CS-417
COMPUTER SYSTEMS MODELING

Spring Semester 2020
Batch: 2016-17
(LECTURE # 12)

FAKHRA AFTAB
LECTURER
DEPARTMENT OF COMPUTER & INFORMATION SYSTEMS ENGINEERING
NED UNIVERSITY OF ENGINEERING & TECHNOLOGY

Recap of Lecture # 11

Reliability Block Diagrams

Series Systems

Parallel Systems

Series – Parallel Systems

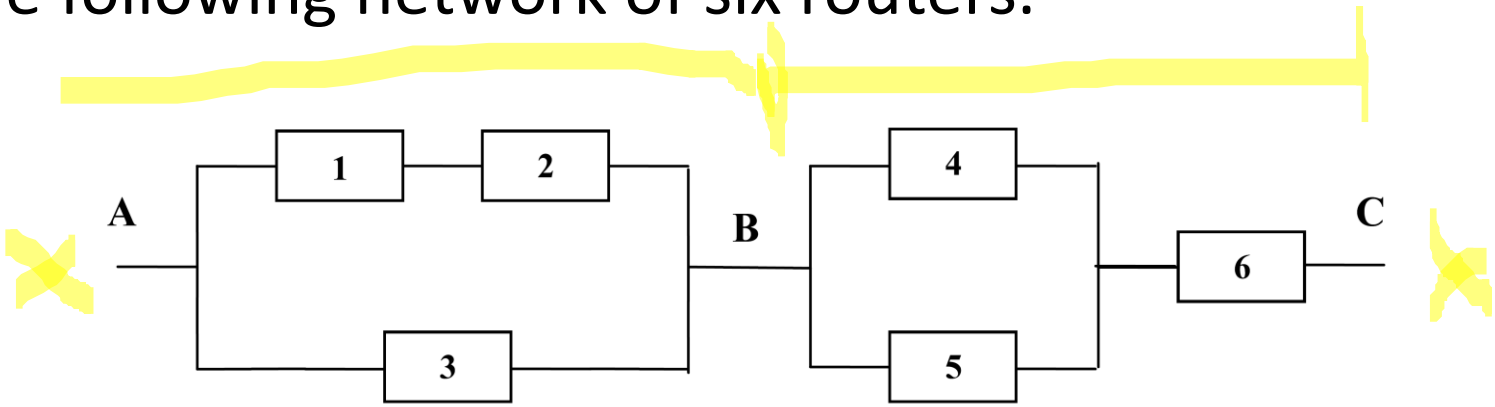
k-out-of-n Systems

Chapter # 4 (Cont'd)

RELIABILITY AND AVAILABILITY MODELING

Task

Consider the following network of six routers.



Each router can fail with probability p. Router failures are mutually independent. Showing all steps, derive expressions for the probability that the node:

a) A can successfully send packets to node B

b) B can successfully send packets to node C

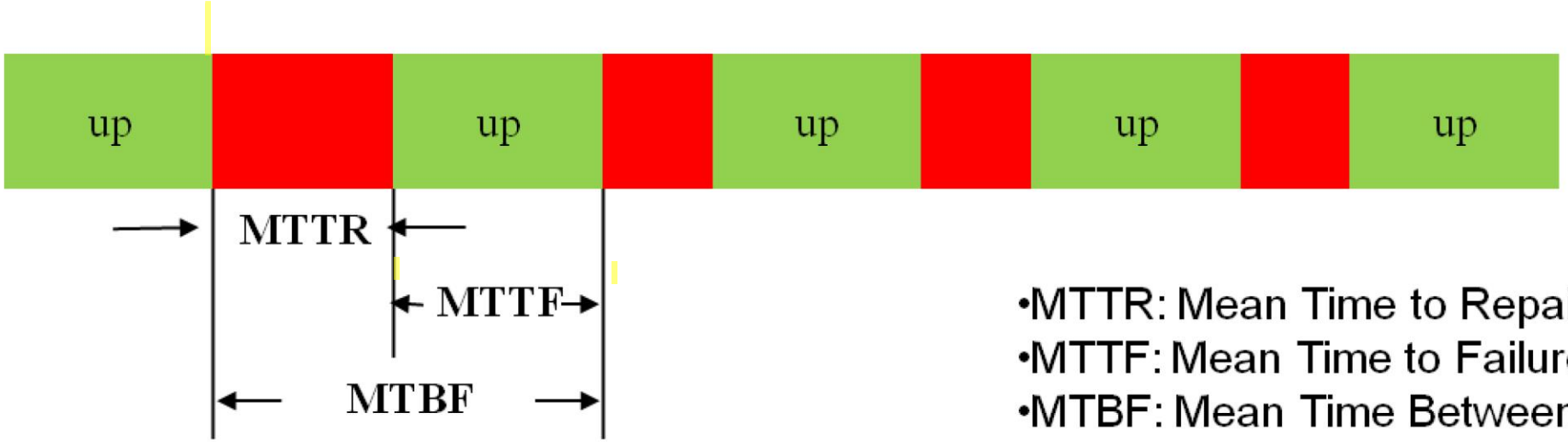
c) A can successfully send packets to node C

SYSTEM AVAILABILITY

Probability that the system will be up and running and able to deliver useful services to users at any given time.

Example:

- For the insulin pump system, the most important dependability properties are:
  - availability (it must work when required),
  - reliability (it must deliver the correct dose of insulin), and
  - safety (it must never deliver a dangerous dose of insulin).
  - Security is ***not*** an issue as the pump will not maintain confidential information.



- MTTR: Mean Time to Repair
- MTTF: Mean Time to Failure
- MTBF: Mean Time Between Failures

Availability (A) during an interval is calculated as the fraction of time a system is up. Therefore,

$$A = \frac{Up\ Time}{Up\ Time + Down\ Time}$$

$$A = \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTBF}$$

We may define unavailability (U) as:

$$U = 1 - A$$

$$U = \frac{MTTR}{MTTF + MTTR} = \frac{MTTR}{MTBF}$$

Example Problem

A computer has an MTTF = 34 hr and MTTR = 2.5 hr.

a) Determine the availability?

b) If the MTTR is reduced to 1.5 hr, what MTTF can be tolerated without decreasing the availability of computer?

Answers:

a) 0.9315

b) 20.4 hrs

FAULT, ERROR AND FAILURE

- **Fault:** an incorrect step, process, or data definition which causes the program to perform in an undesirable manner. e.g. absence of a data validation condition.

- **Error:** A system state that can lead to undesirable system behavior. e.g. assignment of zero value to a variable that has to divide some other variable in the next step.

- **Failure:** a situation in which the system does not deliver a service according to its specification.

System faults do not always result in system errors and system errors do not necessarily result in system failures.

The reasons for this are as follows:

1) Not all code in a program is executed.

2) Errors are transient.

3) The system may include fault detection and protection mechanisms.

