CONTENTS:

4. Ethics in engineering: 4.1 Purpose and concepts of engineering ethics, 4.2 Engineering as social experimentation, 4.3 Types of enquiry, 4.4 Issues in engineering ethics,.

5. Engineer's responsibility and Safety: 5.1 Safety, Risk, Underestimating the Risk, Over-estimating the Risk, Risk-Benefit analysis, 5.2 Cause of an accident and identification of the preventive measures to be taken 5.3 Case studies.

Purpose and concepts: Concepts:

Engineering Ethics is the study of moral issues and decisions confronting individuals and organizations engaged in engineering.

The Study of related questions about moral ideals, character, policies and relationship of people and corporations involved in technological activity.

Engineering ethics is defined by the codes and standards of conduct endorsed by engineering (professional) societies with respect to the particular set of beliefs, attitudes and habits displayed by the individual or group.

Engineering ethics is the discovery of the set of justified moral principles of obligation, rights and ideals that ought to be endorsed by the engineers and apply them to concrete situations. Engineering is the largest profession and the decisions and actions of engineers affect all of us in almost all areas of our lives, namely public safety, health, and welfare.

Approach

There are conventionally two approaches in the study of ethics:

1. Micro-ethics which deals with decisions and problems of individuals, professionals, and companies.
2. Macro-ethics which deals with the societal problems on a regional/national level. For example, global issues, collective responsibilities of groups such as professional societies and consumer groups.

There are two different senses (meanings) of engineering ethics, namely the Normative and the Descriptive senses. The normative sense includes:

(*a*) Knowing moral values, finding accurate solutions to moral problems and justifying moral judgments in engineering practices,

Study of decisions, policies, and values that are morally desirable in the engineering (*b*) practice and research, and

(*c*) Using codes of ethics and standards and applying them in their transactions by engineers. The descriptive sense refers to what specific individual or group of engineers believe and act, without justifying their beliefs or actions.

Purpose/Scope:

The scopes of engineering ethics are twofold:

1. Ethics of the workplace which involves the co-workers and employees in an organization.
2. Ethics related to the product or work which involves the transportation, warehousing, and use, besides the safety of the end product and the environment outside the factory.

Engineering Ethics is the activity and discipline aimed at 2

(*a*) understanding the moral values that ought to guide engineering profession or practice,

Resolving moral issues in engineering, and justifying the moral judgments in

(*b*) engineering.

(*c*) It deals with set of moral problems and issues connected with engineering.

ENGINEERING AS SOCIAL EXPERIMENTATION

Engineering is experimentation:

Experimentation plays an important role in the design process. Preliminary tests are conducted from the time when it is decided to make a product in the following order.

1. Engineering concept
2. Rough design
3. Detailed design
4. Production stage tests
5. Finished product
6. Feedback

Beyond the specific tests and experiments, however, each engineering project may be viewed as an experiment.

Before manufacturing a product or providing a project, we make several assumptions and trials, design and redesign and test several times till the product is observed to be functioning satisfactorily. We try different materials and experiments. From the test data obtained we make detailed design and retests. Thus, design as well as engineering is iterative process as illustrated in Fig. 3.1.

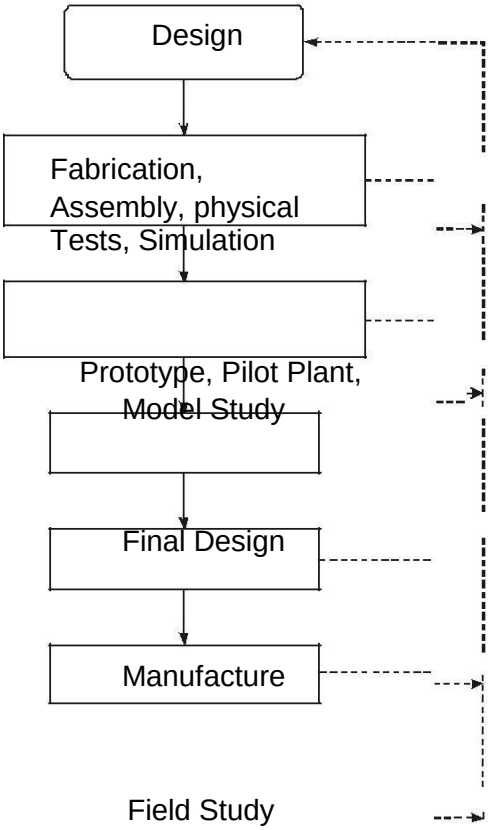


Fig. 3.1 Design as an interactive process

Several redesigns are made upon the feedback information on the performance or failure in the field or in the factory. Besides the tests, each engineering project is modified during execution, based on the periodical feedback on the progress and the lessons from other sources. Hence, the development of a product or a project as a whole may be considered as an experiment.

Engineering Projects vs. Standard Experiments

We shall now compare the two activities, and identify the similarities and contrasts.

A. Similarities

1. **Partial ignorance:** The project is usually executed in partial ignorance. Uncertainties exist in the model assumed. The behavior of materials purchased is uncertain and not constant (that is certain!). They may vary with the suppliers, processed lot, time, and the process used in shaping the materials (e.g., sheet or plate, rod or wire, forged or cast or welded). There may be variations in the grain structure and its resulting failure stress. It is not possible to collect data on all variations. In some cases, extrapolation, interpolation, assumptions of linear behavior over the range of parameters, accelerated testing, simulations, and virtual testing are

resorted.

2. **Uncertainty:** The final outcomes of projects are also uncertain, as in experiments. Sometimes unintended results, side effects (bye-products), and unsafe operation have also occurred. Unexpected risks, such as undue seepage in a storage dam, leakage of nuclear radiation from an atomic power plant, presence of pesticides in food or soft drink bottle, an new irrigation canal spreading water-borne diseases, and an unsuspecting hair dryer causing lung cancer on the user from the asbestos gasket used in the product have been reported.

   The uncertainties in the abstract model used for the design calculations, The uncertainties in the precise characteristics of the materials purchased,
   The uncertainties caused by variations in processing and fabrication of materials and
   The uncertainties about the nature of stresses the finished product will encounter

3. **Continuous monitoring:** Monitoring continually the progress and gaining new knowledge are needed before, during, and after execution of project as in the case of experimentation. The performance is to be monitored even during the use (or wrong use!) of the product by the end user/beneficiary.
4. **Learning from the past:** Engineers normally learn from their own prior designs and infer from the analysis of operation and results, and sometimes from the reports of other engineers. But this does not happen frequently. The absence of interest and channels of communication, ego in not seeking information, guilty upon the failure, fear of legal actions, and mere negligence have caused many a failure,
   e.g., the Titanic lacked sufficient number of lifeboats—it had only 825 boats for the actual passengers of 2227, the capacity of the ship being 3547! In the emergent situation, all the existing life boats could not be launched. Forty years back, another steamship Arctic met with same tragedy due to the same problem in the same region. But the lesson was learned. In most of the hydraulic systems, valves had been the critical components that are least reliable. The confusion on knowing whether the valve was open or closed, was the cause of the Three-Mile Island accident in 1979. Similar malfunctioning of valves and misreading of gauges have been reported to have caused the accidents elsewhere in some power plants. But we have not learnt the lesson from the past. The complacency that it will not happen again and will not happen 'to me' has lead to many disasters.

B. Contrasts

The scientific experiments in the laboratory and the engineering experiments in the filed exhibit several contrasts as listed below:

1. **Experimental control:** In standard experiments, members for study are selected into two groups namely A and B at random. Group A are given special treatment. The group B is given no treatment and is called the ‘controlled group’. But they are placed in the same environment as the other group A.
   This process is called the experimental control. This practice is adopted in the field of medicine. *In engineering, this does not happen, except when the project is confined to laboratory experiments.* This is because it is the clients or consumers who choose the product, exercise the control. It is not possible to make a random selection of participants from various groups. In engineering, through random sampling, the survey is made from among the users, to assess the results on the product. .
2. **Humane touch:** Engineering experiments *involve human souls, their needs, views, expectations, and creative use as in case of social experimentation. This point of view is not agreed by many of the engineers*. But now the quality engineers and managers have fully realized this humane aspect.
3. **Informed consent:** Engineering experimentation is viewed as Societal Experiment since the subject and the beneficiary are human beings. In this respect, it is similar to medical experimentation on human beings*. In the case of medical practice, moral and legal rights have been recognized while planning for experimentation*. *Informed consent is practiced in medical experimentation.* Such a practice is not there in scientific laboratory experiments. Informed consent has two basic elements:
   a) *Knowledge*: The subject should be given all relevant information needed to make the decision to participate.
   b) *Voluntariness*: Subject should take part without force, fraud or deception. Respect for rights of minorities to dissent and compensation for harmful effect are assumed here.

For a valid consent, the following conditions are to be fulfilled:

1. Consent must be voluntary
2. All relevant information shall be presented/stated in a clearly understandable form
3. Consenter shall be capable of processing the information and make rational decisions.
4. The subject's consent may be offered in proxy by a group that represents many subjects of like-interests

Informed consent when bringing an engineering product to market implies letting the customer know the following:
(*a*) The knowledge about the product
(*b*) Risks and benefits of using the product and
(*c*) All relevant information on the product, such as how to use and how not to use (do's and don'ts).
The relevant factual information implies, that the engineers are obliged to obtain and assess all the available information related to the fulfillment of one's moral obligations (i.e., wrong or immoral use of a product one designs), including the intended and unintended impacts of the product, on the society. Still there exists a possibility of a large gap of understanding between the experimenter and the subjects (public). Sometimes, the managements have not been willing to disseminate the full information about the project or product beyond the legal requirements, because of the fear of potential competitions and likely exposure to potential litigation.

