Testing & reliability additional notes

Fault tolerance is the ability of a system to continue performing its function in spite of faults. The main goal of this is to increase the dependability of a system.

- The **dependability** is the ability of a system to deliver its intended level of service to its users.

The level of application can be:

- **Safety critical application:** When it is critical to human safety or the natural environment. Very high probability to be operational for short periods of time (For example 99.999999% for 3 hours).
- **Mission critical applications:** When you have to complete the mission and repair is impossible or prohibitively expensive. (For example 95% for 10 years)
- **Business-critical application** Users need to have a gigh probability of receiving service when it is requested.

Fault, failure and error:

- A **fault** is an underlying defect, imperfection, or flaw that has the potential to cause problems. They can be *latent* if they haven't caused any flaws or *active* it it is causing problems.
  - **Fault tolerance** consists of noticing active faults and component subsystem failures and doing something helpful in response.
- A **failure** is a non-performance of some action that is due or espected
- An **error** is a deviation of correctness or accuracy.

Whe have 3 parameters to measure the fault tolerance of a system:

- **Reliability $R(t)$** is the probability that a system operates without failure in the interval $[0, t]$, given that it worked at time 0.
  - Reliability isn't the same as fault tolerance, fault tolerance is a technique that can improve reliability, but a highly reliable system is not necessarily fault system.
- **Availability $A(t)$** is the probability that a system is functioning correctly at the instant time t. It depends on:
  - How frequently a system becomes non-operational.
  - How quickly can it be repaired.

  The *steady state availability* $A(\infty)$ is when we assume a time-independent value after some initial time interval.

  $$A(\infty) = \frac{t_{\text{on}}}{t_{\text{on}} + t_{\text{off}}}$$

  One difference between *reliability* and *availability* is that the first one depends on an interval of time and the second one is taken at an instant of time.
- **Safety $S(t)$** is the probability that a system will either perform its function correctly or will stop functioning in a safe way. A system is safe if it functions correctly or if it fails, it remains in a safe state. Failures are partitioned into:
  - Fail-safe
  - Fail-unsafe

Common fault tolerance measures:

- **Failure rate λ** is the expected number of failures per unit time. Its units are usually given in terms of failures per hour, normalized fo ra single unit. It isn't really a probability, but rather an "expected value".

Usually the failure rate is divided in 3 sections depending on the life of the device:

1. **Infant mortality:** Failure rate decreases
2. **Lifetime:** Low failure rate
3. **Passed lifetime:** Failure rate increases

insert graphic

- **Failure rate and reliability:** Reliability $R(t)$ is the conditional probability that the system will work correctly throughout $(0, t)$ given that it worked on time 0

$$R(t) = \frac{N_{\text{op}(t)}}{N_{\text{op}(t)} + N_{\text{fail}(t)}}$$

- The **Mean Time To Failure (MTTF)** is the expected time of the occurrence of the first system failure. For a system with N identical components and we measure the time before each component fails:

$$\text{MTTF} = \frac{1}{n}\sum_{i=0}^{n} t_i$$

In terms of system reliability $R(t)$:

$$\text{MTTF} = \int_0^\infty R(t)dt$$

If $R(t) = e^{-\lambda t}$, then MTTF is the inverse of the failure rate:

$$\text{MTTF} = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda}$$

- The **Mean Time To Repair (MTTR)** is the expected time until a system is repaired. If we have a system with N identical components and the i component requires t_i to repair:

$$\text{MTTR} = \frac{1}{n}\sum_{i=0}^{n} t_i$$

Normally it is specified in terms of the repair rate μ which is the average number of repairs that occur per time period

$$\text{MTTR} = \frac{1}{\mu}$$

We can calculate the *steady-state availability* as:

$$A(\infty) = \frac{n\ \text{MTTF}}{n\ \text{MTTF} + n\ \text{MTTR}} \approx \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

- The **fault coverage (C)** is the conditional probability that, given the existence of a fault, the system detects it

$$C = \frac{\text{N. detected faults}}{\text{Total N. faults}}$$