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 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

Analytical Methods

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

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.

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)

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.
6. A failure mode in one component can cause failure in another. Each failure should be listed in echnical 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.

the memory. The event trees are portrayed in a logical structure that branches from left to right and uses only OR gate. In contrast, a Fault Tree is organized 'top to bottom' hierarchy and uses both AND and OR gates logic. More AND gates a tree contains, the more fault tolerant (and safer) a system typically is. A proliferation of OR gates indicate a failure-prone situation.

Human Error

The human-error contribution to overall system failure can be included in a FTA or ETA, if human-error probabilities are described in the same terms as component and hardware failures. To include human error, a detailed task analysis is first required, listing the actions to be done, conditions, speed of operation and the correct sequencing of individual actions. After allowing for deviations and shaping factors, which influence individual performance (such as skill and stress), and recovery factors (most human errors are recoverable), the contribution of human error can be estimated, by using data on human error rates.

4.2.2 Cost Analysis

A quantitative risk analysis is made on (1) primary costs: the loss of human lives, or property (assets), crops, and natural resources are estimated, and (2) secondary costs: the loss of human capability or loss of earning capacity, cost of treatment and rehabilitation, damage to the property, fertility to the soil, salinity to the groundwater etc. are estimated.

4.3 ASSESSMENT OF SAFETY AND RISK

4.3.1 Uncertainties in Assessment

There are many positive uncertainties in determining the risk of a product/service.

1. Restricted access to knowledge on risk: Some organizations do not disclose the data, citing legal restrictions.
2. Uncertain behavior of materials: Test data supplied by the suppliers are only statistical. The individual parts may behave considerably (! 3 σ) different from the statistical mean obtained from the tests on random samples.
3. Uncertain and varying behavior of user environments such as physical shock, thermal shock, fatigue, creep, impulse and self-excited vibrations in components or structures due to winds, snow fall, and rains cause sudden failure of the whole structure. An error or wrong procedure during assembly or joining the components may cause additional stress leading to early failure.
4. The use or misuse of materials/products, remaining untracked, e.g., exposure to rain or snow or damp weather is likely to change the properties.
5. Newer applications of obsolete technologies, remaining unpublished,
6. Substitution of newer materials whose behavior are not disclosed, and
7. The unexpected and unintended outcomes of the product/project.

All these aspects make the estimation of risk complex and unreliable. Hence, the data are to be monitored continuously and risk estimation updated periodically.

For example, a few friends live very near the cement plant, as they are unable to choose a better location for their house. The group work as motor mechanics in an automobile service station nearby.

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

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

1 To know risks and benefits and weigh them each

2 To decide on designs, advisability of product/project

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

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

1. Primarily the benefits may go to one group and risks may go to another group. Is it ethically correct?

2. Is an individual or government empowered to impose a risk on 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.

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.

SAFETY LESSONS FROM 'THE CHALLENGER'

The safety lessons one can learn in the Challenger case are as follows:

1. Negligence in design efforts. The booster rocket casing recovered from earlier flights indicated the failure of filed-joint seals. No deign changes were incorporated. Instead of two O-rings, three rings should have been fixed. But there was no time for testing with three rings. At least three rings could have been tried while launching.

2. Tests on O-rings should have been conducted down to the expected ambient temperature i.e., to 20 oF. No normalization of deviances should have been allowed.

3. NASA was not willing to wait for the weather to improve. The weather was not favorable on the day of launch. A strong wind shear might have caused the rupture of the weakened O- rings.

4. The final decision making of launch or no-launch should have been with the engineers and not on the managers. Engineers insisted on 'safety' but the managers went ahead with the 'schedule'.

5. Informed consent: The mission was full of dangers. The astronauts should have been informed of the probable failure of the O-rings (field joints). No informed consent was obtained, when the engineers had expressed that the specific launch was unsafe.