People object to *involuntary risks* wherein the affected individual is neither a direct participant nor a decision maker. In short, we prefer to be the subjects of our own experiments rather than those of somebody else. If it is an asbestos plant or nuclear plant to be approved, affected parties expect their consent to be obtained. But they are ready to accept *voluntary* risks as in the case of stunts and amazing races.

In case of Koodangulam power project as well as the Sethusamudram Canal Project, Tamil Nadu, several citizen groups including Fishermen Forums have responded. The Central government was able contain many harsh apprehensions and protracted legal and political battles, by providing all relevant information.

4. **Knowledge gained**: *Not much of new knowledge is developed in engineering experiments* as in the case of scientific experiments in the laboratory. Engineering experiments at the most help us to
(*a*) Verify the adequacy of the design,
(*b*) To check the stability of the design parameters,
(*c*) Prepare for the unexpected outcomes, in the actual field environments.
From the models tested in the laboratory to the pilot plant tested in the field, there are differences in performance as well as other outcomes.

Engineers as responsible experimenters:

The engineer, as an experimenter, owe several responsibilities to the society, namely,

1. A conscientious commitment to live by moral values.
2. A comprehensive perspective on relevant information. It includes constant awareness of the progress of the experiment and readiness to monitor the side effects, if any.
3. Unrestricted free-personal involvement in all steps of the project/product development (autonomy).
4. Be accountable for the results of the project (accountability).

Conscientiousness

Conscientious moral commitment means:
(*a*) Being sensitive to full range of moral values and responsibilities relevant to the prevailing situation and
(*b*) the willingness to develop the skill and put efforts needed to reach the best balance possible among those considerations. In short, engineers must possess open eyes, open ears, and an open mind (i.e., moral vision, moral listening, and moral reasoning).

This makes the engineers as social experimenters, respect foremost the safety and health of

the affected, while they seek to enrich their knowledge, rush for the profit, follow the rules, or care for only the beneficiary. The human rights of the participant should be protected through voluntary and informed consent.

Relevant information

"Conscientiousness" is blind without relevant factual information. Hence showing moral concern, involves a commitment to obtain and access all available information pertinent to meeting one's moral obligations.

It is very difficult to anticipate all dangers because engineering projects are generally experimental in nature. Individual engineers cannot privately conduct environmental and social impact studies.

Comprehensive Perspective

The engineer should grasp the context of his work and ensure that the work involved results in only moral ends. One should not ignore his conscience, if the product or project that he is involved will result in damaging the nervous system of the people (or even the enemy, in case of weapon development)

A product has a built-in obsolete or redundant component to boost sales with a false claim. In possessing of the perspective of factual information, the engineer should exhibit a moral concern and not agree for this design. Sometimes, the guilt is transferred to the government or the competitors. Some organizations think that they will let the government find the fault or let the fraudulent competitor be caught first. Finally, a full-scale environmental or social impact study of the product or project by individual engineers is useful but not possible, in practice.

Moral autonomy

Engineers are morally autonomous when their moral conduct and principles of action are of their own. Engineering as social experimentation helps to be of autonomous participation in one's work. As an experimenter, an engineer exercises the sophisticated training that makes his or her identity as a professional.

In government projects, a dead line is fixed which becomes the ruling factor. Also, there are fears of competition. Tight schedule contributes losses in a project as it happened in the case of space shuttle "Challenger" as we shall see later.

Engineers have to look into their professional societies and other outside organizations for rural support. For example, a steam plant worker who refused to dump oil into a river in an unauthorized manner, was threatened with dismissal, but his union saw to it that the threat was never carried out.

Professional societies are meant for exchange of technical information, but they lack power to protect their members. Most engineers have no other group to depend on for such protection at the time of any problem or risk. Their professional societies will have to act and protect the interest of the engineers.

Accountability

Responsible people accept moral responsibility for their actions. "Accountability", sometimes is understood with a sense of being faulty or blame worthy for misdeeds but the term "accountable" generally means that one is willing to submit to one's actions. One is to be open and responsive for the assessment by others.

Submissions to an employer's authority or any authority for that matter creates a narrow sense of accountability for the consequences of their actions. A psychologist says that there is strong psychological tendency among people to abandon personal accountability when they are placed under authority.

The term Accountability means:

1. The capacity to understand and act on moral reasons
2. Willingness to submit one's actions to moral scrutiny and be responsive to the assessment of others. It includes being answerable for meeting specific obligations, i.e., liable to justify (or give reasonable excuses) the decisions, actions or means, and outcomes (sometimes unexpected), when required by the stakeholders or by law.

The tug-of-war between of causal influence by the employer and moral responsibility of the employee is quite common in professions. In the engineering practice, the problems are:

The fragmentation of work in a project inevitably makes the final products lie (*a*) away from the immediate work place, and lessens the personal responsibility of the employee. Further the responsibilities diffuse into various hierarchies and to various people. (*b*) Nobody gets the real feel of personal responsibility. (*c*) Often projects are executed one after another. An employee is more interested in adherence of tight schedules rather than giving personal care for the current project. More litigation is to be faced by the engineers (as in the case of medical (*d*) practitioners). This makes them wary of showing moral concerns beyond what is prescribed by the institutions. In spite of all these shortcomings, engineers are expected to face the risk and show up personal responsibility as the profession demands.

TYPES OF INQUIRIES

1. Normative Inquiry

It seeks to identify and justify the morally-desirable norms or standards that should guide individuals and groups. It also has the theoretical goal of justifying particular moral judgments. Normative questions are about what ought to be and what is good, based on moral values. For example,

1. How far does the obligation of engineers to protect public safety extend in any given situation?
2. When, if ever, should engineers be expected to blow whistle on dangerous practices of their employers?
3. Whose values ought to be primary in making judgment about acceptable risks in design for a public transport system or a nuclear plant? Is it of management, senior engineers, government, voters or all of them?
4. When and why is the government justified in interfering with the organisations?
5. What are the reasons on which the engineers show their obligations to their employees or clients or the public?

2 Conceptual Inquiry

It is directed to clarify the meaning of concepts or ideas or principles that are expressed by words or by questions and statements. For example,

What is meant by (*a*) safety?

How is it related to (*b*) risk?

(c) What is a bribe?

(*d*) What is a profession?

When moral concepts are discussed, normative and conceptual issues are closely interconnected

3. Factual or Descriptive Inquiry

It is aimed to obtain facts needed for understanding and resolving value issues. Researchers conduct factual inquiries using mathematical or statistical techniques. The inquiry provide important information on business realities, engineering practice, and the effectiveness of professional societies in fostering moral conduct, the procedures used in risk assessment, and psychological profiles of engineers. The facts provide not only the reasons for moral problems but also enable us to develop alterative ways of resolving moral problems. For example,

1. How were the benefits assessed?

2. What are procedures followed in risk assessment?
3. What are short-term and long-term effects of drinking water being polluted?
4. Who conducted the tests on materials?

ISSUES IN ENGINEERING ETHICS:

Common Issues:

Common Morality
Decision-Making Process
Engineering Code of Conduct
Engineering Education
Humane Technologies
International Law
Professional Development

MORAL ISSUES

It would be relevant to know why and how do moral issues (problems) arise in a profession or why do people behave unethically? The reasons for people including the employer and employees, behaving unethically may be classified into three categories:

Resource Crunch

Due to pressure, through time limits, availability of money or budgetary constraints, and technology decay or obsolescence. Pressure from the government to complete the project in time (e.g., before the elections), reduction in the budget because of sudden war or natural calamity (e.g., Tsunami) and obsolescence due technology innovation by the competitor lead to manipulation and unsafe and unethical execution of projects.

Involving individuals in the development of goals and values and developing policies that allow for individual diversity, dissent, and input to decision-making will prevent unethical results.

Opportunity

a) Double standards or behavior of the employers towards the employees and the public. The unethical behaviors of World Com (in USA), Enron (in USA as well as India) executives in 2002 resulted in bankruptcy for those companies,
b) Management projecting their own interests more than that of their employees. Some organizations over-emphasize short-term gains and results at the expense of themselves and others,
c) Emphasis on results and gains at the expense of the employees,
d) Management by objectives, without focus on empowerment and improvement of the infrastructure.

This is best encountered by developing policies that allow 'conscience keepers' and whistle blowers and appointing ombudsman, who can work confidentially with people to solve the unethical problems internally.

Attitude:

Poor attitude in the employees due to,

(a) Low morale of the employees because of dissatisfaction and downsizing,
(b) Absence of grievance redressal mechanism,
(c) Lack of promotion or career development policies or denied promotions
(d) Lack of transparency
(e) Absence of recognition and reward system, and
(f) Poor working environments
(g) Giving ethics training for all, recognizing ethical conduct in work place, including ethics in performance appraisal, and encouraging open discussion on ethical issues, are some of the directions to promote positive attitudes among the employees[9].
(h)

To get firm and positive effect, ethical standards must be set and adopted by the senior management, with input from all personnel.

MORAL DILEMMA

Definition

Dilemmas are situations in which moral reasons come into conflict, or in which the application of

moral values are problems, and one is not clear of the immediate choice or solution of the problems. Moral reasons could be rights, duties, goods or obligations. These situations do not mean that things had gone wrong, but they only indicate the presence of moral complexity. This makes the decision making complex. For example, a person promised to meet a friend and dine, but he has to help his uncle who is involved in an accident — one has to fix the priority.

