SEENG 637

Dependability and Reliability of Software Systems

Chapter 9: System Reliability

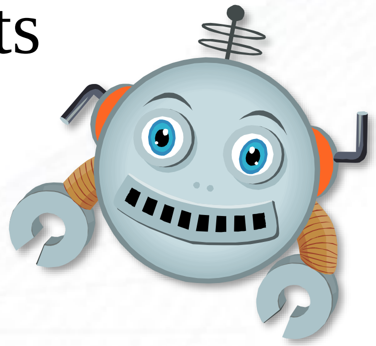
Department of Electrical & Software Engineering, University of Calgary

B.H. Far (far@ucalgary.ca)

http://people.ucalgary.ca/~far

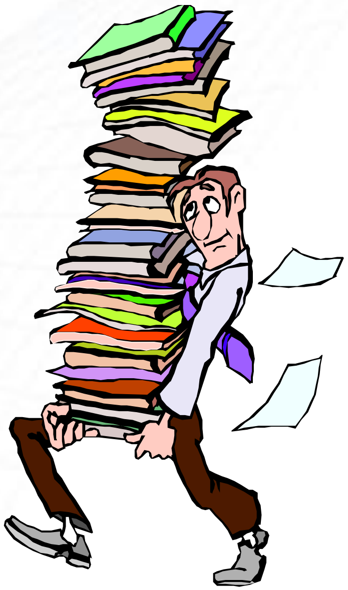
Recap …

- We already know how to define quality and how to calculate reliability for a system
- A system usually has many components
- Components may have
  - Different reliability
  - Different dependencies among each other
- **Q.** Can we calculate system reliability as a function of the reliabilities of its components and of the relationships between the components?



Contents

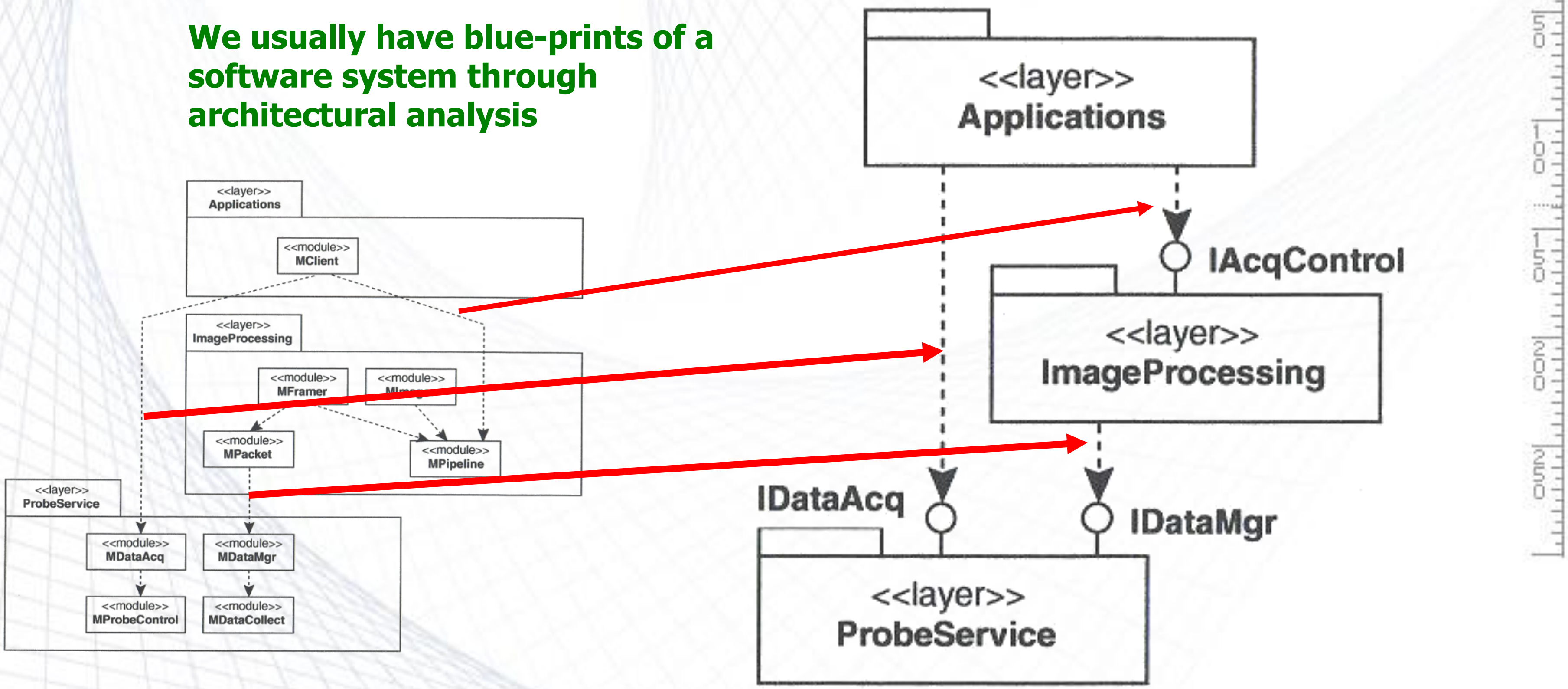
- How to assess system reliability?
- Reliability Block Diagram (RBD)
- Serial and parallel configuration
- Active redundancy
- Hazard analysis:
  - Fault tree analysis (FTA)