6. Conflict of interest (Risk Vs. Cost): There were 700 criticality-1 items, which included the field joints. A failure in any one of them would have cause the tragedy. No back-up or stand- bye had been provided for these criticality-1 components.

7. Escape mechanism or 'safe exit' should have been incorporated in the craft. **McDonnell**

HUMAN RIGHTS

Human rights are defined as moral entitlements that place obligations on other people to treat one with dignity and respect. Organisations and engineers are to be familiar with the minimum provisions under the human rights, so that the engineers and organizations for a firm base for understanding and productivity. Provisions under 'human rights' are as follows:

1. Right to pursue legitimate personal interest
2. Right to make a living
3. Right to privacy
4. Right to property
5. Right of non-discrimination
6. No sexual harassment

Under professional rights, the following provisions are protected:

1. *Right to form and express professional judgment*: It is also called the *right of professional conscience*. In pursuing professional responsibilities, this empowers one to form and exercise the professional judgment. Both technical and moral judgments are included. This right is bound by the responsibilities to employers and colleagues.

2. *Right to refuse to participate in unethical activities*: It is also called the *right of conscientious refusal*. It is the right to refuse to engage in unethical actions and to refuse to do so solely because one views that as unethical. The employer can not force or threaten the employee to do something that is considered by that employee as unethical or unacceptable. For example, unethical and illegal

activities that can be refused are: falsifying data, forging documents, altering test results, lying, giving or taking bribe etc. There may be situations, when there is a disagreement or no shared agreement among reasonable people over whether an act is unethical. Medical practitioners have a right not to participate in abortions. Similarly, the engineers must have a right to refuse assignments that violate their personal conscience, such as when there exists a threat to human life or moral disagreement among reasonable people.

Aspects

There are four aspects of whistle blowing, namely:

1. *Basis of disclosure*: The basis for disclosure may be intentional, or under pressure from superiors or others not to disclose.

2. *Relevance of topic*: The whistle blower believes that the information is about a significant problem for the organization or its business ally. It can be a threat to the public or employees' health, safety and welfare or a criminal activity, or unethical policies or practices, or an injustice to the workers within the organization.

3. *Agent*: The person disclosing the information may be a current or former employee or a person having a close link to the organization.

4. *Recipient*: The person or organization, who receives the information, is in a position to remedy the problem or alert the affected parties. Usually, the recipients are not aware of the information fully or even partially.

Types

Based on the *destination (recipient),* whistle blowing is classified into types, as:

(a) *Internal*: In this case, the information is conveyed to a person within the organization, but beyond the approved channels.

(b) *External*: This happens when the information is transmitted outside the organization. The recipient may be a municipal chairman or member of legislature or minister. It becomes severe if the information reaches the press and through them the public. The damage is maximum and sometimes poses difficulty in remedying the situation.

Based on the origin or source (agent), this can be divided into three types, as follows:

(a) *Open*: The originator reveals his identity as he conveys the information. This information is reliable and true, but sometimes partially true.

(b) *Anonymous*: The identity is concealed. The information may or may not be true. But the agent anticipates perhaps some repression or threat, if identity is revealed.

Partly anonymous (or partly open): Such a situation exists when the individual reveals his identity to the journalist, but insists that the name be withheld .

Testing strategies for safety

***Some commonly used testing methods*:**

Using the past experience in checking the design and performance.
Prototype testing. Here the one product tested may not be representative of the population of products.
Tests simulated under approximately actual conditions to know the performance flaws on safety.
Routine quality assurance tests on production runs.
The above testing procedures are not always carried out properly. Hence we cannot trust the testing procedures uncritically. Some tests are also destructive and obviously it is impossible to do destructive testing and improve safety.
In such cases, a simulation that traces hypothetical risky outcomes could be applied.
Scenario Analysis (Event -> Consequences)
Failure Modes & Effects Analysis (Failure modes of each component)
Fault Tree Analysis (System Failure -> Possible Causes at component level) What if there is a combination of factors?
All Analysis pre-suppose a thorough understanding of the physical system

Failure modes and effect analysis (FMEA) :
This approach systematically examines the failure modes of each component, without however, focusing on relationships among the elements of a complex system.