There are some difficulties in arriving at the solution to the problems, in dilemma. The three complex situations leading to moral dilemmas are:

1. The problem of *vagueness*: One is unable to distinguish between good and bad (right or wrong) principle. Good means an action that is obligatory. For example, code of ethics specifies that one should obey the laws and follow standards. Refuse bribe or accept the gift, and maintain confidentiality
2. The problem of *conflicting reasons*: One is unable to choose between two good moral solutions. One has to fix priority, through knowledge or value system.
3. The problem of *disagreement*: There may be two or more solutions and none of them mandatory. These solutions may be better or worse in some respects but not in all aspects. One has to interpret, apply different morally reasons, and analyze and rank the decisions. Select the best suitable, under the existing and the most probable conditions.

2.4.2 Steps to Solve Dilemma

The logical steps in confronting moral dilemma are:

1. Identification of the moral factors and reasons. The clarity to identify the relevant moral values from among duties, rights, goods and obligations is obtained (conceptual inquiry). The most useful resource in identifying dilemmas in engineering is the professional codes of ethics, as interpreted by the professional experience. Another resource is talking with colleagues who can focus or narrow down the choice of values.
2. Collection of all information, data, and facts (factual inquiry) relevant to the situation.
3. Rank the moral options i.e., priority in application through value system, and also as obligatory, all right, acceptable, not acceptable, damaging, and most damaging etc. For example, in fulfilling responsibility, the codes give prime importance to public safety and protection of the environment, as compared to the individuals or the employers (conceptual inquiry).
4. Generate alternate courses of action to resolve the dilemma. Write down the main options and sub-options as a matrix or decision tree to ensure that all options are included.
5. Discuss with colleagues and obtain their perspectives, priorities, and suggestions on various alternatives.
6. Decide upon a final course of action, based on priority fixed or assumed. If there is no ideal solution, we arrive at a partially satisfactory or ‘satisficing’ solution.

ENGINEER’S RESPONSIBILITY AND SAFETY:

Safety: An action is considered safe when the risk associated with it are known and are considered acceptable. There is an element of judgment involved in considering the safety of something.

Risks: it is the possibility of something bad happening at some time in the future. The probability of getting into a dangerous situation ar achieving an unfavourable result can be considered as a risk. Risk is thus something that is expected to happen in the future, which an element of probability and uncertainty is associated.

Hazards: it is something that can be dangerous or cause damage. Something is hazardous if it has the potential to cause harm or ill effects. An exposed electric wire in your class room is hazardous because it has tha potential give an electric shock. No body may actually get shock, but the potential and probability exists.

4.0 SAFETY DEFINITION

Safety has different connotations. A product or a project is safe, with respect to a person or a group, at a given time, if its risks were fully known, and if the risks are judged to be acceptable, in the light of settled perspectives. When based on judgment safety, can be taken as objective. If the perspectives on values are taken then safety can be subjective as well.

Awareness and maintenance of this situation is called 'safety'. The safety can be incorporated during design, pre-testing, operation, field applications, analog tests, and learning from the past or others.

The perception varies from person to person, based on one's physical condition, age, experience, expertise, and wisdom. A second-hand electric heater when purchased was alright. But when used it might give electric shock and damage the human. Chlorinated municipal water supplied may be considered as unsafe we may judge that the harm to the stomach is unacceptable. But it may really safeguard against *gastroenteritis*. Sometime, the individual or groups think motorbikes are unsafe and scooters are safe. Some may never think about safety at all. An aged person is likely to suffer from dust. A scissor with the child may be unsafe, but with an adult it can be safe.

Various factors that influence the perception of risk are:

1. Probability of risk (the statistical nature of occurrence of risk).
2. Consequence of the risk. This is a quantitative measure. It can be physical damage or death of people, economic loss or damage of property, loss of money or reputation, degradation of the environment, and sometimes mental agony.
3. Voluntaryness (i.e., for thrill and amusement or under compulsion (involuntaryness).
4. Magnitude i.e., number of people or extent of area involved.
5. Proximity, the closeness of relationship with those affected or the gap in time scale.
6. Method of information dissemination on risk.
7. Job-related, i.e., whether it is under compulsion or volition.

The knowledge of risk acceptance is useful to the engineers. The designer can redesign the product/project to include safety measures, so as to (*a*) allow the product fail safely, (*b*) abandon it safely, and (*c*) provide for safe escape/evacuation from the product or site, and thus eliminate or minimize the human loss.

SAFETY AND RISK:

Safety was defined as *the risk that is known and judged as acceptable*. But, risk is a potential that something unwanted and harmful may occur. It is the result of an unsafe situation, sometimes unanticipated, during its use.

Probability of safety = 1 – Probability of risk
Probability of Risk = Probability of occurrence × Consequence in magnitude

Different methods are available to determine the risk (testing for safety)

1. Testing on the functions of the safety-system components.
2. *Destructive testing*: In this approach, testing is done till the component fails. It is too expensive, but very realistic and useful.
3. *Prototype testing*: In this approach, the testing is done on a proportional scale model with all vital components fixed in the system. Dimensional analysis could be used to project the results at the actual conditions.
4. *Simulation testing*: With the help of computer, the simulations are done. The safe boundary may be obtained. The effects of some controlled input variables on the outcomes can be predicted in a better way.

Concept of safety:

Engineering products are designed and manufactured with the aim of serving the public safely and without any risk. In spite of careful design and giving allowance for any unforeseen failures, our machines and control systems malfunction because of unexpected circumstances. Sometimes they fail and cause accidents. As a result “safety” is not there and the “risk” becomes inevitable.

Here, we will study-what is safety? What is risk? How risk can be assessed? How risks can be reduced?
Nuclear Power Plant accidents at Three Miles Island and Chernobyl tell us about the complexity in engineering systems and the need for safe exits.
Engineers are to work as a team in a company. They are paid salary for their work. They are expected to be loyal and honest to their employers. Engineers have moral responsibilities to discharge their duties in the interest of the company. At the same time, they have rights to freely pursue their work. Also they have the right to refuse illegal and unethical activities. Further, we will study- What is loyalty? What are professional rights? What are employee rights? and so on.

We expect engineering projects not to do any harm to the man and to the man and the environment. What may be safe for one person may not be safe for other person. For example, a power saw in the hands of the child is unsafe, but, it is safe in the hands of an adult. A sick adult is more prone to ill effects from air pollution than a healthy adult. Absolute safety is neither attainable nor affordable. Yet for our discussion, let us discuss what we mean by "safety".
"Safety" means the various risks a person judges to be acceptable. According to William W. Lawrence, "A thing is safe, if its risks are judged to be acceptable".
Let us consider first, that we "under estimate" the risks of a thing, say "Toaster" by mistake. We judge that it is very safe and buy it. At home when we make toast using the toaster one receives severe electric shock and burn, so that he is hospitalized. Now we conclude that we were wrong in our earlier judgement. The toaster was not safe at all, that is, its risks should not have been acceptable earlier. By Lawrence definition, we are forced to say that prior to the accident, the toaster was full safe, because at that time we judged the risks to be acceptable.
Second, let us take a case where we, "Over estimate", the risks of a thing. For example, we think fluoride in drinking water will kill a person. According to Lawrence definition, the fluoride water is unsafe since we judge its risks are unacceptable. It is impossible for someone to prove that the water actually safe.
Again according to Mr. Lawrence, the water becomes unsafe the moment we will judge the risks involved are unacceptable for us. The concept of safety allows to say that the water has been safe all along in spite of such irrational judgement.
Third, there is a situation in which people make no judgement at all, about the risks of things that are acceptable or unacceptable. They simply do not think about it. By Lawrence definition, this means that the thing is neither safe nor unsafe with respect to that group. We normally say that some cars are safe and others are unsafe, many people never even think about the safety of cars they drive.
Safety is frequently valued in terms of degrees and comparisons. Hence we speak of something "fairly safe" or "relatively safe".
For example, airplane travel is safer than automobile travel because for each kilometer travelled, the plane travel leads to a fewer deaths and injuries.
For engineer the term "safety" will mean the safe operation of systems and the prevention of natural or human caused disasters.

Discuss the concept of risk.

A risk is a thing if it exposes us to unacceptable danger or hazard. A risk is the potential that something unwanted and harmful may occur. We take a risk when we undertake something or use a product that is unsafe.
Risk, like harm covers many different types of unwanted happenings. In technology, it includes dangers of bodily harm, of economic loss, or of environmental degradation. These are caused by delayed job completion, faulty products or systems or environmentally harmful solutions to technological problems. Natural hazards continued to threaten human population. Floods, storms, heavy snowfall, earthquakes affected our population and cause a greater damage to the technological networks for water, energy and food. Here a word should be said about disasters.
A disaster takes place when a serious accident happens with a state of unpreparedness. Titanic collision with an iceberg happened to be a disaster because emergency preparedness were inadequate. There were only a few life boats. The warning about iceberg was not heeded. The severity of the risk is judged by its nature and possible consequences.

Assessment of Safety and Risk

Absolute safety is not possible. Any improvement in making a product safe involves an increase in the cost of production. A product involves primary cost (Production) and secondary cost, both are taken into consideration in calculating the total cost. The secondary costs are warranty expenses, loss of customer goodwill and loss of even customers and so on. Therefore, it is very important for the manufacturer and the users to have some understanding to know about the risks connected with any product and know how much it will cost to reduce those risks

P - Primary cost of products, including cost of safety measures involved.

S - Secondary costs including warranty, loss of customer goodwill

T - Total cost+P+S

Minimum total cost occurs at M.

H - Highest acceptable risk may fall below risk at least cost M.

H - H and its higher costs must be selected as design or operating cost.

