliability or maintainability. Safety can be defined as an attribute of a system that allows it to function under predetermined conditions with an acceptable minimum accidental loss or risk. *System safety* is a planned disciplined systematically organized and before the fact process characterized by *identify-analyze-control* strategy. In fact the emphasis is placed on an acceptable level of safety designed into the system before it is produced or put to operation. *Hazard analysis* is at the core of system safety approach. Anticipating and controlling hazards at the design stage of an activity is the corner stone of system safety analysis. Incidentally system safety is not *failure analysis* since *hazard* has wider connotation than a *failure*. Hazard involves risk of loss or harm. A failure on the other hand is an unintended state of operation a failure can occur without a loss. On the other hand severe accidents have occurred a unit was operating as intended, *i.e.,* without a failure.

41.1.2 Technological Progress and Risk

All technological developments in the history of mankind had had risks associated with them. Therefore one has to look into the benefits accruing from these developments and the risks that go with the use of such technological innovations. In fact man has to learn to live with them and accept the risks as part of life. But before we come to the subject of acceptability of risk, let us have glance at the technological developments chronologically.

Steam Age Accidents: During the steam age in 1866, there were 74 steam boiler explosions in England resulting in 77 deaths. This was reduced to 17 explosions with 8 deaths in 1900 as a result of inspections performed by Manchester Steam Users Association. Better designs such as tube-fired boilers, and boiler inspections reduced it further to about once every 100, 000 vessel-years.

Rail Accidents: The history of railroad travel is also very old and it is full of accidents of which the causes can be traced either to natural calamities or to technical faults in the locomotives or signaling system or human error. Derailing has been a major cause of accidents. The worst accident was in Sri Lanka in 2004 due to Tsunami where some 1700 persons died followed by one in Bihar, India in 1981. Over 800 persons died due to derailment and plunging of coaches in a river. Sometimes head on collision have been reported. Japanese train crash in 2005 is said to have occurred killing 106 and injuring over 555 passengers due to driver's over speeding to keep train schedule. This was Japan's most serious accident after 1963 Yokohama train accident when two passenger trains collided with a derailed freight train killing 162 passengers. Intercity Express high speed train in Germany near Hanover on June 3, 1998 met an accident due to breaking of rim of axle followed by chain of events leading to crash in which more than 101 were dead and several others injured. The train was travelling at a speed of 200 kmph.

Marine Accidents: Ships being the oldest mode of transport and trade, it had its own risk associated with them. Later on submarines were also added to it. Collision and grounding happened to be major causes of accidents through out the long maritime history. The luxury liner, Titanic was considered unsinkable till it sank on its maiden journey. Besides there have been many cases of engine failures and other technical faults and fires onboard. The main difficulty is facility of repairs while on high seas. Oil tankers had oil spills leading to ecological hazards and threat to marine life.

Road Accidents: with the development of personal vehicles or cars for transport towards the end of

nineteenth Century, the vehicles also became sources of risk. The first human fatality associated with a motor vehicle was a pedestrian killed in 1899. Now, in 1990, about 5 million people died worldwide as a result of injury. It is estimated that by the year 2020, 8.4 million people will die every year from injury, and injuries from road traffic accidents will be the third most common cause of disability worldwide and the second most common cause in the developing world. Also, it is worth noting that the statistics show a ten to one ratio of in-vehicle accident deaths between the least safe and most safe models of car.

Aviation Accidents: Man entered the aviation age around the beginning of the twentieth Century. In the beginning the safety criteria of aircrafts was in terms of mean permissible failure rate but by 1940s the safety criteria began to be expressed in terms of the accident rate and a figure of 1 per 10^5 hours of flying was acceptable. During 1960s it was reduced to 1 in 10^6 landings of the aircraft and finally with automatic landing system it got reduced to 1 in 10^7 and travelling by air became safer and popular.

With the air traffic increasing enormously and the airplane security having been advanced considerably, the accident data analysed between 1970 and 2004 shows that the accidents have decreased from over 300 in the 70's to approximately 250 in the 80's and 90's. The maximum number of accidents was found in the year 1970, with a total of 38 planes. Since the late 90's the number of plane crashes stabilized to approximately 22 per year.

The Tenerife Disaster remains the worst accident in aviation history. In this disaster, which took place on March 27, 1977, 583 people died when a KLM Boeing 747 attempted take-off without clearance and collided with a taxiing Pan Am 747 at Los Rodeos Airport. Pilot error, communications problems, fog, and airfield congestion (due to a bomb threat at another airport) all contributed to this catastrophe. Also, the crash of Japan Airlines Flight 123 in 1985 is the worst single-aircraft disaster. In this crash 520 died on board a Boeing 747. The aircraft suffered an explosive decompression, which destroyed its vertical stabilizer and severed hydraulic lines, making the 747 virtually uncontrollable.

Nuclear Age Accidents: Then came the nuclear age around middle of 1950s and man has attempted rather, successfully, to anticipate the hazards before they would occur and learn to avoid them through designs, control and regulation. But even after taking all these steps, accidents have been taking place in the nuclear plants and the two serious nuclear accidents TMI-2 and Chernobyl-IV had energy planners reconsider the desirability of nuclear option in the energy sector. On Oct. 7, 1957, Windscale Pile No. 1, north of Liverpool, England, a fire in a graphite-cooled reactor spewed radiation over the countryside, contaminating a 200-square-mile area. On March 28, 1979, At Three Mile Island near Harrisburg, Pa, USA, one of two reactors lost its coolant, which caused overheating and partial meltdown of its uranium core. Some radioactive water and gases were released. This was the worst accident in U.S. nuclear-reactor history.

