

GE6075 – Professional Ethics in Engineering

UNIT-4 Safety and Risk

4.0 SAFETY DEFINITION

Safety has different connotations. A product or a project is safe, with respect to a person or a group, at a given time, if its risks were fully known, and if the risks are judged to be acceptable, in the light of settled perspectives.

4.1 SAFETY AND RISK

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

Probability of safety = 1 – Probability of risk

Risk = Probability of occurrence × Consequence in magnitude

UNIT-3

Factors Influencing Perception of Risk

Various factors that influence the perception of risk are:

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

UNIT-3 Factors Influencing Perception of Risk

Various factors that influence the perception of risk are:

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

- ❑ *Probability of Risk*
- ❑ *Consequence of Risk –[Phy Damage, loss of Life, Env Degradation etc]*
- ❑ *Voluntariness*
- ❑ *Magnitude*
- ❑ *Proximity*
- ❑ *Method of Inf dissemination*
- ❑ *Job related[Compulsion or volition]*

Risk Acceptance

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

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

Risk Identification/ Testing for Safety

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

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

Risk analysis

4.2 RISK ANALYSIS

4.2.1 Analytical Methods

Several analytical methods are adopted in testing for safety of a product/project.

1. *Scenario Analysis*

This is the most common method of analysis. Starting from an event, different consequences are studied. This is more a qualitative method.

For example, a disaster recovery plan, for an organization is discussed. When the probability and size of loss (indicating possibility and financial significance, respectively) are both high, risk exists. On the other hand, risk is not associated with very low probability of occurrence, or with losses that under any other circumstances would be considered “affordable”. But there is a gray area between probability/loss combinations that are truly risky, and those that are not. This reflects the fact that the boundary between risky and non-risky events is fuzzy, not exact.

To assess the risk faced by the organization, the planner matches the probability and loss characteristics of various exposures to one’s intuition of risk. This exposure analysis can be most effectively carried out using ‘loss scenarios’. A scenario is a synopsis of events or conditions leading to an accident and subsequent loss. Scenarios may be specified informally, in the form of narrative, or formally using diagrams and flow charts.

Risk Assessment

Steps for Risk Assessment

1. What can go wrong that could lead to an outcome of hazard exposure? (identification and characterization of risk)
2. How likely is this to happen? (quantification of risk, likelihood, and magnitude)
3. If it happens, what are the consequences? Scenarios are constructed and the ways and means of facing the consequences are designed.

FMEA

FMEA is one of the qualitative tools, which support proactive quality strategies. Successful implementation of FMEA requires relevant knowledge and insight as well as engineering judgment. FMEA concept was introduced in 1960s by aerospace companies. Then the use of FMEA was extended to automobile industries and other types of industries, understanding the value of this approach. In the last decade, it has undergone metamorphosis where focus was on severity, occurrence and detection rating. Thus, FMEA is defined as a systematic tool to

- (a) identify possible failure modes in the products/process,
- (b) to understand failure mechanism (process that leads to failure),
- (c) risk analysis, and
- (d) plan for action on elimination or reduction of failure modes.

FMEA

Table 4.1 Worksheet for Design/Process FMEA

<i>Model no.:</i> <i>FMEA team members</i>					<i>Prepared by:</i> <i>Original FMEA date:</i>					<i>Responsibility:</i> <i>Date of revision:</i>					
Design/ Product	Potential cause failure	Potential effects of failure	Seerity	Class	Poten- tial cause/ Mecha- nism of failure	Occu- rence	Current process control	Detection	RPN	Reccom mended actions	Respon sibility & target date	Action results			
												S	O	D	R
												E	C	E	P
												V	U	T	N
												E	R	E	
												R	R	C	
												I	I	T	
												T	T	I	
												Y	N	O	
												C	N	N	
												E	E		

FMEA

A. STEPS TO CONDUCT FMEA

FMEA is a cross-functional team management. Throughout the product development cycles, changes and updates will be introduced to the product and process. These changes have to be reviewed because they can introduce new risks or failure modes. It is thus necessary to review and update changes.

1. Product/process and its function must be understood first. This is the most fundamental concept to be adopted in this methodology. This understanding helps the engineer to identify product/process function that fall with the intended and unintended users.
2. Block diagram of product/process is created and developed. The diagram shows the major components or process steps as blocks, identifies their relations namely, input, function and output of the design. The diagram shows logical relationship of components and establishes a structure for FMEA. The block diagram should always be included in the FMEA form.
3. Header on FMEA form is completed. FMEA form includes part/process name, model date, revision date, and responsibility.
4. The items/functions are listed logically in the FMEA form, based on the block diagram.
5. Then failure modes are identified. A failure mode is defined wherein a component, subsystem, system, and process could potentially fail to meet the design intent.

FMEA

6. A failure mode in one component can cause failure in another. Each failure should be listed in technical terms. Listing should be done component- or process-wise.
7. Then the effects of each risk/failure mode are described. This is done as perceived by both internal and external customers. The examples of risk/failure effect may include injury to the user, environment, equipment, and degraded performance. Then a numerical ranking is assigned to each risk or failure. It depends upon the severity of the effect. Commonly, in the scale, No.1 is used to represent no effect and 10 to indicate very severe failure, affecting system of operation and user. By this, the failures can be prioritized and real critical risks can be addressed first.
8. Then the causes of each failure mode have to be identified. A cause is defined as a design weakness that results in a failure. The potential causes for each failure mode are identified. The potential causes, for example, may be improper torque or contamination or excessive loading or external vibration.