Example: Software System

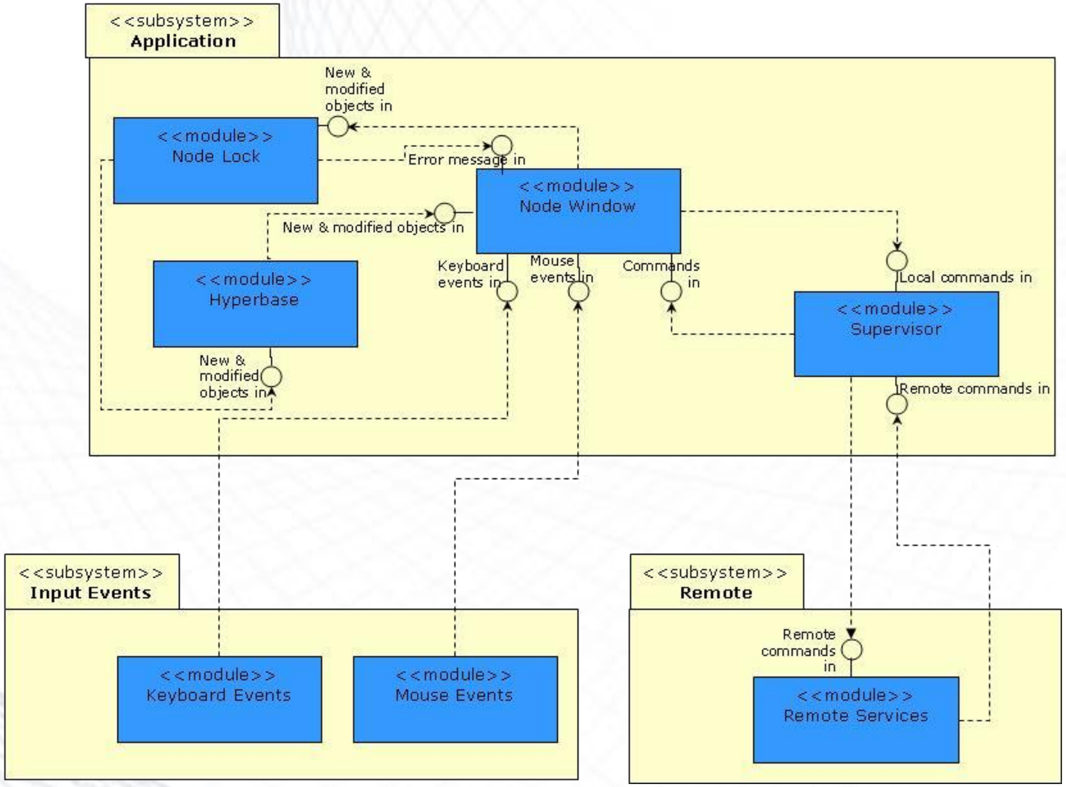
- Image processing system

We usually have blue-prints of a software system through architectural analysis

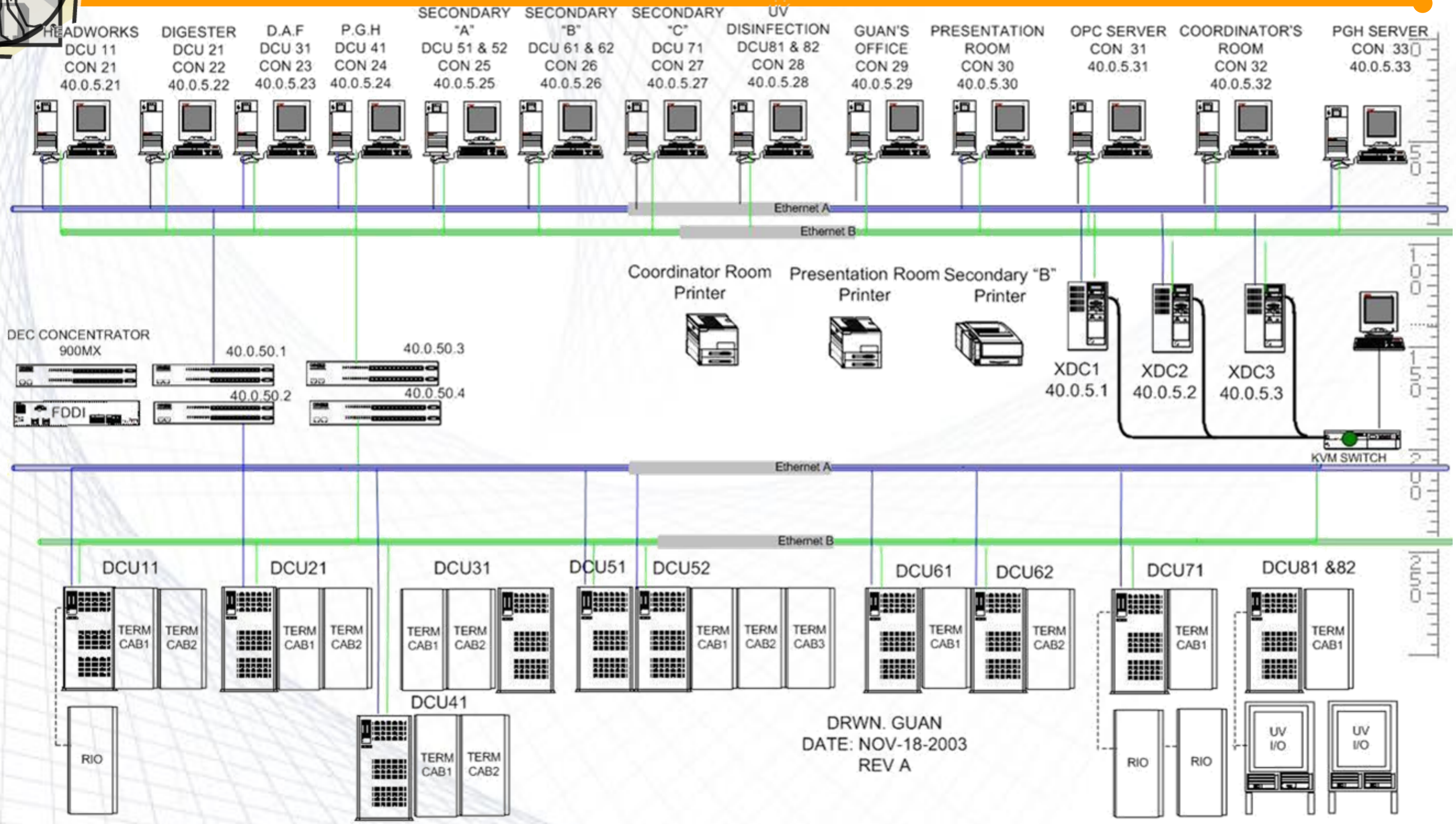


Example: Software System

- Concept map system



Example: Industrial Control



far@ucalgary.ca

Example: Bicycle

- How reliable is it?
- Can you find any redundancy?
  - Handle?
  - Saddle?
  - Frame?
  - Brake?
  - Gear?
  - Wheel?
  - Wheel spokes?

Reliability Block Diagram (RBD)

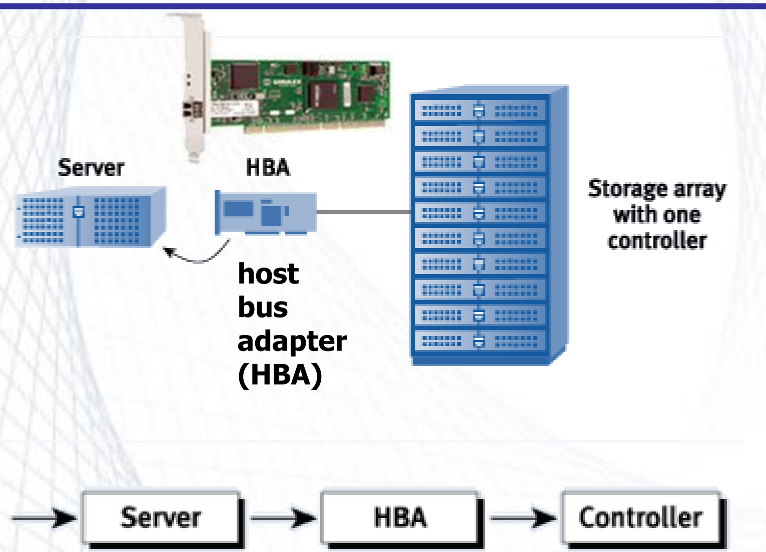