Chernobyl accident was the worst in the history of nuclear power plants, and as a result of this accident some 203 people were hospitalized with severe thermal burns and severe radiation exposure while 31 people died (which is rather a very small number). Some 1,35,000 people in a radius of 30 kms around the reactor were relocated. About one-fifth population of Byelorussia had been subjected to radioactive exposure of various intensities and the Republic lost over 1.6 million hectares or 20% of its farm lands and one million hectares of its forests were affected by the nuclear radiation.

An uncontrolled chain reaction in a uranium-processing nuclear fuel plant in Japan on September 30 1999 spewed high levels of radioactive gas into the air, killing two workers and seriously injuring one other. More recently, on July 17, 2007, radiation leaks, burst pipes, and fires at a major nuclear power plant at Kashiwazaki, Japan, occurred following a 6.8 magnitude earthquake near Niigata. Japanese officials, frustrated at the plant operators' delay in reporting the damage, closed the plant a week later until its safety could be confirmed. Investigations revealed that the plant had been sitting right on the top of an active seismic fault.

Space Age Accidents: The dawn of space age in later half of 1960s brought another technological

feat to the credit of man's achievements and along came with it the host of disasters. In June, 1971 during Soyus 11, all three Soviet cosmonauts were found dead in the craft after its automatic landing. The cause of death was reported to be due to loss of pressurization in the space craft during reentry into Earth's atmosphere. Again on March 18, 1980 a Russian Vostok rocket exploded on its launch pad while being refueled, killing 50 at the Plesetsk Space Center. On January 28, 1986, *Challenger* Space Shuttle exploded 73 seconds after liftoff, killing all 7 American crew members. A booster leak ignited the fuel, causing the explosion. On February 1, 2003, *Columbia* Space Shuttle broke up on reentering Earth's atmosphere on its way to Kennedy Space Center, killing all 7 crew members. Foam insulation fell from the shuttle during launch, damaging the left wing. On reentry, hot gases entered the wing, leading to the disintegration of the shuttle.

Chemical Plants Accidents: Accidents in chemical plants have had a very long history and they have been becoming quite alarming in intensity. Awards totaling $717.5 million were granted to next-of-kin and injured (29 were killed and 56 were injured) following an explosion at a Pyrotechnic plant in 1971, in which, according to the legal testimony, the plant operator had previously classified the ingredients and products as *"Flammable"* instead of "*Explosives*". A chemical company was fined $13.2 million for illegally dumping toxic chemical into a city waste-treatment system. The city itself was fined $10000 previously for permitting discharge of the pollution into the river. The contamination extended down river into a bay and has resulted in a major disruption of both commercial and sport fishing through 1980. According to an estimate, the entire 65 mile stretch of the river that was required to be dredged would require several years and up to $ 200 millions in cost.

In 1974, an explosion took place in Nypro UK Chemical plant at Flixbourough in which twenty-eight people were killed and some 36 million pounds were paid towards the fire and accident damage following this explosion. Bhopal Gas tragedy and its disastrous consequences raise doubts over man's victory over the nature to satisfy his materialistic needs. This tragedy, which struck on the night of December 2-3, 1984 due to leakage of methyl isocyanate gas on the unsuspecting sleeping population near the plant, left over 3700 people dead and about 150,000 affected. The compensation paid to the victims, decided mutually between the Union Carbide Company and the Government of India through a out-of-court settlement, was $470 millions.

Water-reactive chemicals also deserve special mention, since their release almost always results in water contact with the material. In the Somerville, Massachusetts a tank car ruptured on April 3, 1980, leaking phosphorous tri-chloride from the car into a nearby ditch. One observer reported that the responding fire company deliberately applied water to hasten the hydrolysis, and hence increased the acidity and opacity of the cloud. In this event, 23,000 persons were reported evacuated, 120 persons reported to the area hospitals for treatment and the damage alone from the acid gas corrosion was estimated at least half a million dollars.

A liquefied petroleum gas leaking from a pipeline alongside the Trans-Siberian railway in Ural Mountains near Uta , 72 miles east of Moscow, exploded on June 3, 1989 and destroyed 2 passing passenger trains, killing 575 and injuring 723 of an estimated 1,200 passengers on both trains.

Sometimes a deliberate act on the part of a negligent manufacturer can cause havoc to the environment and surrounding habitat of man which may threaten the life support system of earth. A major electric manufacturer was fined $ 4 millions, in addition to an agreement to conduct a research program on environmental effects of PCB, in order to assist in partial clean up of the upper Hudson river, because of its contamination over many years of the PCB used in electric capacitors and transformers. The present level of control is such that the plant now discharges less than one g/day into the river (according to Plant Management). The cost of freeing the 35.7 miles stretch of the river above Troy, New York was estimated at $150 millions as several towns and communities draw their water supply from this river.

Fire Accidents: On May 26, 1954, an explosion and fire on aircraft carrier *Bennington* killed 103 persons on board off Quonset Point, R.I., U.S.A. Again, on July 29, 1967, a fire on U.S. carrier *Forrestal* killed 134 persons on board off North Vietnam. A power-plant fire in Caracas, Venezuela left 128 dead on Dec. 18-21, 1982. A fire on May 10, 1993 in a doll factory near Bangkok, Thailand killed at least 187 people and injured 500 others. It was the World's deadliest factory fire.

Coal Mines Accidents: On January 21, 1960, a coal mine explosion killed 437 in Coalbrook, South Africa. On Nov. 9, 1963 an explosion in coal mine at Omuta, Japan killed 447. A fire in coal mines on May 28, 1965 in Bihar, India killed 375 persons. Another disaster caused by an explosion followed by flooding in coal mine at Dhanbad, India killed 372 persons on December 27, 1975. In China too, a gas explosion at a coal mine on June 20, 2002 killed 111 people. The mining industry is one of the most unsafe industries in China; it is estimated that more than 5,000 mining-related deaths occurred in 2001. Again a gas explosion killed 209 miners at the Sujiawan mine in Liaoning province China on Feb. 14, 2005. It was the single deadliest reported mine disaster in China since 1949. A methane explosion in a coal mine on March 2007 in Ulyanovskaya, Russia killed 110 people, making it the worst mine disaster in recent Russian history.

