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.