- Reliability Block Diagram (RBD) is a graphical representation of how the components of a system are connected from reliability point of view
- Reliability of the system is derived in terms of reliabilities of its individual components
- The most common configurations of an RBD are the serial and parallel configurations
- A system is usually composed of combinations of serial and parallel configurations
- RBD analysis is essential for determining reliability, availability and down time of the system

Reliability Block Diagram (RBD)

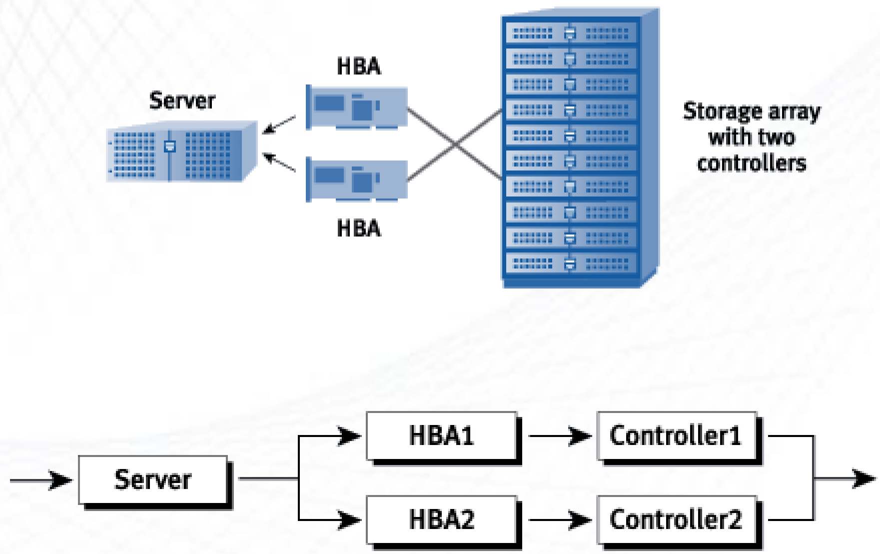
- In a **serial system configuration**, the elements must all work for the system to work and the <u>system fails if ***one*** of the components fails</u>
  - The overall reliability of a serial system is lower than the reliability of its individual components
- In **parallel system configuration**, the components are considered to be redundant and the <u>system will cease to work if ***all*** the parallel components fail</u>
  - The overall reliability of a parallel system is higher than the reliability of its individual components