All these events from the past are just a part of the scenario which is full of hazards of all kinds and only indicate that the technological systems will continue to be used but the least we can do is to improve the performance of plants, systems and products and design them to be safe enough and ensure that they have a very low acceptable risk and the ecological and economic consequences of the possible accidents are minimal.

41.1.3 Risk Perception

Risk acceptability is always a subjective matter and depends upon the perception of the decision maker about the characteristics and severity of a risk. If the decision maker is forced to trade off well-being with monetary benefits, it would be easier to establish a criterion to accept a risk by making sure that the present worth of benefits is greater than the present worth of risk. But to many this approach is not acceptable as it places a value on human life and well being. Several theories have been proposed to explain why different people make different estimates of the dangerousness of risks. Another way of looking at the acceptability of risk to compare the risk under consideration with the previously judged risks those were acceptable. The comparison is by a risk spectrum curve, which shows the relationship between frequency and loss level. Logarithmic scales are generally used on both the axes. Farmer's curve [1] is one such method of judging the risks. Risk spectra that exhibits higher frequency at higher level of loss are less acceptable than otherwise. However higher frequency at low loss levels will not be considered as critical. However generalization based on this approach may not be appropriate.

Two major families of theory have been developed by social scientists: the Psychometric Paradigm and Cultural Theory. The study of risk perception arose out of the observation that experts and lay men often disagreed about how risky various technologies and natural hazards were. For example, most experts concluded that nuclear power is relatively safe, but a substantial portion of the general public sees it as highly dangerous. The obvious explanation seemed to be that the experts, having considered the evidence carefully and objectively, have a more accurate picture of the risks than did general public. Many experts continue to believe this theory. However, social science research on risk perception has been largely challenging it and proposing alternate explanations.

Chauncey Starr in an important paper [2], as early as 1969 offered an explanation to what risks are considered acceptable by the society. He assumed that society had reached equilibrium in its judgment of risks, so whatever risk levels, actually existed in society, were acceptable. His major finding was that people accept risks 1,000 times greater if they are voluntary (*e.g.*, driving a car) than if they are involuntary (*e.g.*, having a nuclear plant in the neighbourhood). In fact there are more people dying of road accidents than due to nuclear accidents [4] but general public is often averse to nuclear power.

41.1.4 Risk Communication

Risk communication is the interactive exchange of information and opinions throughout the risk analysis process concerning risk, risk-related factors and risk perceptions, among risk assessors, risk managers, consumers, industry, the academic community and other interested parties, including the explanation of risk assessment findings and the basis of risk management decisions. Risk communication is a tool for creating the understanding that:

- every choice-making / decision-making requires understanding of their related risks and benefits,
- closing the gap between lay people and experts,
- and helping people make more informed and healthier choices.

Simple steps that can ensure the success of risk communication consist of:

- Understanding the underlying cognitive processes, the values and concerns brought by various sections of the society, and likely responses of these sections to risk issues;
- Developing strategies to enhance trust and minimize conflict between these section on risk issues; and
- Developing organizational policies and messages responsive to the risk concerns of these sections.

41.2 Quantitative Risk Assessment

No industrial activity [5,10,11,15,22,34,54,58,60, 61,68,70,71,76] is entirely free from risk since it is not possible to eliminate every eventuality by safety measures. However, when risks are high, system designers must consider the possibilities of additional preventive or protective and risk reduction measures that can be achieved, and judge whether it would be reasonable to implement these additional measures. Therefore, it becomes imperative to assess the risk of industrial activity/plant quantitatively and ensure their safety before they are undertaken for construction or commissioning.

In fact, quantitative risk analysis [52,76,77]consists of seeking answers to the following questions:

- What possibly can go wrong that could lead to a hazardous outcome?
- How likely is this event?
- If that happens, what consequences can be expected?

To answer the first question, scenarios of events leading to the outcome should be defined and to answer the second question, the likelihood of these scenarios must be evaluated. Lastly to answer the third question the consequences of each scenario should be evaluated. Therefore, quantitatively, the risk is defined by the following triplet:

$$R = <S_i, P_i(\text{or } Fi), C_i> \quad i=1, 2,..., n \tag{41.1}$$

where S_i, P, *(or Fi)*, C_i are the i^{th} scenario of events, leading to hazard exposure, likelihood (or frequency) of scenario i and the consequences of scenario i(a measure of the degree of damage or loss), respectively. The likelihood of event E_i is expressed in terms of probability of that event and the frequency is expressed per year or per event basis in units of time. Lastly, C_i is expressed in terms of damage to property, number of fatalities, dollars loss *etc.*

The results of risk estimation are used to interpret various contributors to risk which can be compared and ranked. The process consists of :

1. Calculating and displaying graphically the risk profile on logarithmic scale.
2. Calculating the total expected risk from,

$$R = \sum_i P_i \; C_i \tag{41.2}$$

There are two ways of interpreting results: one way is to calculate expected values using (41.2) and is useful when the consequences are in financial terms. Another way is construct risk profile In this case risk values are plotted against consequences values. Sometimes the logarithm of probability that the total consequence C exceeds C_i is plotted against the logarithm of C_i. This is also known as *Farmer's Curve* [1] and was a landmark in Reactor Safety Study [4].

Quantitative risk assessment usually involves [8,15,16,20,26,68,69,72,73,74,75,76] three stages. These are: *risk identification* (the recognition that a

hazard with definable characteristic exists); *risk estimation* (the scientific determination of the nature and level of the risks); *risk evaluation* (judgment about the acceptability, or otherwise, of risk probabilities and the resulting consequences).

