CONTENTS

CHAPTER 1

Appraisal of Human Values and Professional Ethics

1.1 UNIVERSAL HUMAN VALUES

Human Values are the *'habits of thought'* each of us acquires as we mature so that we can assess and deal with *'ethical'* problems (where *'ethical'* relates to the fundamental question of how we should live). Should we aim at happiness or knowledge, at virtue or the creation of beautiful objects ? If we choose happiness, will it be our own or will it make proper allowance for the happiness of others ? And what of the more particular questions that face us ? Is it right to be dishonest in a good cause ? Can we justify living in opulence while elsewhere in the world people are starving ? What are our obligations to the other creatures with whom we share this planet, and to the generations of humans who will come after us ? What do we regard as a *'good'* quality of life for us and for others ?

Human values can be formulated or expressed in many ways *i.e.*, anything from practical examples to moral principles at the highest levels of generality. However, genuine human values are not abstract principles developed by academics or preachers, but life-embedded ideas and precepts, along with their various justifications. Because they are human, values are not divinely ordained rules of behaviour - not commandments set in stone. They are related to differing cultures, unique persons and situations and are developed and expressed in human terms for the human aims they collectively represent.

All great people in this world held some values/ ethics very dear and close to their heart and showed results based on the universal human values and their sub-values as mentioned below :

S.No	Human Values	Sub-Values
1.	*Truth*	Truthfulness, honesty, fairness, flection, creativity, determination and trust.
2.	*Love*	Service, tolerance, compassion, forgiveness, friendship and kindness
3.	*Peace*	Positive attitude, thankfulness, concentration, patience, contentment, self-acceptance and self-discipline.
4.	*Justice*	Consideration, cooperation, global stewardship, loyalty, active citizenship, justice and respect.
5.	*Responsibility*	Health, manner, helpfulness, courage, perseverance, responsible and awareness.

1.1.1 Truth

The truth in any matter does not depend upon the will or wish of the individual, but is independent of desires and their related interests and opinions. Truth has both individual and communal aspects. Just as individual truthfulness is the basis of a secure society, the common effort towards truth about life and the cosmos is represented, for example, by the sciences, by jurisprudence and philosophy. The faculty for rational thinking possessed by all humans, however much developed or not - or in whatever form it takes, is in the first and last instance what enables us to distinguish the truth from the false in so far as this is humanly possible. Evidence that truth is an inherent value in the human psyche is found in the fact that no-one likes to be called a liar, not even most liars. Further, it is much harder to sustain a lie than to maintain the truth, because one lie leads to another until the complexity is unmanageable.

1.1.2 Love

The word *'love'* should be taken in the very wide sense of *'care'* or *'concern for'*. This can be taken as a basic category or general human value which relates to concern and respect for others and the environment. The word *'love'* is here used in a broader sense than in common parlance where personal and/or erotic love is the common interpretation. Love as care does not refer to an emotion or a state of mind so much as to a human faculty of identification with others, sympathy with all beings, creation and - in spiritual or religious beliefs - of Divinity. Love seeks many and various channels of realisation. It's essence can be characterised by the words *"Love is unselfish care and concern for the well-being of others and the world at large."* The less selfish it is, the more it enriches life. Being universal, it takes on different general forms in different relations ; mother love, fatherly love, conjugal love of one's partner, loving friendship etc. Patriotic love is for one's country, true brotherhood expresses love of mankind, care and respect for nature is love of creation and - for those who profess religious belief - devotion is love of the Creator. All these have in common the 'heart' and an intuitive identification with spirit, with the universal miracle of being. Thus, love of oneself (contrasted with egocentricity) is also a valid expression of this power and, moreover, a duty to all at the same time. Being neither a sensation, an emotion nor a mere conception, but being identifiable only at the heart or core of the human consciousness, love in this universal sense is the characteristic par excellence of the human soul or psyche. It is common to include altruism, understanding and forgiveness under the more encompassing (but vague and ambiguous) word 'love'. Universally valid human value can be most difficult to determine in respect of any given situation. Not all would agree that one must forgive wrongdoers regardless of what they did, whether they admit guilt and show remorse or whether they would do the same again if they could. For most people, forgiveness may have to wait upon the remorse of the guilty party, and far from all would see it as right to forgive certain crimes even so. This shows how human values cannot be fixed or unchanging 'universal' commandments, for in every case of a value being applied (or ignored) in practice, many situation-specific circumstances are unavoidably involved in moral decisions.

1.1.3 Peace

Peacefulness in a person's life, in society and in world terms is a product of all positive values working together sufficiently. Without truth, caring concern (or *'love'*) and justice, conflicts arise and peace is endangered or lost. While peace is the absence of disturbance, violence, war and wrongdoing generally, it is tangible present when experienced individually as peace of mind, the mutual respect and pleasure of friendliness and tolerance. As a universally-accepted positive value, peace refers to the experience of harmony, a balanced but nevertheless dynamic mental condition. Peace of mind can be independent of *'externals'* like the absence of disturbance in *'peace and quiet'*, or the intrusion of an environment through noise, violence, terror etc.). Peace of mind - as contrasted to mental agitation - is a primary goal for human strivings to reach happiness. Peacelessness, in whatever respect, is not conducive to the happiness of equanimity. Peacefulness is not to be confused with lack of activity or mere physical quiet. As a psychic condition it is closely related to control of the mind, positivity of attitude together with calmness of mind. Inner blissfulness which is not dependent upon external sensory or physical conditions is a high expression of peacefulness. The peace of nations at least partly arises and is sustained through the cumulative efforts of society, including the peaceful and just behaviour of at least an aggregate of individuals. It can first be fully realised when we have confidence in the inherent ability of humans to see good, do good and be good. Thus, its internal connection with rightness of action and other human values becomes evident. As a social condition, peacefulness is clearly a state of freedom from violence and from destructive influences generally, whether it is war, the over-exploitation of people or the destruction of nature. Because of the emotional and mental dependencies that arise from attachment to material things, peacefulness is related to controlling one's desires, limiting them when necessary. This implies temperance in all things from quantity and type of foodstuffs taken in, the number and type of material possessions as well as the type or quality of *'sensory impressions'* to which one subjects the mind. Peace of mind is individual, but peace in society is the result of positive acts, which are not violent or destructive but tolerant and constructive.

1.1.4 Justice

Humans have long embraced justice as one of the highest human values based upon the widest possible considerations which include right or wrong, good or ill, blame (responsibility) or guiltlessness. The institutions exercising justice take into consideration past events, behaviour, motives, intentions, personal and social change, and the circumstances conditioning all these. It is based on fairness, where the equality of every individual before the law is fundamental. As such it is a social value which aims to resolve and reduce conflict, guided by the principles of care and non-violence (involving the minimum use of force required). The aim to achieve social justice for the perceived common good (however ineffective or wrong in view of current standards) has certainly a long pre-history as a central idea in all human societies. The human value justice also has wide-ranging political relevancy, such as in the strivings of egalitarianism in political democracy and other systems of rule. As such, justice is a major human value that embraces most aspects of social life. This value is to be understood in the deep Vedic sense of Ahimsa, being universal in implying respect for all living beings. This is founded on recognition of the (truth of) the unitary nature or *'integrity'* of creation, in which all individual beings together make up one integral whole within which all parts or aspects are ultimately mutually-interrelated. Justice is expressed in all forms of human interest in and care for living nature, obviously including humans, while it clearly also remains an ideal to be striven for in the interests of peace of mind and love. Human values are the duties we owe towards our fellow men to avoid harming them physically, emotionally or otherwise. Many people consider forgiveness of one's enemies or wrongdoers as of high moral value, something which is *'truly human'*.

1.1.5 Responsibility

Human actions are physical events brought about through physical behaviour. However, no definitive and specific codes of behaviour can be prescribed for all times and places independently of environmental, social and other conditions. The human values themselves provide the general criterion for good behaviour, but because of the changing nature of life and society, they cannot be formulated as explicit norms, laws, rules or regulations. Towards living nature in general, the human value of doing one's duty is closely related to non-violence. This is the reasonable tendency to wish to avoid harm to creatures or their environment wherever avoidable. Respecting the integral nature of eco-systems or of a social-natural environment as against the destructive influences of pollution, misuse and excessive exploitation exemplify the spirit of non-violence (the Hindu concept of ahimsa as well-developed by Gandhi). It is the inherently-sensed value that prompts us to draw back from unethical meddling in life processes, such as where its consequences are beyond the range of well-tried and proven knowledge. Knowledge of what is true combined with insight into what is good are the basis of duty, also conceived as *'acting rightly'*. Behind any conscious act lies the thought. If the thought is fed by the will towards the true and the good - in contrast to purely selfish aims - the act is *'right'*. This is also found in the Eastern concept of dharma or action in accordance with the universal laws of nature (both physical and human nature).

Central to dharma is truth, that is - action based on truth and in accordance with one's deeper or potential nature. A full understanding of right action, whatever the circumstances, presumes thorough insight into the mutual relations of dependence between humans, between all beings and within creation as a whole.

1.1.6 Harmony with Self, Family, Society and Nature

1.1.6A Harmony with Self

Human being is co-existence of self and body. The body is the instrument of self and self is the seer, doer and enjoyer. Self is continuously active to fulfill its need for happiness. The self is the basis of everything we do. All the desires and expectations we have are all due to self. Happiness and unhappiness are the states in self. Study of self enables us to know our weaknesses and method to remove it.

The self is conscious in nature while the body is physic-chemical in nature. Our focus of attention is on two categories of attributes of the self, *i.e.*, the powers of the self and the corresponding activities. Self receives sensations from body, we see a car through the information given by the *'eyes'*, we start thinking about the car which further results in desire to have one. When desire is set we start forming thoughts about fulfilling this desire. The following is the pattern of activities of self and body.

Selection ⟶ Thoughts ⟶ Desires ⟶ Thoughts ⟶ Selection

Activity of imagination in *'I'* is continuous and not temporary. The power and taste may change but the activity of selecting/tasting is continuous. These activities keep going on in us irrespective of whether we want them or not.

Desires, thoughts and expectations are largely being set by pre-conditioning and sensations. Preconditioning means we have assumed something about our desires on the basis of prevailing notion about it. We have not verified the desires in our own right. Sensation is a perception associated with stimulation of a sense organ or with a specific body condition.

Since the desires are in conflict, the thoughts they give rise to, are also in conflict and in turn, the selection from the thoughts are also in conflicts. This conflict affects us in different manners *i.e.*,

(*i*) Wavering aspirations
(*ii*) Lack of confidence
(*iii*) Unhappiness/conflicts
(*iv*) Lack of qualitative improvement in us, and
(*v*) State of resignation.

The pleasure obtained from sensations is short-lived. We are driven by five sensations (sound from the ears, touch from the skin, sight through eyes, taste from the mouth, and smell from the nose). No matter how much we try to be become happy via the senses, or via bodily

sensation, it does not last. We can thus understand that living on the basis of preconditioning (*e.g., "good life means having a nice car"*) or sensations (*i.e.*, happiness out of taste from the body) means we are in a state which is being decided by the others. Start verifying your desires, thoughts and expectations on the basis of your natural acceptance. Accessing of natural acceptance resolves our misunderstanding. The basis of our *'natural acceptance'* leads to operating on the basis of our *'realization'* and *'understanding'*. Realization means to be able to see the reality as it is. Understanding means to be able to understand the self organization in all entities of nature/ existence which are inter-connected.

1.1.6B Harmony in Family

A family can be defined as a group of persons related by blood, adoption or marriage and whether or not living and cooking together as a single housekeeping unit. Family as a basic unit of interaction is a natural learning ground for the human being to understand the harmony in relationship with others in the society. Family relations give us strength to face the world. It feels wonderful to return to a happy home after a hard day's work, otherwise a person would actually hate going home having an oppressive atmosphere.

A Family with feuds can cause depression, anxiety, sadness, confusion and rage. No one wants to live like that. It is not surprising that children who grow up in happy families are more successful and well-adjusted in life. Some simple rules for turning family feuds into family fun are ;

(*i*) Parents are the real role models for the kids. Their wellbeing depends largely on parents conduct.

(*ii*) Children need strong emotional support along with adequate monetary support.

(*iii*) Complete respect to old generation can be a very good guide as they carry a very rich experience with them.

(*iv*) To maintain good relations, avoid any kind of disconnect and establish a dialogue.

When we live in relationships then, as a natural process we constantly evaluate ours' and the other's feelings. We are embedded in relationships, they are there and all that we need to do is to recognize them and understand. We may try to suppress them, or argue against them, or undermine them but, the feelings remain very much there. When we 'trust' someone, it is the person, and not the body. Trust is something to do with the self ('*I*') of the other person *i.e.*, the feelings in relationship are between '*I*' and the other '*I*'.

The main factors/values on whose strength family harmony stands are :

(*i*) ***Justice.*** We need to evaluate for ourselves whether we are able to ensure justice in relationships,

(*ii*) ***Trust.*** It is the expectation of people that they can rely on our word. It is built through integrity and consistency in relationships,

(*iii*) ***Respect.*** Any kind of over, under or otherwise evaluation makes us uncomfortable, we find it unacceptable and say we have been disrespected,

(*iv*) ***Affection.*** It is a process of social interaction of feelings for love between two or more persons,

(*v*) ***Care.*** The feeling of care is the feeling to nurture and protect the body of our relative, and

(*vi*) ***Love.*** It is the emotion of strong affection and personal attachment with others in the family.

1.1.6C Harmony in Society

Society or human society is the set of relations including their social status and roles among people. Society denotes the people of a region or country and even the world. Used in the sense of an association, a society is a body of individuals outlined by the bonds of functional interdependence, possibly comprising characteristics such as national or cultural identity, social solidarity, language or hierarchical organization. Human societies are characterized by patterns of relationships between individuals sharing a distinctive culture and institutions. Like other communities or groups, a society allows its members to achieve needs or wishes they could not fulfill alone. The word society may also refer to an association of people for religious, benevolent, cultural, scientific, political, patriotic, or other purpose.

As we begin to understand our relationship in the family and live harmoniously in these relationships, we become aware of our relatedness to all human beings. Family is the first place to understand our relationships to recognize the feelings in them and live according to these feelings to attain mutual happiness. Our natural acceptance is to feel related to everyone. We find that in reality we not only want ourselves to be happy but also want to make other happy. Our competence might be limited but we wish for their happiness as well. We enjoy company and feel relaxed when we are with people who feel related to us.

Harmony in the family is the building block for harmony in the undivided society. Our natural acceptance is related to all which can expand into the world family. A feeling of relatedness with all is the basis of an undivided society.

1.1.6D Harmony with Nature

The world family order is the state of realizing the freedom of individual in context of this universe. The respect towards mankind and nature is must to establish the universal order. Having understood the comprehensive human goal, we are able to be in harmony not only with human beings, but also with the rest of nature. We are able to see that we are related to every unit in the nature and ensure mutual fulfilment in that relationship. Working on the five dimensions of human endeavour in the light of right understanding, we are able to work for an orderly living of the human society, whose foundational unit is the family and the final destination is the world family.

All of us know how we have multiplied the environment problems in the process and how we have increased consumerism today. We have disturbed the ecological balance and our production activities have upset the cycles in the nature.

Following are some more facts :

(*i*) While nature's processes are all cyclic (close ended) our processes are acyclic (open ended). If nature functions in such a way that all resources are continuously renewed and replenished (like, water, manure in the soil, etc), man's process deplete them.

(*ii*) Are we enriching nature, or are we not ? Largely the answer is NO. Take the example of pesticides and fertilizers. It is common knowledge today that the land that has seen heavy use of chemical fertilizers becomes unfit for agriculture.