UNIVERSITY OF CALGARY

RBD Example: Storage System



$$R_{sys} = R_{server} R_{HBA} R_{controller}$$



$$R_{sys} = R_{server}[1-(1-R_{HBA1}R_{controller1})(1-R_{HBA2}R_{controller2})]$$

Host Bus Adapter (HBA) is the interface card which connects a host to a Storage Area Network (SAN)

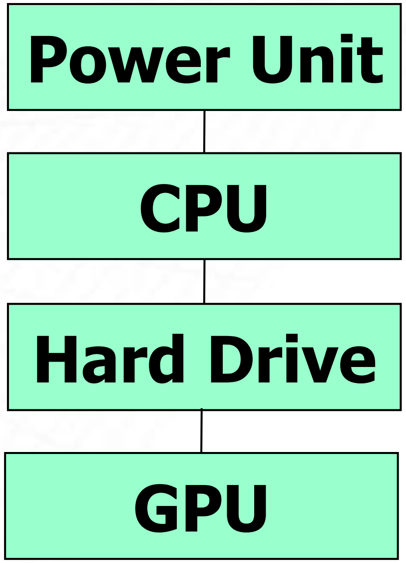
RBD: Process Steps

1. Define boundary of the system for analysis
2. Break system down into functional units
3. Determine serial-parallel configurations
4. Represent each components as a separate block in the diagram
5. Draw lines connecting the blocks in a logical order for mission success

Serial System Reliability /1

- No redundancy
- ALL component of the system are needed to make the system function properly
- If any one of the components fails, the system fails
- **Example**

System block diagram



Serial System Reliability /2

- Reliability Block Diagram
- System is composed of *n* independent serially connected components
- Failure of any component has a cross system effect, *i.e.*, results in failure of the whole system

R_1/λ_1 — R_2/λ_2 — …

- **Example**

Power Unit R_1/λ_1 — **CPU** R_2/λ_2 — **Hard Drive** R_3/λ_3 — **GPU** R_4/λ_4

Combining Reliabilities

- ***Serial system reliability*** can be calculated from component reliabilities, if the components fail independently of each other
- For serial systems:

$$R = \prod_{k=1}^{Q_p} R_k \quad and \quad \lambda = \sum_{k=1}^{Q_p} \lambda_k$$

Q_p number of components

R_k component reliability

- Components reliabilities (R_k) must be expressed with respect to a common interval
- A serial system has always smaller reliability than its components (because $R_k \leq 1$)

Example: Serial System

- The system is composed of 3 independent serially connected components
  - $R_1 = 0.95$
  - $R_2 = 0.87$
  - $R_3 = 0.82$

Note: all Rs must be given for a common duration, e.g., 10 hours of operation.