Fault Tree Analysis (FTA) :
A system failure is proposed and then events are traced back to possible causes at the component level. The reverse of the fault-tree analysis is „event – tree analysis method most effectively illustrates the disciplined approach required to capture as much as possible of everything that affects proper functioning and safety of a complex system

Difficulties in establishing Safeguards

Incomplete knowledge of the engineering subject
Refusal to face hard questions caused by lack of knowledge False sense of security e.g. Nuclear waste disposal problem
Caution in stating probabilities of rare events
Varying understanding of risk based on presentation of facts
Risk assessments based on incorrect/unacceptable assumptions/data Only a few persons/groups participate in the exercise
Some of the ways by which engineers may try to reduce risks.

In all the areas of works, engineers should give top priority for product safety. They should believe that accidents are caused by dangerous conditions that can be corrected. Negligence and operator errors are not the principal causes of accidents.

If a product is made safe, the initial costs need not be high if safety is built into a product from the beginning. It is the design changes done at a later **date** that are costly.
Even then life cycle costs can be made lower for the redesigned or retrofitted product (for safety).
If safety is not built into the original design, people can be hurt during testing stage itself.
They should get out of the thinking that warnings about hazards are adequate and that insurance coverage is cheaper than planning for safety.
All it takes to make a product safe is to have different perspective on the design problem with emphasis on safety.

Liability

Early logic and social philosophy: (Richard C. Vaughan)
"Caveat Emptor": buyer beware Examine what you want before you buy
If he is negligent, he suffers the bad bargain.
Law will not aid those who are negligent
"Privet of Contract": User, if he is not a party to the contract, has no rights for any claim (user buys from the retailer and not from the manufacturer) Gradually....
Manufacturer was made liable for injuries resulting from negligence in the design/manufacture
The new law: concept of Strict Liability was established in the case „Green man vs. Yuba Power Products" in California.
If the product sold is defective, the manufacturer is liable for any harm that results to users

SAFE EXIT'

It is almost impossible to build a completely safe product or one that will never fail.
When there is a failure of the product *SAFE EXIT* should be provided.
Safe exit is to assure that
i) when a product fails, it will fail safely,

ii) That the product can be abandoned safely and iii) that the user can safely escape the product.

More than the questions of who will build, install, maintain and pay for a safe exit, the most important question is who will recognize the need for a safe exit. This responsibility should be an integral part of the experimental procedure.
Some examples of providing „SAFE EXIT“:
• Ships need lifeboats with sufficient spaces for all passengers and crew members.
• Buildings need usable fire escapes
• Operation of nuclear power plants calls for realistic means of evacuating nearby communication

Classifications of Loyalty

Agency-Loyalty

- Fulfill one's contractual *duties* to an employer.
- Duties are particular *tasks for which* one is *paid*
- *Co-operating* with colleagues
- *Following* legitimate *authority* within the organization.

Identification-Loyalty

- It has to do with attitudes, emotions and a sense of *personal identity*.
- Seeks to meet one's moral duties with personal *attachment and affirmation*

- ***It is against***
- *detesting* their employers and companies, and do work
- *reluctantly* and *horribly* (this is construed as *disloyalty*) This means

- ***Avoid conflicts of interest,***
- Inform employers of any possible conflicts of interest,
- Protect confidential information,
- Be honest in making estimates,
- Admit one's errors, etc.

Loyalty - *Obligation of Engineers Agency-Loyalty*

- ***Engineers are hired to do their duties.***
- Hence *obligated* to employers within proper limits

Identification-Loyalty

Obligatory on two conditions;

1. When some important *goals are met* by and through a group in which the engineers participate
2. When employees are *treated fairly*, receiving the share of benefits and burdens.

But clearly, identification-loyalty is a *virtue* and *not* strictly an *obligation*.