(*iii*) In terms of exchange and storage, we have developed efficient ways of selling and buying, but with these rising modes of exchange and storage, the exploitation of mankind and nature has shot up. The disparities have increased, and the madness for profit has become the general motivation.

(*iv*) The respect towards mankind and nature is must to establish the universal order. Having understood the comprehensive human goal, we are able to be in harmony not only with human beings, but also with the rest of nature.

1.2 REVIEW OF PROFESSIONAL ETHICS

Professional ethics means development of professional competence with ethical human conduct. Ethical human conduct means definitiveness of human conduct. Ethical human conduct is the foundation of professional ethics. The only effective way to ensure professional ethics is through correct appraisal and systematic development of ethical competence in the person (the human being). Profession is a significant domain of human activity targeted towards participating in the larger order which includes the society and nature around. Thus, it is a meaningful participation for each one in one or more of the five domains of human endeavor needed for a harmonious society. Of this, one important domain happens to be in the form of production and production related activities. It also makes available the necessary physical facilities (livelihood) for oneself and one's family. Here, one has to interact with other human beings as well as the living and non-living entities of rest of nature. Through professional education, one acquires the specific skills and knowledge in order to make this contribution in the larger order. Ethical conduct of profession implies the right utilization of one's professional skills towards the fulfillment of comprehensive human goal and thus, meaningfully participate in the larger order.

> *"Professional ethics may be defined as a form of applied ethics that examines ethical principles and moral or ethical problems that arise in a business environment."*

Professional ethics are concerned with the moral issues that arise because of the specialist knowledge that a professional attains, and uses this knowledge while providing a service to the public. However, to be able to achieve this, it is essential to develop the value competence or the ethical competence in the human beings along with the requisite skills. It may be easily appreciated that a significant implication of the right understanding is to develop this ethical competence and thereby facilitate professional ethics.

1.2.1 Professional Accountability

Professional accountability is a virtue in career practice that requires practitioners or service providers to show responsibility for all action that they undertake during their practice. It is aimed at eliminating or reducing malpractice among professionals. In ethics and governance, accountability is answerability, blameworthiness, liability, and the expectation of account-giving. Accountability conveys the notion of holding someone (or some organisation) responsible for failure to deliver services to an appropriate standard. Accountability in the workplace is defined as doing the right thing consistently, day in and day out, in tasks, relationship and interactions to fulfill or further the mission of the organization. There are many models of accountability, but one way to view it is as having three components :

(*i*) The individual's professional accountability for the quality of his or her own work.

(*ii*) The accountability of any/engineering professional within the organisations in which they work.

(*iii*) Accountability (with others), as a senior member of staff, for the organisation's performance and more widely for its provision of local services.

Everyone is accountable for Health and Safety of workers. Management is responsible for providing workers with the necessary tools, training and protective equipment to perform. Accountability is important because :

(*i*) It assures someone that the needs will be met. If someone is accountable, you can trust that they will do what they claimed. Without accountability you would not be able to put your trust in someone to complete a job for you, or even show up on time to an important event.

(*ii*) Holding individuals accountable for serious violations of the laws of war is important because it may deter future violations, promote respect for the law.

(*iii*) Investigating and prosecuting individuals responsible for serious violations of international human rights and humanitarian law is an obligation under international law.

(*iv*) It works as deterrence to future crimes.

(*v*) In accounts it is responsible for handling payments. They pay bills and receive payments. They also handle payroll for employees.

(vi) The forensic accounting is something that could be (or will be) used in a court of law.

(vii) When employers and employees are mutually accountable to each other, employees can trust that their work will be rewarded appropriately.

1.2.2 Collegiality

Colleagues are those explicitly united in a common purpose and respecting each other's abilities to work toward that purpose. A colleague is an associate in a profession or in a civil or ecclesiastical office. Sometimes *colleague* is taken to mean a fellow member of the same profession. Thus, the word collegiality can connote respect for another's commitment to the common purpose and ability to work toward it. Collegiality is the relationship between at least two people/colleagues. Collegiality means valuing diversity and recognizing the bare fact that everyone has something different and important to offer. Collegiality means being open with others, sharing with them and collaborating for the good of the profession, including acting as guides or mentors. Our shared expertise and wealth of knowledge can make our profession strong and much more viable in our field. A focus on the concept of abundance for all, rather than territory or turf, will serve us better than a divisive, suspicious, backbiting approach.

Collegiality is often contrasted with a managerial approach which has a more hierarchical structure, with professional managers in leading positions. A managerial approach is often proposed as being more agile and effective at quick decision making, whilst critics suggest that its appeal is rather that it is more likely to comply with commercial and government wishes.

There has traditionally been a strong element of collegiality in the governance of universities and other higher education institutions, where individual independence of thought and mutual respect are necessary. Professionalism and collegiality are very highly regarded attributes of the legal profession. In court, lawyers refer to each other as '*my friend*' or '*learned counsel*'. A lawyer would never publicly insult another lawyer nor suggest that they were not smart or perceptive. If such an insult were made in court, a judge would stop the proceedings and publicly reprimand the rude lawyer.

1.2.3 Loyalty

Loyalty is faithfulness or a devotion to a person, country, group, or cause. Organisational loyalty is a general term and denotes a person's commitment and attachment to the place they work. Loyalty is giving one's best when one is attached to a particular organisation. Loyalty to the current organisation and furthering one's career are not always mutual and are in fact in most cases closely related. The very skills one needs to acquire for his/her career growth may also be essential for the current company. Therefore, employers can foster loyalty, by encouraging career development and helping employees to master new skills required for their progression, ideally within the same company. In order to balance the

growth of the company and that of the employees, it is also favourable to strategically align career growth of the individuals to the goals of the company. Limited career progress is not the only cause that hinders loyalty because ; monotonous work routines, high stress levels and dictatorial management styles are factors that can also get in the way. In reality, the old definition of organisational loyalty of lifetime commitment is no longer valid for the modern organisations. However, compromises are possible and this will solely depend on how a company behaves in terms of, its transparency in decisions, allowing the employees time for adjusting in the face of crisis, keeping them happy and secure in both good and bad times and firing only in extreme conditions.

Loyalty is a bad quality when it is interpreted to mean in the wrong context *e.g.*, as was done by some Govt. officers during the investigations of cheating scandals/scams protecting friends who had done something wrong. This is immoral, because it puts the interests of individuals ahead of the interests of the group.

1.2.4 Responsibility

It involves around a few ethical principles to be adopted and followed by a person in any profession. The guiding principles can be described as below :

(i) ***Integrity.*** To provide professional services with integrity. It demands honesty which must not be subordinated to personal gain and advantage. Allowance can be made for innocent error and legitimate differences of opinion, but integrity cannot co-exist with deceit or subordination of one's principles.

(ii) ***Objectivity.*** To provide professional services objectively. It requires intellectual honesty and impartiality. Regardless of the particular service rendered or the capacity in which a professional functions, one should protect the integrity of his/her work, maintain objectivity and avoid subordination of his/her judgment.

(iii) ***Competence.*** To maintain the knowledge and skill necessary to provide professional services competently. Competence means attaining and maintaining an adequate level of knowledge and skill, and application of that knowledge and skill in providing services to clients. Competence also includes the wisdom to recognize the limitations of that knowledge and when consultation with other professionals is appropriate or referral to other professionals necessary.

(iv) ***Fairness.*** Be fair and reasonable in all professional relationships. Fairness requires impartiality, intellectual honesty and disclosure of material conflicts of interest. It involves a subordination of one's own feelings, prejudices and desires so as to achieve a proper balance of conflicting interests. Fairness is treating others in the same fashion that you would want to be treated.

(v) ***Confidentiality.*** Protect the confidentiality of all customer information. Confidentiality means ensuring that information is accessible only to those authorized to have access. A relationship of trust and confidence with the customer can only be built upon the understanding that the customer's information will remain confidential.

(*vi*) ***Professionalism.*** To act in a manner that demonstrates exemplary professional conduct. Professionalism requires behaving with dignity and courtesy to clients, fellow professionals, and others in business-related activities. Professionals should cooperate with fellow professionals to enhance and maintain the profession's public image and improve the quality of services.

(*vii*) ***Diligence.*** Provide professional services diligently. Diligence is the provision of services in a reasonably prompt and thorough manner, including the proper planning for, and supervision of, the rendering of professional services.

1.2.5 Ethical Living

The right understanding gained through self-exploration enables us to identify the definition of human conduct which may also be called the ethical human conduct. It is the same for all human beings. So we are also able to understand the universality of ethical human conduct which is in consonance with the universal human values. Accordingly, all debates and confusion about what is ethical for one may not be ethical for others etc. also lose their base. Let us now understand the salient features of this definite human conduct *i.e.*, the ethical human conduct.

Each one of us wants to have a definite conduct but presently we may not be able to ensure that. This is because we are presently living on the basis of our pre-conditionings or assumptions which do not match with the truth or the right understanding. But, this situation neither gives satisfaction to us nor to others. We do see the human beings struggling to find out what the right conduct is and in the process, exhibit a wide variety of attributes. We also see people debating endlessly about what they consider to be ethical. But unless we have the right understanding, we are not able to identify the definitiveness of ethical human conduct. It can be understood in the following terms

Values (Mulya)

They give us the Competence of living in accordance with universal human values or the participation of a unit in the larger order- its natural characteristics or svabhava. Values are a part of our ethical conduct. They are the natural outcome of realization and right understanding, which are always definite. Values need not to be imposed through fear, greed or blind belief.

Policy (Niti)

Having been convinced about the values and about the inherent harmony in the existence, we are able to develop an ethical sense in all our actions. We always think, behave and work towards nurturing this harmony. It leads us to adopt policies conducive to human welfare which are conducive to enrichment, protection and right utilization of mind, body and wealth. This is an outcome of the definiteness of our desire and expectation.

The policy has *three* parts :

(*a*) **Economic Policy** (*Artha Niti*). The policy for enrichment of wealth.
(*b*) **Political Policy** (*Rajya Niti*). The policy for protection of body and wealth.
(*c*) **Policy for Universal Human Order** (*Dharma Niti*). The policy for right utilization of mind, body and wealth.

Character (Charitra)

A definite desire, thought and selection gives definiteness to our living. A definite character is the outcome of our definite behavior and work. This can be mainly characterized in terms of the following :

(*a*) Chastity in conjugal relationship *i.e.*, chastity in husband - wife relationship.
(*b*) Rightful production, acquisition and utilization of wealth.
(*c*) Kindness in behavior and work.

This definitiveness of human conduct in terms of values, policies and character is termed as ethics. The ethics in the living of an individual can be imbibed only through inculcation of values, policies and character, and this is possible through the process of ensuring right understanding through self-exploration. In other words ethics addresses questions about morality *i.e.*, concepts such as good *vs.* bad, noble vs. ignoble, right *vs.* wrong, and matters of justice, love, peace and virtue.

A human being with ethical human conduct having professional skills only, can be a good professional, *e.g.*, a good engineer, a good manager, a good teacher and researcher, and a good technocrat, etc.

- Ethical conduct implies that it is naturally acceptable to us and does not give rise to conflict within.
- Ethical conduct implies that it is in consonance with the right understanding of the reality.
- Ethical conduct implies that it leads to mutual fulfillment with other people and mutual enrichment with rest of nature.

Thus, the ethical conduct is self-satisfying, people friendly, eco-friendly and universal.

1.2.6 Engineer as a Role Model for Society

Engineering is an important and learned profession. As members of this profession, engineers are expected to exhibit the highest standards of honesty and integrity. Engineering has a direct and vital impact on the quality of life of all people in the society. Accordingly, the services provided by engineers require honesty, impartiality, fairness, and equity, and must be dedicated to the protection of the public health, safety, and welfare. Engineers must perform under a standard of professional behavior that requires adherence to the highest principles of ethical code of conduct.

(A) Engineers shall hold paramount the safety, health, and welfare of the public

(i) If his/her judgment is overruled under circumstances that endanger life or property, they shall notify their employer or client and such other authority as may be appropriate.

(ii) He/she will approve only those engineering documents that are in conformity with applicable standards.

(iii) He/she will not reveal facts, data, or information without the prior consent of the client or employer except as authorized or required by the law.

(iv) He/she will not permit the use of his/her name or associate in business ventures with any person or firm that they believe is engaged in fraudulent or dishonest enterprise.

(v) He/she will not aid or abet the unlawful practice of engineering by a person or firm.

(vi) Engineers having knowledge of any alleged violation of this code shall report there upon to appropriate authorities and cooperate assistance as may be required.

(B) Engineers shall perform services only in the areas of their competence

(i) Engineers shall undertake assignments only when qualified by education or experience in the specific technical field involved.

(ii) They will neither affix their signatures to any plans or documents dealing with subject matter in which they lack competence, nor to any plan or document not prepared under their direction and control.

(iii) Engineers may accept assignments and assume responsibility for coordination of an entire project, provided that each technical segment is signed by the qualified engineers who prepared the plan.

(C) Engineers shall issue public statements only in an objective and truthful manner

(i) Engineers shall be objective and truthful in professional reports.

(ii) They may express publicly technical opinions that are founded upon knowledge of the facts and competence in the subject matter.

(iii) Engineers shall issue no statements, criticisms, or arguments on technical matters that are inspired or paid for by interested parties.

(iv) They will act for their employer or client as faithful agents or trustees.

(v) Engineers shall not accept compensation, financial or otherwise, from more than one party for services on the same project.

(vi) Engineers shall not solicit or accept financial or other valuable consideration, directly or indirectly, from outside agents in connection with the work for which they are responsible.

(vii) They will not solicit or accept a contract from a governmental body on which an officer of their organization serves as a member.

(D) Engineers shall avoid deceptive acts

(i) Engineers shall not falsify their qualifications or permit misrepresentation of their or their associates' qualifications.

(ii) They shall not misrepresent or exaggerate their responsibility of prior assignments.

(iii) Engineers shall not offer, give, solicit, or receive, either directly or indirectly, any bribe to influence the award of a contract.

(iv) They shall not offer any gift or other valuable consideration in order to secure work.

(v) They shall not pay a commission, percentage, or brokerage fee in order to secure work, except to a bona fide established commercial or marketing agencies retained by them.

(E) Engineers shall be guided in all relations by the highest standards of honesty and integrity

(i) They shall acknowledge their errors and shall not distort or alter the facts.

(ii) They shall advise their client or employers when they believe a project will not be successful.

(iii) Engineers shall not accept outside employment to the detriment of their regular work or interest.

(iv) They shall not attempt to attract an engineer from another employer on false or misleading pretenses.

(v) Engineers shall not promote their own interest at the expense of the dignity and integrity of the profession.

(F) Engineers shall at all times strive to serve the public interest

(i) Engineers should participate in career guidance to their juniors ; and work for the advancement of the safety and well-being of their community.

(ii) Engineers shall not complete and sign specifications that are not in conformity with applicable engineering standards. If the client or employer insists on such unprofessional conduct, they shall notify the proper authorities and withdraw from further service on the project.

(iii) They should encourage to extend knowledge and appreciation of engineering and its achievements to the public.

(iv) They should work to protect the environment for future generations.

(G) Engineers shall avoid all conduct or practice that deceives the public

(i) Engineers shall avoid the use of statements containing a material misrepresentation of fact or omitting a material fact.

(ii) Consistent with the above engineers may advertise and recruit personnel.

(iii) Consistent with the foregoing, engineers may prepare articles for the technical press, but such articles shall not take self credit for work performed by others.

(H) Engineers shall not disclose, without consent, confidential information concerning the business affairs or technical processes of any present or former client or employer, or public body on which they serve

- Engineers should not, participate in proceedings in which the engineer has gained particular specialized knowledge on behalf of a former client or employer.

