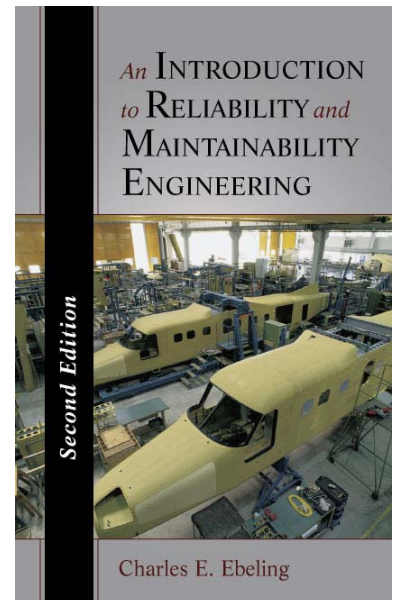# An Introduction to Reliability & Maintainability Engineering

Chapter I Introduction

Things Fail!

- 1946 – the fleet of Lockheed Constellation aircraft was grounded following a crash killing four of the five crew members.
  - The crash was attributed to a faulty design in an electrical conduit which caused the fuselage to burn.
- 1978 - Ford Pinto, was recalled for modifications to the fuel tank to reduce fuel leakage and fires resulting from rear-end collisions.
  - Numerous reported deaths, lawsuits, and the negative publicity eventually contributed to Ford discontinuing production of the Pinto.
- 1979 - the left engine of a DC-10 broke away from the aircraft during take-off killing 271 people.
  - Poor maintenance procedures and a bad design lead to the crash. Engine removal procedures introduced unacceptable stresses on the pylons.

More Things Fail!

- 2000 - Firestone's steel-belted radials failed at an abnormal rate as a result of the outer tread coming apart from the main body of the tire.
  - Based strictly on the excessive number of failures, Firestone was forced to recall 7.5 million tires.
- 1940- the Tacoma Narrows Bridge, five months old, collapsed into Puget Sound from vibrations caused by high winds.
  - Metal fatigue induced by several months of oscillations led to the failure.
- 1983 -The Manus River Bridge (Greenwich, Connecticut) collapsed killing three and injuring three people.
  - blame has been placed on the original design, on corrosion that caused undetected displacement of the pin-and-hanger suspension assembly, poor maintenance and inadequate inspections.

More of More Things Fail!

- 1978 - the Hartford (Connecticut) Civic Center Coliseum roof collapsed from structural failure due to the weight of the snow and ice which accumulated on the roof.
  - A major shortcoming in the roof frame system was the lack of redundancy of members to carry extra loads when other individual members fail. An inadequate safety margin may also have contributed.
- 1979 - The Three Mile Island disaster which resulted in a partial meltdown of a nuclear reactor was a result of both mechanical and human error.
  - A backup cooling system was down for routine maintenance when air cut off the flow of cooling water to the reactor. Warning lights were hidden by maintenance tags. An emergency relief valve failed to close causing additional water to be lost from the cooling system. Operators were reading gauges that were not working properly or taking the wrong actions from those that were operating.

Things keep failing!

- 1986 - Explosion of the space shuttle Challenger was a result of the failure of the rubber O-rings which were used to seal the four sections of the booster rockets.
  - The below freezing temperatures prior to launch contributed to the failure by making the rubber brittle.
- 2003 - Space Shuttle Columbia disintegrated over Texas during re-entry into the Earth's atmosphere, with the loss of all seven crew members
  - loss was a result of damage sustained during launch when a piece of foam insulation the size of a small briefcase broke off the Space Shuttle external tank under the aerodynamic forces of launch.
- 2007 - The entire span of the Interstate 35W bridge collapsed where the freeway crosses the river in Minneapolis
  - Failure of undersized, steel gusset plates was reason for collapse. Engineers who designed the bridge in the 1960s either failed to calculate or improperly calculated the thickness needed for the plates that were to hold the bridge together.

What is the Objective of Reliability Engineering?

