Reliability Engineering: Will my design work over the long term?

CMPE349 Intro to Professional Practic

The "ilities"

- Reliability
- Availability
- Integrity
- Supportability
- Maintainability
- Portability

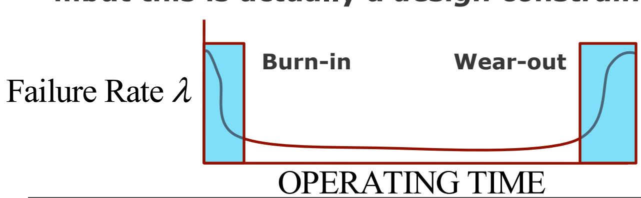
- Tend to be driven by the hardware/software architecture and *not* functional considerations
- Definitions are the key! YOU are responsible!
- Should be considered at block diagram level
- An analysis task that no one teaches or talks about

Strawman “ility” definitions

- **Reliability**
  - **Probability that the system remains operational over some time interval**
  - **Generally a long term average over a large population**
  - **Statistic: Mean time between failure**
- **Availability**
  - **Probability that the system will be operating within its performance specifications when needed by the user**
  - **Generally a long term average over a large population**
  - **Statistic: Mean time between outage**
- **Continuity**
  - **Probability that the system will *remain in service* over a specified (short) interval, given that it was in service at the start of that interval**
  - **Sometimes equivalent to Probability of Mission Success**
  - ***Not* just short-term availability!**

The foundations

- **Physical devices are characterized by a number called the *failure rate,* λ , usually given in “failures per million hours”**
- **The failure rate is assumed constant over time…**
- **…except at the very beginning of operation**
- **…and at the very end of lifetime**
- **Failures are assumed to be independent of each other…**
- **…but this is actually a *design constraint***



Independence

- **Two events X and Y are called *independent* if**

$$\Pr\{X \text{ and } Y\} = \Pr\{X\} \times \Pr\{Y\}$$

- **If X and Y are independent, their *complements* are as well**

$$\begin{aligned}\Pr\{\text{NOT}(X) \text{ and NOT}(Y)\} &= \Pr\{\text{NOT}(X \text{ or } Y)\} \\ &= 1 - (\Pr\{X \text{ or } Y\}) \\ &= 1 - \left(\Pr\{X\} + \Pr\{Y\} - \Pr\{X \text{ AND } Y\}\right) \\ &= 1 - \Pr\{X\} - \Pr\{Y\} + \Pr\{X\}\Pr\{Y\} \\ &= (1 - \Pr\{X\}) \times (1 - \Pr\{Y\}) \\ &\ \Pr\{\text{NOT}(X)\} \times \Pr\{\text{NOT}(Y)\}\end{aligned}$$

Some additional clarifications

- **The *reliability* is the probability that the system is operational over some period.**
- **The *unreliability* is the probability that the system has failed over some period.**
- **Both the reliability and the unreliability are functions of time, and are frequently written as R(t), and U(t), respectively.**
- ***Reliability* and *Unreliability* are complements of each other, because the element is either operating or not operating. Therefore, U(t)=1-R(t)**
- **The general assumption is that the time before a failure is an exponentially distributed random variable**

$$p_T(t) = \lambda e^{-\lambda t},\ 0 \le t \qquad E(t) = \int_0^\infty \lambda \tau e^{-\lambda \tau}\, d\tau = \frac{1}{\lambda} \triangleq MTBF$$

$$\Pr\left\{t < T\right\} = \int^T p_T(t)\, dt = 1 - e^{-\lambda T} = U(T) = \Pr\left\{\text{at least one failure in } T\right\}$$

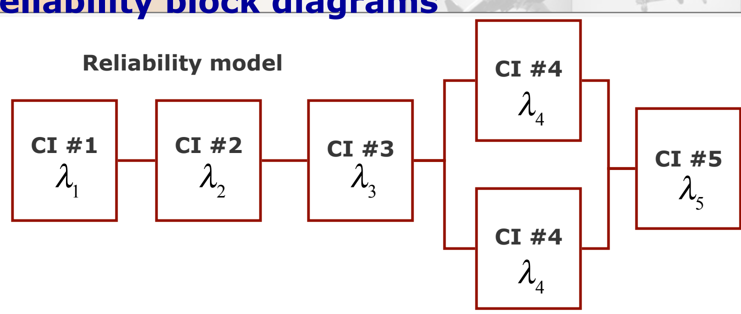
$$\Pr\left\{t \ge T\right\} = \int_T^\infty p_T(t)\, dt = e^{-\lambda T} = R(T) = \Pr\left\{\text{no failures in time } T\right\}$$