FMEA

9. The probability factor indicating the frequency of occurrence is considered. A numerical weightage can be assigned to each cause depending upon the probability of occurrence. A standard scale is used, 1 indicating 'not likely' and 10 indicating 'inevitable'.
10. Design or Process mechanism has to be identified, which can prevent the cause of failure or detect failure, before it reaches customer. Accordingly, the team has to identify tests, analysis, monitoring and other techniques to detect the risk or failure. Previously undetected or unidentified failures may appear when a new product/process are introduced. Therefore, FMEA should be updated and the required plans for the elimination of risks or failures have to be drawn.
11. Assessment of detection rating is done by assigning a numerical weightage. Value 1 indicates design control will certainly detect the potential cause, 10 indicates design control will not detect the cause or mechanism. A normal scale of 1 – 10 is used.
12. Risk Priority Number (RPN) is calculated and reviewed.

$$\text{RPN} = \text{Severity} \times \text{Probability} \times \text{Detection}$$

It is used to prioritise failure modes and viewed as a relative measure of the design risk

13. Recommended actions are determined to address potential risks or failures with high RPN.
14. Revalidate each action by reassessing severity, probability and detection and review the revised RPN. Check any further action is needed. FMEA has to be updated as and when the design or process is modified or changed.

Fault Tree Analysis

3. Fault-tree Analysis

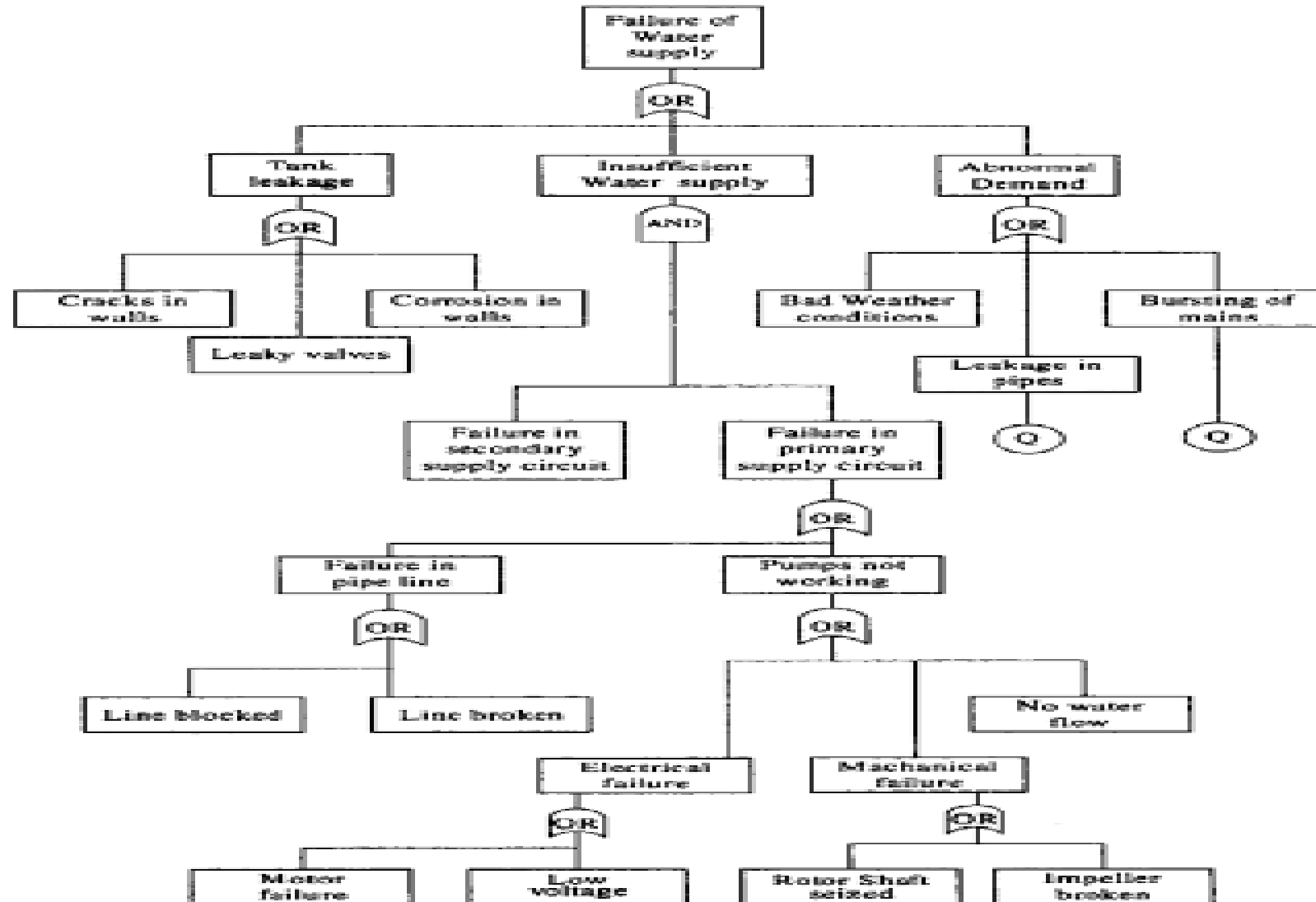
This is a qualitative method and was originated by Bell Telephones. It is technology-based deductive logic. The failure (undesirable event) is initially defined, and the events (causal relationships) leading to that failure are identified at different components level. This method can combine hardware failures and human failures

Example 1: Consider the failure of the steam flow in a thermal station. The water is pumped from a big reservoir nearby. The details are shown in Fig. 4.1