Reliability and maintainability engineering attempts to study, characterize, measure, and analyze the failure and repair of systems in order to improve upon their operational use by increasing their design life, eliminating or reducing the likelihood of failures and safety risks, and reducing downtime thereby increasing available operating time.

Deterministic Versus Random Failures

- Traditional approach to safety in engineering is to design into a product a high safety margin or safety factor.
  - a **deterministic** method in which a safety of factor of perhaps 4 to 10 times the expected load or stress would be allowed for in the design.
  - Safety factors often result in overdesign thus increasing costs or less frequently in underdesign when an unanticipated load or a material weakness results in a failure.
- Approach taken in reliability is to treat failures as random or probabilistic occurrences.
  - In theory, if we were able to comprehend the exact physics and chemistry of a failure process, many internal failures of a component could be predicted with certainty.
  - With limited data on the physical state of a component, and an incomplete knowledge of the physical, chemical (and perhaps biological) processes which cause failures, failures will appear to occur at random over time.
  - This random process may exhibit a pattern which can be modeled by some probability distribution.

Random Phenomena
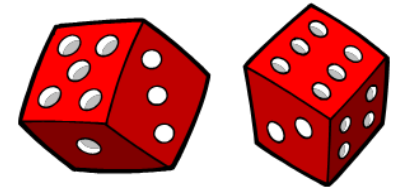
- Observed in practice when dealing with large numbers of components.

- Statistically can predict the failure or of these components.

- Failures caused by events external to the component, such as environmental conditions like excessive heat or vibration, hurricanes or earthquakes, will appear to be random.

  - with sufficient understanding of the conditions resulting in the event as well as the effect such an event would have on the component, then we should also be able to predict these failures deterministically.

  - This uncertainty, or incomplete information, about a failure process is therefore a result of its complexity, imprecise measurements of the relevant physical constants and variables, and the indeterminable nature of certain future events.

Some Definitions

Reliability is defined to be the probability that a component or system will perform a required function for a given period of time when used under stated operating conditions - R(t).

Maintainability is defined to be the probability that a failed component or system will be restored or repaired to a specified condition within a period of time when maintenance is performed in accordance with prescribed procedures - M(t).

Availability is defined as the probability that a component or system is performing its required function at a given point in time when used under stated operating conditions - A(t).
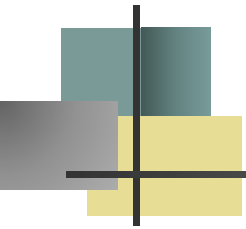
Why Study Reliability?

- the increased complexity and sophistication of systems,

- public awareness and insistence on product quality,

- new laws and regulations concerning product liability,

- government contractual requirements to meet reliability and
- maintainability performance specifications,

- profit considerations resulting from the high cost of failures,
- their repairs, and warranty programs.