(I) Engineers shall not be influenced in their professional duties by conflicting interests

(i) Engineers shall not accept financial or other considerations, including free engineering designs, from material or equipment suppliers for preparing specifications of their required product.

(ii) Engineers shall not accept commissions or allowances, directly or indirectly, from contractors or other parties dealing with the work for which the engineer is responsible.

(J) Engineers shall not attempt to obtain professional engagements by untruthfully criticizing other engineers

(i) Engineers shall not request, propose, or accept a commission on a contingent basis under the circumstance in which their judgment may be compromised.

(ii) Engineers in salaried positions shall not accept any part-time engineering work without approval of his employer.

(iii) Engineers shall not, without consent use equipment, supplies, laboratory, or office facilities of an employer to carry on with any outside private practice.

(K) Engineers shall not attempt to injure, directly or indirectly, the professional reputation of other engineers. Engineers who believe others are guilty of unethical or illegal practice shall present such information to the proper authority for action

(i) Engineers in private practice shall not review the work of another engineer for the same client, except with the knowledge of such engineer, or unless the connection of such engineer with the work has been terminated.

(ii) Engineers in governmental, industrial, educational employment are entitled to review and evaluate the work of other engineers when so required by their employment duties.

(iii) Engineers in sales or industrial employment are entitled to make engineering comparisons of their products with products of other suppliers.

(L) Engineers shall accept personal responsibility for their professional activities

(i) They should conform with state registration laws if any, in the practice of engineering.

(ii) They will not use association with a non-engineer, a corporation, or partnership as a "cloak" for unethical acts.

(M) Engineers shall give credit for engineering work to those to whom credit is due, and will recognize the proprietary interests of others

(i) They should name the person or persons who may be individually responsible for designs, inventions, writings, or other accomplishments.

(ii) Engineers using designs supplied by a client should recognize that the designs being the property of the client may not be duplicated.

(iii) Before undertaking any work he/she should enter into a positive agreement regarding ownership/ copyrights/patents.

(iv) Engineers' designs, data, records, and notes referring exclusively to an employer's work are the employer's property. The employer should indemnify the engineer for use of the information for any purpose other than the original purpose.

(v) They should continue their professional development throughout their careers and should keep current in their specialty fields by engaging in professional practice, participating in continuing education courses, reading in the technical literature, and attending professional meetings and seminars.

1.2.7 Four Orders of Living

The *four* different levels of our living in harmony are described below :

(i) ***Living with harmony in myself.*** We all are having thoughts, belief and choices. It indicates the first levels of our living. We should start to study ourselves *i.e.*, to study our own wants, behavior, requirements etc. We are not the same person in every situation at all the time. We could be five different people in one given day in different areas. They all contain fragments of us, hidden beneath. If you could reach the point of acknowledgment that your work is to find harmony with you, then what anybody else thinks about it, has nothing to do with your experience. You would be of much more value to all.

(ii) ***Living with harmony in family.*** All of us have born in a family. Unlike basic physical needs of food, sleep and shelter, a child's mental and emotional needs may not be visible. A child who is mentally and emotionally stable is able to think clearly, learn new skills, is self-confident, and is also able to adapt to new situations easily. To develop into emotionally stable individuals, children need unconditional love and opportunities to develop self-confidence. His mistakes and failures should be expected and accepted. Praise and encourage them to explore. Your attention helps to build their self-confidence and self esteem. Let them know that we all make mistakes and that adults are also not perfect. Playtime helps children to be creative and to learn problem-solving skills. Playing allows for a special bonding and kinship to develop between you and your child. Help your children to understand that while playing, winning is not as important. It is more important for children to participate and enjoy themselves than to have winning as a focus. As members of a family, children need to learn the rules of the family unit. You can offer fair and consistent guidance

and discipline to your children. It is natural for children to feel afraid sometimes. If your children have fears that will not go away and affect his or her behavior, therefore support them.

*(iii) **Living with harmony in society.*** Society is also a broader group of our family where we live. In society we are interdependent of many physical needs life housing, health, medical services, education, transport etc.

To live with harmony in society :

(*a*) Follow your heart,
(*b*) Be responsible for yourself,
(*c*) Be responsible to others,
(*d*) Be open and honest,
(*e*) Respond to others from your heart,
(*f*) Be compassionate,
(*g*) Act inclusively rather than exclusively,
(*h*) Be true to your own feelings,
(*i*) Grow in positive directions and
(*j*) Share your knowledge with others.

*(iv) **Living with harmony in nature or existence.*** We live on this earth with birds, animals, plants in a large eco-system called nature. Nature is giver as well as doer. Nature teaches us humility which is regarded as one of the first step towards self-realization. Man asserts his own needs and this makes him arrogant and selfish. Living in dynamic harmony with nature allows one to find ancient and new wisdom. The capitalist development is a threat to life because it prioritizes consumerism and the generation of profits over common well-being and the satisfaction of basic needs. Accumulation of wealth and maximization of economic growth destroys nature. It is necessary to re-establish harmony with nature. We must respect for human rights and the Right of Mother Earth as an articulated, complementary, and reciprocal processes. Harmony with nature is not possible if, equality does not exist between human beings and the environment.

1.2.8 Holistic Technology (Eco-friendly systems)

Any of the methods used in industry to create goods and services from various resources is called a production system *i.e.*, these are processes that transform resources into useful goods and services. The transformation process typically uses common resources such as labour, capital (for machinery and equipment, materials, etc.), and space (land, buildings, etc.) to effect a change. Economists call these as resources and usually refer to them as labour, capital, and land. Production managers refer to them as the "five M's": men, machines, methods, materials, and money. There are thousands of items developed in the industry using eco-friendly systems.

Environment-friendly (also eco-friendly, nature friendly, and green) production systems are ambiguous terms used to refer to goods and services with laws, guidelines and policies claimed to inflict minimal, or no harm upon eco-systems or the environment. Companies sometimes use these terms to make environmental marketing claims when promoting goods and services, for example with eco-labels

The International Organisation for Standardization has developed ISO 14020 and ISO 14024 to establish principles and procedures for environmental labels and declarations that certifiers and eco-labellers should follow.

An eco-friendly production system should keep the following points into consideration :

(*i*) Evaluating the human health and environmental impacts of its processes and products.
(*ii*) Identifying what information is needed to make human health and environment decisions
(*iii*) Conducting an assessment of alternatives
(*iv*) Considering cross-media impacts and the benefits of substituting chemicals
(*v*) Reducing the use and release of toxic chemicals through the innovation of cleaner technologies that use safer chemicals.
(*vi*) Implementing pollution prevention, energy efficiency, and other resource conservation measures.
(*vii*) Making products that can be reused and recycled
(*viii*) Monitoring the environmental impacts and costs associated with each product or process
(*ix*) Recognizing that although change can be rapid, in many cases a cycle of evaluation and continuous improvement is needed.

There are *four* main concepts of the Design for Environment friendly systems for the Industry :

(*i*) ***Design for environmental processing and manufacturing.*** This ensures that raw material extraction (mining, drilling, etc.), processing (processing reusable materials, metal melting, etc.) and manufacturing are done using materials and processes which are not dangerous to the environment or the employees working on said processes. This includes the minimization of waste and hazardous by-products, air pollution, energy expenditure and other factors.

(*ii*) ***Design for environmental packaging.*** This ensures that the materials used in packaging are environmentally friendly, which can be achieved through the reuse of shipping products, elimination of unnecessary paper and packaging products, efficient use of materials and space, use of recycled and/or recyclable materials.

(*iii*) ***Design for disposal or reuse.*** The end of life cycle of a product is very important, because some products emit dangerous chemicals into the air, ground and water after they are

disposed of in a landfill. Planning for the reuse or refurbishing of a product will change the types of materials that would be used, how they could later be disassembled and reused, and the environmental impacts such materials have.

(iv) ***Design for energy efficiency.*** The design of product to reduce overall energy consumption throughout the product's life.

The following are the few examples of environment and eco-friendly non-conventional sources of energy used in production systems :

S.No	System	Product/use
1.	Solar Energy System (replacement of thermal power)	(*i*) Electricity Generation (*ii*) Pumping of Water (*iii*) Lighting of bulbs (*iv*) Battery Charging (*v*) Pelletier Cooling
2.	Hydel Power System (replacement of thermal power)	(*i*) Electricity Generation
3.	Wind Power System	(*i*) Electricity Generation
4.	Wave Energy System	(*i*) Electricity Generation
5.	Nuclear Power Energy System (replacement of thermal power)	(*i*) Electricity Generation
6.	Different kinds of wastes	(*i*) Heating (*ii*) Electricity Generation
7.	Night soil based biogas plant	(*i*) Electricity Generation
8.	Muscle power	(*i*) Replace use of petrochemicals
9.	Tidal Energy	(*i*) Electricity Generation

CHAPTER 2

Engineers' Responsibility for Safety

2.1 INTRODUCTION

To assure public safety and welfare it is important that Engineers should understand their responsibilities. It is central to professional conduct, but often an individual engineer faces obstacles in the form of other duties which conflict with it. Sometimes an engineer has to sacrifice one safety concern for another. In some cases, an engineer's duty to maintain client confidentiality can come in conflict with his duty to ensure safety *i.e.*, an engineer sometimes has to make a compromise between safety and cost. For example, we might be able to make a vehicle most safer, but only at an incredible cost to the company and consumer. Therefore then the question arises is, how much safe is safe enough ?

Discussion on this topic has to start from the stage of technical education in the professional courses at the college level. Teachers should discuss these obligations faced by the engineers in their professional life *i.e.*, the kinds of conflicts that arise while handling them and should show students how to recognize these conflicts in the course of their work. Have the students learn to identify the people to whom they will likely have to oblige in the course of their work *i.e.*, co-workers, managers, clients, general public, themselves (family), and their profession. To make them understand better students may be asked to list the obligations they believe they have towards each of these groups of people.

2.2 SAFETY ENGINEERING

The primary goal of safety engineering is to manage risk, eliminate or reduce it to acceptable levels. Risk is the combination of the probability of a failure event, and the severity resulting from the failure. For instance, the severity of a particular failure may result in fatalities, injuries, property damage, or nothing more than annoyance. It may be a frequent, occasional, and/or rare occurrence, however the failure depends on any/or the combination of

these two frequencies. Probability is often more difficult to predict than severity due to the many factors that could lead to a failure, such as mechanical failure, environmental effects, and operator error etc.

Safety engineering attempts to reduce the frequency of failures, and to ensure that when failures do occur, the consequences are not life-threatening. For example, bridges are designed to carry loads well in excess of the heaviest truck likely to use them. This reduces the likelihood of being overloaded. Most bridges are designed while multiplying the redundant load with a huge factor of safety, so that if any one structural member fails, the structure will remain standing. This reduces the severity if the bridge is overloaded.

Ideally, safety engineering starts during the early design of a system. Safety engineers consider what undesirable events can occur under what conditions, and project the related accident risk. They may then propose or require safety mitigation requirements in specifications at the start of development or changes to existing CAD designs or in-service products to make a system safer. This may be done by full elimination of any type of hazards or by lowering accident risk. Far too often, rather than actually influencing the design, safety engineers are assigned to prove that an existing or completed design is safe. If the engineer discovers significant safety problems late in the development process, correcting them at that stage can be very expensive. This type of error has the potential to waste large sums of money and likely more important, human lives and environmental damage.

The exception to this conventional approach is the way some large government agencies approach safety engineering from a more proactive and proven process perspective, known as "*system safety*". The system safety philosophy is to be applied to complex and critical systems, such as commercial airliners, complex weapon systems, spacecraft, rail and transportation systems, air traffic control system and other complex and safety-critical industrial systems. The proven system safety methods and techniques are to prevent, eliminate and control hazards and risks through designed influences by a collaboration of key engineering disciplines and product teams. Software safety is a fast growing field since modern systems' functions are increasingly being put under control of software. The whole concept of system safety and software safety, as a subset of systems engineering, is to influence safety-critical systems' designs by conducting several types of hazard analysis to identify hazards, validate hazards and verify design, assess and if needed to specify (new) design safety features and procedures to strategically mitigate risk to acceptable levels before the system is certified.

Additionally, failure mitigation can go beyond design recommendations, particularly in the area of maintenance. There is an entire realm of safety and reliability engineering known as Reliability Centered Maintenance (RCM), which is a discipline that is a direct result of analyzing potential failures within a system and determining maintenance actions that can mitigate the risk of failure. This methodology is used extensively on aircraft and involves understanding the failure modes of the serviceable replaceable assemblies in addition to the means to detect or predict an impending failure. Every automobile owner is familiar with this concept when in their car they recommend to have the oil changed or brakes checked. Even filling up one's car with fuel is a simple example of a failure mode (failure due to fuel exhaustion), a means of detection (fuel gauge), and a maintenance action (filling the car's fuel tank). (The use of a car's odometer to gauge fuel also illustrates the concept of "*redundant sensors*".)

For large scale complex systems, hundreds if not thousands of maintenance actions can result from the failure analysis. These maintenance actions are based on conditions (*e.g.*, gauge reading or leaky valve), hard conditions (*e.g.*, a component is known to fail after 100 hrs of operation with 95% certainty), or require inspection to determine the maintenance action (*e.g.*, metal fatigue). The RCM concept then analyzes each individual maintenance item for its risk contribution to safety, mission, operational readiness, or cost to repair if a failure does occur. Then the sum total of all the maintenance actions are bundled into maintenance intervals so that maintenance is not occurring around the clock, but rather, at regular intervals. This bundling process introduces further complexity, as it might stretch some maintenance cycles, thereby increasing risk, but reduce others, thereby potentially reducing risk, with the end result being a comprehensive maintenance (also called preventive maintenance) schedule, purpose built to reduce operational risk and ensure acceptable levels of operational readiness and availability.

2.3 RISK-BENEFIT ANALYSIS

Risk-benefit analysis, is the comparison of the risk of a situation to its related benefits. Exposure to personal risk is recognized as a normal aspect of everyday life. We accept a certain level of risk in our lives as necessary to achieve certain benefits. With most of these risks we feel we have some sort of control over the situation. For example, driving an automobile is a risk most people take daily. "*The controlling factor appears to be their perception of their individual ability to manage the risk-creating situation.*" Analyzing the risk of a situation is, however, very dependent on the individual doing the analysis. 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.

2.4 SAFETY ANALYSIS TECHNIQUES

Analysis techniques can be split into two categories: qualitative and quantitative methods. Both approaches share the goal of finding causal dependencies between a hazard on system level and failures of individual components. Qualitative approaches focus on the question "*What must go wrong, such that a system hazard may occur ?*", while quantitative methods aim at providing estimations about probabilities, rates and/or severity of consequences. Safety analysis techniques rely solely on skill and expertise of the safety engineer. In the last decade model-based approaches have become prominent. In contrast to traditional methods, model-based techniques try to derive relationships between causes and consequences.

2.5 TESTING METHODS FOR SAFETY

The *two* most common fault modeling techniques are called :

(*i*) failure mode and effects analysis and

(*ii*) fault tree analysis.

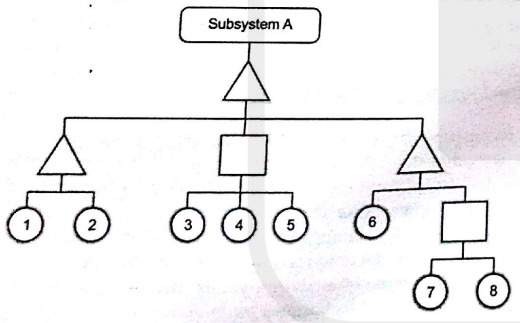
These techniques are just ways of finding problems and for making plans to cope with failures, and the related risk assessment. One of the earliest complete studies (known as Reactor Safety Study) using this technique was carried out on a commercial nuclear plant.

