RELIABILITY

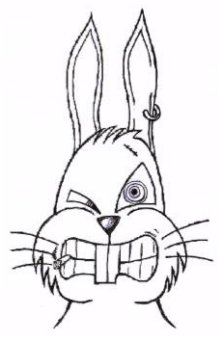
Definition - **Reliability**

The probability that a system or piece of equipment performs its specified functions within specified limits under defined conditions for a prescribed length of time.

In other words it is a measure of the system's likelihood of meeting the requirement specification - i.e. maintaining its **Quality.**

A related concept: - **Availability**
The probability that a system or piece of equipment will be capable of performing its specified functions within specified limits under defined conditions at any given time during the life of the system or equipment. (Covered further in the Maintenance lecture).

WARNING - WHAT IT ISN'T!
Reliability is <u>not</u> the equivalent to safety - unreliable systems can be safe and reliable systems can be dangerous.



Of course the reliability of those functions that are in a hazard path are a part of the overall safety of a system. But there are many other factors that contribute to the overall safety.

RESILIENCE

When considering system Quality it must be remembered it is the system ability to meet the specification that is important - not the failure of specific components within it.

A systems ability to continue to meet its specification, that is maintain its "quality", with failed components is known as its resilience.

In a completely optimised system all components would contribute to the specified functions - so the loss of any component would mean the loss of quality. That is the system would have no resiliency.

To provide resiliency, multiple components are used to do the same job. If one fails the others carry on doing the job - a concept called redundancy.

REDUDANCY

Three routes to redundancy:

1 - Hot redundancy: A number of systems do the task all of which are in use but if one is lost the performance of the remaining units still enable the specification to be met. Example; engines on a passenger aircraft.

(a variant on hot redundancy is to accept a degraded performance – i.e. below the full specification -with the loss of a unit)

2 - Cold Redundancy: Again a number of units are installed which can perform the function but only one is switched on and in use. If the hot unit fails another unit is brought into the system.

3 - Alternative Routing: In complex systems it sometimes possible to configure the system after a component failure to maintain the function using other components which nominally would be performing other functions.

An example of combining hot reundancy and alternative routing is the Integrated Modular Avionics philosphy adopted in many modern aircraft.

MEASURING RELIABILITY

The technical meaning of reliability is the same as the common sense definition. However in technical use we need to quantify what we mean by reliability.

There are two normal methods of defining a system's reliability

- Probability of failure over operational lifetime which is the generally accepted definition of "**reliability**". Normally used when only a few systems are constructed or purchased and system failure is not anticipated.

- The failure rate; expressed as **Mean Time Between Failures (MTBF)** or as a "Failure Rate per Unit time". Normally use when a large number of systems or components are purchased and failure of some systems is expected.

These are linked by the expression R = 1 - (time/MTBF).

HOW DO YOU FIND RELIABILITY VALUES?

For **established components**
– For small simple components - batch testing from the production line
…- For more complex components – data derived from in service experience.

For **new components** - comparison with similar sorts of component

(With electrical systems there are other methods - see Blanchard and Fabrycky Chapter 13 and Aslaksen and Belcher Chapter 10)

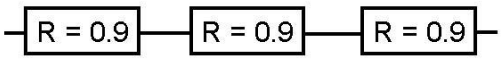
For **complete systems** - Reliability Models

A reliability model (normally express as a diagram) is a representation of all the elements and then all the separate reliabilities of each elemment are combined to assess the overall system reliability. Thus you must have the reliabilities of all your components (see above) to produce a Reliability model.

For real systems this modelling is normally done on a computer (of course).

COMBINING RELIABILITIES IN A RELIABILITY MODEL

Series - All components in the chain must work for the system to meet its specification. Multiply together to get the total reliability:

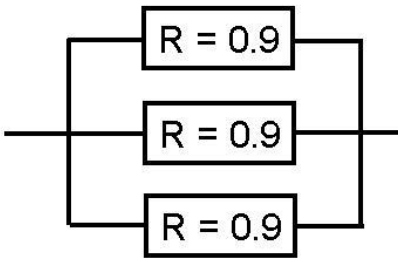


Total Reliability = 0.729

$$R = R_1 * R_2 * R_3 \text{ etc.}$$

Since values of R must be less than one, total reliability is reduced by more components.

