Reliability and Availablity

This set of notes is a combination of material from Prof. Doug Carmichael's notes for 13.21 and **Chapter 8 of Engineering Statistics Handbook**. NIST/SEMATECH e-Handbook of Statistical Methods, http://www.itl.nist.gov/div898/handbook/, 2005.
available free from:
see: **NIST/SEMATECH e-Handbook of Statistical Methods on CD**

Including and improving reliability of propulsion (and other) systems is a challenging goal for system designers. An approach has developed to tackle this challenge:
1. a design and development philosophy
2. a test procedure for components and total systems
3. a modelling procedure based on test results, field tests and probability (statistics

Design and development philosophy
recognition that reliability is a product is essentiall the abscence of failures or substandard performance of all critical systems in the design, followed by an examination of the factors leading to failure.

Causes of failure:
a. loading: (inaccurate estimates of) thermal, mechanical or electriacl including vibrations
b. strength: (inaccurate estimates of) the load carrying capacity of the components
c. environment: presence of dirt, high temperature, shock, corrosion, moisture, etc.
d. human factors: heavy handed operators ("sailor proof"), wrong decisions (operator error), criminal activities (sabatoge), poor design, tools left in critical components, use of incorect replacements
e. quality control: or lack thereof; loose control of materials and manufacture, lack of inspection, loose specifications
f. accident; act of God, freak accidents, collisions
g. acts of war: terorism, war damage

designer should recognize these potential causes for failure and try to design devices that will resist failure.

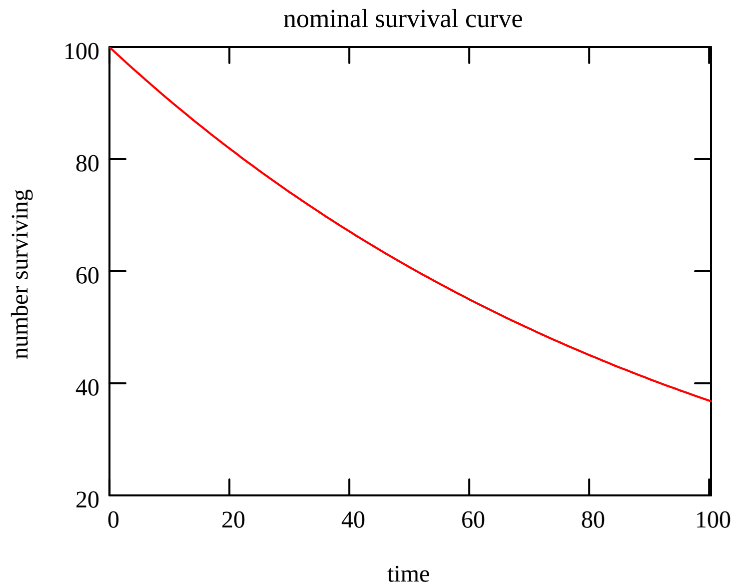
Detailed Design Features
a. try to account for all possible situations in the design stage and eliminate possible failures. Delivering maximumloads and minimum strengths
b. assume that every component can fail, examine the outcome of the failure and try to reduce the risk of damage. Failure Modes and Effects Analysis (FEMA)
c. institute strict quality control in manufacture and maintenance
d. have cleaarly defined specifications (including material specifications and methods of testing)
e. develop technology to meet new challenges. conduct development testing.
f. consider possible war damage and ship collision
g. carry out development testing in arduous conditions

System Design Features
a. calculate probability of failures. (reliability and availability analysis
b. improve system design by standby or redundant systems
c. analyze failures, note trends
d. specify clearly all operating procedures (good operating manuals)
e. require inspection, maintenance and replacement procedures (trend analysis)

Failure testing and analysis
from field or laboratory tests on components or systems determine number of operating units as a function of time (life):

set up N_surv

a typical survival curve might look like this:



define the failure rate at time t as

$$\lambda = \frac{proportion\_failing\_in\_\delta t}{\delta t} = \frac{-\delta N(t)}{N(t)} \cdot \frac{1}{\delta t} = \frac{-1}{N(t)} \cdot \frac{d}{dt} N(t)$$