Failure Mode and Effects Analysis (FMEA)

Failure Mode and Effects Analysis (FMEA) is a bottom to top study and inductive analytical method which may be performed at either the functional or piece-part level. For functional FMEA, failure modes are identified for each function in a system or equipment item, usually with the help of a functional block diagram. For piece-part FMEA, failure modes are identified for each piece-part component (such as a valve, connector, resistor and diode etc). The effects of the failure mode are described and assigned a probability, based on the failure rate and failure mode ratio of the function or component. This quantization is difficult for software *i.e.*, a bug exists or not, and the failure models used for hardware components do not apply. Temperature, age and manufacturing variability affect a resistor whereas they do not affect software. Failure modes with identical effects can be combined and summarized in a Failure Mode Effects Summary. When combined with criticality analysis, FMEA is known as Failure Mode, Effects, and Criticality Analysis or FMECA, pronounced *"fuh-MEE-kuh"*.

Fault Tree Analysis (FTA)

Fault tree analysis (FTA) is a top to down study and deductive analytical method. In FTA, initiating primary events such as component failures, human errors, and external events



A typical example of a fault tree diagram

are traced through logic gates to an undesired top event such as an aircraft crash or a nuclear reactor core melt. The intent is to identify ways to make top events less probable, and verify that safety goals have been achieved.

Fault trees are a logical inverse of success trees, and may be obtained by applying de Morgan's theorem to success trees (which are directly related to reliability block diagrams). FTA may be qualitative or quantitative. When failure and event probabilities are unknown, qualitative fault trees may be analyzed for minimal cut sets. For example, if any minimal cut set contains a single base event, then the top event may be caused by a single failure. Quantitative FTA is used to compute top event probability, and usually requires computer software such as CAFTA or SAPHIRE.

Some industries use both fault trees and event trees. An event tree starts from an undesired initiator (loss of critical supply, component failure etc.) and follows further possible system events through and to a series of final consequences. As each new event is considered, a new node on the tree is added with a split of probabilities of taking either branch. The probabilities of a range of "*top events*" arising from the initial event can then be seen.

Usually a failure in *safety-certified systems* is acceptable if, on average, less than one life per 109 hours of continuous operation is lost to failure. Most Western nuclear reactors, medical equipment, and commercial aircraft are certified to this level. The cost versus loss of lives has been considered appropriate at this level (by FAA for aircraft systems under Federal Aviation Regulations).

2.5.1 Containing/Preventing Failure

It is a common practice to plan for the failure of safety systems through containment and isolation methods. The use of isolating valves, also known as the block and bleed manifold, is very common in isolating pumps, tanks, and control valves which may fail or need routine maintenance. In addition, nearly all tanks containing oil or other hazardous chemicals are required to have containment barriers set up around them to contain 100% of the volume of the tank in the event of a catastrophic tank failure. Similarly, in a long pipeline, there are remote-closing valves at regular intervals so that a leak can be isolated. Fault isolation boundaries are similarly designed into critical electronic systems or computer software. The goal of all containment systems is to provide means of mitigating the consequences of failure. Fault isolation might also refer to the extent to which detected failures might be isolated for successful recovery. The isolation level shows the system identity level at which the failure cause can be recovered (often by a replaceable unit).

Once a failure mode is identified, it can usually be mitigated by adding extra or redundant equipment to the system. For example, nuclear reactors contain dangerous radiation, and nuclear reactions can cause so much heat that no substance might contain them. Therefore reactors have emergency core cooling systems to keep the temperature down, shielding to contain the radiation, and engineered barriers (usually several, nested, surmounted by a containment building) to prevent accidental leakage.

Safety-critical systems are commonly required to permit no single event or component failure to result in a catastrophic failure mode. Most biological organisms have a certain amount of redundancy: multiple organs, multiple limbs, etc.

2.5.2 Safety and Reliability

Safety is not reliability. If a medical device fails, it should fail safely ; other alternatives will be available to the surgeon. If an aircraft fly-by-wire control system fails, there is no backup. Electrical power grids are designed for both safety and reliability ; telephone systems are designed for reliability, which becomes a safety issue when emergency calls are to be made.

Probabilistic risk assessment has created a close relationship between safety and reliability. Component reliability, generally defined in terms of component failure rate, and external event probability are both used in quantitative safety assessment methods such as FTA. Related probabilistic methods are used to determine Mean Time Between Failure (MTBF) for the system, system availability and/or probability of mission success or failure. Reliability analysis has a broader scope than safety analysis, wherein non-critical failures are considered. On the other hand, higher failure rates are considered acceptable for non-critical systems.

Safety generally cannot be achieved through component reliability alone. Catastrophic failure probabilities of 10^{-9} per hour correspond to the failure rates of very simple components such as resistors or capacitors. A complex system containing hundreds or thousands of components might be able to achieve a MTBF of 10,000 to 100,000 hours, meaning it would fail at 10^{-4} or 10^{-5} per hour. If a system failure is catastrophic, usually the only practical way to achieve 10^{-9} per hour failure rate is through redundancy. Two redundant systems with independent failure modes, each having an MTBF of 100,000 hours, could achieve a failure rate on the order of 10^{-10} per hour because of the multiplication rule for independent events.

When adding equipment is impractical (usually because of expenses), then the least expensive form of design is often "*inherently fail-safe*" *i.e.*, change the system design so that its failure modes are not catastrophic. Inherent fail-safes are common in medical equipment, traffic and railway signals, communications equipment, and safety equipment.

The typical approach is to arrange the system so that ordinary single failures cause the mechanism to shut down in a safe way (for nuclear power plants, this is termed a passively safe design, although more than ordinary failures are covered). Alternately, if the system contains a hazard source such as a battery or rotor, then it may be possible to remove the hazard from the system so that its failure modes cannot be catastrophic.

One of the most common fail-safe systems is the overflow tube in baths and kitchen sinks. If the valve sticks open, rather than causing an overflow and damage, the tank spills into an overflow. Another common example is, that in an elevator (lift) the cable supporting the car keeps spring-loaded brakes open. If the cable breaks, the brakes grab rails, and the elevator cabin does not fall.

Some systems can never be made fail safe, as continuous availability is needed. For example, loss of engine thrust in flight is dangerous. Redundancy, fault tolerance, or recovery procedures are used for these situations (*e.g.*, multiple independent controlled and fuel fed engines). This also makes the system less sensitive for the reliability prediction errors or quality induced uncertainty for the separate items. On the other hand, failure detection and correction and avoidance of common cause failures becomes here increasingly important to ensure system level reliability.

SUMMARY

- *To assure public safety and welfare it is important that Engineers should understand their responsibilities. It is central to professional conduct, but often an individual engineer faces obstacles in the form of other duties which conflict with it. Safety engineering attempts to reduce the frequency of failures, and to ensure that when failures do occur, the consequences are not life-threatening. The primary goal of safety engineering is to manage risk, eliminate or reduce it to acceptable levels. Safety engineering attempts to reduce the frequency of failures, and to ensure that when failures do occur, the consequences are not life-threatening. Safety engineers consider what undesirable events can occur under what conditions. Failure mitigation can go beyond design recommendations, particularly in the area of maintenance engineering known as Reliability Centered Maintenance (RCM). Risk–benefit analysis, is the comparison of the risk of a situation to its related benefits. The two most common fault modeling techniques are : (i) failure mode and effects analysis (FMEA) is a bottom to top study, and (ii) fault tree analysis (FTA) is a bottom to top study. It is a common practice to plan for the failure of safety systems through containment and isolation methods.*
- *Safety is not reliability, e.g., if a medical device fails, it should fail safely. Component reliability is generally defined in terms of component failure rate.*

Short Question Answers

1. *Write an engineers' responsibility towards society in conduct of his professional duties.*

   Ans. To assure public safety and welfare it is important that Engineers should understand their responsibilities. Sometimes an engineer has to sacrifice one safety concern for another. In some cases, an engineer's duty to maintain client confidentiality can come in conflict with his duty to ensure safety *i.e.*, an engineer sometimes has to make a compromise between safety and cost, but it should not be at the cost of public.

2. *Describe the aspects of safety engineering to manage risks and eliminate/ reduce it.*

   Ans. Safety engineering attempts to reduce the frequency of failures, and to ensure that when failures do occur, the consequences are not life-threatening. Ideally, safety engineering starts during the early design of a system. Safety engineers consider what

undesirable events can occur under what conditions, and project the related accident risk. The exception to this conventional approach is the perspective, known as "system safety". The system safety philosophy is applied to complex and critical systems, such as commercial airliners, complex weapon systems, spacecraft, rail and transportation systems, air traffic control system and other complex and safety-critical industrial systems. There is an entire realm of safety and reliability engineering known as Reliability Centered Maintenance (RCM), which is a discipline that is a direct result of analyzing potential failures within a system and determining maintenance actions that can mitigate the risk of failure.

3. *What is the responsibility of an engineer while designing any system ?*

Ans. Ideally, safety engineering starts during the early design of a system. Safety engineers consider what undesirable events can occur under what conditions, and project the related accident risk. They may then propose or require safety mitigation requirements in specifications at the start of development or changes to existing CAD designs or in-service products to make a system safer. This may be done by full elimination of any type of hazards or by lowering accident risk.

4. *How do you conduct comparison of the risk of a situation to it's related benefits ?*

Ans. Risk–benefit analysis, is the comparison of the risk of a situation to its related benefits. We accept a certain level of risk in our lives as necessary to achieve certain benefits. With most of these risks we feel we have some sort of control over the situation. For example, driving an automobile is a risk most people take daily. "*The controlling factor appears to be their perception of their individual ability to manage the risk-creating situation.*" Analyzing the risk of a situation is, however, very dependent on the individual doing the analysis.

5. *Justify the term "Safety is not reliability".*

Ans. Safety is not reliability because, if a medical device fails, it should fail safely so that, other alternatives can be available to the surgeon. If an aircraft fly-by-wire control system fails, there is no backup. Electrical power grids are designed for both safety and reliability ; telephone systems are designed for reliability, which becomes a safety issue when emergency calls are to be made.

Exercise

1. How can the teachers in the college show students as how to handle conflicts in their profession ?
2. How can proper and reliable maintenance reduce the risks of failure of any system ?
3. Describe in brief traditional methods for safety analysis.
4. In order to contain failure how can we increase safety and reliability of any system ?
5. What are the containment and isolation methods for containing the failure of safety systems ?
6. How is Mean Time Between Failures (MTBF) important for a component, explain ?

2.6 CASE STUDIES OF FAILURE IN SAFETY SYSTEMS

Man has developed science for his comforts and dominance over others and has set up industries, power plants and many other facilities in last few decades. Many industrial accidents /disasters have happened in the world in which lots of lives were lost and there are thousands who are still suffering for years without any respite. Given below are few of the cases which got prominence in news on account of the failure of nuclear plants and equipments and sufferings of mankind at the hands of the installation of industry/facilities.

(*i*) On *December 12, 1952*, a partial meltdown of a reactor's uranium core at the Chalk River plant near Ottawa, Canada, resulted after the accidental removal of four control rods. Millions of gallons of radioactive water poured out of the reactor but, there were no injuries.

(*ii*) In *October, 1957*, fire destroyed the core of a plutonium-producing reactor at Britain's Windscale nuclear complex, sending clouds of radioactivity into the atmosphere. An official report said the leaked radiation caused dozens of cancer deaths in the vicinity of Liverpool.

(*iii*) In *1957-58*, a serious accident occurred near the town of Kyshtym in the Urals. A Russian scientist who first reported the disaster estimated that hundreds died from radiation sickness.

(*iv*) On *January 3, 1961*, three technicians died at a U.S. plant in Idaho Falls in an accident at an experimental reactor.

(*v*) On *July 4, 1961*, radiation spread through the Soviet Union's first nuclear-powered submarine, when a pipe in the control system of one of the two reactors had ruptured. The Captain and seven crew members died.

(*vi*) On October 5, 1966, the core of an experimental reactor near Detroit, Mich., USA melted partially when a sodium cooling system failed.

(*vii*) On *January 21, 1969*, a coolant malfunction from an experimental underground reactor at Lucens Vad, Switzerland, released a large amount of radiation into a cave, which was then sealed.

(*viii*) On *December 7, 1975*, at the Lubmin nuclear power complex on the Baltic coast in the former East Germany, a short-circuit caused by an electrician's mistake started a fire. Some news reports said there was almost a meltdown of the reactor core.

(*ix*) On *March 28, 1979*, near Harrisburg, Pennsylvania, America's worst nuclear accident occurred. A partial meltdown of one of the reactors forced the evacuation of the residents after radioactive gas escaped into the atmosphere. It was later known as Three Mile Island nuclear power plant accident.

(*x*) On *February 11, 1981*, eight workers were contaminated when more than 100,000 gallons of radioactive coolant fluid leaked into the contaminant building of the Tennessee Valley Authority's Sequoyah 1 plant in Tennessee.

(*xi*) On *April 25, 1981*, officials said around 45 workers were exposed to radioactivity during repairs to a plant at Tsuruga, Japan.

(xii) On *April 26, 1986*, the world's worst nuclear accident occurred after an explosion and fire at the Chernobyl nuclear power plant. It released radiation over much of Europe. Thirty-one people died in the immediate aftermath of the explosion. Hundreds of thousands of residents were moved from the area and a similar number are believed to have suffered from the effects of radiation exposure.

(xiii) On *March 24, 1992*, at the Sosnovy Bor station near St. Petersburg, Russia, radioactive iodine escaped into the atmosphere. A loss of pressure in a reactor channel was the source of the accident.

(xiv) In *November 1992*, in France's most serious nuclear accident, three workers were contaminated after entering a nuclear particle accelerator in Forbach without protective clothing. Executives were jailed in 1993 for failing to take proper safety measures.

(xv) In *November 1995*, Japan's Monju prototype fast-breeder nuclear reactor leaked two or three tons of sodium from the reactor's secondary cooling system.

(xvi) In *March 1997*, the state-run Power Reactor and Nuclear Fuel Development Corporation reprocessing plant at Tokaimura, Japan, contaminated at least 35 workers with minor radiation after a fire and explosion occurred.

(xvii) On *September 30, 1999*, an accident at the uranium processing plant at Tokaimura, Japan, exposed fifty-five workers to radiation. More than 300,000 people living near the plant were ordered to stay indoors. Workers had been mixing uranium with nitric acid to make nuclear fuel, but had used too much uranium and set off the accidental uncontrolled reaction.

(xviii) At Fukushima Japan, on *11th March, 2011* following an earthquake of 9 Mw magnitudes, a 15mtrs tsunami disabled the power supply and stopped cooling of three nuclear reactors thus melting all the cores which resulted in release of very high radioactive materials.

2.6.1 The Bhopal Gas Tragedy

(i) Historical Back Ground of the Gas Plant

Union carbide of USA embarked on a mission of devising a product to exterminate a wide range of parasites, which soon came to be known as '*Sevin*'. To manufacture Sevin, phosgene gas was made to react with another gas called monomethylamine. The reaction of these two gases produced a new molecule, MIC, which was one of the most dangerous compounds ever invented in the chemical history. Experiments had shown that animals exposed to MIC vapours would face instantaneous death. MIC was so volatile that as soon as it came into contact with a few drops of water or a few ounces of metal dust, it got off to an uncontrollably violent reaction. No safety system, no matter how sophisticated, would then be able to stop it emitting a fatal cloud into the atmosphere. To prevent explosion, MIC had to be kept permanently at a temperature near zero. Therefore, provision had to be made for the refrigeration of any drums or tanks that were to hold it.

