Reliability and Availability

Aleksandr Lenin

Topics for this lecture:

1. Reliability and availability basics
2. Calculating system reliability from reliability infromation for its components

Reliability is a measure of the ability of a product or its component to perform its intended function under a prescribed set of conditions.

In fact, reliability is probability.

Reliability 0.90 means that:

- 90% of functioning as intended.
- Failure rate (probability it will fail) is 10%.
- On average, 1 out of every 10 such items will fail
- A single item is expected to fail on average once in every 10 trials

Similarly, reliability 0.985 imples 15 failures per 1000 components or trials.

Reliability may be thought of in two ways:

1. Reliability when activated
   - Focuses on one point in time
   - Systems, which are intended to operate for one time – i.e.: missile, or airbag in a car
2. Reliability for a given time period
   - Focus on length of service

The probability that a component or a system will operate as planned is an important concept in system design.

There are four commonly used metrics related to reliabiity:

- *Failure Rate per Hour* (λ) – the number of failures divided by the total operating hours.
- *Mean Time To Failure* (MTTF) – the average length of time (in hours) before failure.
- *Mean Time Between Failures* (MTBF) – the average time from the uptime after the repair following a failure, to the next failure.
- *Mean Time To Repair* (MTTR) – the average time it takes to repare a failed module.

200 units of a particular component were subjected to testing equivalent to 2500 hours of normal use. One unit failed after 1000 hours, another after 2000 hours. All other units were still working at the conclusion of the test.

The failure rate per hour

$$\frac{2}{198 \cdot 2500 + 1000 + 2000} = 0.000004016$$

failures per hour.

NOTE: this formula assumes constant failure rate over time, which might not always be the case for real-life components!

The inverse of failure rate per hour is *Mean Time To Failure* (MTTF) – the average length of time (in hours) before failure.

$$\text{MTTF} = \frac{1}{\text{Failure rate per hour}} = \frac{1}{0.000004016}$$
$$= 249'000 \text{ hours.}$$

NOTE: This formula assumes that failure rate is constant.

A similar term, *Mean Time Between Failures* (MTBF) is usually used for reparable or replacible items.

MTBF – the average time from the up time after the repair following a failure to the next failure.

Mean Time To Repair (MTTR) – the time taken to repare a failed module.

For HW modules MTTR – mean time to replace a failed module.

For SW modules MTTR – mean time taken to reboot after a fault is detected.

One of the system design goals should be:

- Keep the HW MTTR as high as possible (low MTTR requirement means high operational cost for the system).
- Keep the SW MTTR as low as possible.

Spares location	Site manned hours	Estimated MTTR
Onsite	24/7	30 min
Onsite	Operator on call 24/7	2 hours
Onsite	Regular working hours	3 days
Offsite, shipped by courier	Operator notified when fault is detected	1 week
Offsite in an operator controlled warehouse	Operator needs to be flown in to replace the module	2 week

Reliability depends on:

- frequency of failure
  - reflects the quality of the system
  - reflects the system's architectural capability
  - Mean Time Between Failure (MTBF) measures average failure rate
- restoration time
  - depends on the support capability
  - Mean Time To Repair (MTTR) measures average restoration time

$$\text{Reliability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \ .$$

A copier is expected to operate for 200 hours after repair, and the mean repair time is expected to be 2 hours.

$$\begin{aligned} \text{MTBF} &= 200 \text{ hours} \ , \\ \text{MTTR} &= 2 \text{ hours} \ , \\ \text{Reliability} &= \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = \frac{200}{200 + 2} = 0.99 \ . \end{aligned}$$

Another way to look at reliability is to consider a time dimension.

Probabilities are determined relative to a specified period of time.

This approach is most common – i.e., product warranties (e.g., one year free repair) are based on this definition of reliability.

The time to failure of a component is modeled by a distribution (exponential,normal) with an average equal to the MTTF.

The probability that the component put into service at time 0 will fail before some specified time T is equal to the area under the curve between 0 and T.

