1 Introduction, Definitions & Overview

Reliability

- ... is a characteristic of an item, expressed by the probability that the item performs its required function under given conditions during a stated time interval, i.e. $(0, t]$
- Item = entity for investigation, i.e. component, assembly, equipment, subsystem, system
- from a **qualitative** point of view, reliability is defined as the ability of an item to **remain functional**
- from a **quantitative** point of view, reliability is defined as the probability that **no operational interruptions** will occur during a stated time interval $R(t)$

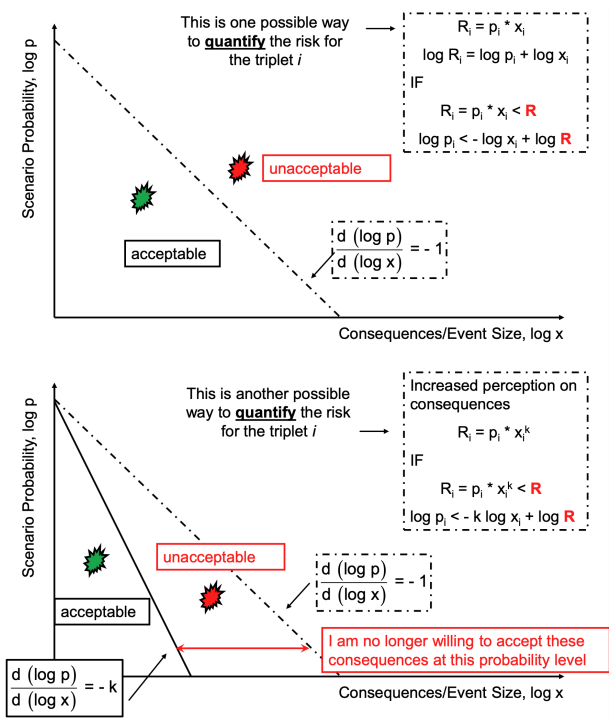
Availability

- Point Availability (PA) is a characteristic of an item expressed by the probability that the item performs its function **at an instant of time** t
- Qualitatively, it can be described as the dependebility
- Average Availability (AA), is the expected time at which the item can perform its required function
- Availability is used to express Point Availability in a sloppy way or Average Availability

In comparison to Availability, the Reliability analysis includes the fact that no item is allowed to fail. This means, the function performed cannot be interrupted (redundant system however can be repaired). Availability incurs that failures can happen on the item level.

Risk

- RISK = POTENTIAL DAMAGE x UNCERTAINTY
- Dictionary: RISK = probability of damage to a person or an object
- We define RISK as a function of an...
  - Accident Scenario, S
  - Probability, p
  - Consequence, x
- We can quantify RISK on the so-called "Farmer's Curve'



The total Risk can be calculated as follows:

$$\text{Total Risk} = \sum p_i x_i^k, k \geq 1 \tag{1}$$

It is entirely possible that the risk of different events can be dominated by either it's probability or its consequence.

- A large probability p is prevented of (minimisation based on high probability)
- A large consequence x is mitigated, protected (minimisation given its large impact)

2 Probability Theory and Reliability Analysis

Definitions:

- Experiment ϵ
- Sample space Ω
- Event E

An event E is a subset of the sample space Ω and the experiment ε yields a set of possible outcoms ($= E$) of the experiment

Certain Events follow Boolean Logic, an event E can occur or not occur, meaning an Indicator Variable X_E is 0 when E does not occur and 1 if E occurs

Uncertain Events follow can either be true or false, with each a probability associated to it. Event E in sample space Ω is triggered with a probability that the outcome has happened or not

Classical Probability

- The experiment ϵ has N possible, elementary, mutually exclusive and equally probable outcomes $A_1, A_2, ..., A_N \in \Omega$
- The event $E = A_1 \cup A_2 \cup ... \cup A_M, M \leq N$
- The probability of event E is defined as $p(E) = M/N$

Kolmogorov Axioms

1. $0 \leq P(E) \leq 1$
2. $P(\Omega) = 1, P(\emptyset) = 0$
3. Mutually exclusive events: $P(\cup_i E_i) = \sum p(E_i)$
4. Non-mutually exlusive events: $P(A \cup B) = P_A + P_B - P(A \cap B)$
5. Conditional probability: $P(A|B) = P(A \cap B)/P(B)$
6. Theorem of total probability: Given an event A in Ω where the space is consisting of exclusive and exhaustive events $\cup_j E_j = \Omega$: $P(A) = \Sigma_i (P(A|E_i)P(E_i))$

Random Variables

- **CDF**: Is a non-decreasing function and returns the probabilty (state) from random variable X from 0 to a given point A: $F_X(X = A) = P(0 < X \leq A)$
- **pdf**: Probability of per unit x (continuous)
- **pmf**: Histogram, it assignes the probability to discrete values x

Summary

- Distribution Percentile x_α:
  - $F_X(x_\alpha) = \alpha/100 = \int_{-\infty}^{x_\alpha} f_X(x)dx$
- Median:
  - $F_X(x_50) = 0.5$
- Mean:
  - $\mu_X = E[X] =< X >= \sum_i x_i p_i$ (discrete)
  - $= \int_{-\infty}^{\infty} x f_X(x)dx$ (continuous)
- Variance:
  - $\sigma_X^2 = \sum (x_i - \mu_X)^2 p_i$ (discrete)
  - $= \int_{-\infty}^{\infty} (x - \mu_X)^2 f_X(x)dx$ (continuous)

Hazard Function (Failure Rate)

For risk and reliability analyses, we can use models whereas the time to failure of a component T can be expressed through a CDF $F_T(t)$ and a pdf $f_T(t)$. The complementary, cumulative function is

$$R(t) = 1 - F_T(t) = P(T \geq t) \tag{2}$$

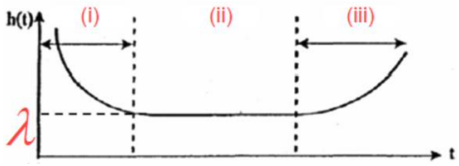
which is decribed as the **Reliability or Survival Function** of the component T at time t and gives the probability of it surviving up to time t without failures.