In 1966 the Govt. of India (GOI) granted a license to Union Carbide India Ltd. (UCIL) to produce Sevin and all the required chemical ingredients in India. UCIL's agronomic engineer, felt that manufacturing 5,000 tons of Sevin would require considerable quantities of MIC to be manufactured, but was not in favour of storing huge quantity of MIC. He was also against the proposed site of the factory as it was too close to areas where people lived, as according to municipal planning regulations, no industry likely to give off toxic emissions could be set up on a site where the prevailing wind might carry effluents into densely populated areas. At the plants site wind usually blew toward the slums, the railway station and finally toward the overpopulated parts of the old town. Under such circumstances, the application should have been rejected.

In May 1982, three UCIL engineers came from U.S.A. to Bhopal, to appraise the running of the plant and confirm that everything was functioning according to the laid down standards. The report presented by them revealed that all was not well with the Bhopal plant, so much so, that the surroundings of the site was '*strewn with oily old drums, used piping, pools of used oil and chemical waste likely to cause fire*,' apart from the shoddy workmanship on certain connections, the warping of equipment, the corrosion of several circuits, the absence of automatic sprinklers in the MIC and phosgene production zones. It also reported leaks of phosgene, MIC and chloroform, ruptures in pipework and sealed joints, absence of any earth wire on one of the three MIC tanks and poor adjustment of certain devises where excessive pressure could lead to water entering the circuits. At the same time, the report expressed concern at the inadequately trained staff, unsatisfactory instruction methods and sloppy maintenance reports.

In 1983, the manpower in each shift was cut by half. In the control room, only one man was left to oversee some seventy dials, counters and gauges, which relayed, among other things, the temperature and pressure of the three tanks containing the MIC. According to analysts the plant management did not pay heed to the fact that sixty tons of MIC were stored in the tanks, and violated a fundamental rule, which stipulated that MIC must in all circumstances be kept at a temperature close to zero degree Celsius. In order to save coal and money the flames which in the event of an accident burnt off any toxic gases emitted into the atmosphere day and night at the flare tower were also extinguished. The scrubber cylinder used to decontaminate any gas leaks, was also deactivated.

(ii) The Catastrophe

On the night of December 3rd/4th 1984, forty tons of toxic gases made a poisonous grey cloud from Union Carbide India Limited (UCIL's) pesticide plant at Bhopal which spread throughout the city. It was result of a water carrying catalytic material which entered Methyl Isocyanate (MIC) storage tank. It proved to be a killer gas which spread throughout the city. No alarm from the plant ever sounded a warning and hence no evacuation plan was prepared. When victims arrived at hospitals breathless and blind, doctors did not know how to treat them. Next morning the magnitude of the devastation was observed. Dead bodies of humans and animals blocked the streets, leaves turned black, the smell of burning chilli peppers lingered in the air. As many as 10,000 persons died immediately and 30,000 to 50,000 were critically ill.

(iii) Analysis of the Catastrophe

The catastrophe raised some serious ethical issues. The pesticide factory was built in the midst of densely populated settlements. UCIL chose to store and produce MIC, one of the most deadliest chemicals, in a densely populated Bhopal city. When the uncontrolled reaction started, MIC was flowing through the scrubber (meant to neutralize MIC emissions) at more then 200 times its designed capacity. MIC in the tank was filled to 87% against a maximum permissible limit of 50%. It was not stored at zero degree centigrade as prescribed because due to economic drive all the refrigeration and cooling systems had been shut down five months before the disaster. Vital gauges and indicators in the MIC tank were defective. The flare tower meant to burn off MIC emissions was under repair and the scrubber contained no caustic soda.

The work force for MIC plant in the factory was brought down to half, which had serious consequences on safety and maintenance. Not only the maintenance supervisor's position was eliminated but the period of safety training to workers in the MIC plant was also brought down from 6 months to 15 days. UCIL never provided any information on chemicals like MIC, which caused death of many people due to lack of proper treatment in time.

(iv) Tragedy of Victims

In December 1987, a Bhopal District Court Judge passed an order directing UCIL to pay ₹3.5 billion as interim relief. UCIL challenged this order in the MP high court. The High Court upheld the liability of UCIL for the Bhopal disaster, but reduced the interim compensation to ₹2.5 billion. UCIL appealed to the Supreme Court of India against the High Court order saying, *"No court that we know of in India or elsewhere in the world has previously ordered interim compensation where there is no proof of damages or where liability is strongly contested."* The Supreme Court of India strangely ruled that the $470 million settlement against all claims (*i.e.*, ₹10000 per victim) was just, equitable and reasonable. Thus UCIL escaped with a petty amount as settlement and the lakhs of Indians still continue to suffer the catastrophe heaped upon them by shear deliberate negligence of UCIL management in connivance with the Indian authorities at different levels.

SUMMARY

- *Union carbide (UCIL) of USA embarked on a mission of producing a new molecule "MIC" at Bhopal, which was one of the most dangerous compounds ever invented in the chemical history. Animals exposed to MIC vapours faced instantaneous death. MIC was so volatile that as soon as it came into contact with a few drops of water or a few ounces of metal dust, it got off to an uncontrollably violent reaction. No safety system would then be able to stop it emitting a fatal cloud into the atmosphere. To prevent explosion, MIC had to be kept permanently at a temperature near zero. UCIL engineers came to confirm that everything was functioning according to the laid down standards. The report presented by them revealed that all was not at all well with the Bhopal plant. It also reported leaks of phosgene, MIC and chloroform, ruptures in pipework and sealed joints. The report expressed concern at the inadequately trained staff and sloppy maintenance. In 1983, the manpower in each shift was cut by half. In the control room, only one man was left to*

oversee some seventy dials, counters and gauges, which relayed the temperature and pressure of the three tanks containing the MIC. On the night of December 3rd/4th 1984, forty tons of toxic gases made a poisonous grey cloud from the plant which spread throughout the city. As many as 10,000 persons died immediately and 30,000 to 50,000 were critically ill.

Short Question Answers

1. *How and why the Bhopal Gas Plant set up ?*

   Ans. In 1966 the Govt. of India (GOI) granted a license to Union Carbide India Ltd. (UCIL) to produce Sevin and all the required chemical ingredients in India. Union carbide of USA embarked on a mission of devising a product to exterminate a wide range of parasites, which soon came to be known as 'Sevin'. To manufacture Sevin, phosgene gas was made to react with another gas called monomethylamine. The reaction of these two gases produced a new molecule, MIC, which was one of the most dangerous compounds ever invented in the chemical history.

2. *Describe the accident at the plant and it's after effects.*

   Ans. On the night of December 3rd/4th 1984, forty tons of toxic gases made a poisonous grey cloud from Union Carbide India Limited (UCIL's) pesticide plant at Bhopal. It proved to be a killer gas which spread throughout the city. No alarm from the plant ever sounded a warning and hence no evacuation plan was prepared. When victims arrived at hospitals breathless and blind, doctors did not know how to treat them. Dead bodies of humans and animals blocked the streets, leaves turned black, the smell of burning chilli peppers lingered in the air. As many as 10,000 persons died immediately and 30,000 to 50,000 were critically ill.

3. *How were the gas tragedy victims treated and helped by the administration ?*

   Ans. In December 1987, a Bhopal District Court Judge passed an order directing UCIL to pay ₹3.5 billion as interim relief. UCIL challenged this order first in the MP high court and later in the supreme court.. The High Court reduced the interim compensation to ₹2.5 billion. Later on the Supreme Court of India strangely ruled that the $470 million settlement against all claims (*i.e.*, ₹10000 per victim) was just, equitable and reasonable. Thus UCIL escaped with a petty amount as settlement and the lakhs of Indians still continue to suffer the catastrophe heaped upon them by shear deliberate negligence of UCIL management in connivance with the Indian authorities at different levels.

Exercise

1. What was the UCIL engineers report after the Bhopal Gas Plant in May 1982 ?
2. Mention, which fundamental rules of the plant were broken endangering its safety ?
3. Describe the analysis done after the accident.

2.6.2 Chernobyl Nuclear Power Plant Accident 1986

History of Chernobyl Plant and Site

The Chernobyl Power Complex, consisted of four nuclear reactors of the RBMK-1000 design, units 1 and 2 being constructed between 1970 and 1977, while units 3 and 4 of the same design were completed in 1983. Two more RBMK reactors were under construction at the site at the time of the accident. An artificial lake of some 22 square kilometers, situated beside the river Pripyat, was constructed to provide cooling water for the reactors. At Chernobyl, within a 30 km radius of the power plant, the total population was between 115,000 and 135,000.

The RBMK-1000 is a Soviet-designed and built graphite moderated pressure tube type reactor, using slightly enriched (2% U-235) uranium dioxide fuel. It is a boiling light water reactor, with two loops feeding steam directly to the turbines, without an intervening heat exchanger. Water pumped to the bottom of the fuel channels boils as it progresses up the pressure tubes, producing steam which feeds two 500 MW turbines. The water acts as a coolant and also provides the steam used to drive the turbines. The vertical pressure tubes contain the zirconium alloy clad uranium dioxide fuel, around which the cooling water flows. The moderator, whose function is to slow down neutrons to make them more efficient in producing fission in the fuel, is graphite, surrounding the pressure tubes, A mixture of nitrogen and helium is circulated between the graphite blocks to prevent oxidation of graphite and to improve the transmission of the heat produced by neutron interactions in the graphite to the fuel channel. The core itself is about 7 m high and about 12 m in diameter. In each of the two loops, there are four main coolant circulating pumps, one of which is always on standby. The reactivity or power of the reactor is controlled by raising or lowering 211 control rods, which, when lowered into the moderator, absorb neutrons and reduce the fission rate. The power output of this reactor is 3200 MW. Various safety systems, such as an emergency core cooling system, were incorporated into the reactor design.

The Accident

On 25 April, 1986 prior to a routine shutdown, the reactor crew at Chernobyl 4 began preparing for a test to determine how long turbines would spin and supply power to the main circulating pumps following a loss of main electrical power supply. This test had been carried out at Chernobyl the previous year, but the power from the turbine ran down too rapidly, so new voltage regulator designs were to be tested. A series of operator actions, including the disabling of automatic shutdown mechanisms, preceded the attempted test early on 26 April. By the time that the operator moved to shut down the reactor, the reactor was in an extremely unstable condition.

The interaction of very hot fuel with the cooling water led to fuel fragmentation along with rapid steam production and an increase in pressure. The design characteristics of the reactor were such that substantial damage to even three or four fuel assemblies can – and did - result in the destruction of the reactor. The overpressure caused the 1000 tonnes cover plate of the reactor to become partially detached, rupturing the fuel channels and jamming all the control rods, which by that time were only halfway down. Intense steam generation then spread throughout the whole core (fed by water dumped into the core due to the rupture of the emergency cooling circuit) causing a steam explosion and releasing fission products to the atmosphere. About two to three seconds later, a second explosion threw out fragments from the fuel channels and hot graphite. There is some dispute among experts about the character of this second explosion, but it is likely to have been caused by the production of hydrogen from zirconium-steam reactions.

The graphite (about a quarter of the 1200 tonnes of it was estimated to have been ejected) and fuel became incandescent and started a number of fires, causing the main release of radioactivity into the environment. A total of about 14 EBq (14×10^{18} Bq) of radioactivity was released, over half of it being from biologically-inert noble gases.

About 200-300 tones of water per hour was injected into the intact half of the reactor using the auxiliary feed water pumps but this was stopped after half a day owing to the danger of it flowing into and flooding units 1 and 2. From the second to tenth day after the accident, some 5000 tons of boron, dolomite, sand, clay and lead were dropped on to the burning core by helicopter in an effort to extinguish the blaze and limit the release of radioactive particles.

Impact of the Accident

The accident caused the largest uncontrolled radioactive release into the environment ever recorded for any civilian operation, and large quantities of radioactive substances were released into the air for about 10 days. This caused serious social and economic disruption for large populations in Belarus, Russia and Ukraine. Two radionuclides, the short-lived iodine-131 and the long-lived caesium-137, were particularly significant for the radiation dose they delivered to members of the public.

The next task was cleaning up the radioactivity at the site so that the remaining three reactors could be restarted, and the damaged reactor shielded more permanently. About 200,000 people (*'liquidators'*) from all over the Soviet Union were involved in the recovery and clean-up during 1986 and 1987. They received high doses of radiation, averaging around 100 millisieverts (mSv). Some 20,000 of them received about 250 mSv and a few received 500 mSv. Later, the number of liquidators swelled to over 600,000 but most of these received only low radiation doses.

Effects of the Chernobyl accident on Environment and health. Several organizations have reported on the impacts of the Chernobyl accident, but all have had problems assessing the significance of their observations because of the lack of reliable public health information before 1986. In April 2005, the reports prepared by two expert groups – "*Environment*", coordinated by the IAEA, and "*Health*", coordinated by WHO said that "*apart from this [thyroid cancer] increase, there is no evidence of a major public health impact attributable to radiation exposure even 14 years after the accident*".

Chernobyl today

Chernobyl unit 4 is now enclosed in a large concrete shelter which was erected quickly (by October 1986) to allow continuing operation of the other reactors at the plant. However, the structure is neither strong nor durable. Some 200 tones of highly radioactive material remains deep within it, and this poses an environmental hazard until it is better contained.

The hermetically sealed building will allow engineers to remotely dismantle the 1986 structure that has shielded the remains of the reactor from the weather since the weeks after the accident. It will enable the eventual removal of materials containing nuclear fuel and accommodate their characterization, compaction and packing for disposal. This task represents the most important step in eliminating nuclear hazard at the site – and the real start of decommissioning.

Used Fuel and Wastes

In 1999, a contract was signed for construction of a radioactive waste management facility to store 25,000 used fuel assemblies and other operational wastes, as well as material from units decommissioned anywhere. The contract included a processing facility, able to cut the fuel assemblies and to put the material in canisters, which would be filled with inert gas and welded shut. They would then be transported to dry storage vaults in which the fuel containers would be enclosed for up to 100 years.

The storage area is designed to hold 55,000 m^3 of treated waste which will be subject to radiological monitoring for 300 years, by when the radioactivity will have decayed to such an extent that monitoring is no longer required.

Another contract has been signed for a Liquid Radioactive Waste Treatment Plant, to handle some 35,000 cubic metres of low-and intermediate-level liquid wastes at the site. This will need to be solidified and eventually buried along with solid wastes on site.

Lesson Learned from the Chernobyl Disaster

Leaving aside the verdict of history on its role in melting the Soviet 'Iron Curtain', some very tangible practical benefits have resulted from the Chernobyl accident. The main ones concern reactor safety, notably in Eastern Europe. (The US Three Mile Island accident in 1979 had a significant effect on Western reactor design and operating procedures. While that reactor was destroyed, all radioactivity was contained – as designed – and there were no deaths or injuries.)

While no-one in the West was under any illusion about the safety of early Soviet reactor designs, some lessons learned have also been applicable to Western plants. Certainly the safety of all Soviet-designed reactors has improved vastly. This is due largely to the development of a culture of safety encouraged by increased collaboration between East and West, and substantial investment in improving the reactors.

Modifications have been made to overcome deficiencies in all the RBMK reactors still operating. In these, originally the nuclear chain reaction and power output could increase if cooling water were lost or turned to steam, in contrast to most Western designs. It was this effect which led to the uncontrolled power surge and the destruction of Chernobyl 4. All of the RBMK reactors have now been modified by changes in the control rods, adding neutron absorbers and consequently increasing the fuel enrichment from 1.8 to 2.4% of U-235, making them very much more stable at low power. Automatic shut-down mechanisms now operate faster, and other safety mechanisms have been improved. Automated inspection equipment has also been installed. A repetition of the 1986 Chernobyl accident is now virtually impossible, according to a German nuclear safety agency report.