Reliability of the item is the probability that it will last *at least until* time T.

$$\text{Reliability} = \Pr[\text{no failure before } T] \approx e^{-T/MTTF} \ ,$$

where:

e	≈ 2.7183
T	length of service before failure
MTTF	mean time to failure

The probability that failure will occur before time T is

$$\Pr[\text{failure before T}] \approx 1 - e^{-T/MTTF} \ .$$

A more general distribution is the Weibull distribution.

The probability density function of a Weibull random variable x is:

$$f(x;\lambda,k) = \begin{cases} \frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{k-1} e^{-(x/\lambda)^k} & x \geqslant 0 \ , \\ 0 & x \leqslant 0 \ , \end{cases}$$

where:

$k > 0$ is the shape parameter

$\lambda > 0$ is the scale parameter

x represents the time T

- if $k == 1$ the failure rate is constant over time
- if $k < 1$ the failure rate decreases over time
- if $k > 1$ the failure rate increases over time

Reliability is an important dimension of product quality.

Reliability of a system (probability it is functioning properly) depends on:

- the reliability of its components
- the type of system

Reliability of a system is determined from the reliability of its components.

This course will focus on reliability measurement based on statistics and probability theory.

System reliability is calculated by modeling the system as an interconnection of its components in series or in parallel.

Rules to decide how to place the components:

- If failure of a part leads to the combination becoming inoperable, the two parts shall be placed in a series.
- If failure of a part leads to the other part(s) taking over the operations of the failed part, they shall be placed in parallel.

The process of calculating system reliability is done in several stages:

- Stage 1 create a block-diagram of the system under consideration.
- Stage 2 create a *reliability model* of the system.
- Stage 3 calculate reliability of individual components.
- Stage 4 calculate reliability of the entire system.

In general, a system may be composed of some parallel components and some series of components.

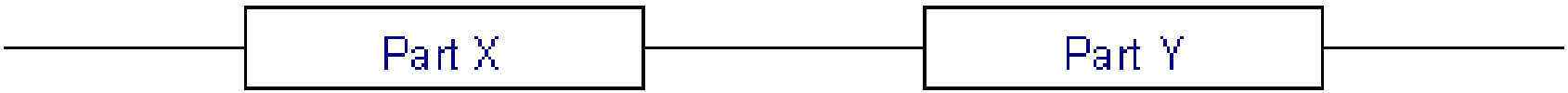
The system reliability is calculated in two stages:

1. calculate the reliability of parallel component(s)
2. use these to calculate the reliability of the resulting series of components for the entire system

Determining the reliability of a system which consists of a number of independent components requires the use of rules of probability for independent events (events that have no relation to occurrence or nonoccurrence of each other).

Rule 1. If two or more events are independent, and "success" is defined as the occurrence of all of the events, then the probability of success p_s is equal to the product of the probabilities of the occurring events.

$$p_s = p_1 \times p_2 \times \dots$$



The system is operational iff both Part X and Part Y are operational.

The reliability of the system is:

$$\text{Rel} = \prod p_i = p_1 \times p_2 \times \ldots \quad .$$

Implication: the reliability of a series of components is always lower than the reliability of its individual components.

Component	Reliability
X	99%
Y	99.99%
X and Y	98.99%

Even through a highly reliable Part Y was used, the overall reliability of the system was ”pulled down” by the low reliability of Part X.

The chain is weaker than its weakest link.

As the number of components in a series increases, the system reliability decreases.

I.e. 8 components in a series, each with a reliability 0.99 result in a reliability of only $0.99^8 = 0.923$.

