Dependability Fundamentals

1

Changing Reliability Landscape

Historically, integrated circuits were among the most reliable computer components. However, as we move to feature sizes of 32 nm and smaller, both transient and permanent faults become more common.

2

Abstraction Layers

Computers are designed at different layers of abstraction. Failure of a module at one level may be considered merely a component error in a higher-level module.

3

Service Level Agreements

SLAs and SLOs define when a system is operating properly, providing concrete metrics for dependability in services like networking or power.

Key Reliability Measurements

Module Reliability

- Mean Time To Failure (MTTF): Measure of continuous service accomplishment
- Failures In Time (FIT): Failures per billion hours of operation
- 1,000,000 hours MTTF = 1000 FIT

Module Availability

- Mean Time To Repair (MTTR): Service interruption duration
- Mean Time Between Failures (MTBF) = MTTF + MTTR
- Module availability = MTTF/(MTTF + MTTR)

If a collection of modules has exponentially distributed lifetimes—meaning that the age of a module is not important in probability of failure—the overall failure rate of the collection is the sum of the failure rates of the modules.

Example 1

- Assume a disk subsystem with the following components and MTTF:
  - 10 disks, each rated at 1,000,000-hour MTTF
  - 1 ATA controller, 500,000-hour MTTF
  - 1 power supply, 200,000-hour MTTF
  - 1 fan, 200,000-hour MTTF
  - 1 ATA cable, 1,000,000-hour MTTF
- Using the simplifying assumptions that the lifetimes are exponentially distributed and that failures are independent, compute the MTTF of the system as a whole.

Answer

- $$FailureRate_{System} = 10 \times \frac{1}{1{,}000{,}000} + \frac{1}{500{,}000} + \frac{1}{200{,}000} + \frac{1}{200{,}000} + \frac{1}{1{,}000{,}000}$$
  $$= \frac{10+2+5+5+1}{1{,}000{,}000} = \frac{23}{1{,}000{,}000} = \frac{23{,}000}{1{,}000{,}000{,}000\ (hours)}$$
  $$= 23{,}000\ FIT$$
- $$MTTF_{System} = \frac{1}{FailureRate_{System}} = \frac{1{,}000{,}000{,}000\ hours}{23{,}000} = 43{,}500\ hours$$

Example 2

- Disk subsystems often have redundant power supplies to improve dependability. Calculate the reliability of redundant power supplies. Assume one power supply is sufficient to run the disk subsystem and that we are adding one redundant power supply.
  - Power supply, 200,000-hour MTTF
  - Power supply, 24-hour MTTR

Answer

- MTTF for our redundant power supplies is the mean time until one power supply fails divided by the chance that the other will fail before the first one is replaced.
- Thus, if the chance of a second failure before repair is small, then the MTTF of the pair is large.
- $$MTTF_{Pair} = \frac{MTTF_{Single}/2}{\frac{MTTR_{Single}}{MTTF_{Single}}} = \frac{MTTF^2_{Single}}{2 \times MTTR_{Single}} = \frac{200{,}000^2}{2 \times 24}$$

$$= 830{,}000{,}000$$