Complexity and Reliability
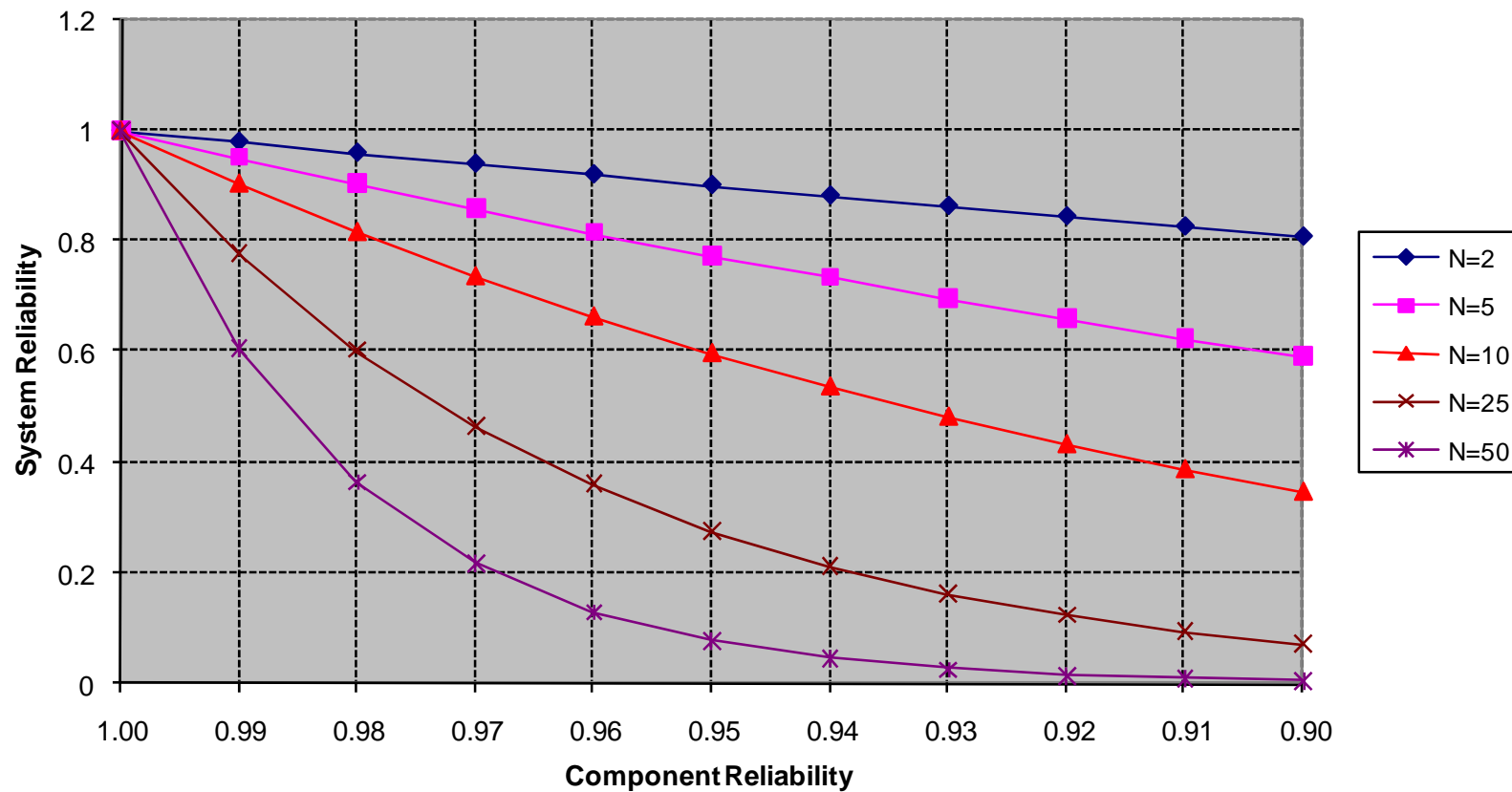
Government Regulations

Food and Drug Act

Flammable Fabrics Act

Federal Hazardous Substance Act

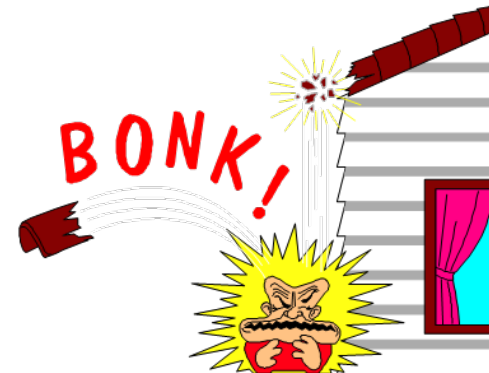National Traffic and Motor Vehicle Safety Act

Fire Research and safety Act

Child Protection and Toy Safety Act

Poisson Prevention Packaging Act

Occupational Safety and Health Act

Federal Boat Safety Act

Consumer Product Safety Act

Gallup Survey

Attribute	Average Score
Performance	9.5
Lasts long time (reliability)	9.0
Service	8.9
Easily Repaired (maintainability)	8.8
Warranty	8.4
Easy to Use	8.3
Appearance	7.7
Brand Name	6.3
Packaging/Display	5.8
Latest Model	5.4

Reliability vs Quality

Quality is the amount by which a product satisfies the users' (customers') requirements. Product quality is in part a function of design and conformance to design specifications during manufacture.