Risk identification and estimation are both concerned with collecting information on:

- The nature and extent of the source.
- The chain of events, pathways and processes that connect the cause to the effects.
- The relationship between the characteristics of the impact (dose) and the types of effects (response)

Through risk identification, we recognize that a hazard exists and try to define its characteristics such as chemical, thermal, mechanical, electrical ionizing or non-ionizing radiation, biological *etc*. Each of the identified hazards is examined to determine all physical barriers that contain it or can intervene to prevent or minimize the exposure to the hazard. Identification of each of the barriers is followed by a concise definition of the requirements for maintaining each of them.

Identification of Sources or Risk:

The first step in a system risk analysis is the identification of the sources of risk to the system. In being able to identify sources of risk it is essential for the analyst to be familiar with the system under consideration. Typically, a study or review team should be established. The team will comprise mainly managers, engineering staff, operators and other personnel who are involved in the operation of the system or who contribute to its performance. The range of knowledge and experience of the study team is a major factor in its effectiveness and hence in the competence of the study. However, it should be recognized that it may not be possible for the team to identify all possible failure scenarios or hazards particularly where these arise from 'unforeseen' events or processes.

The following techniques have been used in the identification of sources of risk:

1. Preliminary Hazard Analysis (PHA) [3];
2. Failure Modes and Effect Analysis (FMEA)[26,56,57];
3. Failure Mode, Effect and Criticality Analysis (FMECA)[22];
4. Hazard and Operability studies (HAZOP)[3] ; and
5. Incident Databanks.

These techniques have been used for a large range of engineering systems, with the possible exception of HAZOP which tends to be specific to the chemical and process industries. In addition, various other methods have been proposed, although these are often adoptions of the above methods to suit a specific system or problem. It will be seen that the methods to be described tend to be complementary; for example, guide lists, checklists or reference to incident databanks are often used to check that no source of risk has been omitted from the analysis. A Preliminary Hazard Analysis (PHA) is used to identify the major hazards for a system, their causes and the severity of the consequences. Typically it is used at the preliminary design stage. The identification in a PHA of major hazards usually will invoke more detailed analyses using methods such as FMEA, FMECA and HAZOP because of its preliminary status, it would not be expected that a PHA will identify failure of specific individual equipment which has the potential to lead to a major hazard. This is the role for FMEA, FMECA and HAZOP. FMEA is an inductive analysis because it starts at the possible outcomes and works backwards to obtain all possible causes. Hence it is essential that the identification of failure modes be as extensive as possible. This may be difficult, particularly for large systems. For this reason, generic guidelines or checklists are often used to ensure that all failure modes are considered. The analysis involved in a FMEA generally is presented in a tabulated format in a manner similar to that used for a PHA. A Failure Mode, Effect and Criticality Analysis (FMECA), or simply Criticality Analysis, is a logical extension of FMEA in which failure events are categorized according to the seriousness of their possible effect. In the FMECA both the failure frequency (probability) and the failure effect (consequence) are assessed subjectively to determine the criticality of each failure mode. This should take account of each component and each sub-system. The failure frequency is rated in terms of a subjective likelihood such as expressed by 'very low, low, medium and high'. The severity is

assessed into one of a number of subjective severity levels. The HAZOP (Hazard and Operability Studies) technique was developed by Lawley [3] in, 1974 at ICI and is used widely in the chemical and in the process industries to identify hazards or operating problems in new or existing plants. The HAZOP technique is a systematic process in which process flow diagrams are used to consider each plant item (*e.g.*, pipes, valves, computer software) in turn so that problems which could occur with these items may be considered.
Results from a HAZOP usually are summarized in tabular worksheet form. The tables normally contain the following entries:

1. *Item:* individual components in the system *(e.g.* pipes, vessels, relief valves)
2. *Deviation:* identify what can go wrong *(e.g.* more pressure, no transfer, less flow)
3. *Causes:* causes of each deviation (*e.g.* equipment failure, operator error)
4. *Consequences:* identify effects on other components, operability and hazards associated with each deviation (*e.g.* line fracture, backflow, leakage, fire, explosion, toxic release, personnel injury).
5. *Actions:* measures or actions required to further reduce the deviations or the severity of the consequences *(e.g.,* process design changes, equipment changes or modifications).

Risk Estimation:

The next step in the risk assessment is to define those scenarios in which the barriers may be breached and then make the best possible estimate of the probability or frequency for each exposure. Often, risks are measured for some time before their adverse consequences are recognized. These include the magnitude, spatial scale, duration and intensity of adverse consequences and their associated probabilities as well as a description of the cause and effect links. Both risk estimation and identification [26] can involve modeling, monitoring, screening and diagnosis.

Accident data, 'near misses', reliability data and other statistics that describe the part performance of systems also may be used to help identify potential major hazards in a system, and their causes and their consequences. The techniques described above assist in the identification of those individual system elements (components and sub-systems) that are potentially hazardous. This information may be used in the development of a representation of the overall system in terms of logic diagrams. These identify the sequences or combinations of events or processes necessary for system failure to occur. As noted earlier, such system representation for system failure to occur. As noted earlier, such system representation diagrams are an aid in the understanding of the behavior of the system and hence may suggest, without formal risk analysis, obvious measures for reducing the risk of system failure. Of course, detailed understanding of the system and its representation in a logical fashion is required for quantitative analysis of the system. Such analysis also requires quantification of system element performance. The quantification of the overall system reliability has been discussed in more detail in chapter 19 in this handbook.

The essential (and most common) techniques used for schematic representation of a system (*i.e.* its 'modeling') are:

(1) Fault trees [13, 17,20,21, 23,27,31,32,36,42, 59, 63,79] and
(2) Event trees [7, 18, 26, 33, 45 ,51, 76] .