Parallel - Represents redundancy - only one Component in the group needs to work for system to meet its specification To get the total reliability find the probability of all components failing, then can combine get probability at least one works.



Total Reliability = 0.99

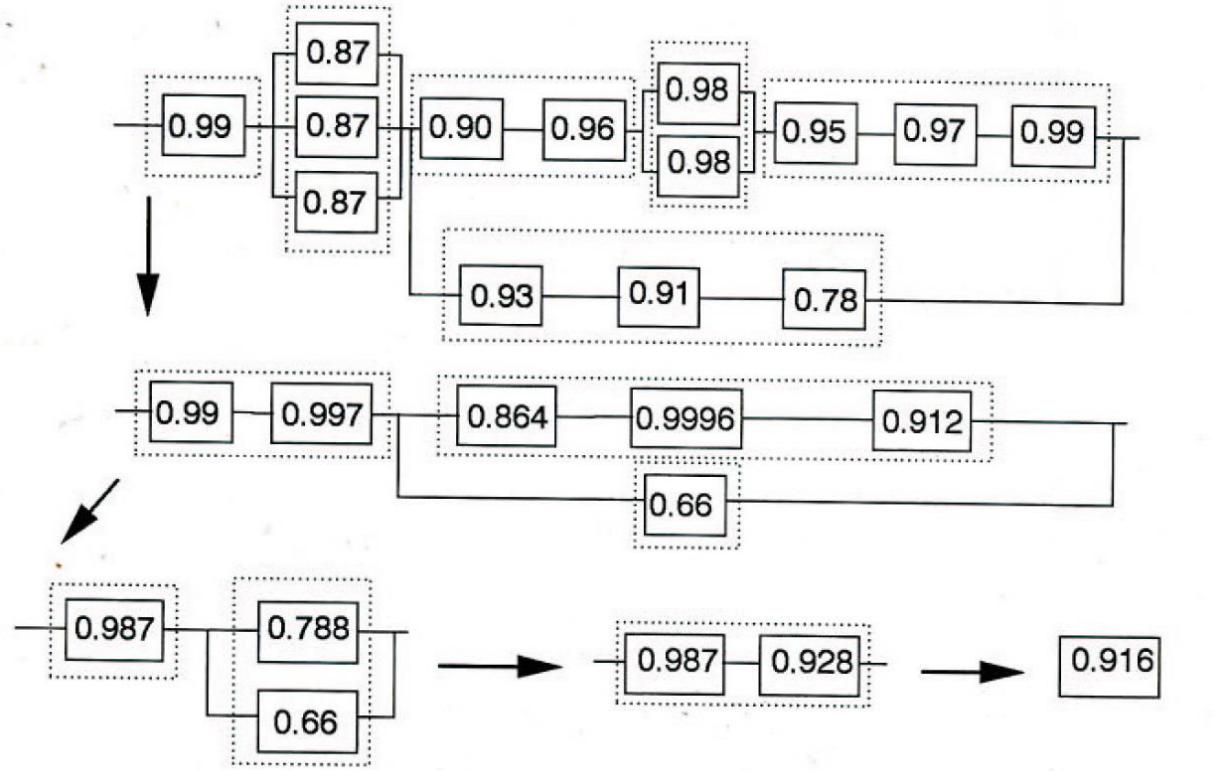
$$R = 1 - ((1 – R_1) * (1 - R_2) * (1 - R_3) \text{ etc.})$$

In this case reliability is increased by more components

Warning: sometimes things that are physically configured in parallel in a system are all required to work for the system to meet its specification and thus are not redundant (e.g landing gear on an aircraft). For reliability purposes they are in series and their reliabilities should be multiplied.

A Reliability Model successively simplifies the overall system model by grouping components into series and parallel and combining them until only one box remains.