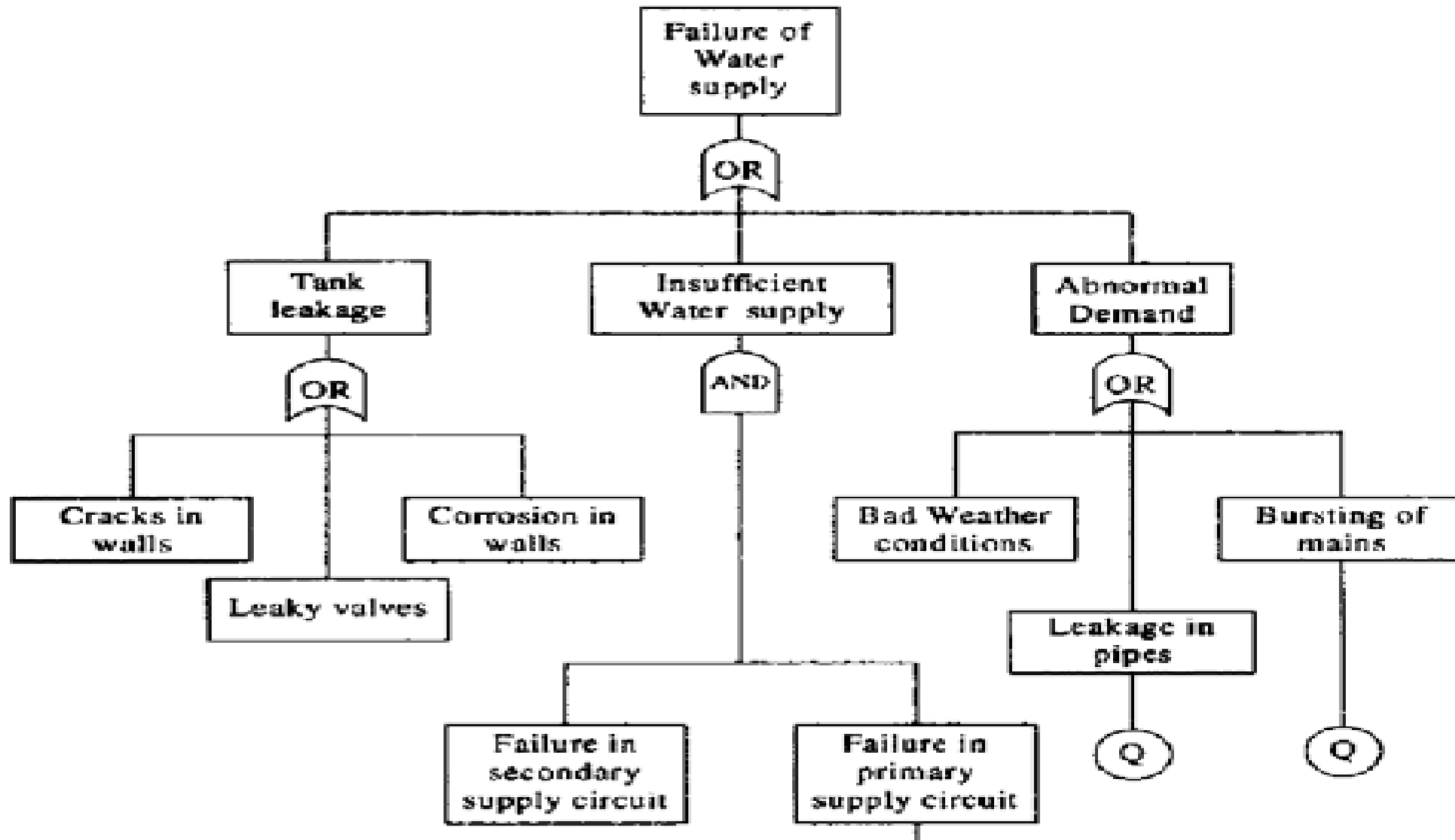
Fault Tree Analysis

- **Fault tree analysis (FTA)** is a **top down, deductive failure analysis**
- Uses **Boolean logic** to combine a series of lower-level events.
- Mainly used in the fields of **safety & Reliability** engineering.
- To understand **how systems can fail**
- To identify the best ways to **reduce risk** .
- Used in the **aerospace**, nuclear power, chemical, pharmaceutical, petrochemical and other **high-hazard industries**;
- Used in software engineering for **debugging purposes** and is closely related to **cause-elimination technique** used to **detect bugs**.