- as "rate" > 0 consistent with population decline units are: $time^{-1}$

$$-1 \cdot \frac{\frac{d}{dt} N(t)}{N(t)} = \lambda \qquad -1 \cdot \frac{d\,N(t)}{N(t)} = \lambda \cdot dt \qquad \ln\left(\frac{N(t)}{N(0)}\right) = -\int_0^t \lambda(\tau)\, d\tau \qquad N(t) = N_I \cdot \exp\left(-\int_0^t \lambda(\tau)\, d\tau\right)$$

to make some estimates based on this sample:

$$fail\_rate(t, \delta t) := -\frac{N(t + \delta t) - N(t)}{N(t) \cdot \delta t}$$

calculate for modest δt = 0.01 and t =10, 40, 60, 120

$fail\_rate(40, 0.01) = 0.01$ $\quad$ $fail\_rate(10, 0.01) = 0.01$ $\quad$ $fail\_rate(60, 0.01) = 0.01$ $\quad$ $fail\_rate(120, 0.01) = 0.01$

looks like λ = failure rate is a constant, not unusual $\quad \lambda = \frac{-1}{N(t)} \cdot \frac{d}{dt} N(t) = constant$

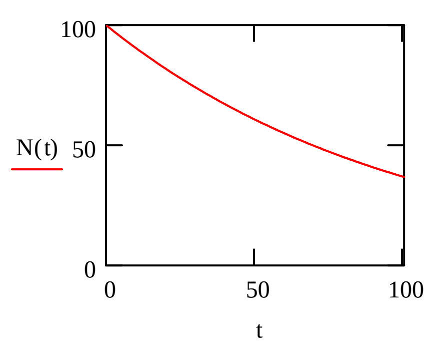
define ... $N_I = N(t = 0)$ $\qquad -1 \cdot \frac{\frac{d}{dt} N(t)}{N(t)} = \lambda \qquad -1 \cdot \frac{\frac{d}{dt} N(t)}{N(t)} = \lambda$

integrate from 0 to t $\quad \ln\left(\frac{N(t)}{N(0)}\right) = -\int_0^t \lambda\, d\tau$

or ... $N(t) = N_I \cdot \exp\left(-\int_0^t \lambda\, d\tau\right)$

set ... $\lambda := 0.01$ $\quad N_I := 100$

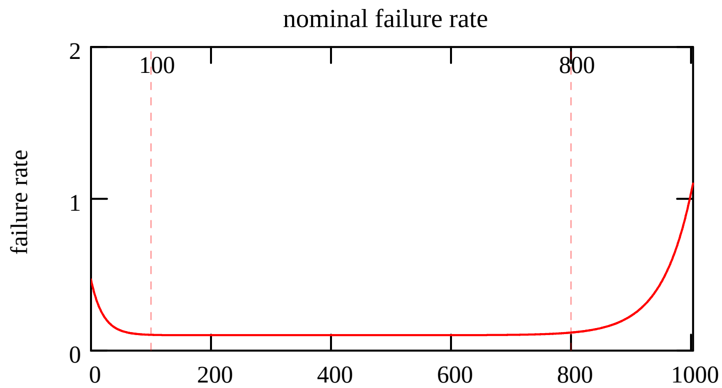
or ... $N(t) := N_I \cdot \exp(-\lambda \cdot t)$



N.B. failure rate is not necessarily the same as (but can be related to) (in this case it is) the probability of failure
see Engineering Statistics Handbook

an actual failure rate curve might look like this:

set up bath tub



three regions are evident:

0 - 100 early failure period = infant mortality rate

100 - 800 intrinsic failure period aka stable failure period => intrinsic failure rate

> 800 wearout failure period - materials wear out and degradation failures occur at an ever increasing rate

for most systems, the failure rate is relatively constant except for wer in and wear out. If the failure rate is constant, the component is said to have random failure.