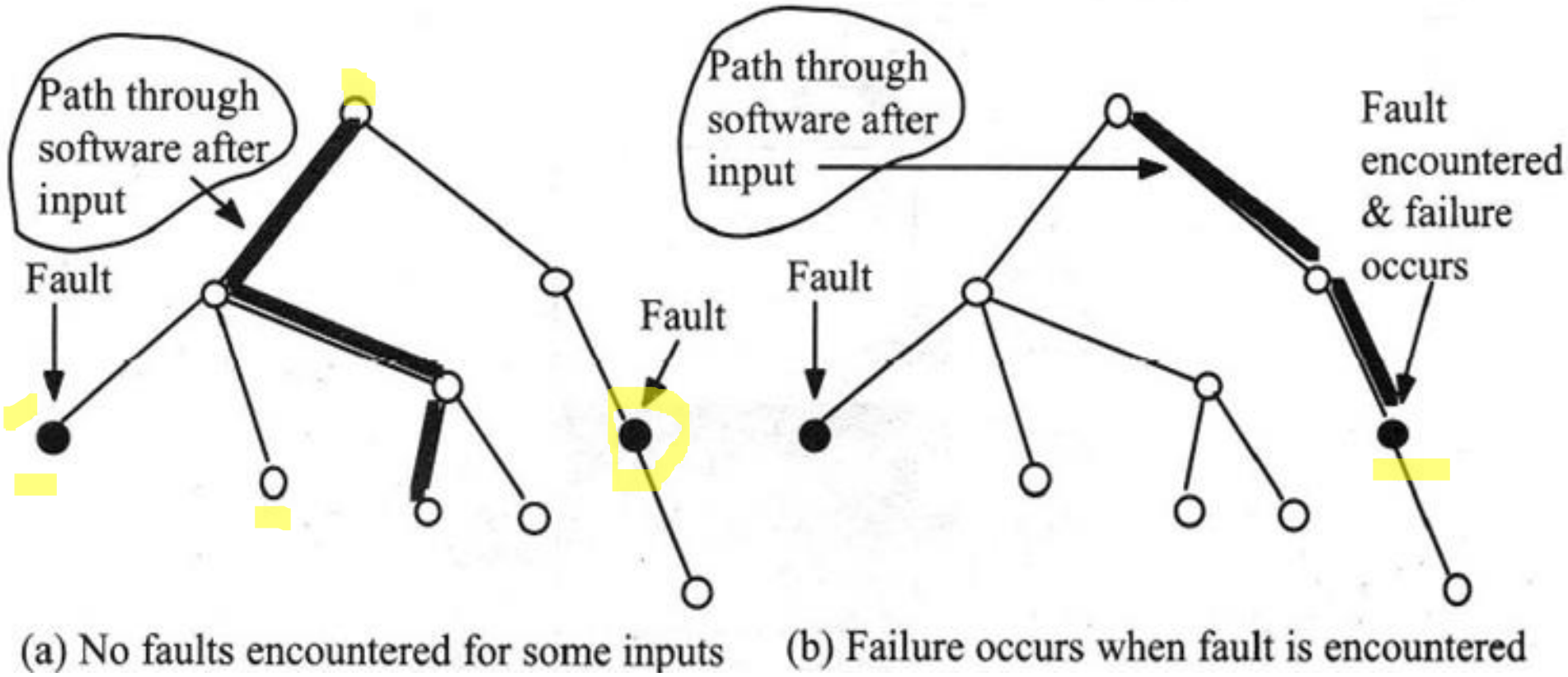


Fig 1: Execution of software modules

Software Reliability vs Hardware Reliability

1) Software has *no aging property* (no parts to wear out).

2) There are different *sources of improving reliability*.

3) Copies of software systems are identical.

RELIABILITY METRICS

1) Probability of Failure on Demand (POFOD):

- The likelihood that the system will fail when a service request is made.
- Most appropriate for systems where services demanded at relatively long time intervals and there are serious consequences if service is not delivered.
- It might be used to specify protection systems such as the reliability of a pressure relief system in a chemical plant or an emergency shutdown system in a power plant.
- A POFOD of 0.001 means that one out of a thousand service requests may result in failure.

RELIABILITY METRICS (Cont'd)

2) Rate of Occurrence of Failures (ROCOF)

- This metric should be used where regular demands are made on system services and where it is important that these services are correctly delivered.
- A ROCOF of 2/100 means that two failures are likely to occur in each 100 operational time units.
- It might be used in the specification of a bank teller system that processes customer transactions or in a hotel reservation system.
- Sometimes called the *failure intensity*.