Fault Tree analysis



Fault Tree analysis



Fault Tree analysis

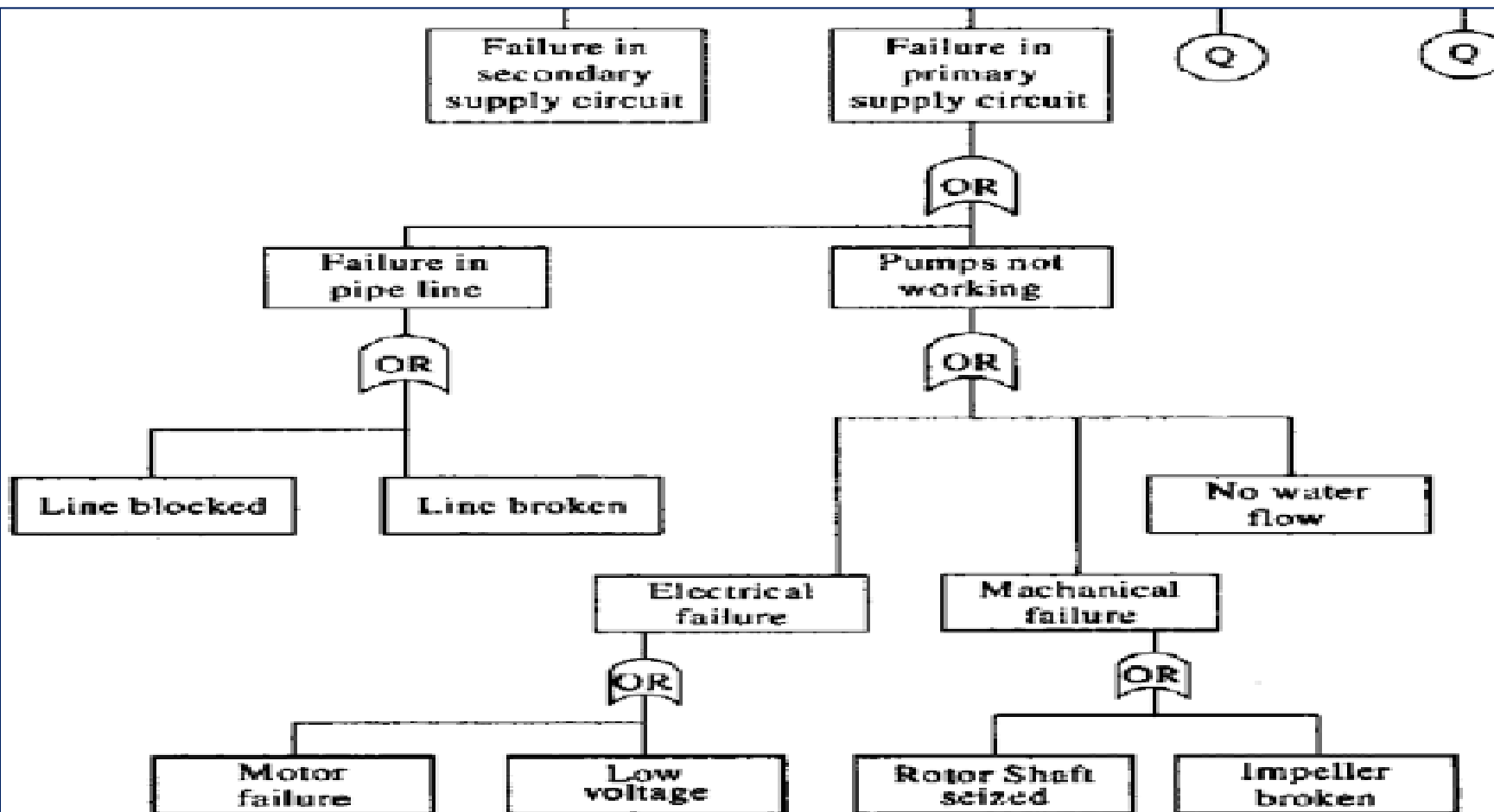


Fig. 4.1 Fault-free analysis

Example-2 (FTA)

Example 2: A crash at main road junction

The details of this Fault-tree Analysis are shown in Fig. 4.2

Consider the probability of the crash at a road junction and construct a tree with and AND or GATE logic. The tree is constructed by deducing in turn the pre-conditions for the final event and then successively for the next levels of events, until the basic causes are identified.

By ascribing probabilities to each event, the probability of a top event can be calculated. This requires knowledge of probable failure rates. At an OR gate, the probabilities must be added to give the probability of the next event, whereas at an AND gate, the probabilities are multiplied. This is a powerful technique for identifying the failures that have the greatest influence on bringing about the end event.

Example-2 (FTA)

