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*.