RELIABILITY METRICS (Cont'd)

3) Mean time to failure (MTTF)

- Average time between observed system failures.
- Should be used in systems with long transactions.
- MTTF should be longer than the average transaction length.
- Examples of systems using this metric are word processor systems and CAD systems.
- An MTTF of 500 means one failure can be expected every 500 time units.

RELIABILITY METRICS (Cont'd)

4) Availability (AVAIL)

- This metric should be used in non-stop systems where users expect the system to deliver a continuous service.
- Examples of such systems are telephone switching systems and railway signaling systems.
- Availability of 0.998 means that the system is likely to be available for 998 of every 1,000 time units. It is defined as:

Availability = [MTTF/(MTTF + MTTR)] x 100%

RELIABILITY VALIDATION

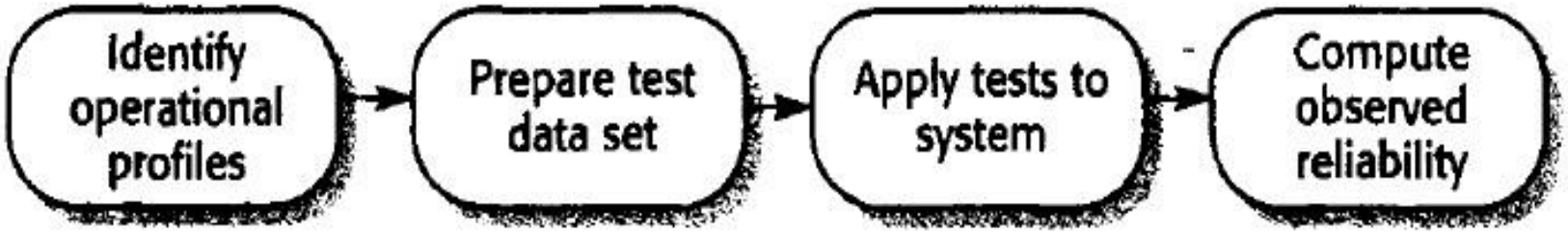


Fig 2: The reliability measurement process

This process involves four stages:

1. Studying existing systems of same type to establish an operational profile.
2. Construct a set of test data that reflect the operational profile.

RELIABILITY VALIDATION (Cont'd)

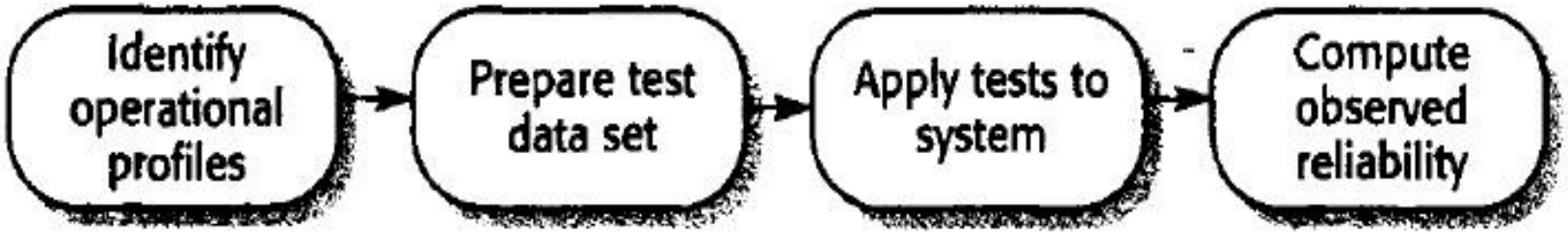


Fig 2: The reliability measurement process

3. Test the system using these data and then count the number and type of failures that occur.
4. After observing a statistically significant number of failures, compute the appropriate reliability metric value. This approach sometimes called *statistical testing.*

Task

Three identical computers are networked together in parallel configuration. Their failure rate is given by $\lambda = 0.2$ failures/year.

Calculate:

i) MTTF of each computer

ii) Reliability at the end of five years

Answers:

i) 5 years

ii) 0.747