Reliability

(applies to a particular mission with a defined duration.)
defined as the probability of operating without degraded performance during a specific time period. At time t_1, the number operating is $N(t_1)$ and N_I is the initial number. The reliability is:

$$R(t_1) = \frac{N(t_1)}{N_I}$$ since ... $$-1 \cdot \frac{d\,N(t)}{N(t)} = \lambda \cdot dt$$ $$\ln\left(\frac{N(t_1)}{N_I}\right) = -\int_0^{t_1} \lambda\, dt$$ $$R(t_1) = \frac{N(t_1)}{N_I} = \exp\left(-\int_0^{t_1} \lambda\, dt\right)$$

with λ = constant $$R(t_1) = \exp(-\lambda \cdot t_1)$$ and expanding in a series ... $$R(t_1) = 1 - \lambda \cdot t_1 + \frac{(\lambda \cdot t_1)^2}{2!} - \frac{(\lambda \cdot t_1)^3}{3!} + ..$$

and if ... λ*t1 << 1, $$R(t_1) = 1 - \lambda \cdot t_1$$ e.g. $\lambda t_1 := 0.05$ $\quad 1 - \lambda t_1 = 0.95 \quad \exp(-\lambda t_1) = 0.951$

Mean Time Between (Operational Mission) Failure (MTB(OM)F

with field testing,data is collected in the form of operating time, failures and repair time.

During the field operation of a component or a system, there is a total number of operating hours and a total number of failures. MTB(OM)F is defined

$$MBT(OM)\,F = \frac{accumulated\_life}{number\_of\_failures}$$

For random failures, the failure rate $$\lambda = \frac{number\_of\_failures}{accumulated\_life} = \frac{1}{MBT(OM)\,F}$$

if ... $$\frac{t_1}{MBT(OM)\,F} < 1 \qquad R(t_1) = 1 - \lambda \cdot t_1 = 1 - \frac{t_1}{MBT(OM) \cdot F}$$

Probability of Failure (Q or F)

since probability of success + failure = 1 $\quad R + Q = 1 \quad Q = 1 - R = 1 - \exp(-\lambda \cdot t_1) = \lambda \cdot t_1 = \frac{t_1}{MTBF}$ if ... λ*t1 << 1

now consider separate components C1 and C2 having R_1 and R_2 and Q_1 and Q_2. then ...

$$(R_1 + Q_1)\cdot(R_2 + Q_2) = 1 \qquad (R_1 + Q_1)\cdot(R_2 + Q_2) \text{ expand } \rightarrow R_1\cdot R_2 + R_1\cdot Q_2 + Q_1\cdot R_2 + Q_1\cdot Q_2$$

$R_1\cdot R_2 = \text{probability\_both\_C1\_and\_C2\_operating}$

$R_1\cdot Q_2 = \text{probability\_C1\_operating\_and\_C2\_failed}$

$R_2\cdot Q_1 = \text{probability\_C2\_operating\_and\_C1\_failed}$

$Q_1\cdot Q_2 = \text{probability\_C1\_and\_C2\_failed}$

Series Systems

If it is necessary for all systems to operate, then this termed a series system and is represented as a circuit as:

From above; the probability that both are operating is ... $\quad R_{series} = R_1\cdot R_2$

more generally, $\quad R_{series} = R_1\cdot R_2\cdot R_3 .. R_n = \exp\left[-\sum_n (\lambda_i\cdot t_1)\right] = \prod_n R_i$

e.g. ... $\quad R_1 := 0.9 \quad R_2 := 0.9 \quad R_3 := 0.9 \quad$ 2 components $\quad R_1\cdot R_2 = 0.81$

$R_n := 0.9$

6 components $\quad R_n^{\,6} = 0.531$

Parallel Systems

If there is redundancy, and either C1 or C2 is required for operation then this is a parallel scheme ...