A decision tree is a special case of event tree. Other methods, such as fault graphs [30], cause – consequence diagrams [58] and reliability block diagrams [59] incorporate significant features of event tree and fault tree techniques and will not be discussed. Fault trees and event trees have much in common. Whether one or the other or some combination is applied depends much on the preferences and practices within a given industry.

Fault trees and event trees have been applied extensively for qualitative and quantitative risk studies in the nuclear industry and the chemical process industries and to a lesser extent elsewhere. Automated fault tree generation [12, 13, 14, 36] had also received attention of researchers but today experts system can be developed to carry out FMEA, FTA and reliability and safety analysis as was discussed in chapter 19 of this handbook. Diagraphs and causal trees [64] have also been used in system safety and risk analysis. Two landmark risk analysis applications of fault trees

and event trees were the US nuclear safety study (RSS, 1975) [4]. It is the main method recommended for US nuclear risk studies [7, 46], in part because of its ability to model very complex accident sequences, including those involving dependency between events. Considerable amount of work has been done in the area of human reliability analysis [18,19,35,39,40,43,47,55,66,73, 76]. Also, the work in the aerospace industry for human reliability analysis has made use of event tree methods, extensively. Event trees and fault trees are best developed by a study team (*i.e.*, a panel of specialists), and their discussions may be likened to a 'brain-storming' session where specific risks, events and scenarios and their control are suggested. It is at this stage that decisions can be made as to which risks are to be included and omitted from a risk analysis. In other words, the scope of the risk analysis can be defined.

We have included a detailed and exclusive coverage of fault trees in chapter 38 of this handbook.

It is sometimes assumed, for ease of analysis, that any dependence between the outcomes of events may be ignored. This assumption usually is incorrect. System risk estimates calculated on the basis of assumed complete dependence between events may be considerably greater than estimates determined for the same events being assumed to be completely independent. Dependence between event failures (also known as cascade failures) can occur when more than one component in a system fails simultaneously due to a common cause. In this case the components do not fail independently of each other. For example, an external cause (such as environmental load --wind, earthquake – or man-imposed factors) may affect more than one component in the system. In general, dependent failures can have a dramatic effect on the risk associated with a project and must be properly identified and accounted for. It follows that the treatment of dependency between events is an important matter for risk analysis. There has been considerable amount of research in handling common cause failures in risk and safety analyses [6,9,14,28,29,37,38,44,65,67,76,78].

The estimation of system risk requires the quantitative description of both the frequency and the performance of those system elements directly influencing system risk. This means that the performance of components, items of equipment, loads, resistances, and human actions must be known and the consequences of failure able to be estimated. The quantitative description of the performance of each system element usually will be as a variable; either a point estimate (*i.e.*, deterministic) variable (*e.g.*, mean failure rate) or a random variable (*e.g.*. probability distribution of failure rates).

In order to cover common cause failures and human aspects of risk assessment problem, we have included chapter 39 exclusively on common cause failure modeling and chapter 40 on human-system interaction for the benefit of the readers.

Risk Evaluation:

The range of effects produced by exposure to the hazard may encompass harm to the people, damage to equipment and contamination of land and facilities. Therefore in the third component of *risk assessment*, risk evaluation in which judgment is made about the significance and acceptability of risk probabilities and corresponding consequences. This stage leads to a policy formulation. Evaluation techniques seek to compare risks against benefits, as well as providing ways in which the social acceptability of risks can be judged.

After the risk has been identified, estimated and evaluated (or any combination of the three) there comes a point where some kind of intervention (or deliberate decision not to intervene or to delay action) must be made. What is the course of development that is `safe enough'? A safe or less risky course of development would be one, which would be compatible with the environment - and can be called as *eco-development*. It would not only minimize or reduce risks to acceptable levels for those who are subjected to risk, but also for those who create risks and those responsible for managing them. There is always a cost attached to the risk and the benefits flowing from a project, plant or a system. Therefore one has to work out

the *risk/benefit* ratio. In considering risk/benefit trade-offs, it is essential to remember that for every benefit we usually incur some risk or cost, however small it may be.

Through safe design and better performance of these systems, we can minimize the ecological impacts and associated losses. Lastly, we have work out the advantages accruing from these systems vis-à-vis the risk involved in using them. In other words, we must address the issue of acceptable risk *vis-à-vis* employing the technologies.

41.3 Probabilistic Risk Assessment

Definition of Objectives: As the first step, the objectives of probabilistic risk assessment (PRA) or probabilistic safety assessment (PSA) are set and defined. The resources required for each analytical options are evaluated and the most effective alternative is selected.

Physical Layout of the System: The physical layout of the system or process including facility, plant and design , administrative controls, maintenance and test procedures as well as protective systems (those which maintain safety) is necessary to start the PRA. This will help generate all possible scenarios. All major safety and emergency systems must be identified and taken into consideration.

Identification of Initiating Events: Here we identify all those sets of events that could result in hazard exposure. The first step is to identify sources of hazards and barriers around these hazards. The next step is of course to identify events that can lead to a direct threat to the integrity of barriers.

Sequence of Scenario Development: In this step all possible scenarios that encompass all the potential paths that can lead to loss of containment of the hazard following the occurrence of an initiating event. The scenarios are often displayed by event trees.

System Analysis: The procedure followed in this step is to develop a fault tree for each event tree heading. Model dependencies and common cause failures models. All potential causes of failures such as hardware, software, test and maintenance and human errors are included in the fault tree. External events are also considered.

Data Analysis: Determine generic values of failure rates and failures on demand probabilities for each component in the fault tree. .Determine test , repair and maintenance from generic sources or from experience. Determine the frequency of initiating events and other component from experience or generic sources. Determine the common cause failures probabilities likewise.