Reliability is concerned with how long the product continues to function once it becomes operational. Therefore reliability can be viewed as the quality of the product's operational performance over time, and as such it **extends quality into the time domain.**

Example 1.1

- Company manufactures small motors for use in household appliances

- designed a new motor which has experienced an abnormally high failure rate with 43 failures reported from among the first 1000 motors produced.

- Possible causes of these failures included faulty design, defective material, or a manufacturing (tolerance) problem.

- The company initiated an aggressive accelerated life testing program where they observed that those motors produced near the end of a production run were failing at a higher rate than those at the start of the run.
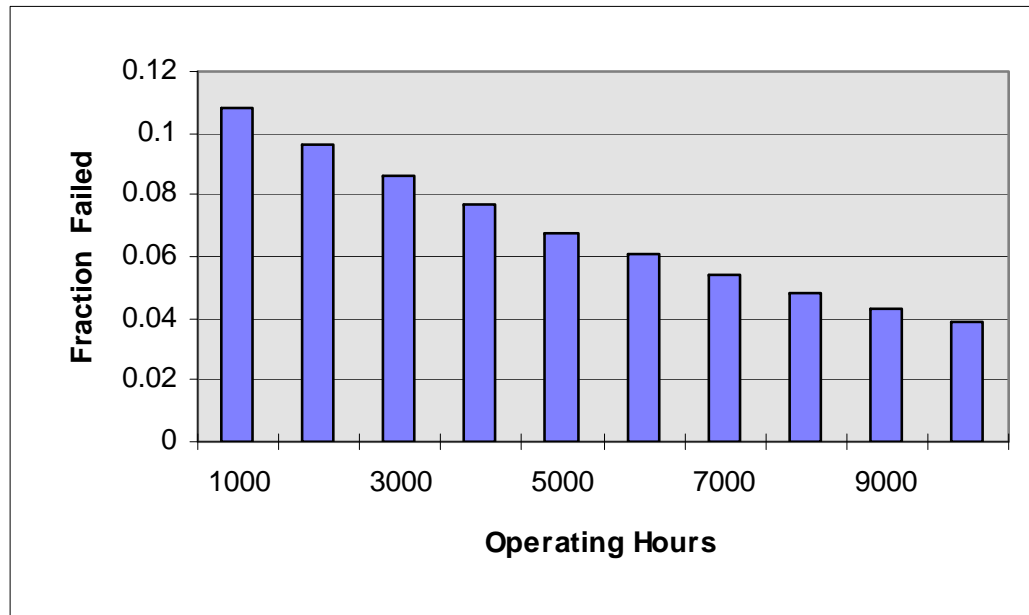
Example 1.1

- Table 1.1 summarizes the results of testing program
- The failure rate is computed by dividing the number of failures by the total number of hours on test.
- It was assumed that the production process was going "out of control" and design tolerances were not being met.
- Additional emphasis placed on quality control

motor	# 1-100	# 101-200	# 201-300	# 301-400	# 401-500	Total
nbr tested	12	11	12	12	15	62
hours on test	2540	2714	2291	1890	2438	11873
number failed	1	0	1	5	7	14
failure rate	0.000394	0	0.000436	0.002646	0.002871	0.001179

Example 1.2

- For a new VCR unit produced by the XYZ Company, the following distribution of the time to failure was obtained from a reliability testing program.

Example 1.2

- From this data, F(t) was derived where F(t) is the probability of a VCR failure occurring by time t (in operating hours):

$$F(t) = 1 - e^{-\frac{t}{8750}}$$

- Assuming the typical consumer will use the VCR an average of 3 hours a day, then for the first year 1095 operating hours (3 x 365) will be observed. Therefore, the probability of a unit failing is

$$F(1095) = 1 - e^{-\frac{1095}{8750}} = 1 - .8824 = .1176$$

- With over ten percent of the units sold expected to fail during the first year, the company decided to initiate a reliability growth to improve product reliability, reduce warranty costs, and increase customer satisfaction.