And still more

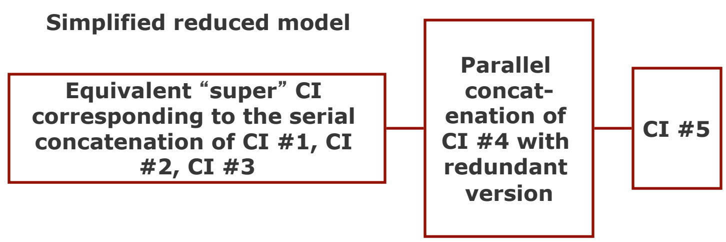
- **For serial elements, *all* must be operating in order for the system to be operating. The reliability is, therefore, the *product* of the individual reliabilities.**
- **For parallel elements with only a single element required, *all* must be failed before the combination fails. The unreliability is, therefore the product of the unreliabilities, and the reliability R(t) = 1 – U(t)**
- **The “M-of-N” combinations are harder to analyze…**
- **…but you can find your way using the binomial distribution**

Reliability block diagrams

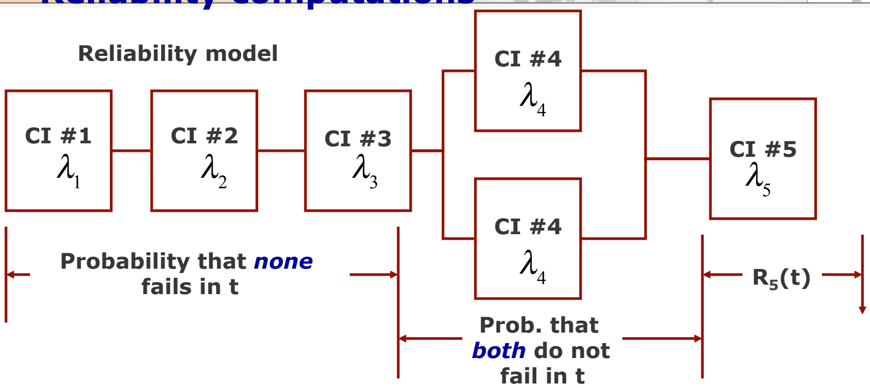
Reliability model



Simplified reduced model



Reliability computations



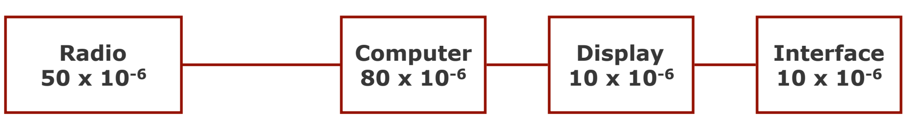
$$R(t) = e^{-\lambda_1 t} e^{-\lambda_2 t} e^{-\lambda_3 t} \times \underbrace{\left(1 - \underbrace{\left(1 - e^{-\lambda_4 t}\right)^2}_{\substack{U_4(t)^2 \\ = \Pr\left[\text{both failed in time } t\right]}}\right)}_{\text{Probability that } both \text{ did not fail}} \times e^{-\lambda_5 t}$$

- **R(t) is not strictly exponential!**

Let's do an (extended) example

- **Consider the airborne part of your landing system**
- **λ is given in failure rate per hour or per million hours**
- **The system spec is to have a system availability of at least**

$$1 - 2\times10^{-4} \text{ per 2 hour mission}$$



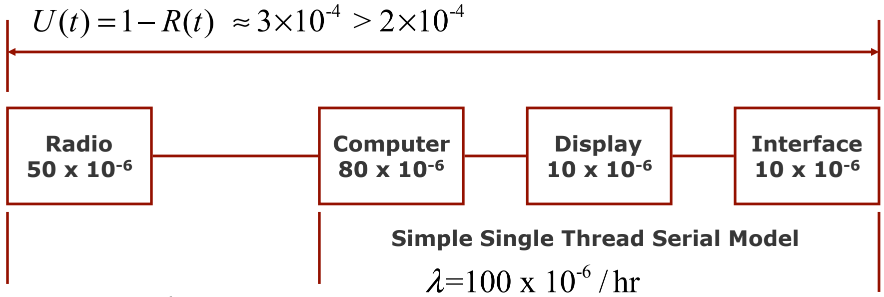
UMBC ENEE 661 System Architecture & Design / CMPE451
© EFCLaBerge 2004,2009 All rights reserved

First: How does the simple system perform?