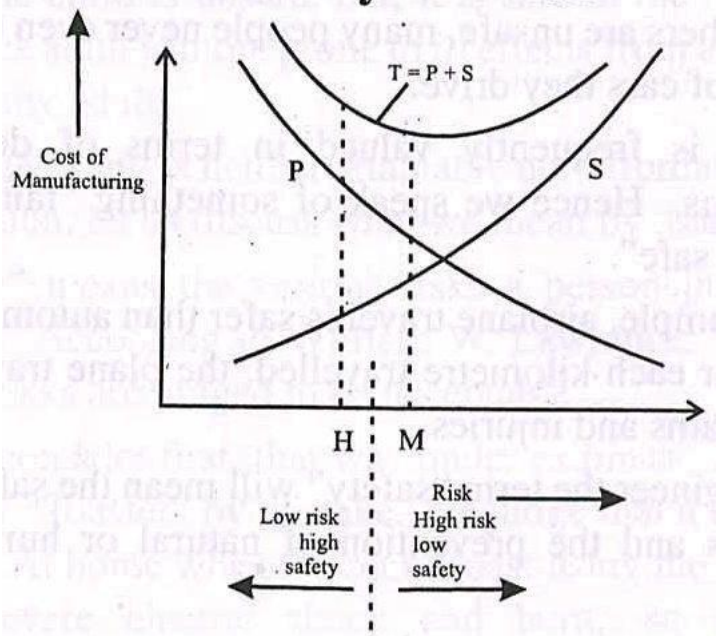


Fig. 1 indicates how high safety and low risks lead to high primary cost and low secondary cost. The other extreme is low safety and high risks. One saves on primary cost but pays more because of high secondary costs. In between where the slopes of the primary and secondary costs, curves are equal in magnitude but opposite in direction, is the point of minimum total cost (M). If all costs can be quantified, that optimum point will be the goal. For an optimal design, we must be clear about how to determine the risk and how to compare losses with benefits.

But generally among the industries the information regarding losses and profits are not freely shared. New engineers and new companies have to start from scratch, although sometimes past experience be used effectively to educate the beginners or freshers.

1. Uncertainties in design

Risk is never intentionally incorporated into a product, Risk arises because of the many uncertainties faced by the design engineers, the manufacturing engineer and even applications engineers.

There are uncertainties regarding the quality of materials by which the products are made. The level of skill in manufacturing a product is also factor for uncertainties.

Even a careful analyst will face difficulties when confronted with data as illustrated in the figure. The Fig.2 gives the thermal conductivity of the copper over a wide range of temperatures as observed by different investigators. The variation in result will influence engineering decision about safety.

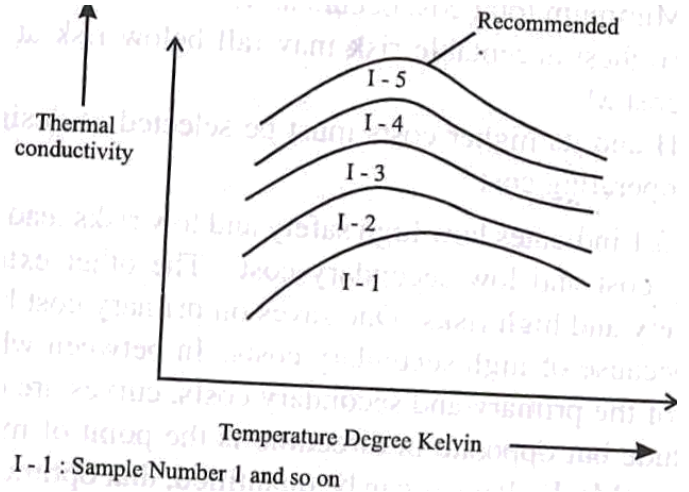


Fig.2.Thermal conductivity of copper wire under different temperatures studied by different investigators.

An engineer has to be cautious even with the standard materials specified for normal use. For example, the compressive strength of concrete is routinely carried out, where as the strength of steel is often taken for granted.

To account for uncertainties about materials or components, as well as incomplete knowledge about the actual operating conditions of the projects, engineers have introduced a factor called "factor of safety". Factor of safety is defined as ultimate stress by working stress (Safe or allowable stress). When actual stress on the member exceeds the allowable stress it will fail. That is, the product may be said to be safe when the actual stress less than the allowable stress.

2. Testing for safety

Somehow the engineers have to ensure safety for this, mostly he has to rely on experience. But the experience gained by one engineer is not often passed on to others. Another way of ensuring safety is gaining experience through test. Under certain conditions, testing can be a valuable source of information, if testing the materials of a product is carried out to destruction. The more useful procedure is prototype testing. Even prototype test and routine quality assurance test are not carried out frequently and properly. For example, the general motor company at one time was found to have false emission test data. In short we cannot trust testing procedures uncritically. Time pressure is one factor that will result in cheap testing. Sometimes the testers are bribed to give false results. Sometimes even without testing, the tester on the job certifies that testing have been undertaken.

RISK-BENEFIT ANALYSIS

Explain the concept of risk-benefit analysis.

A **risk–benefit ratio** is the ratio of the risk of an action to its potential benefits. **Risk–benefit analysis** is analysis that seeks to quantify the risk and benefits and hence their ratio.

Analyzing a risk can be heavily dependent on the human factor. A certain level of risk in our lives is accepted as necessary to achieve certain benefits. For example, driving an automobile is a risk most people take daily, also since it is mitigated by the controlling factor of their perception of their individual ability to manage the risk-creating situation. When individuals are exposed to involuntary risk (a risk over which they have no control), they make risk aversion their primary goal. Under these circumstances individuals require the probability of risk to be as much as one thousand times smaller than for the same situation under their perceived control (a notable example being the common bias in the perception of risk in flying vs. driving). [1]

Evaluations of future risk can be:

Real future risk, as disclosed by the fully matured future circumstances when they develop.

Statistical risk, as determined by currently available data, as measured actuarially for insurance premiums.

Projected risk, as analytically based on system models structured from historical studies. **Perceived risk**, as intuitively seen by individuals. ^^

Ethical Implications

Whenissomeone entitled to impose a risk on another in view of a supposed benefit to others?

Considertheworstcase scenarios of persons exposed to maximum risks while they are reaping only minimum benefits. Are their rights violated? Are they provided safer alternatives? Engineersshouldkeepin mind that risks to known persons are perceived differently from statistical risks
Engineersmayhaveno control over grievance redressal.

Conceptual difficulties in Risk-Benefit Analysis

Both risks and benefits lie in future

Heavydiscounting of future because the very low present values of cost/benefits do not give a true picture of future sufferings.

Bothhaverelated uncertainties but difficult to arrive at expected values Whatifbenefits accrue to one party and risks to another?

Canweexpress risks & benefits in a common set of units?

Riskscanbeexpressed in one set of units (deaths on the highway) and benefits in another (speed of travel)?

Many large projects, especially public works are undertaken based on risk-benefit analysis. The following are the questions to be answered:

i) Is the product worth risks connected with its use?
ii) What are the benefits?
iii) Are benefits more than the risks and so on?
iv) Are we willing to take a risk as long as the project gives sufficient benefit or gain?
v) If the risk and benefit can be readily expressed in a common set of units, say lives or rupees, it is relatively easy to carry out risk benefit analysis and we can try to come out on their benefit side. For example, an inoculation programme may result in some deaths, but it is worth the risk if more lives are saved by controlling an epidemic.

Another Example may be given to indicate the risk benefit ratio, which is as follows.

When a dam is constructed across a river, due to impounding of water on the upstream side of dam, large area will be submerged. Sometimes a number of villages have to be evacuated due to submergence by water on the upstream side.
These are the risks, Compared to those risks, benefits are more in the long run. Water stored can be used for irrigation, power production, drinking purpose, fishing and industries. Since here, the benefits are more than risks, it is worth taking up the dam project.

When risk can be expressed and measured in one set of units say deaths on highways and benefits in another set of units, say speed of travel, we can easily calculate the ratio of risk to benefits for different designs, when applied to the field. Risk benefit analysis like cost benefit analysis advises us about an undertaking a project.
While calculating the risks, the rights of the people should not be violated. If so, they should be provided with safer alternatives. Engineer's decisions have direct impact for people who feel the impact directly.

For example, Mr. Raman had a discomfort over living near a refinery. Let us assume that the public was in favor of building a new refinery at that location. Mr. Raman already lived in that area. The following questions arise.

1. Will others prevent the construction of "Refinery" at that location?
2. Are the local people entitled for any compensation if the plant is built even after objections?
3. How much compensation will be adequate?

These questions arise in many instances. Building a nuclear power plant is another example. The problem of quantification raises many problems in assessing personal safety and risk. For example: "how to assess the value of an individual's life in terms of rupees? This question is as difficult as deciding whose life is worth saving.
The result of these difficulties in assessing personal risks is that analysis use whatever quantitative measures are readily available on hand. In respect of voluntary risks, one may make judgements on the basis by an individual or it is much easier to use statistical average to calculate the personal risk in terms of rupees.

The major reasons for the analysis of the risk benefit are:

1 To know risks and benefits and weigh them each
2 To decide on designs, advisability of product/project

3 To suggest and modify the design so that the risks are eliminated or reduced

There are some limitations that exist in the risk-benefit analysis. The economic and ethical limitations are presented as follows:

1. Primarily the benefits may go to one group and risks may go to another group. Is it ethically correct?
2. Is an individual or government empowered to impose a risk on someone else on behalf of supposed benefit to somebody else? Sometimes, people who are exposed to maximum risks may get only the minimum benefits. In such cases, there is even violation of rights.
3. The units for comparison are not the same, e.g., commissioning the express highways may add a few highway deaths versus faster and comfortable travel for several commuters. The benefits may be in terms of fuel, money and time saved, but lives of human being sacrificed. How do we then compare properly?
4. Both risks and benefits lie in the future. The quantitative estimation of the future benefits, using the discounted present value (which may fluctuate), may not be correct and sometime misleading.

Both risks and benefits may have uncertainties. The estimated probability may differ from time to time and region to region.