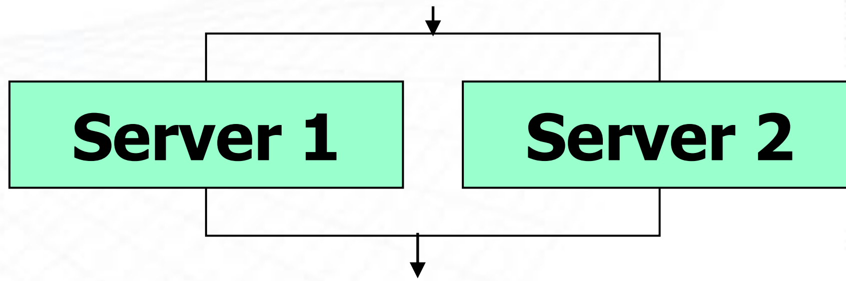
$$R_{system} = 0.95 \times 0.87 \times 0.82 = 0.6777$$

- Serial system reliability is smaller than any individual reliability of the components

Parallel System Reliability /1

- System with Redundancy
- Only ONE out of *n* (identical) components is needed to make the system function properly
- If ALL of the components fail, the system fails
- **Example**

System block diagram



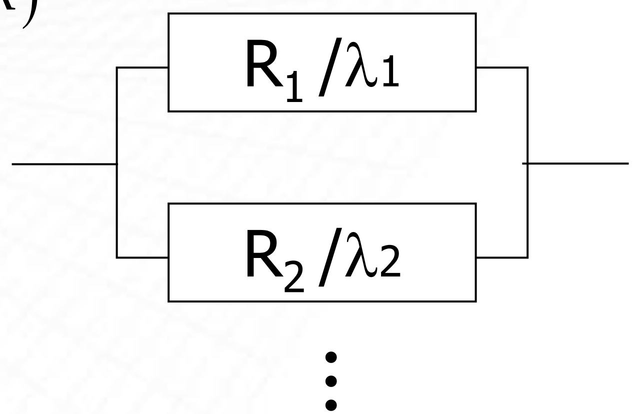
Parallel System Reliability /2

- System is composed of n independent components connected in parallel
- Failure of all components results in the failure of the whole system (principle of active redundancy)

$$F = \prod_{k=1}^{Q_p} F_k \qquad F \text{ is unreliability} \quad (F = 1 - R)$$

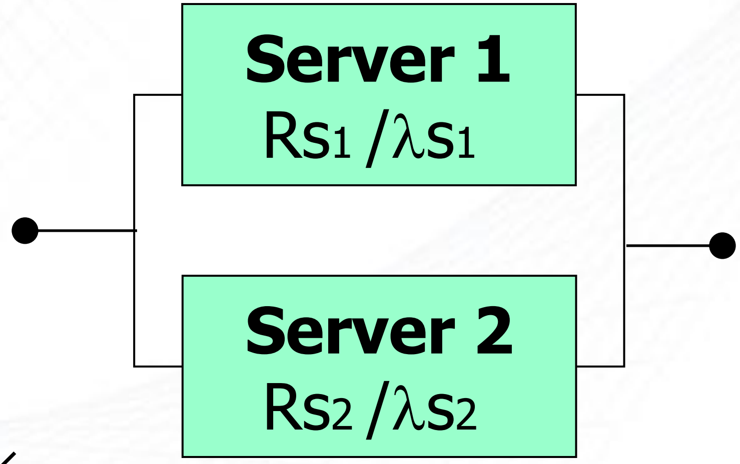
$$R = 1 - \prod_{k=1}^{Q_p} F_k = 1 - \prod_{k=1}^{Q_p} (1 - R_k)$$

$$\frac{1}{\lambda} = \sum_{k=1}^{Q_p} \frac{1}{\lambda_k} \quad or \quad MTTF = \sum_{k=1}^{Q_p} MTTF_k$$



Parallel System Example

- The system is composed of 2 identical servers connected in parallel
  - $R_1 = 0.6777$
  - $R_2 = 0.6777$