EXAMPLE OF A RELIABILITY MODEL



A WORD OF WARNING ABOUT SYSTEM RELIABILITY FIGURES

A reliability figure is often specified in the requirements and this is verified during development by analysis using Reliability models. The problem the figure that is arrived at by analysis is nearly always optimistic and the real system in operation will fail more often. The reasons for this include

- It is often difficult to get everything included (e.g. electrical harness, structure etc.).
- Neglecting the reliability switching of redundant components.
- Situations where system stresses some components more than specification and this is not identified.
- It does not include manufacturing and maintenance problems.

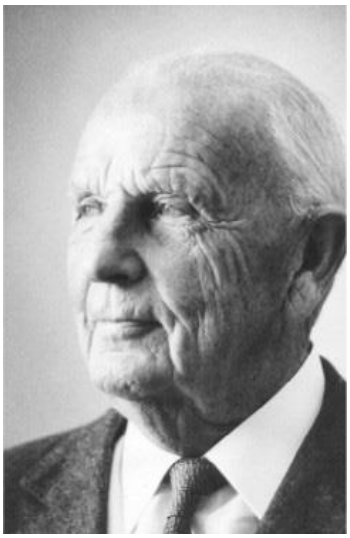
This is particularly true of Space systems. Aircraft have test flights and maintenance between flights. As a result they are in the flat part of the bathtub curve. Space systems fly only once and are effectively are on the wear in part of the curve. As a result space systems (and missiles) generally are very noticeably lower in reliability than the theoretical models predict.

WEIBULL DISTRIBUTIONS

So far we have assumed reliability to be independent of time.

In real life it isn't.

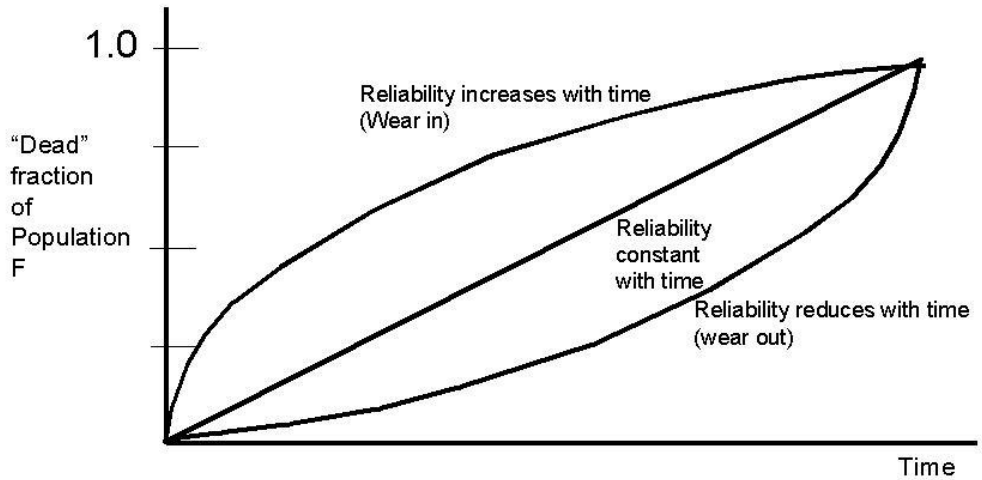
The maths to deal with this is called the Weibull distribution after Waloddi Weibull, the Swedish Engineer who highlighted the value of these distributions in reliability analysis.



Waloddi Weibull (1887-1979). Weibull's first paper on the subject was published in 1939 (A Statistical Theory of the Strength of Materials),", but the method did not attract much attention until the 1950's after his most famous paper "A Statistical Distribution Function of Wide Applicability," (ASME Journal Of Applied Mechanics). Dispite widespread uncertainity as to the validity of the conclusions (including by Weibull himself) quick confirmation with practical examples showed it to be both accuarate and useful.

Much of the theoretical work had been done in the 1920's by the German statistician Emil Gumbel.