Over estimation of the Risk:

Often the risk of something not working out is not nearly as high as we think, and the odds of it working out well are often far better. As Nobel Laureate and noted psychologist Daniel Kahneman found through years of research, when we're assessing risk, potential losses loom larger than potential gains. That is, we tend focus more on what might go wrong – what we might lose– than what might go right. What we focus on magnifies in our imagination, and it causes us to misjudge (and over-estimate) the likelihood of risks.
e.g. accidents associated with airplane

Cost of overestimation

Overestimation creates the problem that the estimate become self-fulfilling. The task takes longer than it would have done with a more accurate estimate in place. There are two ideas behind this linked to how people behave. Firstly, Student's Syndrome states that people often won't start working until very close to a deadline. Secondly, Parkinson's Law states that work expands to fill the time available. Therefore, if you have a task with overestimated length, the impact is the task might take longer than it 'should' do.

Under estimation of risks:

Hand in hand with the above, most of us underestimate our abilities. If you're a woman, then even more so! Too often we let our misgivings get the better of us. The result is that we often avoid taking on new challenges or proactively pursuing new opportunities because we don't trust sufficiently in our ability to rise to the challenges they involve. The truth is, you are capable of more than you think you are (and if you're a woman, double that!), which includes your ability to manage risk and to intervene in the event that plans start derailing.
e.g: drive in night.

Costs of underestimation

If a task is assumed to take long time than it actually needs, one of two things will happen. Either the task gets done at lower quality, or the task doesn't get done on time and any tasks dependent on it are pushed out.

Causes of an accident:

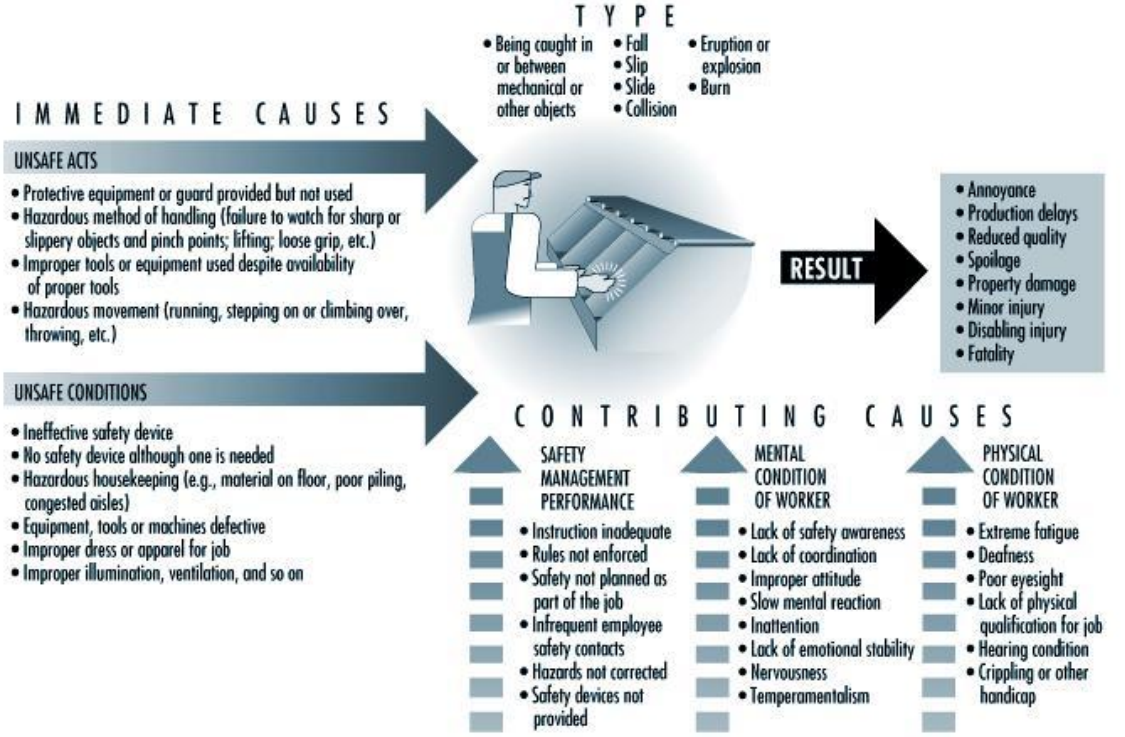
An "accident" is an unplanned, undesired event which may or may not result in injury or property damage, that interferes with the completion of an assigned task.
A "near miss" is a form of an accident that does not result in injury or property damage. While much effort and time is expended on accident investigation, this information tells us that we should be focusing on accident prevention. The majority of accidents are near-miss and may never be reported. The causes of accidents can be broken down into two basic components, **unsafe conditions and unsafe acts**.
Unsafe conditions are hazardous conditions or circumstances that could lead directly to an accident.

An unsafe act occurs when a worker ignores or is not aware of a standard operating procedure or safe work practice designed to protect the worker and prevent accidents.

A worker needs a electrical switch rewired. A work request is submitted and the work scheduled for the following week. The employee decides, I need this sooner and tries to rewire the switch. The employee receives an electrical shock after failing to lock out the energy source.

This above example illustrates how an employee may cut corners and commit an unsafe act. TABLE 1

SUMMARY OF UNSAFE ACTS AND CONDITIONS



Unsafe Acts	**Unsafe Conditions**
Operating equipment or machinery without permission vs	Lack of guarding on machinery
Defeating safety devices	Defective tools or equipment
Usine defective equipment	Crowding workers into one area
Using the wrong tool for the job	Inadequate alarm systems
Not using personal protective equipment	Fires & explosions
Incorrect lifting techniques	Poor housekeeping
Working while intoxicated	Hazardous atmospheres
Horseplay	Excessive noise
	Inadequate lighting

Accidents are defined as unplanned occurrences which result in injuries, fatalities, loss of production or damage to property and assets. Preventing accidents is extremely difficult in the absence of an understanding of the causes of accidents. Many attempts have been made to develop a prediction theory of accident causation, but so far none has been universally accepted. Researchers from different fields of science and engineering have been trying to develop a theory of accident causation which will help to identify, isolate and ultimately remove the factors that contribute to or cause accidents. In this article, a brief outline of various accident causation theories is presented, followed by a structure of accidents.

Accident Causation Theories:

The domino theory

According to W.H. Heinrich (1931), who developed the so-called domino theory, 88% of all accidents are caused by unsafe acts of people, 10% by unsafe actions and 2% by “acts of God”. He proposed a “five-factor accident sequence” in which each factor would actuate the next step in

the manner of toppling dominoes lined up in a row. The sequence of accident factors is as follows:

1. ancestry and social environment
2. worker fault
3. unsafe act together with mechanical and physical hazard
4. accident
5. damage or injury.

In the same way that the removal of a single domino in the row would interrupt the sequence of toppling, Heinrich suggested that removal of one of the factors would prevent the accident and resultant injury; with the key domino to be removed from the sequence being number 3. Although Heinrich provided no data for his theory, it nonetheless represents a useful point to start discussion and a foundation for future research.

Multiple causation theory

Multiple causation theory is an outgrowth of the domino theory, but it postulates that for a single accident there may be many contributory factors, causes and sub-causes, and that certain combinations of these give rise to accidents. According to this theory, the contributory factors can be grouped into the following two categories:

Behavioural. This category includes factors pertaining to the worker, such as improper attitude, lack of knowledge, lack of skills and inadequate physical and mental condition.

Environmental. This category includes improper guarding of other hazardous work elements and degradation of equipment through use and unsafe procedures.

The major contribution of this theory is to bring out the fact that rarely, if ever, is an accident the result of a single cause or act.

The pure chance theory

According to the pure chance theory, every one of any given set of workers has an equal chance of being involved in an accident. It further implies that there is no single discernible pattern of events that leads to an accident. In this theory, all accidents are treated as corresponding to Heinrich's acts of God, and it is held that there exist no interventions to prevent them.

Biased liability theory

Biased liability theory is based on the view that once a worker is involved in an accident, the chances of the same worker becoming involved in future accidents are either increased or decreased as compared to the rest of workers. This theory contributes very little, if anything at all, towards developing preventive actions for avoiding accidents.

Accident proneness theory

Accident proneness theory maintains that within a given set of workers, there exists a subset of workers who are more liable to be involved in accidents. Researchers have not been able to prove this theory conclusively because most of the research work has been poorly conducted and most of the findings are contradictory and inconclusive. This theory is not generally accepted. It is felt that if indeed this theory is supported by any empirical evidence at all, it probably accounts for only a very low proportion of accidents without any statistical significance.

The energy transfer theory

Those who accept the energy transfer theory put forward the claim that a worker incurs injury or equipment suffers damage through a change of energy, and that for every change of energy there is a source, a path and a receiver. This theory is useful for determining injury causation and evaluating energy hazards and control methodology. Strategies can be developed which are either preventive, limiting or ameliorating with respect to the energy transfer.

Control of energy transfer at the source can be achieved by the following means:

- elimination of the source
- changes made to the design or specification of elements of the work station
- preventive maintenance.

The path of energy transfer can be modified by:

- enclosure of the path
- installation of barriers
- installation of absorbers
- positioning of isolators.

The receiver of energy transfer can be assisted by adopting the following measures:

- limitation of exposure
- use of personal protective equipment.

The "symptoms versus causes" theory

The "symptoms versus causes" theory is not so much a theory as an admonition to be heeded if accident causation is to be understood. Usually, when investigating accidents, we tend to fasten upon the obvious causes of the accident to the neglect of the root causes. Unsafe acts and unsafe conditions are the symptoms—the proximate causes—and not the root causes of the accident.