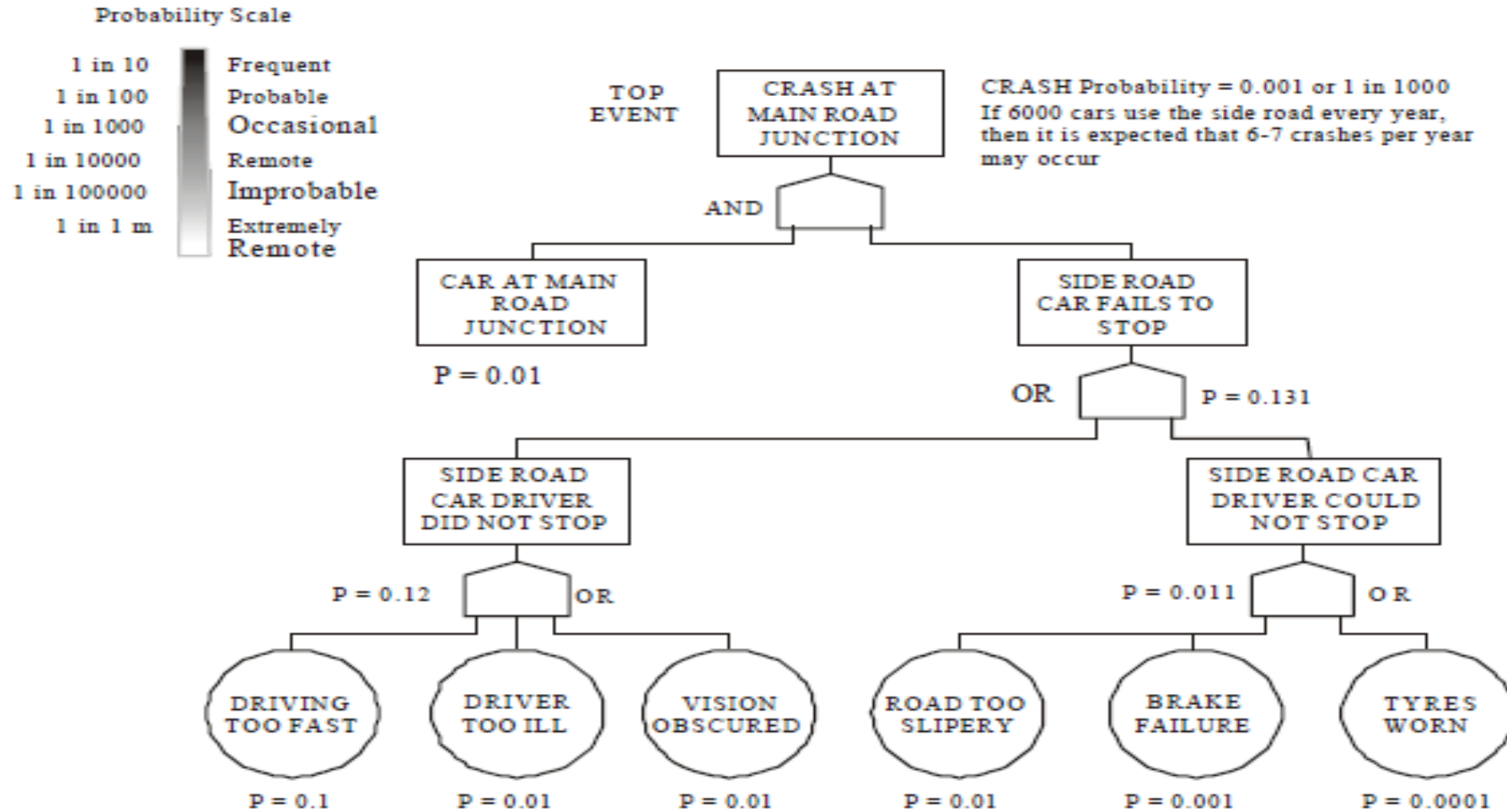


Fig. 4.2 Quantification for fault-tree analysis

Example-3

Example 3: An automobile car does not start. The details of this case are shown in Fig. 4.3.

The advantages of FTA are (a) the primary cause can be located easily, and (b) It is useful in emergent situations i.e., a fire-fighting approach.

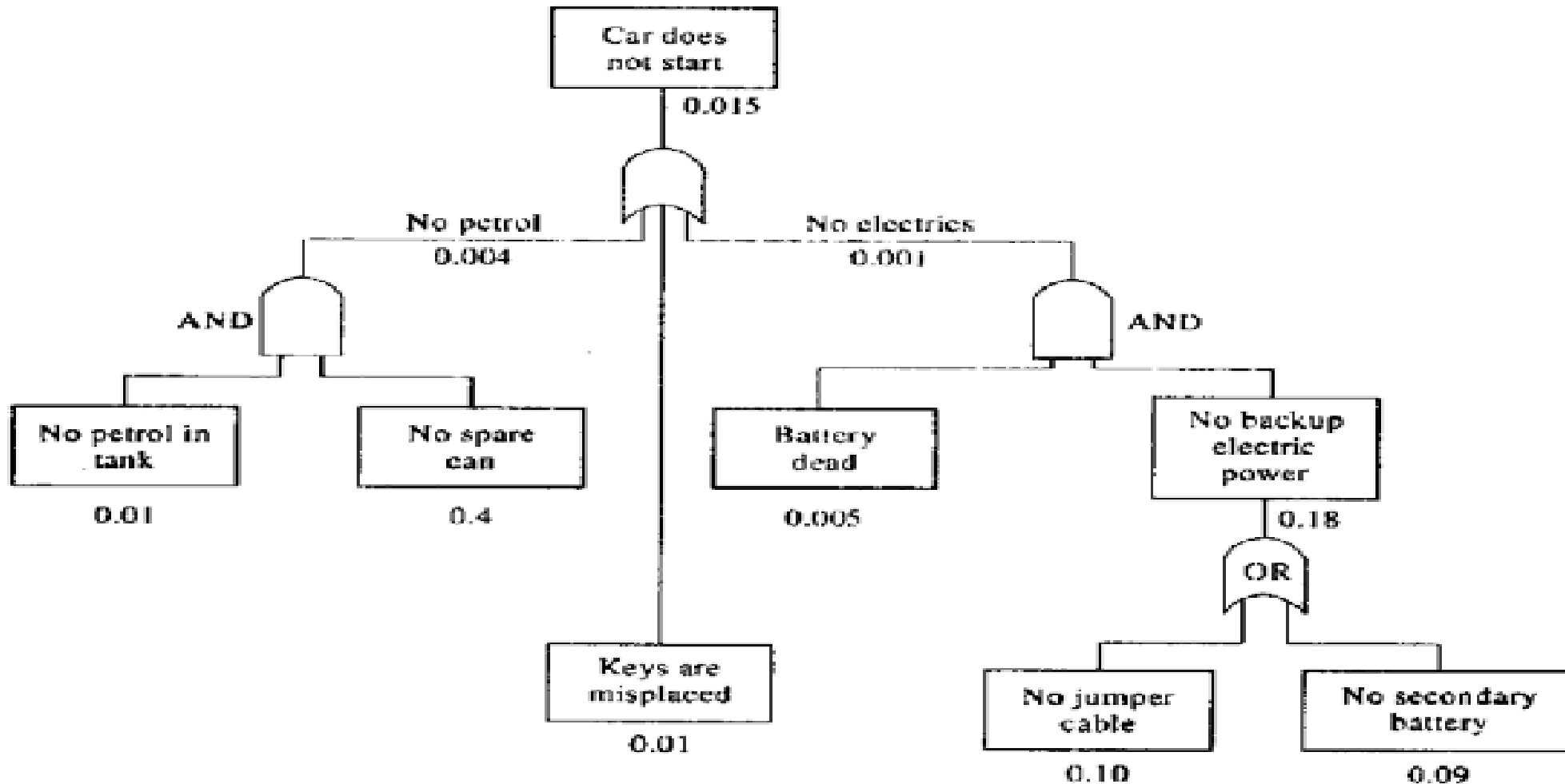


Fig. 4.3 Fault-tree analysis

Event-tree Analysis

4. Event-tree Analysis

This method illustrates the sequence of outcomes which may arise after the occurrence of a selected initial event. This method uses inductive logic. It is mainly used for consequence analysis and in identifying the potential hazardous existing situation in the system. It is the inverse of the FTA. FTA allows one to proceed back in time from possible catastrophic accidents to examine the components of sequences with probability of failure. But, the ETA allows the observer to proceed forward in time from potential component failures to final accident.

