**Chapter 20: Safety, Risk, and the Engineer**

Managing and reducing *risk* and increasing its opposite, *safety,* are paramount engineering responsibilities.

**20.1 Evaluating Risk in Design**

* Hazards tend to increase in design because of factors such as greater complexity, greater use of toxic dangerous substance, higher speeds, pressure, etc.
* Demand for safety also increases
* Risk Management: structured approach for analyzing, evaluating and reducing risk

**20.2 Risk Management**

* Hazard: anything that has the potential to cause death, property damage, financial waste, any undesirable consequence. The purpose of risk management is to reduce/ eliminate the danger caused by hazards
* The three-step process:
  1. Risk Analysis: identify hazards or their undesirable consequences, and estimating the probability of their occurrence. It is objective and mathematical.
  2. Risk Evaluation (assessment): alternative courses of action to reduce hazards are generated, costs and benefits are calculated, risk perception of people affected is assessed and value judgments are made. Therefore, less objective than risk analysis
  3. Management Decisions: selecting the risks that will be managed, implementing these decisions, allocating the required resources, and controlling, monitoring, reviewing and revising these.
* Good Practice: following established methods for safe design or construction
* From the perspective of liability, good practice is the min. acceptable level of care expected, and more advanced risk management methods are usually essential

**20.3 Analytical Methods**

**20.3.1 Checklist**

* Used when a design has evolved from a previous design whose hazards were carefully listed, so that the consequences of the evolution are easy to identify
* Should be developed as early as possible, should be part of the design criteria
* Checklists are built on past experience. For new products use *predictive techniques* like the following

**20.3.2 Hazard and Operability Studies**

* A.K.A. *structured brainstorming*
* Used mainly in process industries to uncover hazards and problem that may arise during plant operation
* Design must be beyond the concept stage and in more concrete form before the technique can be used
* The study is carried out by a team of experts who have a FULL understanding of the process to be examined
* Some of the concepts used in HAZOP studies are:
  + *Nodes:* points in the process that are to be studied
  + *Parameters:* the characteristics of the process at a node
  + *Design intent:* how an element in the process is supposed to perform, or the intended values of the parameters at each node
  + *Deviations:* the manner in which the elements or the parameters deviate from the design intent
  + *Causes:* the reasons why the deviations occur
  + *Consequences:* what happens as a result of the deviations
  + *Hazards:* the serious consequences (note: the different meaning of hazard in this context)
  + *Guide words:* simple words applied to the elements or parameters to stimulate creative thinking to reveal all of the possible deviations

**20.3.3 Failure modes and effects analysis**

* “Bottom-up” process that estimates the reliability of a complex system from the reliability of its components
* The basic components to investigate depend on the desired resolution of the analysis
* FMEA Process:
  1. List each of the components or subsystems in the unit
  2. Identify each of the components by part name and number
  3. Describe each component and its function
  4. List all the ways (modes) in which each component can fail
  5. For each mode of failure determine the failure effect on other components and on the unit as a whole. Enter the info in the table
  6. Describe how each failure mode can be detected

In addition to FMEA analysis, criticality analysis continues with the following:

* 1. Indicate the action to be taken to eliminate the hazards and identify who is responsible for taking that action
  2. Assess the criticality of each failure mode and its probability of occurrence

The measure of criticality is the seriousness of the consequences

* The FMECA method is effective in determining the consequences of single component failures; but not suitable for determining the effect on the system of the concurrent failure of several system elements

**20.3.4 Fault-tree Analysis**

* “top-down” process
* When a “top” event occurs, all the events that could’ve cause the top event to occur are determined and analyzed. This process continues on subsequent events until it cannot be further broken down
* Independent events are *primary/ basic*
* Events that are not broken down are called *undeveloped events*
* Fault-tree analysis can be used at any stage in the evolution of a product or process

**Ex:** blow dryer



* Events caused by users: some of the events depend solely on the action of the user and cannot be prevented from the design. However, instructions on the proper use and warnings should decrease the probability of injury and lessen the liability of the engineer

**20.4 Safety in Large Systems**

* Examples of systems containing many interconnected parts for which safety analysis is difficult are space navigation, vehicle control, power generation and almost any system with an embedded computer
* Complexity: a system can be thought of as a graph with a set of nodes representing variables or parameters, joined by branches representing processes or basic subsystems. If the # of branches is of the same order as the # of nodes= low complexity, if the number of branches is large compared to the # of nodes= high complexity.
* Coupling: in a tightly coupled system, a perturbation in one part may cause changes in other parts. In a loosely coupled system, perturbations on one part have little effect on other parts
* Response rate: the system response rate affects the opportunity for operator intervention
* Stability: feedback and stability are related to response time and complexity. Interdependence, through info and control feedback paths can lead to unstable modes of operation
* Robustness: a design is considered robust if it brings about fail-safe or fail-soft conditions in the event of trouble. *Fail-safe* system can suffer complete loss of function without any attending damage. *Fail-soft* system may suffer loss of functionality but retains a min level of performance and safety, such as the possibility of manual control

**20.5 System Risk**

* Engineering management risk requires quantification of the probability of hazardous events and their cost of occurrence
* Risk *r* is the product of the probability *p* and the cost *c.* r=pc or log(r)= log(p)+log(c)



* Defining the exposed population: the probability of a hazardous event must be determined relative to the people affected by it
* Event-cost: may be even more difficult to define. Some costs, such as warranty replacement may be relatively easy to estimate, meanwhile the cost borne to others such as society as a whole may be impossible to estimate

**20.6 Expressing the Costs of a Hazard**

* Cost consequences are normally measured in monetary terms. However, the costs to society of an event are not as simple to predict
* Risk to humans is usually measured in terms of *mortality*: the probability of death per year for exposed members of the population, or loss of life expectancy in days
* The wealth of an industrialized society depends on the creativity of its engineering sector, and technical advances almost always involve some risk