Risk assessment

. Risk assessment is the cornerstone of the European approach to prevent occupational accidents and ill health. It is the start of the health and safety management approach. If it is not done well or not at all the appropriate preventative measures are unlikely to be identified or put in place.

Risk assessment can be defined as "the process of evaluating the risk to health and safety of workers while at work arising from the circumstances of the occurrence of a hazard at the workplace".

The process can be described as a continuous improvement cycle which can be implemented in the management processes in the company. The fundamental steps in risk assessment are:

Step 1: identifying hazards and those at risk Step 2: evaluating and prioritising risks
Step 3: Deciding on preventive action Step 4: Taking action
Step 5: Monitoring and reviewing

Prevention measures of reducing risks.

The engineer is faced with a difficult task of designing and manufacturing safe products. They have to give a fair accounting of benefits and risks for those products. They have to meet production schedule and help his or her company to maintain profits all the time. Of these objectives, the product safety is to be given top priority. The various steps towards reducing risks are as follows:

1. The operator should not do any error in operation. He should not be negligent towards discharging his duties. Accidents are caused by dangerous conditions that can be corrected. Dangerous design characteristics are to be given due consideration in the design. Safety devices may be provided to reduce accidents.
2. It safety is built into a product in the beginning itself it may not increase the cost. Any changes in the design later, may lead to increase in the cost.
3. We become aware about safety after a product has been manufactured and tested. If safety is not built into the original design, people can be hurt during the time of usage. Hence one should not be reluctant to change the design, safety point of view.
4. Warnings about hazards should be adequate. It is also better to have insurance coverage, but a warning merely indicates that a hazard is known to exist. This provides only minimal protection against harm. Sometimes, insurance rates are sky rocketing.

Engineers should understand that reducing risk is not an impossible task even under financial and time constraints. Hence in the design, safety I sto be given top priority by an engineer.

Hierarchy of prevention and control measures

Main article: Hierarchy of prevention and control measures

Risks should be avoided/eliminated and (if not possible) reduced by taking preventative measures, in order of priority. The order of priority is also known as the hierarchy of control. There different hierarchies of prevention and control measures which have been developed by different institutions. Common are five steps in the hierarchy of control in accordance to the BS OHSAS 18001 management system. [14] The five steps are:

Step 1 Elimination: Elimination of hazards refers to the total removal of the hazards and hence effectively making all the identified possible accidents and ill health impossible. The term 'elimination' means that a risk is reduced to zero without a shifting it elsewhere. Elimination is the ideal objective of any risk management. [19] This is a permanent solution and should be attempted in the first instance. If the hazard is removed, all the other management controls, such as

workplace monitoring and surveillance, training, safety auditing, and record keeping will no longer be required.

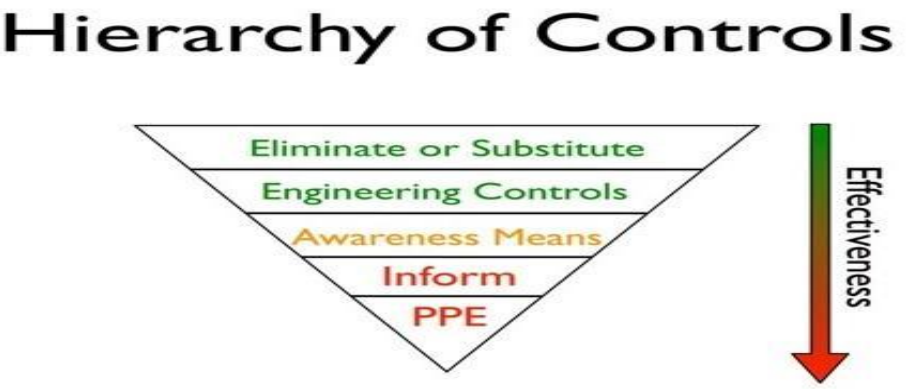
Step 2 Substitution: Substitution means replacing the hazard by one that presents a lower risk. The elimination is immediately combined with a shift to another but much lower risk . [19]

Step 3 Engineering Controls: Engineering controls are physical means that limit the hazard. These include structural changes to the work environment or work processes, erecting a barrier to interrupt the transmission path between the worker and the hazard. Local exhaust ventilation (LEV) to control risks from dust or fume is a common example as is separation of the hazard from operators by methods such as enclosing or guarding dangerous items of machinery/equipment. Priority should be given to measures which protect collectively over individual measures.

Step 4 Administrative Controls: Also known as organisational measures administrative controls reduce or eliminate exposure to a hazard by adherence to procedures or instructions. Documentation should emphasise all the steps to be taken and the controls to be used in carrying out the activity safely.

Step 5 Personal Protective Equipment (PPE): PPE should be used only as a last resort, after all other control measures have been considered, or as a short term contingency during emergency / maintenance / repair or as an additional protective measure. The success of this control is dependent on the protective equipment being chosen correctly, as well as fitted correctly, worn at all times and maintained properly. The reason that the use of PPE is at the bottom of the hierarchy of controls and is effectively a last resort is because of the higher likelihood (compared to controls higher up the hierarchy) of failing to danger because they place so much reliance for their success on the individual - be that in terms of them actually using the PPE or how well they use it or it actually fits them.

Figure 1: Hierarrchy of Controls



Explain with examples the methods of improved safety.

Examples of improved safety

1. The “magnetic door catch” introduced on refrigerators. This prevents death by suffocation of children trapped in them. The catch provided to the door makes possible, door to be opened from the inside without major effort. This is also cheaper compared to old type of latches.
2. The “Dead man-handle” used by the engineer (engine-driver) to control train’s speed. The train is accelerated only as long as some pressure is applied on the handle. If the engine driver reduces the pressure on the handle, the speed of the train also comes down. When the pressure is zero, the train automatically stops.
3. A car “safety belt” is a simple attachment on the door ensures that the belt automatically goes into the position whenever one enters the car.

CASE STUDIES: BHOPAL

GAS TRAGEDY:

On December 3, 1984, Union Carbide's pesticide-manufacturing plant in Bhopal, India leaked 40 tons of the deadly gas, methyl isocyanate into a sleeping, impoverished community – killing 2,500 within a few days, 10000 permanently disabled and injuring 100,000 people. Ten years later, it increased to 4000 to 7000 deaths and injuries to 600,000.

Risks taken:

Storage tank of Methyl Isocyanate gas was filled to more than 75% capacity as against Union Carbide‘s spec. that it should never be more than 60% full.
The company‘s West Virginia plant was controlling the safety systems and detected leakages thro‟ computers butBhopalthe plant only used manual labour for control and leak detection. The Methyl Isocyanate gas, being highly concentrated, burns parts of body with which it comes into contact, even blinding eyes and destroying lungs.

Causal Factors:
• Three protective systems out of service
• Plant was understaffed due to costs.
• Very high inventory of MIC, an extremely toxic material.
• The accident occurred in the early morning.
• Most of the people killed lived in a shanty (poorly built) town located very close to the plant fence.

Workers made the following attempts to save the plant:
• They tried to turn on the plant refrigeration system to cool down the environment and slow the reaction. (The refrigeration system had been drained of coolant weeks before and never refilled - - it cost too much.)
• They tried to route expanding gases to a neighboring tank. (The tank's pressure gauge was broken and indicated the tank was full when it was really empty.)
• They tried to purge the gases through a scrubber. (The scrubber was designed for flow rates, temperatures and pressures that were a fraction of what was by this time escaping from the tank. The scrubber was as a result ineffective.)
• They tried to route the gases through a flare tower -- to burn them away. (The supply line to the flare tower was broken and hadn't been replaced.)
• They tried to spray water on the gases and have them settle to the ground, by this time the chemical reaction was nearly completed. (The gases were escaping at a point 120 feet above ground; the hoses were designed to shoot water up to 100 feet into the air.)
In just 2 hours the chemicals escaped to form a deadly cloud over hundreds of thousands of people incl. poor migrant laborers who stayed close to the plant.

Case Study: Three Mile Island Accident

On March 28, 1979 the most serious United States commercial nuclear power plant accident happened outside of Middletown , Pennsylvania . Although no deaths occurred, the accident at Three Mile Island Unit 2 was the worst in operating history. It highlighted the need for changes in emergency response planning, reactor operator training, human factors engineering, and radiation protection. The accident was a result of equipment malfunctions, worker errors, and design related problems that ultimately led to a partial core meltdown and a small release of radioactivity.

The Accident

Early morning on March 28, 1979 the Three Mile Island plant, which used pressurized water reactors, “experienced a failure in the secondary, non-nuclear section of the plant” (NRC). Due to a mechanical or electrical failure, the central feedwater pumps terminated and “prevented the steam generators from removing heat” (NRC). As a consequence the turbine and reactor shut down, this caused an increase in pressure within the system. When pressure increases in the primary system a monitored pilot-operated relief valve opens until pressure reaches an acceptable level then shuts. In the case of the Three Mile Island accident the pilot-operated relief valve never closed and no signal was given to the operator. Consequently, the open valve poured out cooling water to assist in the lowering of pressure “and caused the core of the reactor to overheat” (NRC). The indicators which were designed to let the operator know when malfunctions were occurring provided conflicting information. There was no indicator displaying the level of coolant in the core nor was there a signal that the relief valve was open; therefore, the operators assumed the core was properly covered. Alarms went off in the plant due to the loss of coolant but the

operators were confused on what was wrong thereby making the situation worse. The overheating caused a rupture in the zirconium cladding and melting of the fuel pellets. Thankfully, the worst case consequences of a dangerous meltdown such as a breach of the walls f the containment building or releases of large amounts of radiation did not happen.