LOSS DUE TO FAILURES IN A POPULATION



If we assume the form of the curve is an exponential with a generic equation:

$$F(t) = 1 - e^{-\left(\frac{t}{\alpha}\right)^{\beta}}$$

The rate at which a population declines will be the differential of

$$F(t) = 1 - e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \qquad (1)$$

Which is:

$$f(t) = \frac{ß}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1} e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \qquad (2)$$

The probability of failure of any member of the population (i.e.the reliability) as a function of time will be given by

$$R(t) = \frac{\text{Rate population declines}}{\text{Remaining population}} = \frac{\text{Eq(2)}}{1 - \text{Eq(1)}}$$

$$= \frac{\frac{ß}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1} e^{-\left(\frac{t}{\alpha}\right)^{\beta}}}{1 - \left(1 - e^{-\left(\frac{t}{\alpha}\right)^{\beta}}\right)} = \frac{ß}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1}$$

$R(t) = \frac{ß}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1}$ is the Weibull Distribution

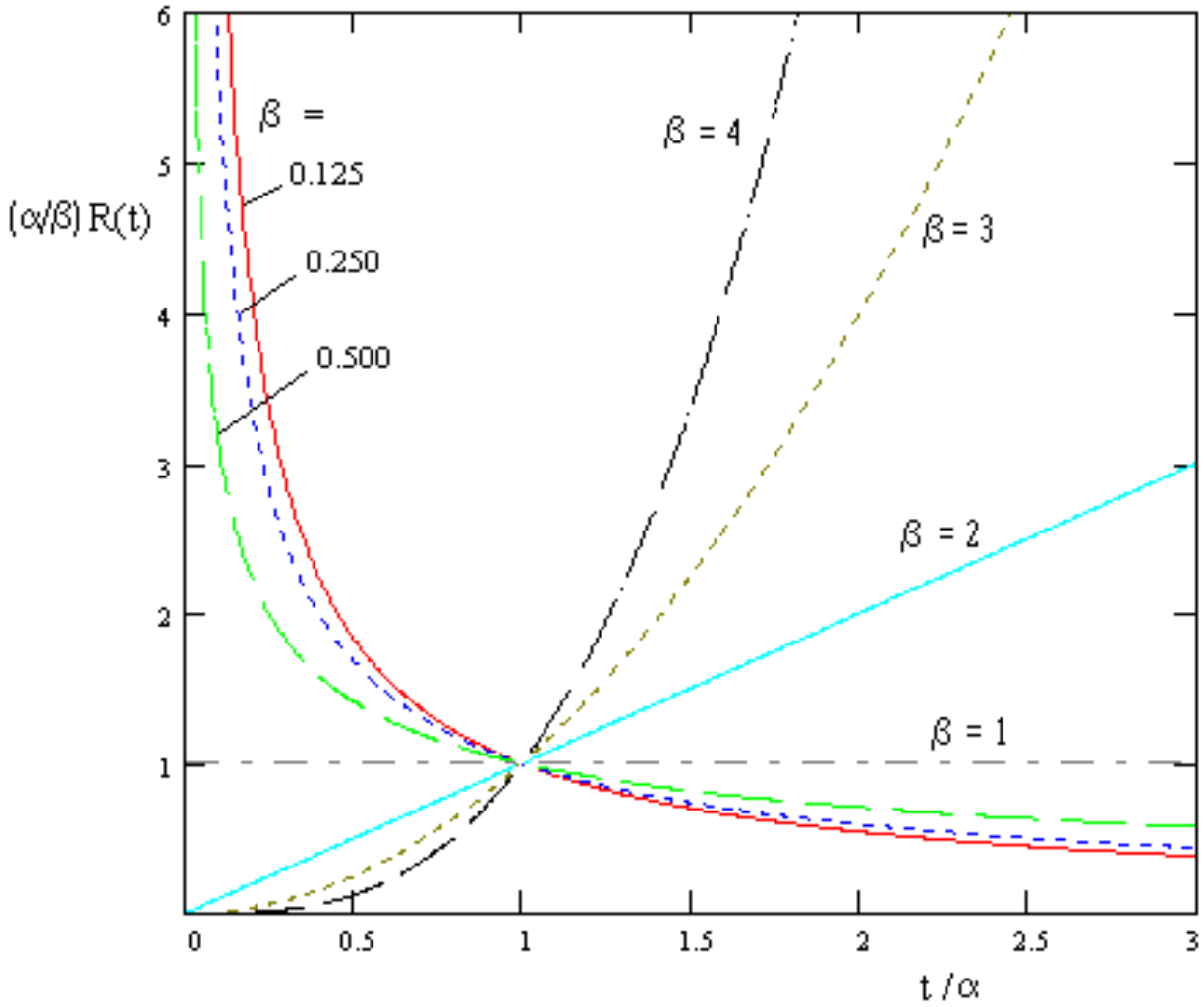
α and β are constants for any distribution:

α is called the "Scale Parameter "
- it scales the function

β is called the " Shape Parameter "
- it gives the distribution its shape

β is of particular importance as using different values enables the basic formula to model many different reliability cases.

THE EFFECT OF β ON DISTRIBUTION SHAPE



THREE FAILURE FACTORS

Wear-in (β < 1)

Failures due to manufacturing factors (e.g tolerance mismatches, build errors) and good design with production in mind can help reduce this. This period is also known as "infant mortality."

Testing should cover the wear in period before delivery to customer. For example military standard electronic components are "burnt in" before delivery.

Constant Failure (β = 1)

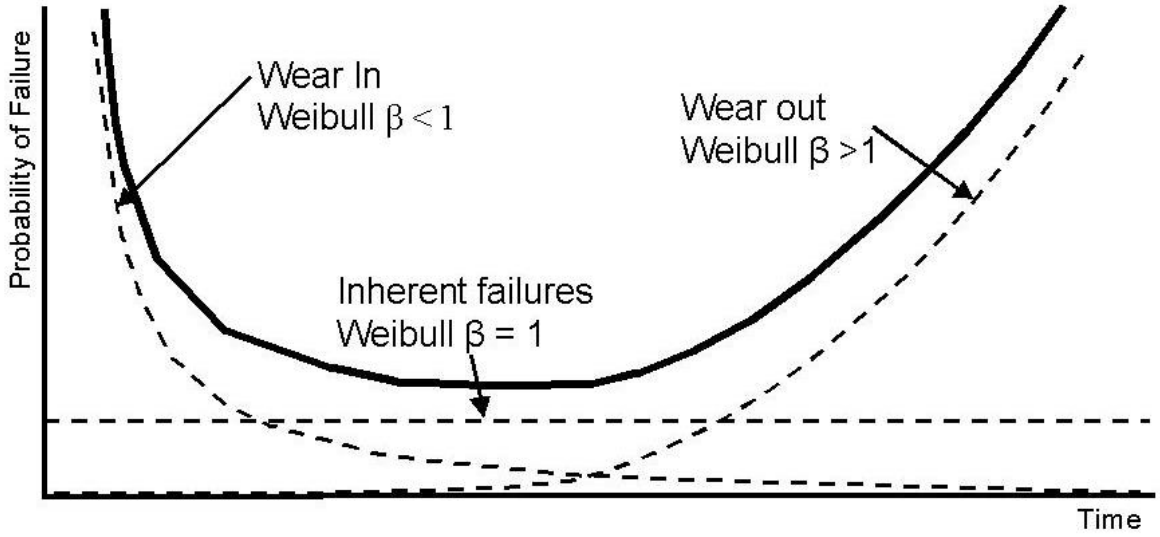
This is the region where the reliability (or MTBF) is both constant and the lowest over the system lifetime. Failures are due to random events that are equally likely at any time in the component life. This is the region where it is desirable to place the operational life for obvious reasons.