Example 1.3

- A continuous flow production line requires a product to be processed sequentially on 10 different machines.

- When a machine breaks down, the entire line must be stopped until the failure is repaired – an average downtime of 12 hours.

- Machine specs require a .99 reliability for each machine over an 8 hour production run. Therefore the reliability of the production line over an 8 hour run is $.99^{10}$ = 90 percent.

- Assuming a constant failure rate (exponential failure distribution), this is equivalent to a Mean Time Between Failures (MTBF) of 75.9 operating hours, found by solving the following for the MTBF:

$$R(8) = e^{-\frac{8}{MTBF}} = .90$$

Example 1.3

- Under fairly general conditions, the steady-state availability of the line is given by

$$A = \frac{MTBF}{MTBF + MTTR} = \frac{75.9}{75.9 + 12} = .86$$

  where MTTR = the Mean Time to Repair.

- In order to meet production quotas, the line must maintain at least a .92 availability.

- Since improvements in machine reliability above .99 did not appear feasible, the company decided to increase availability by improving the maintainability (i.e. decreasing the MTTR).

- A minimum MTTR is obtained by solving the following availability formula for x:

$$\frac{75.9}{75.9 + x} = .92; \ x = 6.6 \, hr.$$
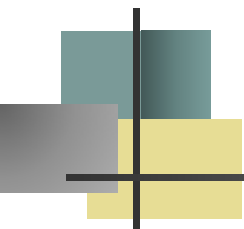
Reliability Specification

I'm a failure!

Define failure - what function is performed?

Identify failure modes

Unambiguous

Observable
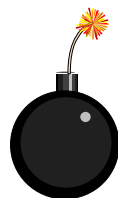
Time to failure

Calendar time

Operating hours

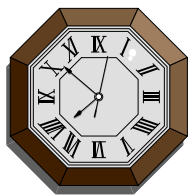Number of cycles (on/off, load reversals, missions)

Vehicle miles - incidents per 1000 vehicles (IPTV)

State normal conditions

Design loads (weight, voltage, pressure, etc.)

Environment (temp., humidity, vibration, contaminants, etc.)

Operating (usage, storage, maintenance, shipment, etc.)

Reliability Specification (continued)

$$\boxed{R(t)}$$

Avoid vagueness

    e.g. "as reliable as possible"

Be realistic

    e.g. "will not fail under any operating conditions

Avoid using only the MTTF (or MTBF)