Impact of the Accident

The Three Mile Island accident prompted several upgrades in the maintenance and building of nuclear power plants. As described by the United States Nuclear Regulatory Commission Three Mile Island Fact Sheet, some of the changes which occurred post accident are the following: upgrading and strengthening of plant design and equipment requirements, identifying human performance as a critical part of plant safety, revamping operator training and staffing requirements, improved instruction to avoid the confusing signals that plagued operations during the accident, enhancement of emergency preparedness, regular analysis of plant performance, and expansion of performance-oriented as well as safety-oriented inspections.

In addition, the accident permanently changed the nuclear industry and the Nuclear Regulatory Commission's approach to regulation. The Nuclear Regulatory Commission (NRC) developed broader and more vigorous regulations and inspections in order to circumvent the public's worry and distrust. Since the Three Mile Island accident, the NRC has expanded its method of regulation. As shown in Figure 2.5, the NRC's "primary mission to protect the public health and safety, and the environment from the effects of radiation from nuclear reactors, materials, and waste facilities" is carried out in five different manners: regulations and guidance, licensing and certification, oversight, operational experience, and support for decisions (NRC website). By promoting each facet of its regulation method, the NRC strives to protect plant workers, the environment, and society as a whole.

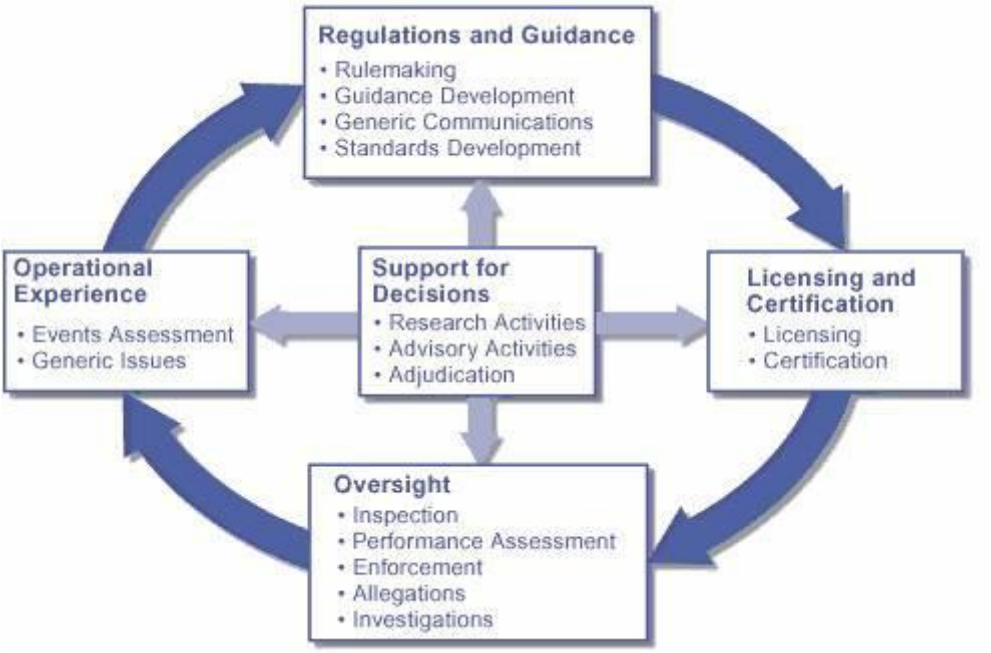


Figure 2.5: Nuclear Regulatory Commission's Regulation Process

Although no injuries occurred due to the accident, the idea of an extremely dangerous

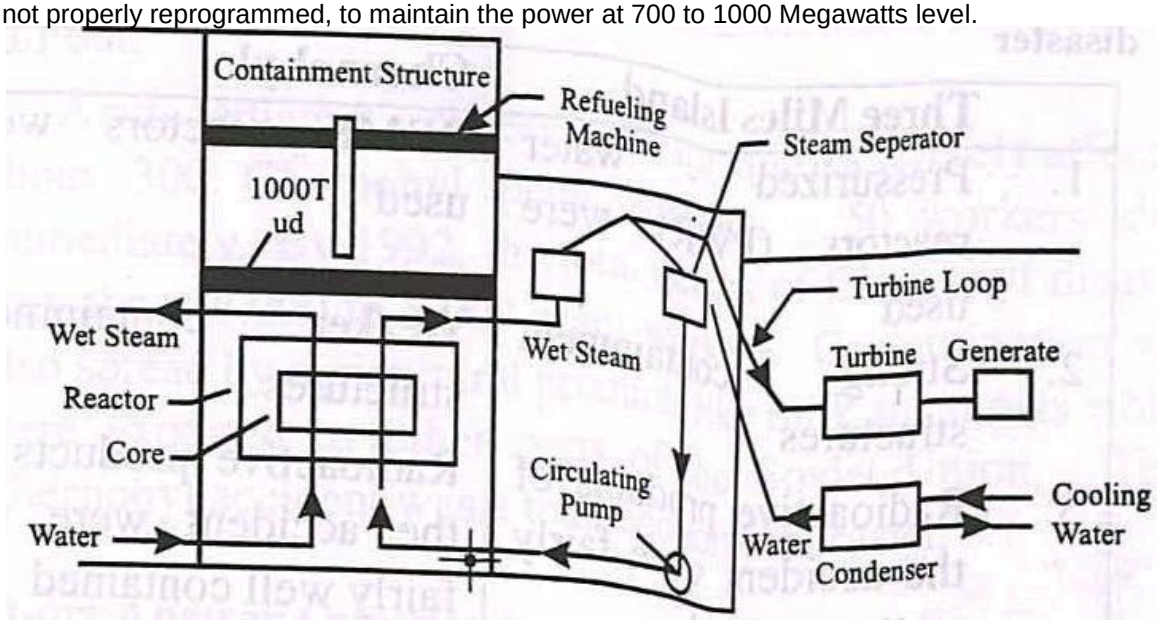
nuclear meltdown happening near one's household is disturbing. Yes, nuclear power provides 15% of the United States ' electricity but the risks of disposal and possible radiation exposure outweighs the desperateness of electrical power. What if X number of people were injured or killed due to the accident? Would taking that risk and sacrificing those people be worth nuclear power?

Chernobyl Nuclear reactor plant disaster

The Nuclear Power Plant at Chernobyl (Ukraine-then USSR) had six reactors by 1986. The output of the plant was 6,000 Megawatts.

The reactors were of a type called RBMK. They are graphite moderated and use boiling water pressure tubes. What happened in Chernobyl was "a terrible reactor fire". On April 25th1986, a test was under taken by the plant personnel and the plant was shut down for general maintenance purposes.

During the course of servicing and maintenance work, the reactor operators disconnected the emergency core-cooling system. So, its power consumption will not affect the test results. This was the first one of the many safety violations. Another error occurred when a control device was not properly reprogrammed, to maintain the power at 700 to 1000 Megawatts level.



This left the reactor in a dangerous position. The reactor was now running free, its control rods out, and its safety system disconnected. The reactor was free to do as it wished. As the core becomes hotter it allows fission to increase. This produced a sudden increase in power, in reactor 4, from 7% to many times of its rated thermal output. The effect was equal to that of half tone of TNT, exploding in the core. The fuel did not have time to melt. It simply shattered in to fragments.

The fuel came in contact with water. A second explosion took place and it lifted and shifted a 1000 tonne concrete roof, separating the reactor from the refueling area above it. The fuel rods interacted with the circulating water to form hydrogen. This produced a wonderful display of fireworks. The radioactive fine materials were driven sky-high by the heat.

What followed was a large scale accident, while the fire fighters lost their lives extinguishing the blaze. It took many hours to warn the surrounding people. Not only the Soviet Republic but also the entire Europe had not prepared themselves to handle such a grave disaster, that is, radioactive fallout.

Acute radiation sickness and burn injuries severely affected about 300 Chernobyl plant workers. 50 workers died immediately. By 1992, the total deaths of Chernobyl disaster was about 6,000 to 8,000 plant workers. Contamination was also spread by agricultural products like milk and meats which were exported to other parts of the Soviet Union. Thus Chernobyl accident was a total economic disaster.

Distinguish between Three Miles Island and Chernobyl disaster Three Miles Island Chernobyl

RBMK reactors were used

1. Pressurized – water reactors (PWR) were

used

2. Strong containment structures	Weaker containments structures
3. Radioactive products of the accident were fairly well contained	Radioactive products of the accident were not fairly well contained
4. Reactors were sensitive to perturbations	Reactors were sensitive to perturbations
5. Lack of emergency preparedness created disaster	Lack of emergency preparedness created disaster
6. Operating procedures were not continuously and thoroughly reviewed by engineers	The test protocol had not been discussed with plan engineers.
7. The operators were not fully conversant with the operating principles of the plant equipment	The operators were not fully conversant with the operating principles of the plant equipment

THE CHALLENGER

Challenger disaster-discuss.

The space shuttle by name "Challenger" was launched by "National Aeronautical Society of America (NASA) in the year 1986. The main components of the space shuttle 'challenger' are:

1. Main rocket
2. Booster rocket
3. Orbiter
4. O-rings in the field joint
5. Satellite
6. Shuttle

Challenger – The Space Shuttle

For launching satellites and other missions, U.S. Air Force was directed to use the NASA (National Aeronautics and Space Administration) shuttle, instead of its own shuttle. In the Space Shuttle, each orbiter has three main engines, fueled by a few million – newtons of liquid hydrogen. The fuel is carried in a very big external divided fuel tank, which is abandoned when becomes empty.

During liftoff, immediately after firing, much of the thrust is supplied by two "booster rockets". These booster rockets are of the "solid-fuel type", each burning about a million - newtons load of a mixture of aluminum, potassium chloride and iron oxide.