Quantification: Fault trees and event trees sequences are quantified to determine the frequencies of scenarios and associated uncertainties in the computation.

To provide an insight of PRA to a reader, chapter 43 on probabilistic risk assessment including a case study is included in this handbook. Also another chapter 71 on PRA as applied to nuclear power plants is included in this handbook to provide detailed in formation to a reader. In fact, PRA in case of nuclear plants has three levels. Level I PRA simply calculates core melt probability and is purely a system failure event. Level II considers probability of failure of containment and the level III considers the probability of release of radio activity to the surroundings and its consequences.

41.3.1 Possibilistic Approach to Risk Assessment

Since we have seen there is always a gap between perceived risk and statistical risk. This is basically, due to the fact that statistical risk is based on probability theory of random ocurrences of events wheras the human thinking works on the basis of possibility. Attempts have been made to capture the subjectivity in human thinking by objectively formulating the risk assessment problem on the platform of fuzzy set theory which appears to make this possible. Several contributions [25, 48,49,50, 53,60,62] have been made in the direction of possibilitistic approach using fuzzy set theory. But at this moment, the researchers are transforming the problem by taking recourse to probability and possiblity compatibility principle as has been

suggested in [25, 48 and 50]. Better approach would be to assess the system performance in possibilitic framework directly (as is suggested in [49]) and thus bringing modeling close to the way human brain processes the situation.

Dempster Shafer theory also provides an alternative approach to probabilistic approach. For the benefit of readers, we have included chapter 31 on these aspects of the problem in this handbook. In fact, in the opinion of the author, fuzzy set theory provides a natural and very appropriate approach to overcome the problem of statistical risk and uncertainties associated with it and to resolve the problem of perceived and statistical risk. Human thinking is close to Possibilistic approach and does not believe in statistical values even if supported by tight confidence limits.

41.4 Risk Management

Risk management is an activity which integrates recognition of risk, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources. The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. Some traditional risk managements are focused on risks stemming from physical or legal causes (*e.g.*, natural disasters or fires, accidents, death and lawsuits). Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments.

The objective of *risk management* is to reduce different risks related to a pre-selected domain to the level accepted by society. It may refer to numerous types of threats caused by environment, technology, humans, organizations and politics. On the other hand it involves all means available. In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process can be very difficult, and balancing between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Intangible risk management identifies a new type of risk - a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, when deficient knowledge is applied to a situation, a knowledge risk materializes. Relationship risk appears when ineffective collaboration occurs. Process-engagement risk may be an issue when ineffective operational procedures are applied. These risks directly reduce the productivity of knowledge workers, decrease cost effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Risk management also faces difficulties allocating resources. This is the idea of opportunity cost. Resources spent on risk management could have been spent on more profitable activities. Again, ideal risk management minimizes spending while maximizing the reduction of the negative effects of risks.

Steps in the risk management process:

- Identification of risk in a selected domain of interest
- Planning the remainder of the process.
- Mapping out the following: the social scope of risk management, the identity and objectives of stakeholders, and the basis upon which risks will be evaluated, constraints.
- Defining a framework for the activity and an agenda for identification.
- Developing an analysis of risks involved in the process.
- Mitigation of risks using available technological, human and organizational resources.

The chapter 44 has been included in the handbook to discuss the subject of risk management in detail.

41.5 Risk Governance

It is true that individual capacities and responsibilities of different players,*viz.*,

government departments, scientific community, NGOs, business community or society at large in the arena of risk are limited and it is absolutely desirable to have some kind of coordination and understanding between their goals, perceptions and activities, particularly to cope up with disasters that require coordinated efforts of all sections cutting across the boundaries of the countries, sectors, hierarchical levels, disciplines.

The risk governance is a concept that only includes 'risk management' or 'risk analysis', it also looks at how risk-related decision-making can be affected to meet the major challenges facing society today, particularly those related to natural disasters, food safety or critical infrastructures. The risk governance also takes in view such as historical and legal backgrounds, guiding principles, value systems and perceptions as well as organisational imperatives.

To put in place the framework and coordinate risk governance efforts, an independent organization, named *International Risk Governance Council* (IRGC) was founded in June 2003 at the initiative of the Swiss government. The charter of IRGC is to help an understanding and management of global emerging risks that impact on human health and safety, the environment, the economy and society at large besides developing the concepts of risk governance, anticipating major risk issues and providing risk governance policy recommendations for key decision makers.

IRGC undertakes project work in four main areas:

- Risks associated with the mitigation of or adaptation to the effects of climate change
- The security of energy supplies
- Disaster risk governance
- Risks associated with new technologies

IRGC is a foundation funded by several governments and industries. The organizational structure comprises a Board, a Scientific and Technical Council, an Advisory Committee and a full-time Secretariat based at the foundation's Headquarters being located in Geneva, Switzerland.

Looking to the importance of the subject, this handbook has included chapter 45 on risk governance.

References

[1] Farmer FR. Reactor safety and siting: A proposed risk criterion. Nuclear Safety 1967; 8: 539.

[2] Starr Chauncey. Social benefits versus technological risk. Science 1969; 165 :1232-1238.

[3] Lawley HG. Operability studies and hazard analysis. In, Howe J (editor) Chemical Engineering Progress. American Institute of Chemical Engineers 1974; 70(4): 45-56.

[4] WASH-1400 (NUREG-75/014). Reactor Safety Study: An assessment of accident risks in commercial nuclear power plants, Nuclear Regulatory Commission, U.S.A. Oct. 1975.

[5] Brown DB. Systems analysis and design for safety. Prentice-Hall, Englewood, N.J.,1976.

[6] Apostolakis GE. The effect of certain class of potential common-cause failures on the reliability of redundant systems. Nucl. Engg. Design. 1976; 36: 123-133.