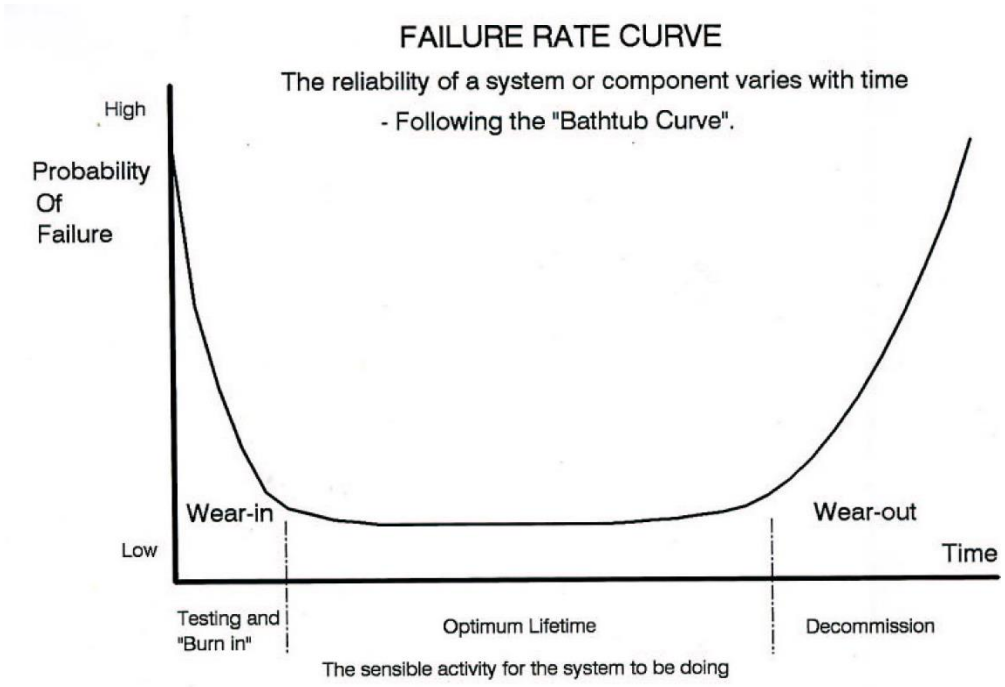
Wear-out (β > 1)

Failures due to system use, wear, material degradation, environmental damage etc.

Some aspects of wear out can be controlled with service and maintenance but in the end all products have a planned life after which the reliability (and safety) is expected to drop and the system should be decommissioned.

When the Weibull distributions for these three failure types are superimposed we get the "Bathtub Curve" (because it looks like the cross section of a bathtub).





FAILURE MODE, EFFECT, AND CRITICALITY ANALYSIS (FMECA)

This is a document produced while defining the system (i.e. in Phase B but it is normally updated thereafter). It typically takes the form of a very long series of tables and aims to identify every possible failure that can happen on a system, and the impact if that failure should occur.

It can either be a

FMEA (only looks at modes and effects) more normal at the component or element level

or a

FMECA which also looks at criticality - i.e. how important is the failure and action to prevent or correct the failure which is more appropriate as a system level analysis.

Of each item in the system the document gives:

- Description of all the ways it can fail (Modes)
- What could cause the failure
- What would be the effect (Effect)
- How likely is it to happen
- What is the impact of the failure on the system (Criticality) - FMECA only
- What do you do about it - FMECA only

EXAMPLE FMCEA - AN ELECTRIC KETTLE

Component	Failure Mode	Likely Cause	Effect	Prob.	Criticality	Prevention Or Action
Plug	Distortion or break	Mechanical abuse	No current	Low	Loss of operation	Replace plug
	Wires disconnect	Load	No current	Medium	Loss of operation	Rewire plug
Fuse	Blow	Over-current	No current	Medium	Loss of operation	Replace fuse
Flex	Overheating	Over-current	Heating	Medium	Fire	Fuse blows first
	Break	Mechanical abuse	No Current	Medium	Loss of operation	Replace flex
Element	Overheating	No water	Heating	High	Fire, Burnout	Cut off trip switch
	Break	Mechanical abuse	No current	Low	Loss of operation	Replace
Trip Switch	Triggers incorrectly	Wear	No current	Low	Loss of operation	None
Container	Hole	Mechanical abuse	Leak, Heating	Low	Fire, Burnout	See element overheating
Handle	Break	Mechanical Abuse	Unable to Handle	Low	Loss of Operation	None