Many other international programmes were initiated following Chernobyl. The International Atomic Energy Agency (IAEA) safety review projects for each particular type of Soviet reactor are noteworthy, bringing together operators and Western engineers to focus on safety improvements. These initiatives are backed by funding arrangements. The Chernobyl Forum report said that some seven million people or/are now receiving or eligible for benefits as 'Chernobyl victims', which means that resources are not targeting the needy few percent of them.

Conclusion by International Agencies

International Atomic Energy Agency's (IAEA's) International Nuclear Safety Advisory Group (INSAG) accepted the view of the Soviet experts that

> *"the accident was caused by a remarkable range of human errors and violations of operating rules in combination with specific reactor features which compounded and amplified the effects of the errors and led to the reactivity excursion".* In particular, according to the INSAG-1 report: *"The operators deliberately and in violation of rules withdrew most control and safety rods from the core and switched off some important safety systems."*

However, the IAEA's 1992 INSAG-7 report, *The Chernobyl Accident : Updating of INSAG-1*, was less critical of the operators, with the emphasis shifted towards "the contributions of particular design features, including the design of the control rods and safety systems, and arrangements for presenting important safety information to the operators. The accident is now seen to have been the result of the concurrence of the following major factors :

(*i*) specific physical characteristics of the reactor ;

(*ii*) specific design features of the reactor control elements, and

(*iii*) the fact that the reactor was brought to a state not specified by procedures or investigated by an independent safety body.

Most importantly, the physical characteristics of the reactor made possible its unstable behaviour." But the report goes on to say that the International Nuclear Safety Advisory Group remains of the opinion that critical actions of the operators were most ill-judged. As pointed out in INSAG-1, the human factor has still to be considered as a major element in causing the accident.

It is certainly true that the operators placed the reactor in a dangerous condition, in particular by removing too many of the control rods, resulting in the lowering of the reactor's operating reactivity margin (ORM). However, the operating procedures did not emphasise upon the vital safety significance of the ORM but rather treated the ORM as a way of controlling reactor power. It could therefore be argued that the actions of the operators were more a symptom of the prevailing safety culture of the Soviet era rather than the result of recklessness or a lack of competence on the part of the operators.

In what is referred to as his *Testament* – which was published soon after his suicide two years after the accident – Valery Legasov, who had led the Soviet delegation to the IAEA

Post-Accident Review Meeting, wrote: "After I had visited Chernobyl NPP I came to the conclusion that the accident was the inevitable apotheosis of the economic system which had been developed in the USSR over many decades. Neglect by the scientific management and the designers was everywhere with no attention being paid to the condition of instruments or of equipment. When one considers the chain of events leading up to the Chernobyl accident, why one person behaved in such a way and why another person behaved in another etc, it is impossible to find a single culprit, a single initiator of events, because it was like a closed circle."

Although most reports on the Chernobyl accident refer to a number of graphite fires, it is highly unlikely that the graphite itself burned. Numerous tests and calculations have shown that it is virtually impossible to burn high-purity, nuclear-grade graphites. Graphite played little or no role in the progression or consequences of the accident. The red glow observed during the Chernobyl accident was the expected color of luminescence for graphite at 700°C and not a large-scale graphite fire, as some have incorrectly assumed. It is stated : *"The fire teams experienced no unusual problems in using their fire-fighting techniques, except that it took a considerable time to extinguish the graphite fire."*

SUMMARY

- *The April 1986 disaster at the Chernobyl nuclear power plant in Ukraine was the product of a flawed Soviet reactor design coupled with serious mistakes made by the plant operators. The resulting steam explosion and fires released at least 5% of the radioactive reactor core into the atmosphere and downwind. Two Chernobyl plant workers died on the night of the accident, and a further 28 people died within a few weeks as a result of acute radiation poisoning. UNSCEAR says that apart from increased thyroid cancers, "there is no evidence of a major public health impact attributable to radiation exposure 20 years after the accident." Resettlement of areas from which people were relocated is ongoing. The accident destroyed the Chernobyl 4 reactor, killing 30 operators and firemen within three months and several further deaths later. Acute radiation syndrome (ARS) was originally diagnosed in 237 people on-site, of these 28 people died within a few weeks of the accident. Large areas of Belarus, Ukraine, Russia and beyond were contaminated in varying degrees. The Chernobyl disaster was a unique event and the only accident in the history of commercial nuclear power where radiation-related fatalities occurred.*

Short Question Answers

1. *How and where was Chernobyl Nuclear Power Plant set up ?*

Ans. The Chernobyl Power Complex, consisted of four nuclear reactors of the RBMK-1000 design, An artificial lake of some 22 square kilometers, situated beside the river Pripyat, was constructed to provide cooling water for the reactors. At Chernobyl, within a 30 km radius of the power plant, the total population was between 115,000 and 135,000.

2. *Describe briefly it's functional design set up.*

Ans. The RBMK-1000 is a Soviet-designed and built graphite moderated pressure tube type reactor, using slightly enriched (2% U-235) uranium dioxide fuel. It is a boiling light water reactor, with two loops feeding steam directly to the turbines, without an intervening heat exchanger. The water acts as a coolant and also provides the steam used to drive the turbines. The core itself is about 7 m high and about 12 m in diameter. The reactivity or power of the reactor is controlled by raising or lowering 211 control rods. The power output of this reactor is 3200 MW.

3. *What were the impacts/ effects of this accident on the environment ?*

Ans. The accident caused the largest uncontrolled radioactive release into the environment ever recorded for any civilian operation, and large quantities of radioactive substances were released into the air for about 10 days. This caused serious social and economic disruption for large populations in Belarus, Russia and Ukraine. Two radionuclides, the short-lived iodine-131 and the long-lived caesium-137, were particularly significant for the radiation dose they delivered to members of the public.

4. *Describe the steps taken to eliminate nuclear hazard at the accident site.*

Ans. Chernobyl unit 4 is now enclosed in a large concrete shelter which was erected quickly (by October 1986) to allow continuing operation of the other reactors at the plant. However, the structure is neither strong nor durable. Some 200 tones of highly radioactive material remains deep within it, and this poses an environmental hazard until it is better contained. The hermetically sealed building will allow engineers to remotely dismantle the 1986 structure that has shielded the remains of the reactor. It will enable the eventual removal of materials containing nuclear fuel and accommodate their characterization, compaction and packing for disposal.

5. *What steps have been taken to take care of the used fuel and nuclear waste ?*

Ans. In 1999, a contract was signed for construction of a radioactive waste management facility to store 25,000 used fuel assemblies and other operational wastes, as well as material from units decommissioned anywhere. The cut fuel assemblies will be put the material in canisters, which would be filled with inert gas and welded shut and transported to dry storage vaults in which the fuel containers would be enclosed for up to 100 years. The storage area is designed to hold 55,000 m3 of treated waste which will be subject to radiological monitoring for 300 years, by when the radioactivity will have decayed to such an extent that monitoring is no longer required.

Exercise

1. Describe in brief the accident that took place at Chernobyl Nuclear Power Plant in Year 1986.
2. What safety precautions have been taken to stop radiation from the Chernobyl Nuclear Power Plant and the used fuel nuclear waste produced ?
3. Write and describe the conclusion drawn by the International Atomic Energy Agency after the accident review.
4. What lesson did the world learn from the Chernobyl Nuclear Power Plant disaster ?

2.6.3 The Three Mile Island Nuclear Power Plant Accident

The Three Mile Island (TMI) nuclear power plant is located in central Pennsylvania about 10 miles south of Harrisburg in Londonderry Township U.S.A. It was named after the island on which it was situated on the Susquehanna River near Harrisburg. It was constructed between years 1968 to 1970. Before the 1979 accident at Pennsylvania's Three Mile Island, few had heard of the nuclear power plant on the Susquehanna River. But the crisis that began years ago in the early morning of March 28 quickly turned the plant and its giant cooling towers into icons. The accident at Three Mile Island, though minuscule in its health consequences, had widespread and profound effects on the American nuclear power industry. It resulted in the immediate (though temporary) closing of seven operating reactors like those at Three Mile Island. A moratorium on the licensing of all new reactors was also temporarily imposed, and the whole process of approval for new plants by the Nuclear Regulatory Commission was significantly slowed for years after the accident.

The Cause of Accident

The incident began at 4:00 a.m. on March 28, 1979 because due to an unknown reason, the feed pump (in the turbine water loop) stopped operating. Without this pump, the turbine water could not remove heat from the steam generator. When this happened, the control rods automatically dropped into the reactor stopping the fission process. However, the radioactive fission products still produced heat so the temperature and pressure started to rise. To reduce the pressure, the valve on the pressurizer, called the pilot-operated relief valve (PORV), opened. Up to this time, everything operated as designed.

When the pressure in the pressurizer dropped to a prescribed value, the PORV was supposed to close but it did not. The accident was now underway. The control panel had an indicator that showed the valve to have closed, (*i.e.*, power was going to the valve to close it) but there was no way to determine that the valve was actually closed or not. With the valve open, steam and water escaped the pressurizer ; this water flowed into a drain tank.

When the feed pump failed, the emergency feed pump should have automatically turned on to keep the turbine water flowing. That pump was tested 42 hours prior to the incident and was functional. However, to perform the test, workers must close a valve, perform the test, and then open it. Apparently the workers forgot to open the valve so the emergency water did not flow. Now the reactor was losing water and getting hotter. With the loss of water (and no air or steam in the pressurizer) the pressure dropped.

When the pressure dropped, some of the water in the reactor turned to steam. This had two major consequences ; first it forced water into the pressurizer and filled it completely, and second, steam instead of water surrounded the reactor fuel. Steam does not conduct heat as well, as water, so the fuel pellets heated up.

In case of an accident, a nuclear power plant has tanks of water with pumps that can quickly introduce water to cool the reactor. One of these automatically started. This was noted by the operators, but then they looked at the indicators for the pressurizer, these indicators

were showing that the pressurizer was full of water (it was because of the steam and not water in the reactor core area). A full pressurizer means that the operators cannot control the pressure, so they turned off the entering water.

Now the situation went from bad to worse. About 100 minutes after the accident started, steam bubbles appeared in the coolant pumps, causing them to vibrate. Fearing a complete failure of these pumps, the operators turned them off. With no water flowing into the reactor and a mixture of water and steam escaping the reactor, large portions of the reactor core became uncovered. With no water to remove the heat, the fuel pellets started to melt, resulting in a partial meltdown.

Finally, one operator surveyed the data and concluded that the PORV was open, so at 6:18 a.m., they closed the valve and then introduced water into the reactor, thus ending the immediate emergency. However, between the time that the operators shut off the pumps and when the valve was closed, the core was uncovered, enough to cause some fuel to melt. In fact, at the time of the accident, nobody thought that a major portion of the fuel had melted. When the reactor was opened months later, they were surprised to find that about 60% of the core actually melted.

While the reactor core was melting, the hot zirconium (that held the fuel) was reacting with the water. This chemical reaction produced hydrogen gas, which is combustible. Some of the hydrogen gas escaped from the reactor into the containment building. The operators were unaware of the presence of hydrogen until something ignited the hydrogen at about 2:00 p.m. Burning of Hydrogen lasted for six to eight seconds, but did no damage to any systems in the building. Although the reactor vessel still contained hydrogen, yet nobody seemed to address this problem in light of other, more serious, problems. When somebody gave it a thought two days later, the great fear was that the hydrogen might explode causing a breach of the reactor vessel and maybe of the containment building. Once the presence of hydrogen was verified, the hydrogen was sent though neutralizers and by the fourth day most of the hydrogen was gone. Actually the fear of an explosion was unfounded. To burn, hydrogen must combine with oxygen, but no oxygen was present in the reactor vessel. However, the fear of an explosion caused many of the public to evacuate the area around TMI.

During these first few hours of the accident, all the action occurred in the reactor building. However, the water that escaped through the pressurizer valve had filled the drain tank and overflowed onto the floor in the Auxiliary Building. Because the core had been uncovered resulting in some core melt, radioactivity had escaped to the reactor water and some of that water was now in the Auxiliary Building. Some of the radioactivity was in the form of xenon and krypton (noble gases) and iodine. The gasses could not be contained so they soon leaked into the atmosphere, thus exposing the public to radiation from the radioactivity in the air. Although the release stacks on the Auxiliary building contained radiation monitors, they were designed for much smaller releases. Therefore the actual radioactivity that was released was never measured, but from later calculations, the scientific community estimated that about 17 million Curies escaped the reactor and transported to the Auxiliary building. The Auxiliary building served as something like a holding tank which allowed some of the radioactivity to decay before entering the atmosphere. As a result, a little more than half *i.e.*, 9 million Curies, made it to the environment.

As a result of these noble gas releases, the public received some radiation dose. The actual dose received by any one person will never be known, but experts, according to testimony in the TMI Litigation, gave limits in the 25 to 50 mrem range.

Human Factors Responsible

Critical human factors and user interface engineering problems were revealed in the investigation of the reactor control system's user interface. Despite the valve being stuck open, a light on the control panel indicated that the valve was closed. In fact the light did not indicate the actual position of the valve, but only the status of the valve solenoid, thus giving false evidence of a closed value. As a result, the operators did not correctly diagnose the problem for several hours.

The design of the PORV indicator light was fundamentally flawed. The bulb was simply connected in parallel with the valve solenoid, thus implying that the PORV was shut when it went dark, without actually verifying the real position of the valve. When everything was operating correctly, the indication was true and the operators became habituated to rely on it. However, when things went wrong and the main relief valve stuck open, the unlighted lamp was actually misleading the operators by implying that the valve was shut. This caused the operators considerable confusion, because of the pressure, temperature and coolant levels in the primary circuit. If the PORV was shut, operators could have observed it via their instruments which were not functioning as they should have. This confusion contributed to the severity of the accident because the operators were unable to break out of a cycle of assumptions and confusions which conflicted with, what their instruments were telling them. It was not until a fresh shift came in, who did not have the mind-set of the first shift of operators, that the problem was correctly diagnosed. By this time, major damage had occurred.

The operators had not been trained to understand the ambiguous nature of the PORV indicator and to look for alternative confirmation that the main relief valve was closed. There was a temperature indicator downstream of the PORV in the tail pipe between the PORV and the pressurizer that could have told them the valve was stuck open, by showing that the temperature in the tail pipe remained higher than it should have been had the PORV been shut. This temperature indicator, however, was not part of the "safety grade" suite of indicators designed to be used after an incident, and the operators had not been trained to use it. Its location on the back of the desk also meant that it was effectively out of sight of the operators.

Consequences of Stuck Valve

The pressure in the primary system continued to decrease and reactor coolant continued to flow in boiling state inside the core. Small bubbles of steam formed and immediately collapsed, which is known as nucleate boiling. As the system pressure decreased further, steam pockets began to form in the reactor coolant. This departure from nucleate boiling (DNB) caused steam voids in coolant channels, blocking the flow of liquid coolant and greatly increasing the fuel cladding temperature. As the volume of these steam voids

increased much more quickly than coolant was lost, the overall water level inside the pressurizer rose despite the loss of coolant through the open PORV. Because of the lack of a dedicated instrument to measure the level of water in the core, operators judged the level of water in the core solely by the level in the pressurizer. Since it was high, they assumed that the core was properly covered with coolant, unaware that because of steam forming in the reactor vessel, the indicator provided misleading readings. Indications of high water levels contributed to the confusion, as operators were concerned about the primary loop "*going solid*," (*i.e.*, no air pocket buffer existed in the pressurizer) which in training they had been instructed to never allow. This confusion was a key contributor to the initial failure to recognize the accident as a loss-of-coolant accident, and led operators to turn off the emergency core cooling pumps, which had automatically started after the PORV stuck and core coolant loss began, due to fears the system was being overfilled. With the PORV still open, the pressurizer relief tank that collected the discharge from the PORV overfilled, causing the containment building sump to fill and sound an alarm at 4:11 a.m. This alarm, along with higher than normal temperatures on the PORV discharge line and unusually high containment building temperatures and pressures, were clear indications that there was an ongoing loss-of-coolant accident, but these indications were initially ignored by operators. At 4:15 a.m., the relief diaphragm of the pressurizer relief tank ruptured, and radioactive coolant began to leak out into the general containment building. This radioactive coolant was pumped from the containment building sump to an auxiliary building, outside the main containment, until the sump pumps were stopped at 4:39 AM.