[7] Levine S, Vesely WE. Important event-tree and fault-tree considerations in the reactor safety studies. IEEE Trans. on Rel. 1976; Aug., R-25 (3): 132-139.

[8] Fussell JB, Lambert HE. Quantitative evaluation of nuclear system reliability and safety characteristics. IEEE Trans. on Rel. 1976; Aug., R-25 (3): 178-183.

[9] Vesely WE. Estimating common-cause failure probabilities in reliability and risk analyses: Marshall-olkin specializations. In Fussel JB, Burdick GR, editors. Nuclear systems reliability engineering and risk assessment. SIAM, Philadelphia, PA, 1977; 314-341.

[10] Rowe WD. An anatomy of risk, John Wiley & Sons, New York, 1977.

[11] Lewis EG. Nuclear power reactor safety. John Wiley, New York, 1977.

[12] Misra KB, Thakur R. Development of fault tree for reliability studies of a data processing system. Int. J. of System Sciences 1977; 8(7): 771-780.

[13] Willie RR. Computer aided fault tree analysis. Operation Research Center, ORC, University of California, Berkeley 1978; Aug., 78-14.

[14] Apostolakis G, Garribba S, Volta G. Synthesis and analysis methods for safety and reliability studies, Plenum Press, New York, 1980.

[15] McCormick NJ. Reliability and risk assessment, Academic Press, New York, 1981.

[16] Kaplan S, Garrick J. On the quantitative definition of risk. Risk Analysis 1981; 1(1).

[17] Vesely WE, Goldberg FF, Roberts NH, Haasl DF. Fault tree handbook. NUREG-0492, US NRC, 1981.

[18] Rasmussen J. Human reliability in risk analysis. In Green AE, (Ed.) High risk safety technology. John Wiley & Sons, London 1982; 143-170.
[19] Adams JA. Issues in human reliability. Human Factors 1982; 24: 1-10.
[20] Taylor TR. Algorithm for fault tree construction. IEEE Trans. on Rel. 1982; June, R-31 (2): 137-146.
[21] Joller JM. Constructing fault-trees by stepwise refinement. IEEE Trans. on Rel. 1982; Oct., R-31 (4): 333-338.
[22] Fawcett HH, Wood WS. Safety and accident prevention in chemical operations, John Wiley & Sons, New York, 1982.
[23] Cummings DL, Lapp SA, Powers GJ. Fault tree synthesis from a directed graph model for a power distribution network. IEEE Trans. on Rel. 1983; June, R-32 (2): 140-149.
[24] Dunglinson C, Lambert H. Interval reliability for initiating and enabling events. IEEE Trans. on Rel. 1983; June, R-32 (2): 140-163.
[25] Tanaka H, Fan LT, Lai FS, Toguchi K. Fault-tree analysis by fuzzy probability. IEEE Trans. on Rel. 1983; Dec., R-32 (5): 453-457.
[26] Roland HE, Moriarty B. System safety engineering and management. John Wiley & Sons, New York, 1983.
[27] Modarres M, Dezfuli H. A truncation methodology for evaluating large fault trees. IEEE Trans. on Rel. 1984; Oct., R-33 (4): 320-322.
[28] Evans MGK, Parry GW, Wreathall J. On the treatment of common-cause failure in system analysis. Int. J. of Rel. Engg. 1984; 9(2):107-115.
[29] Walle RA. A brief survey and comparison of common-cause failure analysis NUREG/CR-4314, Los Alamos National Laboratory, Los Alamos, NM, 1985.
[30] Alesso HP, Prassinos P, Smith CF. Beyond fault trees to fault graphs. Int. J. of Rel. Engg. 1985; 12 (2): 79-92.
[31] Lee WE, Grosh DL, Tillman FA, Lie CH. Fault tree analysis, methods and applications- a review. IEEE Trans. on Rel. 1985; Aug., R-34 (3): 194-203.
[32] Wilson JM. Modularizing and minimizing fault trees. IEEE Trans. on Rel. 1985; Oct., R-34(4): 320-322.
[33] Lakner AA, Anderson RT. Reliability engineering for nuclear and other high technology systems: A practical guide. Elsevier Applied Science Publishers, N.Y. 1985.
[34] Westman, WE. Ecology, impact assessment, and environmental planning, John Wiley & Sons, New York, 1985.
[35] Dhillon BS. Human reliability with human factors. Pergamon Press, New York, 1986.
[36] Kumamoto H, Henley EJ. Automated fault tree synthesis by disturbance analysis. Ind. Eng. Chem. Fundamentals. 1986, 24(2): 2333-239.
[37] Heising CD, Luciani DM. Application of a computerized methodology for performing common cause failure analysis: The Mocus-Bacfir Beta Factor (MOBB) code. Reliability Engineering 1987; 17(3):193-210.
[38] Hoghes RP. A new approach to common cause failure. Int. J. of Rel. Engg.1987; 17(3): 211-236.
[39] Sharit J. A critical review of approaches to human reliability analysis. International Journal of Industrial Ergonomics 1988; 2:111-130.
[40] Inagaki T, Ikebe Y. A mathematical analysis of human-machine interface configurations for a safety monitoring systems. IEEE Trans. on Rel. 1988; April, R-37(1): 35-40.
[41] Onisawa T, Nishiwaki Y. Fuzzy human reliability analysis on the chernobyl accident. Fuzzy Sets and Systems 1988; 28:115-127.
[42] Kohda T, Henley EJ. On diagraphs, fault trees and cut sets. Rel. Engg. & System Safety 1988, 20 (1): 35-61.
[43] Apostolakis GE, Bier VM, Mosleh A. A crique of recent models for human error rate assessment. Rel. Engg. and System Safety 1988; 22: 201-217.
[44] Hokstad P. A shock model for common-cause failure. Rel. Engg & System Safety 1988; 23(2):127-145.
[45] Fullwood, RR, and Hall RE. Probabilistic risk assessment in the nuclear industry: Fundamentals and applications, Pergamon Press, Oxford, 1988.
[46] International Nuclear Safety Advisory Group: Basic Safety Principles for Nuclear Power Plants, Safety Series, No. 75-INSAG-3, IAEA, 1988.
[47] Dougherty Jr. EM, Fragola JR. Human reliability analysis: a systems engineering approach with nuclear power plant applications. John Wiley & Sons , New York, 1988.
[48] Onisawa T. An application of fuzzy concepts to modeling of reliability analysis. Fuzzy sets and Systems 1990; 37:389-393.
[49] Misra KB, Weber GG. A new method for fuzzy fault tree analysis. Microelectronics and Reliability 1989; 29(2):195-216.
[50] Misra KB and Weber GG. Use of fuzzy set theory for level-1 studies in probabilistic risk assessment. Fuzzy Sets and Systems 1990; 37: 139-160.
[51] Kenaranuie R. Event-tree analysis by fuzzy probability. IEEE Trans. on Rel. 1991; April, R-40 (1): 120-124.
[52] Inagaki T. Interdependence between safety-control policy and multiple sensor schemes via Dempster-