$$\lambda = 150 \text{ x } 10^{-6} \text{ / hr} = 1.5\times10^{-4} \text{ / hr}$$

$$R(t) = e^{-\lambda t} \approx 1\text{-}\lambda t = 1\text{-}\left(1.5\times10^{-4} \text{ / hr}\times 2 \text{ hr}\right) \approx 1-3\times10^{-4} = 0.9997$$

$$U(t) = 1 - R(t) \approx 3\times10^{-4} > 2\times10^{-4}$$



Simple Single Thread Serial Model

$$\lambda = 100 \text{ x } 10^{-6} \text{ / hr}$$

$$R(t) \approx 1\text{-}\lambda t = 1\text{-}2\times10^{-4}$$

$$U(t) = 1 - R(t) \approx 2\times10^{-4}$$

$$\lambda = 50 \text{ x } 10^{-6} \text{ / hr}$$

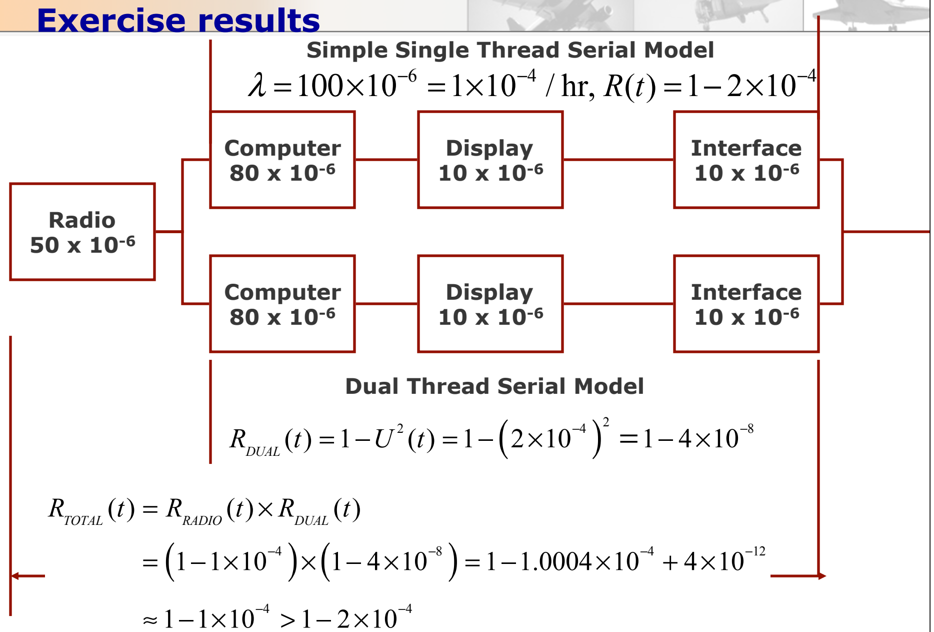
$$R(t) \approx 1 - \lambda t = 1 - 1\times10^{-4}$$

$$U(t) = 1 - R(t) \approx 1\times10^{-4}$$

Exercise results

Simple Single Thread Serial Model

$$\lambda = 100\times10^{-6} = 1\times10^{-4} \text{ / hr}, \ R(t) = 1-2\times10^{-4}$$



Dual Thread Serial Model

$$R_{DUAL}(t) = 1 - U^2(t) = 1 - \left(2\times10^{-4}\right)^2 = 1 - 4\times10^{-8}$$

$$R_{TOTAL}(t) = R_{RADIO}(t)\times R_{DUAL}(t)$$

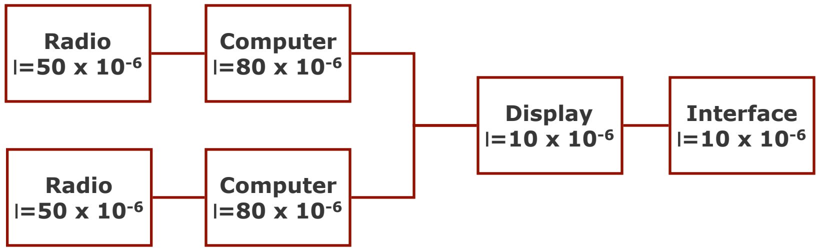
$$= \left(1-1\times10^{-4}\right)\times\left(1-4\times10^{-8}\right) = 1 - 1.0004\times10^{-4} + 4\times10^{-12}$$

$$\approx 1 - 1\times10^{-4} > 1 - 2\times10^{-4}$$

Design for greater availability margin!

$$\lambda = 50\times10^{-6} + 80\times10^{-6} = 1.3\times10^{-4}$$
$$R_{SINGLE}(t) = 1 - 2.6\times10^{-4}$$
$$U_{SINGLE}(t) = 2.6\times10^{-4}$$

$$\lambda = 10\times10^{-6} + 10\times10^{-6} = 2\times10^{-5}$$
$$R_{ID}(t) = 1 - 4\times10^{-5}$$
$$U_{ID}(t) = 4\times10^{-5}$$



$$R_{DUAL}(t) = 1 - \left(2.6\times10^{-4}\right)^2 \approx 1 - 7\times10^{-8} \quad (!)$$
$$U_{DUAL}(t) \approx 7\times10^{-8}$$

$$R_{TOTAL}(2\text{ hrs}) = R_{DUAL}\times R_{ID}$$
$$= \left(1-7\times10^{-8}\right)\times\left(1-4\times10^{-5}\right)$$
$$= 1 - 4.007\times10^{-5} + 2.8\times10^{-12}$$
$$= 1 - 4\times10^{-5} > 1 - 2\times10^{-4}$$