The most serious outcome such as explosion, toxic release, etc. is selected as the final event. A tree is then constructed by relating the sequences of events, which individually or in combination, could lead to the final event.

Event-tree Analysis

- ▶ **Event tree analysis (ETA)** is a **forward, bottom up, modeling technique** for both **success and failure**
- ▶ Explores responses through a **single initiating event**
- ▶ Lays a path for **assessing probabilities of the outcomes** and overall system analysis.
- ▶ ETA is a **powerful tool** that will **identify all consequences** of a system that have a probability of occurring after an initiating event
- ▶ ETA can be applied to a wide range of systems including: nuclear power plants, spacecraft, and chemical plants.
- ▶ This Technique may be applied to a system **early in the design process** to identify potential issues that may arise rather than **correcting the issues after they occur.**
- ▶ With this **forward logic process** use of ETA as a tool in **risk assessment** can help to **prevent negative outcomes from occurring**

Example Event tree Analysis

Example: Going late for duty

The events are listed, arranged chronologically, and in separate clusters, to include only that are relevant and important. Fig. 4.4 shows the ETA for the event of going late to the office as a simple illustrative example. The branching structure starts with the initiating event (initiator) on the left hand side of the tree and lead to a bad end event (final damaged state) shown at the far right side. The sequence starts with the person getting up late and being time pressed to get to duty.

The person has three alternatives to get there, namely, (a) driving his own car along the highway, that is subject to periodic overcrowding and delays while driving, (b) to use the public transport (express train or bus), and (c) call a colleague and share the car.

Example Event tree Analysis

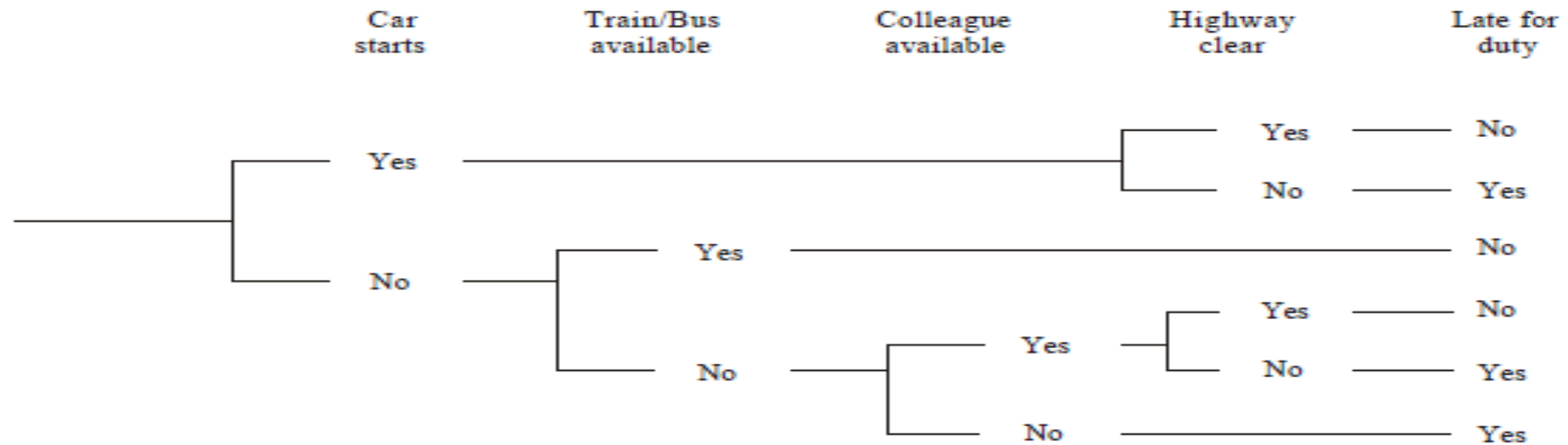


Fig. 4.4 Event-tree analysis

The figure shows the event-tree including the alternatives and different things that could lead to the employee being 'late again'. Alternative outcomes are shown under each column. Trace back from the outcomes towards the left hand side of the tree along horizontal paths. There are series of vertical branches labeled, Yes or No, which are connected to previous paths. The vertical branches represent the response (Yes/No) to the question (or the systems responsible) that appear on the top of the tree.