Shafer theory. IEEE Trans. on Rel. 1991; June, R-40 (2): 182-188.
[53] Guth MAS. A probabilistic foundation for vagueness and imprecision in fault tree analysis. IEEE Trans. on Rel. 1991; Dec., R-40 (5): 563-571.
[54] Greenberg, HR , Cramer JJ (Eds.), Risk assessment and risk management for the chemical process industry, Van Nostrand Reinhold, New York, 1991.
[55] Sharit J, Malon DM. Incorporating the effect of time estimation into human-reliability analysis for high-risk situation. IEEE Trans. on Rel. 1991; June, R-40(2): 247-254.
[56] Zaitri CK, Keller AZ, Fleming PV. A smart FMEA (Failure Modes and Effects Analysis) package. Proc. Annual Rel. and Maint. Symp., Las Vegas, USA 1992; 414-421.
[57] Russomanno DJ, Bonnell RD, Bowles JB. Computer-aided FMEA forward an artificial intelligence approach. Fifth International Symposium on Artificial Intelligence, AAAI press, 1992; 103-112.
[58] Henley EJ, Kumamoto H. Probabilistic risk assessment-reliability engineering, design and analysis. IEEE Press, New York, 1992.
[59] Misra, K.B., Reliability analysis and prediction: A methodology oriented treatment, Elsevier Science Publishers, Amsterdam, 1992.
[60] Misra K.B. (Ed.), New trends in system reliability evaluation, Elsevier Science Publishers, Amsterdam, 1993.
[61] Modarres M. Reliability and risk: What an engineer should know about. Marcel & Dekker Inc, New York. 1993.
[62] Soman KP, Misra KB. Fuzzy fault tree analysis using resolution identity. Int. J. of Fuzzy Sets and Mathematics 1993; 1:193-212.
[63] Kumamoto Hiromitsu. Fault tree analysis. In Misra KB, editor. New trends in system reliability evaluation. Elsevier, 1993; 249-310.
[64] Kohda Takehisa, Inoue Koichi. Diagraphs and causal trees. In Misra KB, editor. New trends in system reliability evaluation. Elsevier, 1993; 313-336.
[65] Hokstad Per. Common cause and dependent failure modeling. In Misra KB, editor. New trends in system reliability evaluation. Elsevier, 1993; 411-441.
[66] Sharit Joseph. Human reliability modeling. In Misra KB, editor. New trends in system reliability evaluation. Elsevier, 1993; 369- 408.
[67] Dhillon BS, Anude OC. Common-cause failures in engineering systems: A review. Int. J. of Rel., Qua. & Safety 1994; 1(1): 103-129.
[68] Misra, K.B. (Ed.). Clean production: environmental and economic perspectives, Springer Verlag, Berlin, 1996.
[69] Stewart MG, Melchers RE. Probabilistic risk assessment of engineering systems, Chapman & Hall, New York, 1997.
[70] Modarres M, Kaminskiy M, Krivtsov V. Reliability engineering and risk analysis: A practical guide. Marcel Dekker, New York, 1999.
[71] Cagno E, Giulio ADi, Trucco P. Risk and causes of risk assessment for an effective industrial safety management. Int. J. of Rel., Qua. & Safety 2000; 7(2): 113-128.
[72] Hayakawa Yu, Paul S. F. Yip. A Gibbs-sampler approach to estimate the number of faults in a system using capture-recapture sampling. IEEE Trans. on Rel. 2000; Dec., 49(4):342-350.
[73] Pasquini Alberto, Pistolesi Giuliano, Rizzo Antonio. Reliability analysis of systems based on software and human resources. IEEE Trans. on Rel. 2001; Dec., 50(4): 337-345.
[74] Jin Tongdan, Coit David W. Variance of system-reliability estimates with arbitrarily repeated components. IEEE Trans. on Rel. 2001; Dec., 50(4): 409-413.
[75] Wang J, Yang JB. A subjective safety and cost based decision model for assessing safety requirements specifications. Int. J. of Rel., Qua. & Safety 2001; 8(1): 35-57.
[76] Modarres M. Risk analysis in engineering: Techniques, tools and trends. Taylor & Francis, New York, 2006.
[77] Latino RJ, Latino KC. Root cause analysis: Improving performance for bottom-line results. Taylor & Francis, New York, 2006.
[78] Lixuan Lu, Lewis G. Reliability evaluation of standby safety systems due to independent and common cause failures. IEEE International Conference on Automation Science and Engineering CASE '06 2006; 8-10 Oct.: 264 – 269.
[79] Limnios Nikolaos. Fault trees. ISTE Ltd. U.K.2007.