A few words about software reliability (C. LaBerge's view)

- The exponential failure rate assumption characterizes the aging of the hardware components as a function of time.
- The exponential failure rate assumption implicitly includes fault-free design!
  - The design faults are so rare that they are masked by component aging failures
- Software components never wear out: the exponential failure assumption does not hold!
- Because there is no masking effect, software faults are always design failures.
- The only recognized technique to eliminate design failures is design process
- Modern research continues in formal techniques to prove correctness, but this just pushes the difficulties to a lower level.

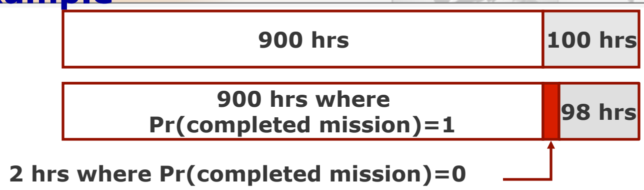
A few more words about software reliability (R. Taylor's view)

- Software "reliability" *can* be modeled as exponential, especially when operating systems are involved
- When software runs for an extended period of time, the complex and non-deterministic interaction between the operating system and the executing software result in a succession of completely unique states that can not have been tested…
- …and this weakens (eliminates) the independence assumption.
- The time-dependent accumulation of minor flaws in the operating system – e.g., memory leaks – tend to accumulate in a random fashion and eventually cause a very low level fault of some kind.
- This fault occurs at a rate that may be somewhat less than exponential, but somewhat more than linear with time.

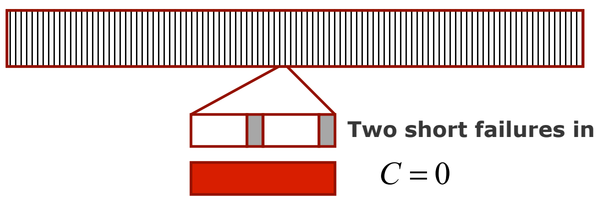
Continuity (of service)

- Conditional Probability
  - It worked when I started the mission, what's the probability that it works throughout the mission?
  - Example: Automatic precision landing
- This is *not* just a short term availability
- Example: Consider two systems with 90% availability over 1000 hours
  - System 1: up for 900 continuous hours, down for 100
  - System 2: up for 0.9 continuous hours, down for 0.1
- Which has better continuity for a 2 hour mission?

Example



$$C = \frac{900 \times 1 + 2 \times 0}{902} = 0.997783 = \frac{450}{451}$$



$$C = 0$$

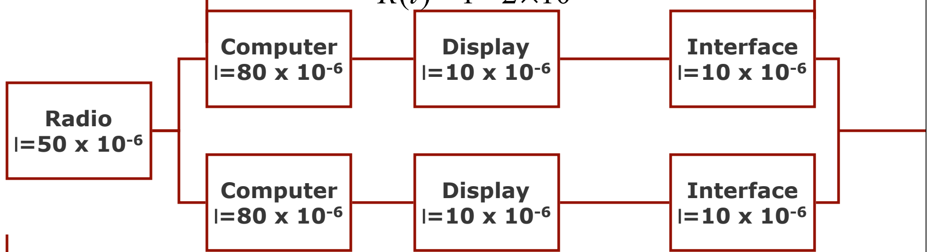
End of Day 1

- **Reliability**
  - **Probability that the system works over a period of time**
  - **Usually assume exponentially distributed failure times**
  - **The failure rate is assumed constant over the lifetime**
- **Redundancy**
  - **Redundancy can improve Availability, but may actually hurt reliability…**
  - **…because there are more parts to fail.**
- **Continuity**
  - **Probability that the system works over my mission time, given that it was working before I started.**
  - **Frequently confused with short term availability…**
  - **…but this can be misleading**
- **Next time: we’ll talk more carefully about availability**

Exercise results

Simple Single Thread Serial Model

$$R(t) = 1 - 2\times10^{-4}$$



Dual Thread Serial Model

$$R_{DUAL}(t) = 1 - U^2(t) = 1 - \left(2\times10^{-4}\right)^2 = 1 - 4\times10^{-8}$$

$$\begin{aligned} R_{TOTAL}(t) &= R_{RADIO}(t)\times R_{DUAL}(t) \\ &= \left(1 - 1\times10^{-4}\right)\times\left(1 - 4\times10^{-8}\right) = 1 - 1.0004\times10^{-4} + 4\times10^{-12} \\ &\approx 1 - 1\times10^{-4} > 1 - 2\times10^{-4} \end{aligned}$$