Event Tree Analysis

Figure 1: Fire Protection System

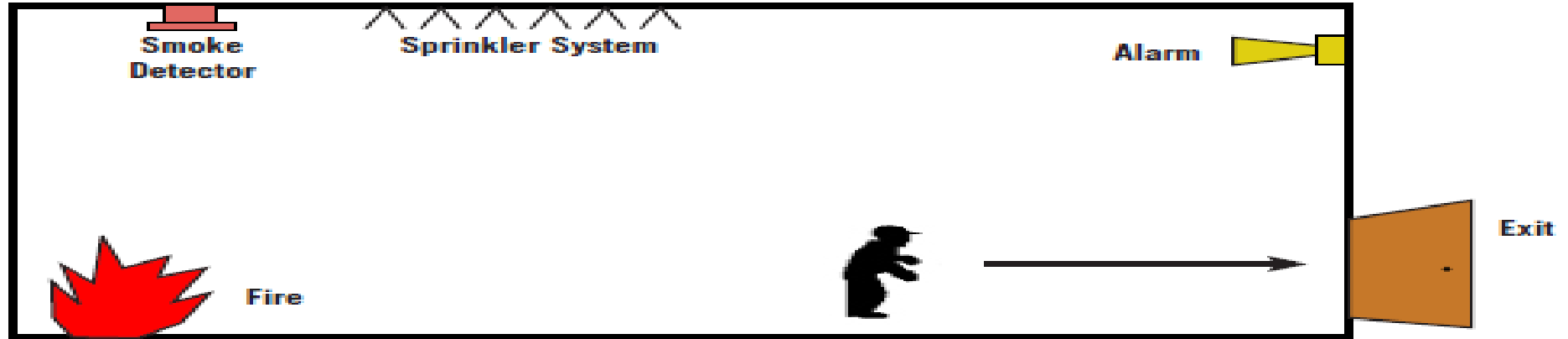
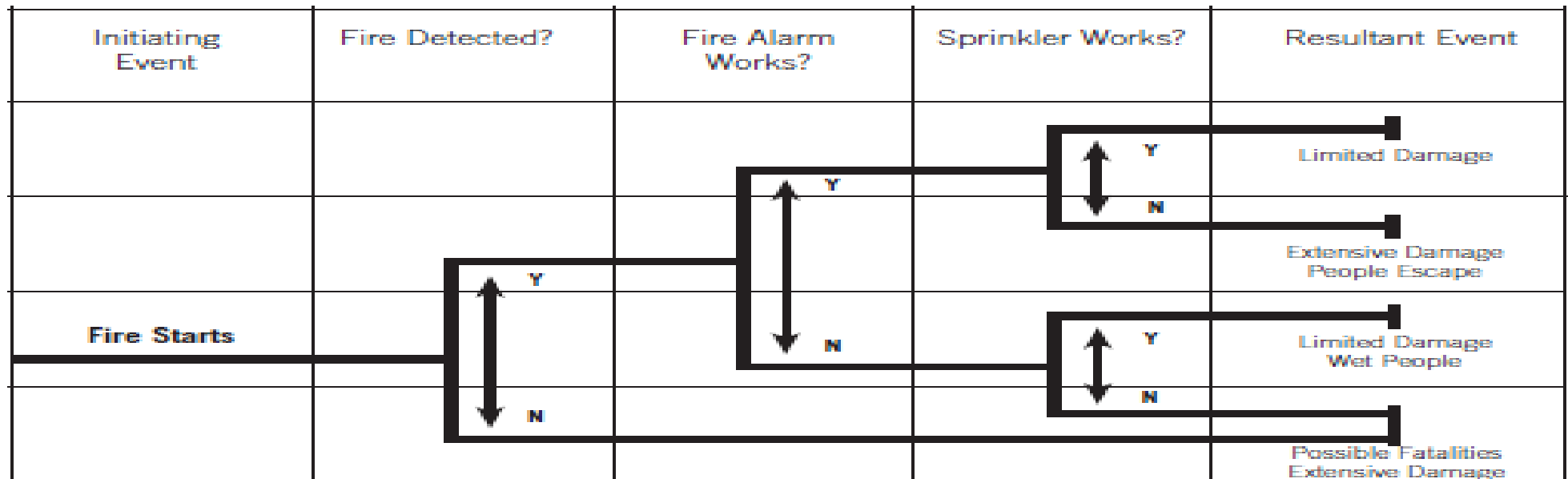


Figure 2: Simplified Event Tree



Event Tree Analysis

Event Tree Analysis (ETA)

Event tree analysis is based on binary logic, in which an event either has or has not happened or a component has or has not failed. It is valuable in analysing the consequences arising from a failure or undesired event.

An event tree begins with an initiating event, for example, a component failure, increase in temperature/pressure or a release of a hazardous substance. The consequences of the event are followed through a series of possible paths. Each path is assigned a probability of occurrence and the probability of the various possible outcomes can be calculated.

In the following example fire protection is provided by a sprinkler system. A detector will either detect the rise in temperature or it will not. If the detector succeeds the control box will either work correctly or it will not - and so on. There is only one branch in the tree that indicates that all the subsystems have succeeded:

Safe Exit

4.4 SAFE EXIT

In the study of safety, the 'safe exit' principles are recommended. The conditions referred to as 'safe exit' are:

- 1 The product, when it fails, should fail safely
- 2 The product, when it fails, can be abandoned safely (it does not harm others by explosion or radiation)
- 3 The user can safely escape the product (e.g., ships need sufficient number of life boats for all passengers and crew; multi-storeyed buildings need usable fire escapes)

Risk Benefit Analysis

4.5 RISK-BENEFIT ANALYSIS

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

- 1 To know risks and benefits and weigh them each
- 2 To decide on designs, advisability of product/project
- 3 To suggest and modify the design so that the risks are eliminated or reduced

Risk Benefit Analysis

Risk-Benefit Analyses

Many large projects, especially public works, are justified on the basis of a risk-benefit analysis. The questions answered by such a study are the following: Is the product worth the risks connected with its use? What are the benefits? Do they outweigh the risks?

Limitations on Risk Benefit Analysis

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

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

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

Reducing Risk

4.5.3 Reducing Risk (Improving Safety)

Several techniques adopted to reduce the risks (or improve safety) in a product or process are listed as follows:

1. Application of inherent safety concepts in design, e.g., LPG cylinder is provided with frame to protect the valve while handling and facilitate cryogenic storage. A magnetic door catch provides an easy escape for children caught inside the 'fridge' accidentally.
2. Use of redundancy principle in the instrument protection/design. For example, use of stand-by device, and back-up for computer storage.
3. Periodical monitoring (inspection) and testing of safety system to ensure reliability, e.g., fire extinguishers, 'earth' system in electric circuits are checked periodically.
4. Issue of operation manuals, training of the operating personnel and regular audits are adopted to ensure that the procedures are understood, followed and the systems are kept in working condition.
5. Development of well-designed emergency evacuation plan and regular rehearsal/drills to ensure preparedness, in case of emergency.

Assessing Personal Risk

4.5.1 Personal Risk

Assessing the involuntary personal risk is not an easy task. For example, a group residing near the cement plant is exposed to a lot of risk. If suppose a cement plant or refinery was to come up in the area where this group already reside, they will object the proposal. The adequacy of compensation amount payable can not be fixed reasonably. How to estimate the rupee value of an individual human being? For example, a person may be a father to his young ones, husband to his beloved wife, son to his aged parents, friend to the needy, and as well a guardian for his pet dogs.