After almost 80 minutes of slow temperature rise, the primary loop's four main reactor coolant pumps began to cavitate a steam bubble/water mixture, rather than water. The pumps were shut down, and it was believed that natural circulation would continue the water movement. Steam in the system prevented its flow through the core, and as the water stopped circulating it was converted to steam in increasing amounts. About 130 minutes after the first malfunction, the top of the reactor core was exposed and the intense heat caused a reaction to occur between the steam forming in the reactor core and the Zircaloy nuclear fuel rod cladding, yielding zirconium dioxide, hydrogen, and additional heat. This reaction melted the nuclear fuel rod cladding and damaged the fuel pellets, which released radioactive isotopes to the reactor coolant, and produced hydrogen gas that is believed to have caused a small explosion in the containment building later that afternoon.

At 6 am, there was a shift change in the control room. A new team arrival noticed that the temperature in the PORV tail pipe and the holding tanks was excessive and used a backup valve – called a "*block valve*" – to shut off the coolant venting via the PORV, but around 12000 litres of coolant had already leaked from the primary loop. It was not until 165 minutes after the start of the problem that radiation alarms activated when contaminated water reached detectors. By that time, the radiation levels in the primary coolant water were around 300 times expected levels, and the plant was seriously contaminated.

At 6:56 a.m., station manager announced a general emergency, defining it to have the "*potential for serious radiological consequences to the general public*". The uncertainty of operators at the plant was reflected in fragmentary, ambiguous, or contradictory statements made by

government agencies stating that though there had been a small release of radiation, no increase in normal radiation levels had been detected. In fact, readings from instruments at the plant and off-site detectors had detected radioactivity releases, at levels that were unlikely to threaten public health as long as they were temporary, and providing that containment of the then highly contaminated reactor was maintained.

After receiving word of the accident Nuclear Regulatory Commission (NRC) activated emergency response at headquarters in Bethesda, Maryland and sent staff members to Three Mile Island. Initially it viewed the accident, as a "cause for concern but not with an alarm" and informed the White House staff.

In a 2009 article, it was stated that it took five weeks to learn that "*the reactor operators had measured fuel temperatures near the melting point*" and it was not learnt for years, until the reactor vessel was physically opened that by the time the plant operator called emergency roughly half of the uranium fuel had already melted.

It was still not clear to the control room staff that the primary loop water levels were low and that over half of the core was exposed. A group of workers took manual readings from the thermocouples and obtained a sample of primary loop water. Seven hours into the emergency, new water was pumped into the primary loop and the backup relief valve was opened to reduce pressure so that the loop could be filled with water. After 16 hours, the primary loop pumps were turned on once again, and the core temperature began to fall. A large part of the core had melted, and the system was still dangerously radioactive.

On the third day following the accident, a hydrogen bubble was discovered in the dome of the pressure vessel, and became the focus of concern. A hydrogen explosion might not only breach the pressure vessel, but, depending on its magnitude, might compromise the integrity of the containment vessel leading to large scale release of radioactive material. However, it was determined that there was no oxygen present in the pressure vessel, a prerequisite for hydrogen to burn or explode. Immediate steps were taken to reduce the hydrogen bubble, and by the following day it was significantly smaller. Over the next week, steam and hydrogen were removed from the reactor using a catalytic re-combiner and, controversially, by venting straight to the atmosphere.

Release of Radioactive Material

Once the first line of containment is breached during a reactor plant accident, there is a possibility that the fuel or the fission products held inside may escape into the environment. This was evidenced by the radiation alarms that eventually sounded. However, since very little of the fission products released were solids at room temperature, very little radiological contamination was reported in the environment. No significant level of radiation was attributed to the TMI-2 accident outside of the TMI-2 facility. The vast majority of the radioisotopes released were the noble gases xenon and krypton.

The United States Environmental Protection Agency (EPA) analysis concluded that the accident did not raise radioactivity far above safe levels to cause even one additional cancer death among the people in the area, but measures of beta radiation were not included. The EPA found no contamination in water, soil, sediment or plant samples.

Investigations and report of Nuclear Regulatory Commission

Several state and federal government agencies mounted investigations into the crisis, the most prominent of which was the President's Commission on the Accident at Three Mile Island, created by Jimmy Carter in April 1979. The commission consisted of a panel of twelve people, specifically chosen for their lack of strong pro- or anti-nuclear views. It was instructed to produce a final report within six months, and after public hearings, depositions, and document collection, it released a completed study on October 31, 1979. The investigation strongly criticized for lapses in quality assurance and maintenance, inadequate operator training, lack of communication of important safety information, poor management, and complacency, but avoided drawing conclusions about the future of the nuclear industry. The heaviest criticism from the Commission concluded that "fundamental changes were necessary in the organization, procedures, practices 'and above all – in the attitudes' of the NRC and the nuclear industry. It said that the actions taken by the operators were "*inappropriate*" but that the workers "*were operating under procedures that they were required to follow, and our review and study of those indicates that the procedures were inadequate*" and that the control room "*was greatly inadequate for managing an accident*". The Commission notes that PORV valve had previously failed on 11 occasions, nine of them in the open position, allowing coolant to escape.

SUMMARY

- *On March 28, 1979, the plant experienced a failure in the secondary, section (one of two reactors on the site). The main feed water pumps stopped sending water to the steam generators. Immediately, the pressure in the primary system (the nuclear portion of the plant) began to increase. In order to control that pressure, the pilot-operated relief valve opened. The valve should have closed when the pressure fell to proper levels, but it became stuck open and cooling water started pouring out of the stuck-open valve, whereas instruments in the control room indicated to the plant staff that the valve was closed. There was no instrument that showed how much water covered the core and plant staff assumed that the core was properly covered with water. The water escaping through the stuck valve reduced primary system pressure so much that the reactor coolant pumps had to be turned off to prevent dangerous vibrations. To prevent the pressurizer from filling up completely, the staff reduced emergency cooling water being pumped in to the primary system. These actions starved the reactor core of coolant, causing it to overheat. Without the proper water flow, the nuclear fuel overheated to the point at which the zirconium cladding (the long metal tubes that hold the nuclear fuel pellets) ruptured and the fuel pellets began to melt. Authorities did not know that the core had melted, but they immediately took steps to try to gain control of the reactor and ensure adequate cooling to the core. By the evening of March 28, the core appeared to be adequately cooled and the reactor appeared to be stable. But on March 30, a significant release of radiation from the plant's auxiliary building caused a great deal of confusion. Within a short time, chemical reactions in the melting fuel created a large hydrogen bubble in the dome of the pressure vessel, which could explode and rupture the pressure vessel and cause a breach of containment. However, the crisis ended when experts determined on Sunday, April 1, that the bubble could not burn or explode because of the absence of oxygen in the pressure vessel.*

Short Question Answers

1. *How and why did the Three Mile Island become famous ?*

   Ans. The Three Mile Island (TMI) nuclear power plant was named after the island on which it was situated on the Susquehanna River near Harrisburg, USA. Before the 1979 accident at Pennsylvania's Three Mile Island, few had heard of the nuclear power plant on the Susquehanna River. But the crisis that began years ago in the early morning of March 28 quickly turned the plant and its giant cooling towers into icons.

2. *Describe in brief the main cause of nuclear power plant accident at the Three Mile Island.*

   Ans. Due to an unknown reason, the feed pump (in the turbine water loop) stopped operating. Without this pump, the turbine water could not remove heat from the steam generator. The control rods automatically dropped into the reactor stopping the fission process. However, the radioactive fission products still produced heat so the temperature and pressure started to rise. To reduce the pressure, the valve on the pressurizer, called the pilot-operated relief valve (PORV), opened. When the pressure dropped, the PORV was supposed to close but it did not. The control panel indicated that the valve had closed but the valve was actually not closed. With the valve open, steam and water escaped the pressurizer ; this water flowed into a drain tank. When the feed pump failed, the emergency feed pump should have automatically turned on to keep the turbine water flowing, but it did not, because the workers forgot to open the valve. With the loss of water the pressure dropped, some of the water in the reactor turned to steam. This had two major consequences ; first it forced water into the pressurizer and filled it completely, and second, steam instead of water surrounded the reactor fuel so the fuel pellets heated up. Operators looked at the indicators for the pressurizer, which were showing that the pressurizer was full of water (it was because of the steam and not water in the reactor core area). A full pressurizer means that the operators cannot control the pressure, so they turned off the entering water. About 100 minutes after the accident started, steam bubbles appeared in the coolant pumps, causing them to vibrate. Fearing a complete failure of these pumps, the operators turned them off. With no water flowing into the reactor and a mixture of water and steam escaping the reactor, large portions of the reactor core became uncovered. With no water to remove the heat, the fuel pellets started to melt, resulting in a partial meltdown and release of radiation.

3. *What role could have been played by presence of hydrogen gas ?*

   Ans. While the reactor core was melting, the hot zirconium (that held the fuel) was reacting with the water. This chemical reaction produced hydrogen gas, which is combustible. Some of the hydrogen gas escaped from the reactor into the containment building. The operators were unaware of the presence of hydrogen until something ignited the hydrogen. The great fear was that the hydrogen might explode causing a breach of the reactor vessel and maybe of the containment building. Once the presence of hydrogen was verified, the hydrogen was sent though neutralizers and by the fourth day most of the hydrogen had dissipated.

4. *Describe the effects of this accident on the environment and the people around.*

   Ans. During this accident, all the action occurred in the reactor building. The water that escaped through the pressurizer valve filled the drain tank and over flowed in the Auxiliary Building. Because the core had melted, radioactivity escaped to the reactor water. Some of the radioactivity was in the form of xenon and krypton (noble gases) and iodine. The gasses could not be contained so they soon leaked into the atmosphere, thus exposing the public to radiation from the radioactivity in the air. The Auxiliary building served as something like a holding tank which allowed some of the radioactivity to decay before entering the atmosphere. A little more than half made it to the environment. As a result of these noble gas releases, the public received some radiation dose.

5. *How did the flawed pilot operated relief valve create confusion for the plant operators ?*

   Ans. The design of the PORV indicator light was fundamentally flawed because, the bulb was simply connected in parallel with the valve solenoid, thus implying that the PORV was shut when it went dark, without actually verifying the real position of the valve. When everything was operating correctly, the indication was true and the operators became habituated to rely on it. However, when things went wrong and the main relief valve stuck open, the unlighted lamp was actually misleading the operators by implying that the valve was shut.

6. *What were the findings of Nuclear Regulatory Commission of USA on this accident ?*

   Ans. The commission consisted of a panel of twelve people, specifically chosen for their lack of strong pro- or anti-nuclear views, which released its report on October 31, 1979. The investigation strongly criticized for lapses in quality assurance and maintenance, inadequate operator training, lack of communication of important safety information, poor management, and complacency. It said that the actions taken by the operators were "*inappropriate*" but that the workers "*were operating under procedures which were inadequate*" and that the control room "*was also greatly inadequate for managing an accident.*" The Commission noted that PORV valve had also failed on 11 previous occasions, nine of them in the open position, allowing coolant to escape.

Exercise

1. Analyse the human factors as cause accident at Three Mile Island.
2. What were consequences of water turning into steam when pressure dropped in the reactor ?
3. How did the reactor water contaminate the auxiliary building ?
4. What is the function of the pilot operator relief valve indicator in a nuclear power plant ? How did it matter in the nuclear power plant accident ?
5. Describe the consequences of the stuck valve.
6. What were the findings of the Environmental Regulatory Commission ?

2.6.4 The Space Shuttle "*Challenger*" Disaster

In March 1970, President Nixon made an important political choice. For budgetary reasons, he scrapped the Mars project and the space platform, but he ordered the development of the shuttle vehicle. Thus the reusable space shuttle, earlier considered only the transport element of a broad, multi-objective space plan, becam' the focus of NASA's team for the near future.

This decision forced NASA to put all its eggs in one basket ; it significantly shaped NASA's goals for the future. From this point on, to prove that the shuttle could be used as a universal launch vehicle, NASA tried to create an operational shuttle system by instituting a heavy schedule of flights.

President Ronald Reagan, in an important policy speech on the national space policy on July 5, 1982, increased the pressure on NASA when he declared that the shuttle was "fully operational". The administration was eager for the shuttle system to become operational because it had developed some rather ambitions commercial and military goals for NASA. One of these goals was for NASA to become an economically self-sufficient cargo hauler, primarily of communication satellites. Thus NASA found itself in the business of launching satellites for a wide variety of customers. Thus as a result of it pressures in NASA increased, perhaps at the expenses of engineering considerations.

Pressures developed because of the need to meet customer's commitments, which translated into a requirement to launch a certain number of flights per year and to launch them on time. Such considerations may occasionally have obscured engineering concerns.

It is evident, that NASA was subjected to strong external pressures to accept very ambitious goals. These goals were internalized within the organizational structure of NASA. The agency committed itself to a frenetic pace of launchings in the 1980,s so much so, that at one point proposing 714 flights between 1978 and 1990. This pressure was undoubtedly felt by individuals at NASA and such external pressures were internalized as organizational goals by NASA, zeroing in on individual decision makers and setting the stage for the challenger explosion.

Structural Strains within NASA

As NASA attempted to meet the increasing flight schedule of the space shuttle and achieve the commercial and military goals that had been laid out for it, the agency encountered a number of constraints and operational problems. These constraints made it increasingly difficult for NASA to reach its goals in an acceptable way, *i.e.*, with the high level of safety expected of it and resorting to means which were less safe.

> *"The genesis of the Challenger accident was the failure of the joint of the right solid rocket motor-began with decisions made in the design of the joint and in the failure of both Thiokol and NASA's solid booster project team to understand and respond to facts obtained during testing. The Commission has concluded that neither Thiokol nor NASA responded adequately to internal warnings about the faulty seal design.*

> *Furthermore, Thiokol and NASA did not make a timely attempt to develop and verify a new seal after the initial design was shown to be deficient."* While NASA worked on solving the problem, it continued with determination to fly, and defined the risk as "*acceptable*" and "*unavoidable.*"

It had put the whole future of the space program on the shuttle. There was no way out. Overwhelming problems were just denied. The safety, reliability, and quality-assurance workforce at NASA had been reduced, which seriously limited NASA's capability in these vital functions.

The Space Shuttle Challenger-disaster occurred on January 28, 1986, when Space Shuttle Challenger (mission STS-51-L) broke apart 73 seconds into its flight, leading to the deaths of its seven crew members. The spacecraft disintegrated over the Atlantic Ocean, off the coast of Cape Canaveral, Florida at 11:38 EST (Eastern Standard Time). Disintegration of the vehicle began after an O-ring seal in its right solid rocket booster (SRB) failed at liftoff. The O-ring failure caused a breach in the SRB joint it sealed, allowing pressurized hot gas from within the solid rocket motor to reach outside and impinge upon the adjacent SRB attachment hardware and external fuel tank. This led to the separation of the right-hand SRB's aft attachment and the structural failure of the external tank. Aerodynamic forces broke up the orbiter.