$R_{parallel} = R_1\cdot R_2 + R_1\cdot Q_2 + Q_1\cdot R_2 = 1 - Q_1\cdot Q_2$

generally ... $\quad R_{parallel} = 1 - Q_1\cdot Q_2\cdot Q_3 .. Q_n = 1 - \prod_n Q_i \quad$ when Qi = Qn $\quad R_{parallel} = 1 - Q_i^{\,n}$

e.g. ... $\quad R_1 := 0.9 \quad R_2 := 0.9 \quad R_3 := 0.9 \quad Q_i := 0.1$

$R_n := 0.9$

2 components $\quad 1 - Q_i^{\,2} = 0.99$

R out of N

see Handbook of Statistical Methods section 8.1.8.4.R out of N model

If a system has n components and reqires any r to be operational; assuming

- all components have thesame reliability Ri
- all components operate independent of one another (as far as failure is concerned)
- the system can survive any (n - r) components failing, but fails at the instant the n - r - 1)th component fails

System reliability is given by the probability of exactly r components surviving to time t + the probability of exactly (r + 1) components surviving to time t ... up to all n surviving. These are binomial probabilities:

$$R_s(t) = \sum_{i=r}^{n} \left[\binom{n}{r}\cdot R_i^{\ i}\cdot\left(1 - R_i\right)^{n-i}\right]$$

for example (where Ri are not necessarily equal ... $n = 4$ $r = 2$ i.e. four components of which two are required for operation

2 components $R_1\cdot R_2\cdot Q_3\cdot Q_4 + R_1\cdot R_3\cdot Q_2\cdot Q_4 + R_1\cdot R_4\cdot Q_2\cdot Q_3 + R_2\cdot R_3\cdot Q_1\cdot Q_4 + R_2\cdot R_4\cdot Q_1\cdot Q_3 + R_3\cdot R_4\cdot Q_1\cdot Q_2$

3 components $R_1\cdot R_2\cdot R_3\cdot Q_4 + R_1\cdot R_3\cdot R_4\cdot Q_2 + R_1\cdot R_2\cdot R_4\cdot Q_3 + R_2\cdot R_3\cdot R_4\cdot Q_1$

n = 4 components $R_1\cdot R_2\cdot R_3\cdot R_4$

sum all these for R_s

$$\begin{aligned}R_s = {} & R_1\cdot R_2\cdot Q_3\cdot Q_4 + R_1\cdot R_3\cdot Q_2\cdot Q_4 + R_1\cdot R_4\cdot Q_2\cdot Q_3 + R_2\cdot R_3\cdot Q_1\cdot Q_4 + R_2\cdot R_4\cdot Q_1\cdot Q_3 + R_3\cdot R_4\cdot Q_1\cdot Q_2 \ldots \\ & + R_1\cdot R_2\cdot R_3\cdot Q_4 + R_1\cdot R_3\cdot R_4\cdot Q_2 + R_1\cdot R_2\cdot R_4\cdot Q_3 + R_2\cdot R_3\cdot R_4\cdot Q_1 \ldots \\ & + R_1\cdot R_2\cdot R_3\cdot R_4\end{aligned}$$

N.B. a series system is one with r = n i.e. all components must operate. a parallel system is one with r = 1

Standby Systems

Standby scenario will be more reliable than parallel as seen in Handbook of Statistical Methods section 8.1.8.5.Standby model

Availability

Availability is the probability that a component is operational, i.e. it is not being repaired

$$\text{MTTR} = \text{mean\_time\_to\_repair} = \frac{\text{total\_time\_for\_repairs}}{\text{number\_of\_repairs}}$$

For every failure there should be a repair, so that the average component is repaired for the average time after it has operated for the average time between failures. Average time between failures is MTBF and for repair MTTR, so assuming component is either operating or being repaired ...

$$\text{availability} = A = \frac{\text{operating\_time}}{\text{operating\_time} + \text{repair\_time}} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

if ... $\text{MTBF} > \text{MTTR}$ (<<) which it should be ...

$$A = \frac{MTBF}{MTBF + MTTR} = 1 - \frac{MTTR}{MTBF} \qquad \frac{1}{1+a} = (1+a)^{-1} = 1 - a \qquad a < 1 \quad (<<)$$

probability that it is being repaired is ... Q_A

$$Q_A = 1 - A = \frac{MTTR}{MTBF}$$

and as above, availability for series systems would be ..

$$A_{series} = A_1 \cdot A_2 \cdot A_3 \,..\, A_n = \prod_n A_i$$

and parallel ...

$$A_{parallel} = 1 - Q_1 \cdot Q_2 \cdot Q_3 \,..\, Q_n = 1 - \prod_n Q_i$$