There are persons who dared to serve people in dire straits, in spite of the risky situations where their lives were in stakes. For example, Mahathma Gandhi served people during Navakali yatra, when dangers were present all over. For such saviors, there was no personal risk.

However, any of the following methodologies may be adopted to assess quantitatively, the personal risk:

1. Assess the voluntary activities (e.g., life insurance policy taken)
2. Assess the degree of occupational hazard (e.g., dust, radiation, and asbestosis) and its effect on health.
3. Loss of senses such as sight (eyes), hearing (ears) and loss of limbs (immobility by the loss/ damage to organs or disfigurement of the limbs or body).
4. Loss of earning capability, especially due to physical disability, and
5. Get assistance by trained arbiters.

Assessing Public Risk

4.5.2 Public Risk

Assessing the public risk is relatively easy, as in the societal value system the cost of disability can be averaged out. For example, the U.S. National Safety Council¹ adopts an equivalent of 6000 days (16.42 years), for death, as per the personal value system for social costs of disability.

To assess the public risk, the loss on the assets and the correction costs are estimated. For example,

- 1 Loss of or reduction in future income or earning capacity due to loss of limbs or their capability
- 2 Costs associated with accident, which includes the transplantation or reinforcement of body parts/limbs, and medical treatment and
- 3 Cost of welfare, which includes rehabilitation, provision of less-demanding alternate jobs, and other disability benefits.

Voluntary risk

4.5.4 Voluntary Risk

Voluntary risk is the involvement of people in risky actions, although they know that these actions are unsafe. The people take these actions for thrill, amusement or fun. They also believe that they have full control over their actions (including the outcomes!) and equipments or animals handled, e.g., people participate in car racing and risky stunts.

Testing becomes inappropriate when the products are

- 1 Tested destructively
- 2 When the test duration is long, and
- 3 When the components failing by tests are very costly. Alternate methods such as design of experiments, accelerated testing and computer-simulated tests are adopted in these circumstances.

Three Miles Island nuclear Power Plant

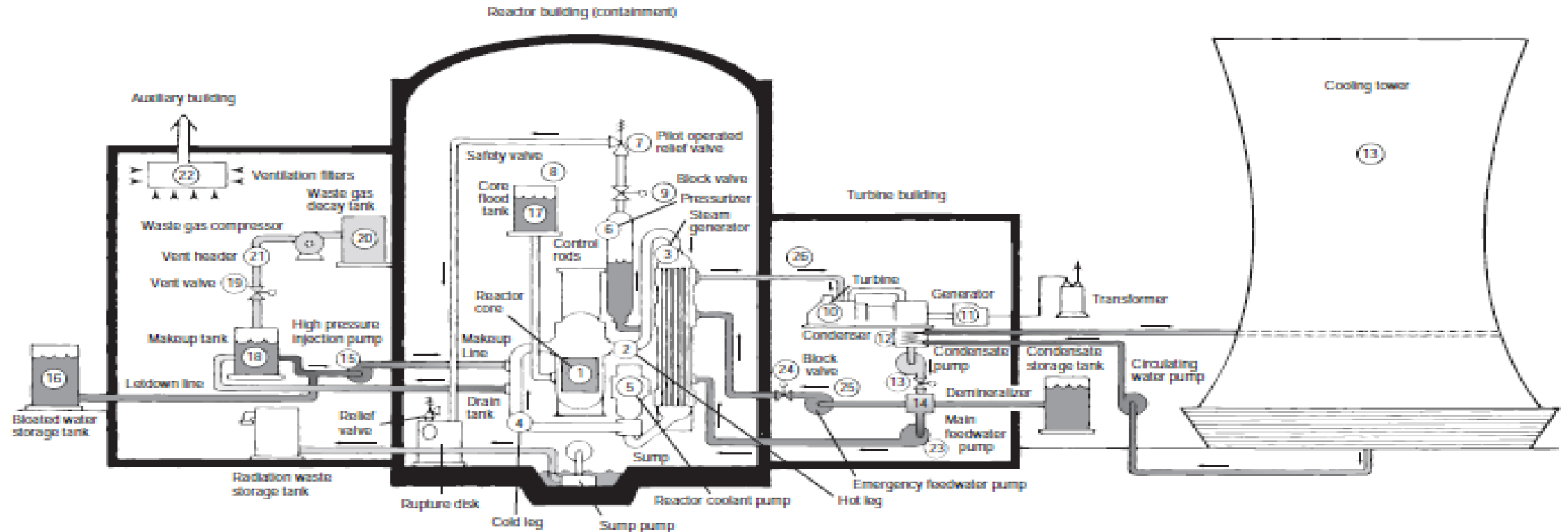


Figure 5-4

Schematic diagram of Three Mile Island nuclear power plant Unit 2. Pressurized water reactor system: Heat from reactor core (1) is carried away by water in a primary loop (1, 2, 3, 5, 4). In the steam generator (3) the heat is transferred to water in a secondary loop (26) at lower pressure. The secondary-loop water turns to steam in the steam generator or boiler (3), drives the turbine (10), turns into water in the condenser (12), and is circulated back to (3) by means of pumps (13, 23, and 25). (Adapted from John F. Mason, "The Technical Blow-by-Blow: An Account of the Three Mile Island Accident," *IEEE Spectrum*, 16 [November 1979], copyright © 1979 by the Institute of Electrical and Electronics Engineers, Inc., and from Mitchell Rogovin and George T. Frampton Jr., *Three Mile Island: A Report to the Commissioners and the Public*, vol. 1, Nuclear Regulatory Commission Special Inquiry Group, NUREG/CR-1250, Washington, DC [January 1980]).