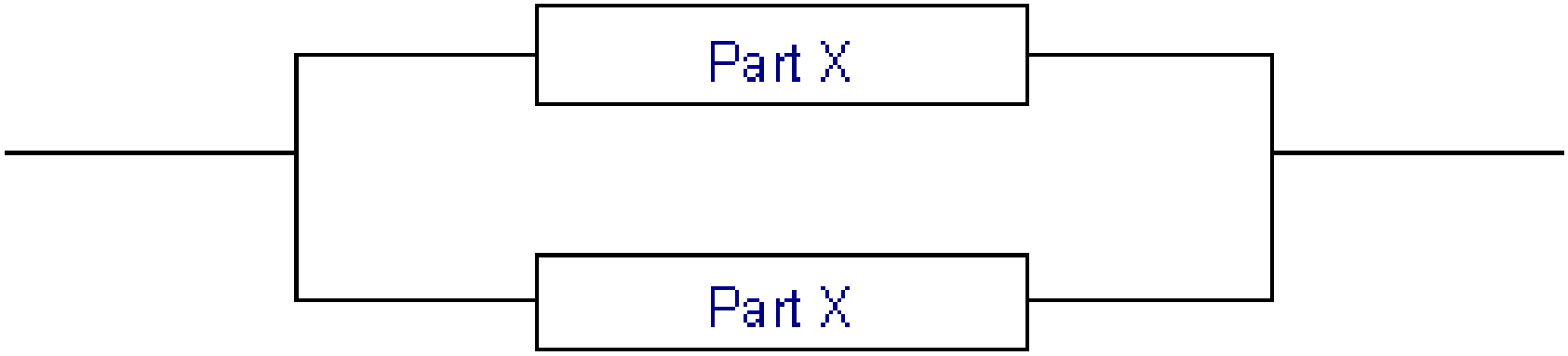
Many products have a large number of components, we need some way to increase reliability.

Options:

- Overdesign – enhance the design to avoid a particular type of failure
- Design simplification – reduce the number of components in the system
- Redundancy – provide backup components in system design

Rule 2. If two or more events are independent and "success" is defined as occurrence of *at least one* of the events, then the probability of success p_s is equal to 1 − probability that none of the events will occur, i.e.:

$$\begin{aligned} p_s &= 1 - (1 - p_1)(1 - p_2)(1 - p_3)\ldots \\ &= p_1 + (1 - p_1) \cdot p_2 + (1 - p_1)(1 - p_2) \cdot p_3 + \ldots \end{aligned}$$



The system is operational if either part is operational, and fails when both parts fail.

The reliability of the system is:

$$\text{Rel} = 1 - \prod (1 - p_i) \quad .$$

Implication: the reliability of two components in parallel is always much higher than the reliability of its individual components.

Component	Reliability
X	99%
X | X	99.99%
X | X | X	99.9999%

Even through a very low reliability Part X was used, the overall reliability of the system is much higher.

Parallel operation provides a very powerful mechanism for making a highly reliable system from components with low reliability.

For this reason, all mission-critical systems are designed with redundant components.

Partial Operational Reliability $R_{n,m}$ – reliability of the system with n components that is considered operational if no more than m components fail (at least $n - m$ components remain operational).

Probability of working without failure exactly m units out of n:

$$f(m, n, p) = \binom{n}{m} p^m (1-p)^{n-m} \quad .$$

Reliability of system with at least m components out of n:

$$\mathrm{Rel} = \sum_{k=m}^{n} f(k, n, p) = \sum_{k=m}^{n} \binom{n}{k} p^k (1-p)^{n-k} \quad ,$$

where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is the binominal coefficient.

If $m = 1$ we have a parallel system, if $m = n$ we have a serial system.

NOTICE

The probability rules for series and parallel systems can also be used to determine reliability of a system for a given length of time based on the reliability of its components over the same period of time.

Availability measures the fraction of time a system is expected to be available for operation (as opposed to being down for repairs).

If a user cannot access the system – it is *unavailable* from the user's point of view.

The term *downtime* is used to refer to periods when a system is unavailable.

Availability of a system or its component is the percentage of time when the system is operational.

$$\text{Availability} = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}} \ .$$

Availability is expressed as a *percentage of uptime* in a given timeframe:

Availability %	Annual down-time	Monthly down-time	Weekly down-time	Daily down-time
90%	36.5d	72h	16.8h	2.4h
99%	3.65d	7.2h	1.68h	14.4m
99.9%	8,76h	43.8m	10.1m	1.44m
99.99%	52.56m	4.38m	1.01m	8.66s
99.999%	5.26m	25.9s	6.05s	864.3ms
99.9999%	31.5s	2.59s	604.8ms	86.4ms
99.99999%	3.15s	262.97ms	60.48ms	8.64ms
99.999999%	315.569ms	26.297ms	6.048ms	0.864ms

SLAs often refer to *monthly* downtime to match the monthly billing cycles.