The crew compartment and many other vehicle fragments were eventually recovered from the ocean floor after a lengthy search and recovery operation. The exact timing of the death of the crew is unknown ; several crew members are known to have survived the initial breakup of the spacecraft. The shuttle had no escape system, and the impact of the crew compartment with the ocean surface was too violent for survival.

The disaster resulted in a 32-month halt in the shuttle program and the formation of the Rogers Commission, a special commission appointed by United States President Ronald Reagan to investigate the accident. The Rogers Commission found NASA's organizational culture and decision-making processes to be the key contributing factors to the accident. NASA managers knew that contractor Morton Thiokol's design of the SRBs contained a potentially catastrophic flaw in the O-rings since 1977, but failed to address it properly. They also disregarded warnings from engineers about the dangers posed by the low temperatures on the morning of launching date and failed to adequately report these technical concerns to their superiors.

Challenger was originally set to launch from KSC in Florida at 14:42 Eastern Standard Time (EST) on January 22. Delays in the previous mission, STS-61-C, caused the launch date to be moved to January 23 and then to January 24. Launch was then rescheduled to January 25 due to bad weather at the Transoceanic Abort Landing (TAL) site in Dakar, Senegal. NASA decided to use Casablanca as the TAL site, but because it was not equipped for night landings, the launch had to be moved to the morning (Florida time). Predictions of unacceptable weather at KSC on January 26, caused the launch to be rescheduled for 09:37 EST on January 27.

The launch was delayed the next day, due to problems with the exterior access hatch. First, one of the micro-switch indicators which were used to verify that the hatch was safely locked, malfunctioned. Then, a stripped bolt prevented the crew from removing a closing fixture of the orbiter's hatch. By the time repair personnel had sawed the fixture off, crosswinds at the Shuttle Landing Facility exceeded the limits for a Return to Launch Site (RTLS) and the crew waited for winds to die down, forcing another rescheduling.

Thiokol-NASA Conference Call

Forecasts for January 28 predicted an unusually cold morning, with temperature close to 31°F (–1°C), the minimum temperature permitted for launch. The low temperatures had prompted concerns from Thiokol engineers. At a teleconference on the evening of January 27, Thiokol engineers and managers discussed the whether conditions with NASA managers from Kennedy Space Center and Marshall Space Flight Center. Several engineers re-expressed their concerns about the effect of low temperatures on the resilience of the rubber O-rings that sealed the joints of the SRBs, and recommended a launch postponement. They argued that they did not have enough data to determine whether the joints would properly seal if the O-rings were colder than 53°F (12°C). This was an important consideration, since the SRB O-rings had been designated as a "*Criticality 1*" component, meaning that there was no backup if both the primary and secondary O-rings failed, and their failure would destroy the challenger shuttle and the crew.

Thiokol management initially supported its engineers' recommendation to postpone the launch, but NASA staff opposed a delay. One argument by NASA personnel contesting Thiokol's concerns was that if that primary O-ring failed, the secondary O-ring would still seal. Although this statement was unproven, yet it was placed as an argument which could not be applied to a "*Criticality 1*" component.

NASA did not know of Thiokol's earlier concerns about the effects of the cold on the O-rings, and did not understand that Rockwell International, the shuttle's prime contractor, viewed the large amount of ice present on the pad as a constraint to launch. Due to NASA's opposition, Thiokol management reversed itself and recommended that the launch may proceed as scheduled.

The skies were clear and the sun shone on the cold freezing morning of January 28, 1986. Kennedy Space Center in Florida was busy preparing the launch of the 25th space shuttle into space. Mission STL-51-L was the 10th flight of Orbiter Challenger. This was one of the most publicized launches because it was for the first time that a civilian, a school teacher, was going into space. The launch of challenger had been delayed five times due to bad weather, whereas January 28 was the coldest day that NASA had ever launched a shuttle.

The temperature at ground level at Pad 39B was 36°F, *i.e.*, 15°F cooler than any other previous launch by NASA. The Solid Rocket Boosters (SRB) was ignited, and the thundering noise started. At 0.68 seconds after ignition, videotape showed black smoke coming from the aft (bottom) field joint of the right SRB. The aft field joint is the lower portion of the SRB. The black smoke suggested that grease, joint insulation and rubber O-ring were burning.

The smoke continued to come from the aft field joint facing the Exterior Tank, with a cycle of 3 puffs of smoke per second. The last puff of smoke was seen at 2.7 seconds. The black smoke was an indication that the aft field joint was not sealing correctly. Later in flight, flashes were seen on Challenger. Three bright flashes shot across the challenger's wings, 45 seconds after lift-off. Each of the three flashes lasted only 1/13 of a second. As these flashes had been seen on other shuttle missions, therefore were not considered as problems. These bright flashes were completely unrelated to the flame that was seen later in flight.

At 58.8 seconds into flight, on an enhanced film, a flame was seen coming from the right SRB. The flame was coming from the aft center and aft joint, at 305° around the circumference of the SRB. The flame was burning gas that was escaping from the SRB. A fraction of a second later, at 59.3 seconds, the flame was well defined, and could be seen without enhanced film. As the flame increased in size, it began to push against the External Tank by rushing the air around the Orbiter. The SRB is attached to the External Tank by a series of struts along the side the External Tank. One of these struts is located at 310° of the circumference of the SRB. The flame as it grew pushed against this strut, with an intense heat of 5600°F, making it hot and weak.

The first sight that the flame was hitting the External Tank was at 64.7 seconds, when the color of the flame changed. Change in the flame colour indicated that it was on account of mixing with another substance. This other substance was liquid Hydrogen which is stored in the External Tank. The External Tank stores Hydrogen and oxygen in two tanks. The top tank containing Oxygen and the bottom one containing Hydrogen. Pressure changes in the Hydrogen tank confirmed there was leakage. Forty-five milliseconds after the color change, a small glowing light developed between the External Tank and Challenger's black tiles.

From 72 seconds onwards there was a very sudden chain of events that destroyed Challenger and the seven crew members on board. All of these events happened in less than two seconds. By now the lower strut, connecting the right SRB to the External Tank was extremely hot and very weak. With the amount of force given by the SRB, the lower strut broke away from both the right SRB and the External Tank, allowing the right SRB to rotate freely around the top struts. The SRB was out of control, the bottom of the SRB swung around hitting, burning and denting Challengers wing. At 73.12 seconds into flight a white vapor was seen from the bottom corner of the right SRB. The External Tank had become weak due to the intense heat given by the flame. The dome structure under the External Tank failed and fell. The tank of Hydrogen inside the External Tank ruptured and released the liquid Hydrogen contents. With the sudden absence of Hydrogen, there was an extreme force that shot the Hydrogen tank forward into the Oxygen tank, which too burst.

As the two inter-tanks collided, the top of the right SRB on the outside hit the top of the External Tank, and also broke the Oxygen tank. The white vapour seen was the mixture of Hydrogen and Oxygen. At 73.14 seconds, all the structures failed. Only milliseconds after the white vapour was seen from the right SRB, the glow had turned to a fireball in a huge

explosion. The main explosion was the Hydrogen and Oxygen that come from the External Tank. Challenger was traveling at a speed of Mach 1.92, at a height of 46,000 feet when it blew up. The last recorded transmission from Challenger was at 73.62 seconds after launch, when it truly fell apart.

Just before challenger had blown up, it was engulfed in a cloud of smoke, that grew larger after the explosion. From under the gray smoke of the explosion, a red smoke was spreading. This red smoke was the reaction control system burning from the wreckage from challenger. Debris from challenger was seen falling and racing towards the ocean. Both of the SRBs flew in opposite directions out of the fireball and cloud. The explosives on the SRB were detonated by the United States Air Force Safety Commander, 110.25 seconds after launch. (36.6 seconds after the explosion.) The SRB have parachutes in the top cone so that, they can slowly come back to the ground in a normal way. The parachutes from the blown SRB had come loose and were floating down to the ground. The watching public thought that the crew had escaped from the shuttle using their escape system. What the watchers did not know was that there was no escape system on any of the shuttles. The SRB was seen speeding away from the gulf of smoke caused by the exploding challenger.

The right aft field joint sealing was the prime suspect to be the cause of the accident, because the smoke after ignition and flame during flight came from the region of the aft field joint. There were a few causes that were found which could have lead to the joint seal failure.

These causes are :

(*i*) *Assembly damage/Contamination.* The joint seal could have been damaged or contaminated during assembly of the SRB.

(*ii*) *Gap opening.* The gap between the joints open as the pressures are applied.

(*iii*) *O-ring compression.* This depends on the width of the gap.

(*iv*) *Joint temperature.* The temperature has effects on the sealing ability of the O-ring.

(*v*) *Putty performance.* Putty, Zinc chromate is applied before assembly inside the joint to stop gases to the O-rings.

Rogers Commission Report

The Presidential Commission on the Space Shuttle *Challenger* Accident, also known as the Rogers Commission (after its chairman), was formed to investigate the disaster. The commission members were Chairman William P. Rogers, Vice Chairman Neil Armstrong, David Acheson, Eugene Covert, Richard Feynman, Robert Hotz, Donald Kutyna, Sally Ride, Robert Rummel, Joseph Shtter, Arthur Walker, Albert Wheelon, and Chuck Yeager. The commission worked for several months and published a report of its findings. It found that the *Challenger* accident was caused by a failure in the O-rings used for sealing a joint on the right solid rocket booster, which unluckily allowed pressurized hot gases and eventually flame to *"blow by"* the O-ring and make contact with the adjacent external tank, causing

structural failure. The failure of the O-rings was attributed to a faulty design, whose performance could be too easily compromised by factors including the low temperature on the day of launch.

More broadly, the report also considered the contributing causes of the accident. Most salient was the failure of both NASA and Morton Thiokol to respond adequately to the danger posed by the deficient joint design. Rather than redesigning the joint, they came to define the problem as an acceptable flight risk. The report found that managers at Marshall had known about the flawed design since 1977, but never discussed the problem outside their reporting channels with Thiokol—a flagrant violation of NASA regulations. Even when it became more apparent how serious the flaw was, no one at Marshall considered grounding the shuttles until a remedial measure was implemented. On the contrary, Marshall managers went as far as to issue and waive six launch constraints related to the O-rings. The report also strongly criticized the decision-making process that led to the launch of *Challenger*, stating that it was seriously flawed.

Failures in communication resulted in a decision to launch the shuttle based on :

(*i*) incomplete and sometimes misleading information,

(*ii*) a conflict between engineering data and management judgments, and

(*iii*) a NASA management structure that permitted internal flight safety problems to bypass key Shuttle managers.

One of the commission's best-known members was theoretical physicist Richard Feynman. During a televised hearing, he famously demonstrated how the O-rings became less resilient and subject to seal failures at ice-cold temperatures by immersing a sample of the material in a glass of ice water. He argued that the estimates of reliability offered by NASA management were wildly unrealistic, differing as much as a thousand fold from the estimates of working engineers. *"For a successful technology"*, he concluded, *"reality must take precedence over public relations, because nature cannot be fooled"*.

2.6.4A Use as Case Study

The *Challenger* accident has frequently been used as a case study in the study of subjects such as engineering safety, the ethics of whistle-blowing, communications, group decision-making, and the dangers of groupthink. It is part of the required readings for engineers seeking a professional license in Canada and other countries. Roger Boisjoly, the engineer who had warned about the effect of cold weather on the O-rings, left his job at Morton Thiokol and became a speaker on workplace ethics. He argues that the caucus called by Morton Thiokol managers, which resulted in a recommendation to launch, *"constituted the uncthical decision-making forum resulting from intense customer intimidation."* For his honesty and integrity leading up to and directly following the shuttle disaster, Roger Boisjoly was awarded the Prize for Scientific Freedom and Responsibility from the American Association for the Advancement of Science. Many colleges and universities have also used the accident in classes on the ethics of engineering.

SUMMARY

- *In March 1970, reusable space shuttle became the focus of NASA's team for the multi- objective space plan. This decision significantly shaped NASA's goals for the future and increased the pressure on it perhaps at the expenses of engineering considerations, so much so, that at one point proposing 714 flights between 1978 and 1990, setting the stage for the challenger explosion. The genesis of the Challenger accident was the failure of the joint of the right solid rocket motor. While NASA worked on solving the problem, it continued with determination to fly, and defined the risk as "acceptable" and "unavoidable." The Space Shuttle Challenger-disaster occurred on January 28, 1986, when it broke apart 73 seconds into its flight, leading to the deaths of its seven crew members. Disintegration of the vehicle began after an O-ring seal in its right solid rocket booster (SRB) failed at liftoff. The O-ring failure caused a breach in the SRB joint it sealed, which led to the structural failure of the external tank. Aerodynamic forces broke up the orbiter. NASA managers knew a potentially catastrophic flaw in the O-rings since 1977, but failed to address it properly. They also disregarded warnings from engineers about the dangers posed by the low temperatures on the morning of launching date. Rogers Commission formed to investigate the disaster worked for several months and it found that the Challenger accident was caused by a failure in the O-rings used for sealing a joint on the right solid rocket booster. The Challenger accident has frequently been used as a case study in the study of subjects such as engineering safety, the ethics of whistle-blowing, communications, group decision-making, and the dangers of groupthink.*

Short Question Answers

1. *How was NASA pressurized to develop a space shuttle ?*

   Ans. In March 1970, President Nixon ordered the development of the reusable space shuttle, earlier considered only the transport element of a broad, multi-objective space plan, became the focus of NASA's team for the near future. This decision forced NASA to prove and create an operational shuttle system by instituting a heavy schedule of flights.

   President Ronald Reagan's administration was eager for the shuttle system to become operational because it had developed some rather ambitions commercial and military goals for NASA. Pressures developed because of the need to meet customer's commitments, so much so, that at one point proposing 714 flights between 1978 and 1990, setting the stage for the challenger explosion.

2. *Write the cause which lead to the joint seal failure.*

   Ans. The genesis of the Challenger accident was the failure of the joint of the right solid rocket motor. While NASA worked on solving the problem, it continued with determination to fly, and defined the risk as "*acceptable*" and "*unavoidable.*" An O-ring seal in its right solid rocket booster (SRB) failed at liftoff which caused a breach in the SRB joint it sealed, allowing pressurized hot gas from within the solid rocket motor to reach outside

and impinge upon the adjacent SRB attachment hardware and external fuel tank. This led to the separation of the right-hand SRB's aft attachment and the structural failure of the external tank. Aerodynamic forces broke up the orbiter.

3. *Describe in brief the findings of Rogers Commission on space shuttle disaster.*

   Ans. The Presidential Commission on the Space Shuttle Challenger Accident found that the Challenger accident was caused by a failure in the O-rings used for sealing a joint on the right solid rocket booster, which unluckily allowed pressurized hot gases and eventually flame to "blow by" the O-ring and make contact with the adjacent external tank, causing structural failure. The failure of the O-rings was attributed to a faulty design known since 1977, whose performance was easily compromised by factors including the low temperature on the day of launch. The report also strongly criticized the decision-making process that led to the launch of Challenger, stating that it was seriously flawed. Failures in communication resulted in a decision to launch the shuttle based on (*i*) incomplete and sometimes misleading information, (*ii*) a conflict between engineering data and management judgments, and (*iii*) a NASA management structure that permitted internal flight safety problems to bypass key Shuttle managers.

Exercise

1. Describe the story about challenger accident.
2. How was very low temperature responsible to the space shuttle disaster ?
3. Why and how do you think that space shuttle disaster should be considered for use as a case study by professionals ?