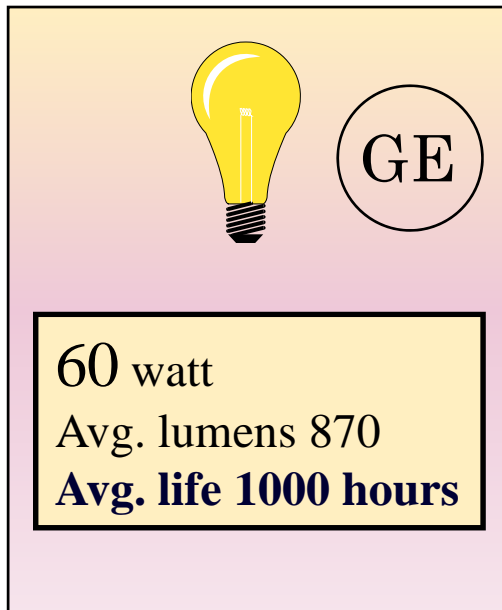   unless failure rate is constant

Frame in terms of reliability or design life

    a 95 percent reliability at 10,000 operating hours

    a design life of 10,000 operating hours with a 95 percent reliability

Example - Reliability Specification
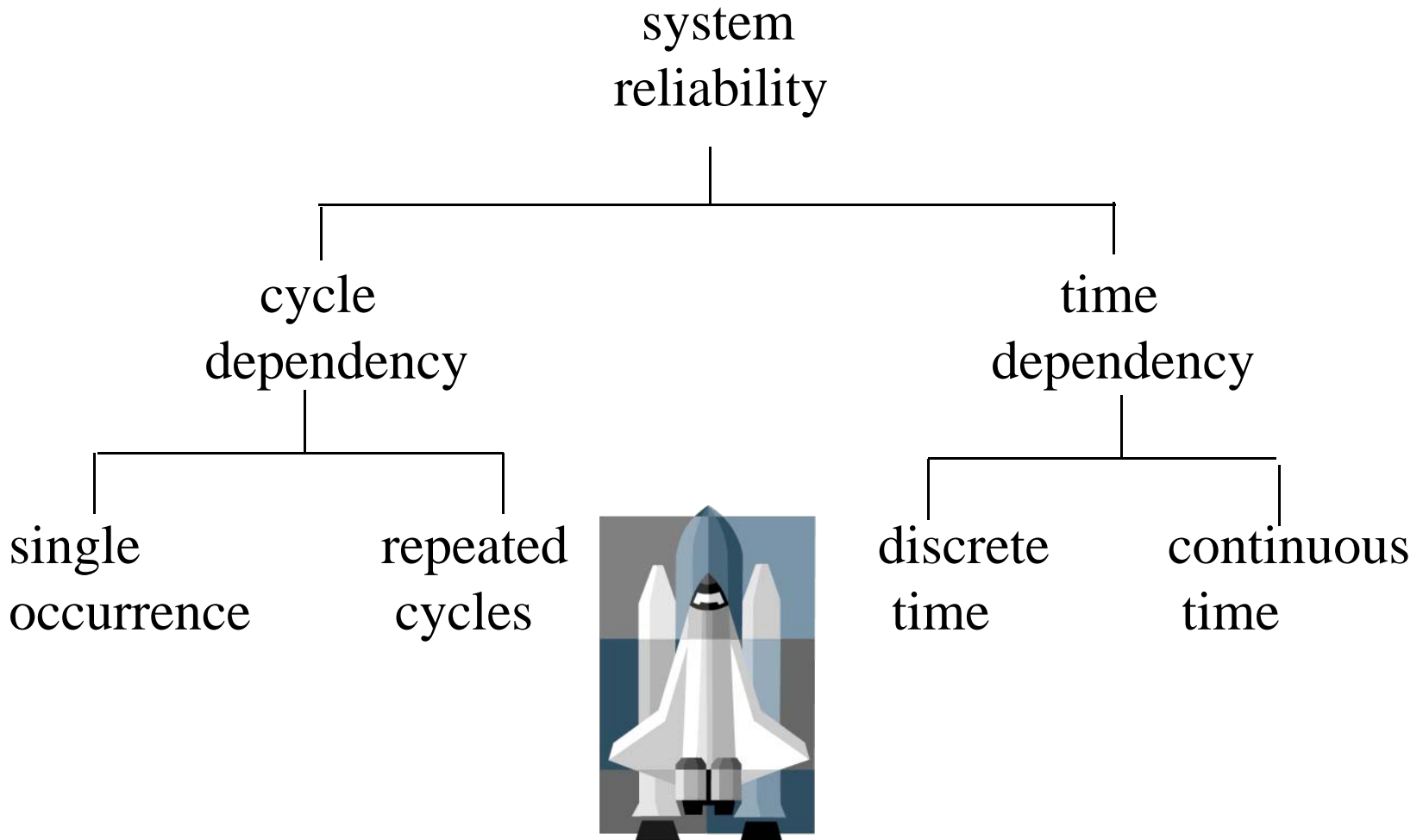

60 watt
Avg. lumens 870
Avg. life 1000 hours

Which average? - mean, median, mode?

Operating hours or clock time?

What about on/off cycles?

What are the operating conditions?