The casing of each booster rocket is about 50 meters long and 4 meters in diameter. It consists of cylindrical segments that are assembled at the launching site. The four field joints use seals made of pairs of O-rings, manufactured from vulcanized rubber which is less heat-resistant. To make it more heat – resistant, a putty barrier made of zinc chromide is provided.

After unexpected delays, Challenger's first flight was set for launching on Tuesday morning, January 28th 1986. Mr. Alan J.McDonald, one of the Design Engineer at Cape Kennedy was worried about the freezing temperature predicted for the night. Also another design engineer of the solid booster rocket, knew the difficulties that were experienced with the field joints, on a previous cold-weather launch.

The seal experts explained to the NASA engineers that how of launching, the booster rocket walls will bulge and the combustion gases will blow past both O-rings of the filed joints. The O-rings

will fail, as had been observed on many previous flights. In cold weather, the problem is still worse because the O-rings and the putty packing are less pliable.
The NASA engineers agreed that there was a problem with safety. According to specifications, no launching should take place at less than 53`F, but the temperature predicted at that night was very near to freezing temperature. This made the engineers to postpone the launching.

In order to save the image of the company which fabricated booster rockets, its engineers thought that the seals could not be shown to be unsafe. Considering the other factors the engineers expressed that the launching will be unsafe, but their suggestion was not heeded. Somehow, the NASA engineers decided to go ahead with launching of the space shuttle. The temperature had risen to 36`F. As the rockets carrying "challenger" rose from the ground, there was puffs of smoke that emanated from one of the filed joints on the right side of booster rocket. Soon these turned into a flame, which hit the external fuel tank. The hydrogen in the tank caught fire, and the challenger's wing was smashed. Within 75 seconds from liftoff, the challenger and its rockets had reached 16,000 metres high and it was totally engulfed in flames. The crew cabin separated and fell into the ocean, killing all the crew.
Thus the challenger's disaster was totally not only a technological disaster but also a financial disaster.

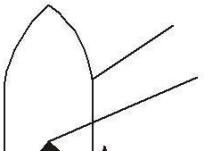
Safety issues that were ignored in launching of the space shuttle challenger.
The space shuttle that carried astronauts to the moon had three stage rockets safety point of view. A similar design was suggested in case of Challenger, but it was rejected by the government sincere it was too expensive. The crew had no escape mechanism. The shuttle programme was an experimental and a research undertaking. Challenger astronauts were not informed about the problems such as the field joints. They were not asked for their consent towards unsafe condition.
Another cause for the failure of the Challenger was the NASA's scientists were unwilling to wait for proper weather condition. Weather was partially responsible for Challenger's disaster. Because, a strong wind shear may result in rupturing of the weak O-rings.
The safety concerns were ignored by the management. One engineer said this "A small amount of professional safety effort and the support of the management will cause an enormous quantum safety improvement with little expenses". The important role of the management is for safety first and the schedules second.

What happened?
The orbiter of the Challenger had three main engines fuelled by liquid hydrogen. The fuel was carried in an external fuel tank which was jettisoned when empty. During lift-off, the main engines fire for about nine minutes, although initially the thrust was provided by the two booster rockets. These booster rockets are of the solid fuel type, each burning a million pound load of aluminum, potassium chloride, and iron oxide.

The casing of each booster rocket is about 150 feet long and 12 feet in diameter. This consists of cylindrical segments that are assembled at the launch site. There are four-field joints and they use seals consisting of pairs of O-rings made of vulcanized rubber. The O-rings work with a putty barrier made of zinc chromate.

The engineers were employed with Rockwell International (manufacturers for the orbiter and main rocket), **Morton-Thiokol** (maker of booster rockets), and they worked for NASA. After many postponements, the launch of Challenger was set for morning of Jan 28, 1986. **Allan J. McDonald** was an engineer from Morton-Thiokol and the director of the Solid Rocket Booster Project. He was skeptic about the freezing temperature conditions forecast for that morning, which was lower than the previous launch conditions. A teleconference between NASA engineers and MT engineers was arranged by Allan.

Arnold Thompson and **Roger Boisjoly**, the seal experts at MT explained to the other engineers how the booster rocket walls would bulge upon launch and combustion gases can blow past the O-rings of the field joints (Fig. 3.2).



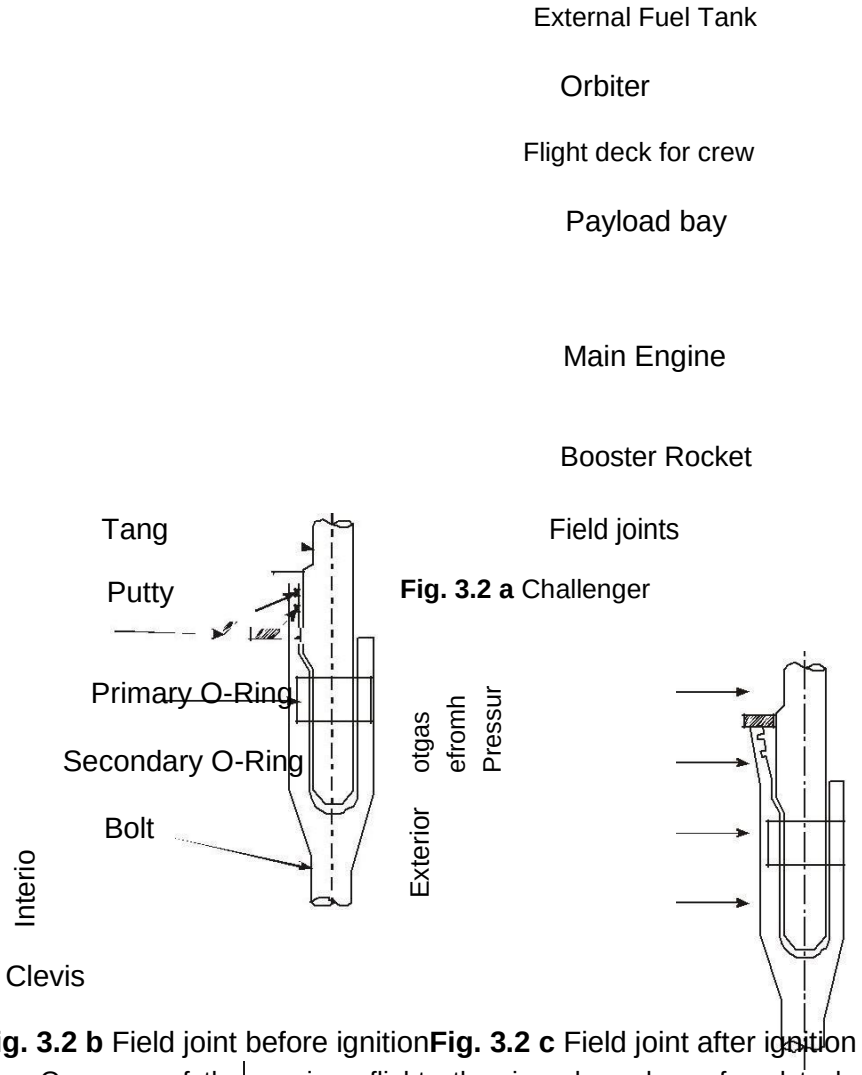


Fig. 3.2 a Challenger

Fig. 3.2 b Field joint before ignition **Fig. 3.2 c** Field joint after ignition

On many of the previous flights the rings have been found to have charred and eroded. In freezing temperature, the rings and the putty packing are less pliable. From the past data gathered, at temperature less than 65 F the O-rings failure was certain. But these data were not deliberated at that conference as the launch time was fast approaching.

The engineering managers **Bob Lund** and **Joe Kilminster** agreed that there was a safety problem. Boisjoly testified and recommended that no launch should be attempted with temperature less than 53 F. These managers were annoyed to postpone the launch yet again. The top management of MT was planning for the renewal of contract with NASA, for making booster rocket. The managers told Bob Lund "to take-off the engineering hat and put on your management hat". The judgment of the engineers was not given weightage. The inability of these engineers to substantiate that the launch would be unsafe was taken by NASA as an approval by Rockwell to launch.

At 11.38 a.m. the rockets along with Challenger rose up the sky. The cameras recorded smoke coming out of one of the filed joints on the right booster rocket. Soon there was a flame that hit the external fuel tank. At 76 seconds into the flight, the Challenger at a height of 10 miles was totally engulfed in a fireball. The crew cabin fell into the ocean killing all the seven aboard.

Some of the factual issues, conceptual issues and moral/normative issues in the space shuttle challenger incident, are highlighted hereunder for further study.

3.5.2 Moral/Normative Issues

1. The crew had no escape mechanism. Douglas, the engineer, designed an abort module to allow the separation of the orbiter, triggered by a field-joint leak. But

such a ‘safe exit’ was rejected as too expensive, and because of an accompanying reduction in payload.

2. The crew were not informed of the problems existing in the field joints. The principle of informed consent was not followed.

3. Engineers gave warning signals on safety. But the management group prevailed over and ignored the warning.

3.5.3 Conceptual Issues

1. NASA counted that the probability of failure of the craft was one in one lakh launches. But it was expected that only the 100000th launch will fail.

2. There were 700 criticality-1 items, which included the field joints. A failure in any one of

   them would have caused the tragedy. No back-up or stand-bye had been provided for these criticality-1 components.

3.5.4 Factual/Descriptive Issues

1. Field joints gave way in earlier flights. But the authorities felt the risk is not high.

2. NASA has disregarded warnings about the bad weather, at the time of launch, because they wanted to complete the project, prove their supremacy, get the funding from Government continued and get an applaud from the President of USA.

3. The inability of the Rockwell Engineers (manufacturer) to prove that the lift-off was unsafe. This was interpreted by the NASA, as an approval by Rockwell to launch.