In order to monitor the failure evolution, given the component has survived up to time t in a time interval dt, one can define a so called **Hazard Function or Failure Rate** $h_T(t)$.

$$h_T(t)dt = P(t < T \leq t + dt | T > t) = \tag{3}$$

$$= \frac{P(t < T \leq t + t + dt)}{P(T > t)} = \frac{f_T(t)dt}{R(t)} \tag{4}$$

The hazard function is depending on time, and is often discribed through the bathtub curve. The failure rate at the beginning is higher (infant mortality, burn in) and decreses after a certain time. The failure rate becomes constant λ and increases at the end through ageing.



Through the definition of $R(t)$ and integrating the hazard function, we receive:

$$F_T(t) = 1 - e^{-\int_0^t h_T(\tilde{t})d\tilde{t}} \tag{5}$$

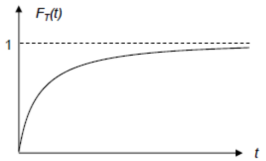
$$R(t) = e^{-\int_0^t h_T(\tilde{t})d\tilde{t}} \tag{6}$$

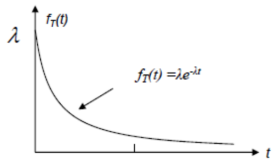
If our hazard function is in its constant phase (constant hazard rate), the failure evolution follows the **Exponential Distribution**:

$$h_T(t)\lambda, t > 0 \tag{7}$$

$$F_T(t) = P(T \leq t) = 1 - e^{-\lambda t} \tag{8}$$

$$R(t) = \begin{cases} f_T(t) = \lambda e^{-\lambda t} & t \geq 0 \\ 0 & t < 0 \end{cases} \tag{9}$$





The mean time to failure (MTTF) can be found through the expectation value

$$E[T] = \frac{1}{\lambda} = MTTF \tag{10}$$

$$Var[T] = \frac{1}{\lambda^2} \tag{11}$$

The failure process is memoryless. Given a component has survived at least until time t_1, the probability of it failing between time t_1 and t_2 is only depending on the time inbetween and not prior to time t_1

$$P(t_1 < T < t_2) = \frac{P(t_1 < T < t_2)}{P(T > t_1)} = \frac{F_T(t_2) - F_T(t_1)}{1 - F_T(t_1)} = \tag{12}$$

$$\frac{e^{-\lambda t_1} - e^{-\lambda t_2}}{e^{-\lambda t_1}} = 1 - e^{-\lambda(t_2 - t_1)} \tag{13}$$

The influence of an ageing process of the components failure rate shows that is not constant through time and hence can be described through the Weibull distribution.

Boolean Logic - Fault Tree Analysis

Fault trees = set of Boolean algebraic equations (one for each gate) $\rightarrow$ structure (switching) function Φ

$$X_T = \Phi(X_1, X_2, X_3, ..., X_N) \tag{14}$$

The top event is connected by an OR-gate, hence if one of each events is true, then the top event will be true. Here some further rules:

- Negation: Given event E, given by the indicator variable X_E, its negation is described by $\overline{X_E} = 1 - X_E$
- Intersection: The event $A \cap B$ is true, if both A and B are simultaneously true:

$$X_{A \cap B} = X_A X_B \tag{15}$$

($X_{A \cap B} = 0$ for mutually exclusive events)

- Union: The event $A \cup B$ is true, if either A or B are true and false if both are false:

$$X_{A \cup B} = 1 - (1 - X_A)(1 - X_B) \tag{16}$$

$$= 1 - \Pi(1 - X_j) = \Pi X_j \tag{17}$$

$$= X_A + X_B - X_A X_B \tag{18}$$

- Probability of event E with expected value Operator $E(\cdot)$: $p(E) = E(X_E)$

$$p(E) = p(X_E = 1) \cdot 1 + p(X_E = 0) \cdot 0 = E(X_E) \tag{19}$$

- Multiple, non-mutually exclusive events:

$$X_\cap = \Pi X_i \tag{20}$$

- Probability of event $E_\cap$ for the intersection of n events:

$$P(E_\cap) = E[X_\cap] = \Pi P(E_j) \text{(if events are independant)} \tag{21}$$

- Union of event $E_\cup$ for the union of n events:

$$X_\cup = 1 - \Pi(1 - X_j) = X_A + X_B + X_C \tag{22}$$
$$-X_A X_B - X_A X_C - X_B X_C - X_A X_B X_C \tag{23}$$

- Probability of even $E_\cup$ for the union of n events:

$$P(E_\cup) = E[X_\cup] = \sum P(E_j) - \tag{24}$$
$$\sum \sum P(E_j \cap E_i) + (-1)^{n+1} P(\cap E_j) \tag{25}$$

Structure Function and Minimal Cut Sets

- Cut Set: Is a logical combination of primary event (**combination of component failures**) which render true the top event (**system failure**)
- Minimal Cut Sets: Cut set that does not have another cut set as a subset. This means repairing one element of the set repairs the entire system. Therefore, removing one element of a MCS makes it no longer a cut set.