Time to failure Cycles versus Time

system
reliability

cycle
dependency

time
dependency

single
occurrence

repeated
cycles

discrete
time

continuous
time

Repeated Cycle Reliability

There are 28 Space Shuttle flights scheduled through 2010 at which time the Shuttle is to be retired.
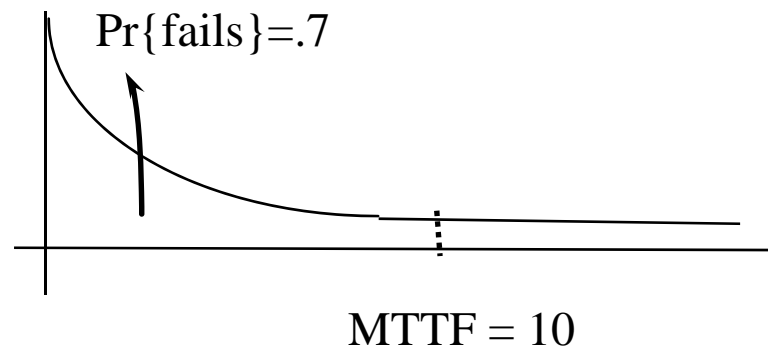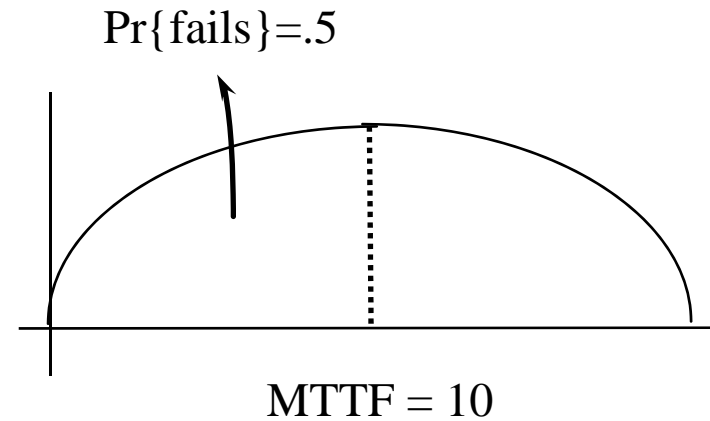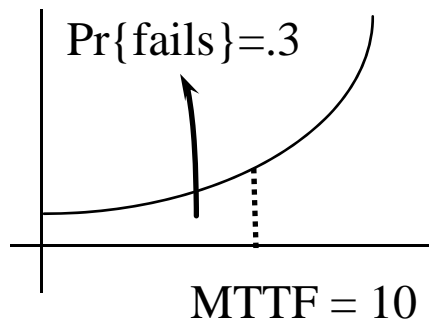
Cycle reliability (historical) = 112/114 = .9824

Prob{at least one failure in 28 flights} = $1 - .9824^{28} = .3917$

Shuttle	Flights
Atlantis	26
Challenger	10
Columbia	28
Discovery	31
Endeavour	19
Total	**114**
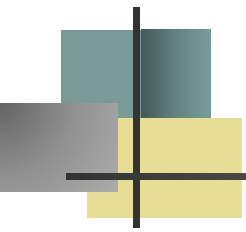
The Failure Distribution and the MTTF

Pr{fails}=.3

MTTF = 10

Pr{fails}=.5

MTTF = 10

Pr{fails}=.7

MTTF = 10

Probability of Surviving to the MTTF

Exponential (constant failure rate) Distribution
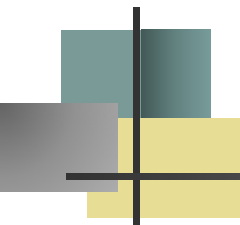
R(MTTF) = .3678

Normal Distribution

R(MTTF) = .5

Weibull with a shape parameter of .5

R(MTTF) = .24

Weibull with a shape parameter of 2

R(MTTF) = .455

The Reliability Engineer

I am going to be a reliability engineer.

Reliability Engineers are a sad and embittered race. A lonely group despised by both the design team and management; their sole function being to generate failures. And generate failures they will! For it is their very life, their ambrosia, their reason for being. Many a good designer has quietly disappeared after receiving one too many failures. Management has lost their stock options because the reliability growth curve did not grow. No wonder the poor reliability engineer dines alone, talks to no one, and has no friends. Their only hope to escape the despair of the day to day job comes with the knowledge that all things must fail, and eventually as the reliability life test runs to its inevitable conclusion, so will they.