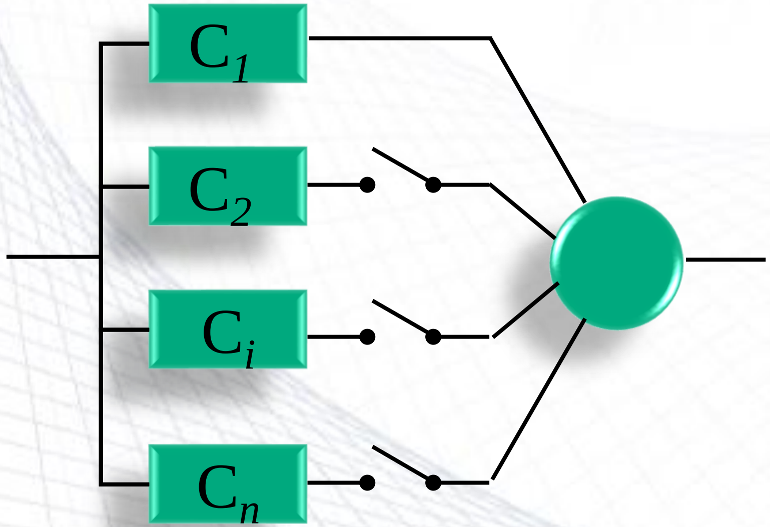


$$R_{system} = 1 - ((1 - 0.6777) \times (1 - 0.6777)) = 0.8961$$

- Parallel system reliability is greater than any individual reliability of the components

Sequential System Reliability

- When one component fails, the next one is assigned to fulfill the job (*e.g.*, telephone switching circuits)
- This is done in sequence until no components left
- Reliability for such system:

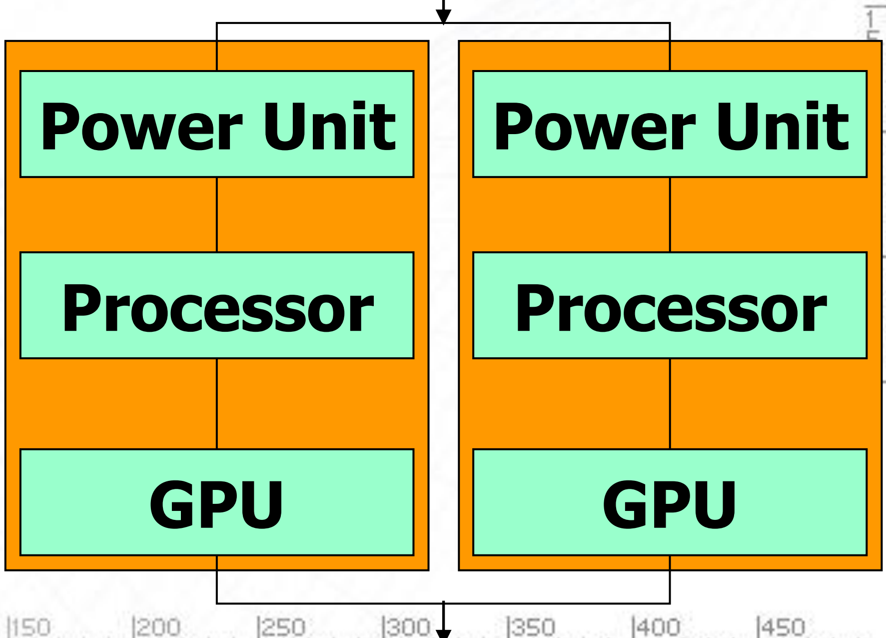


$$R_{sys}(t) = \sum_{i=0}^{n-1} \frac{(\lambda_i t)^i}{i!} e^{-\lambda_i t}$$

Mixed System Reliability /1

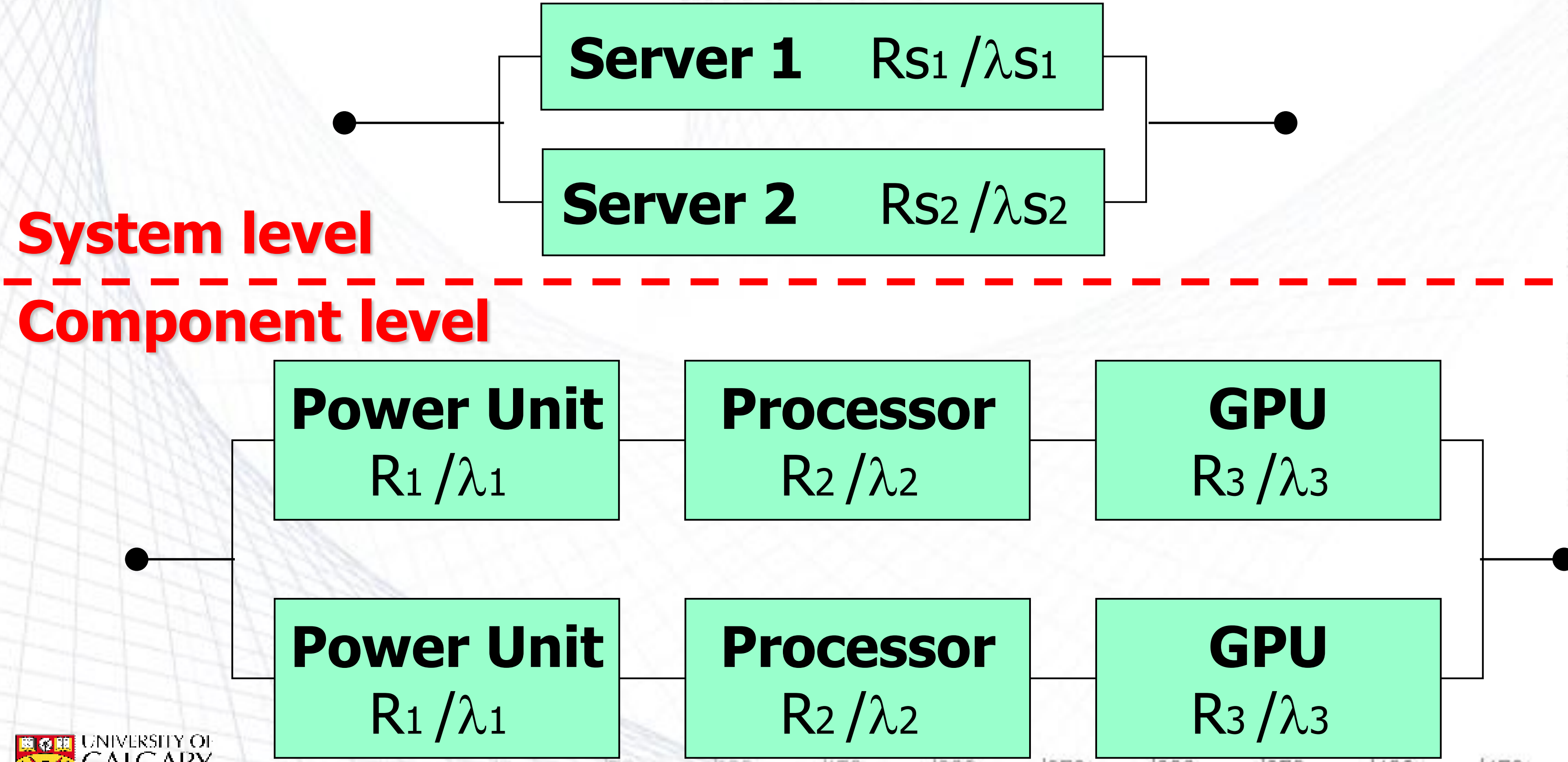
- System with Redundancy
- Only ONE out of *n* set of components is needed to make the system function properly
- If ALL sets of components fail, the system fails
- **Example**

System block diagram

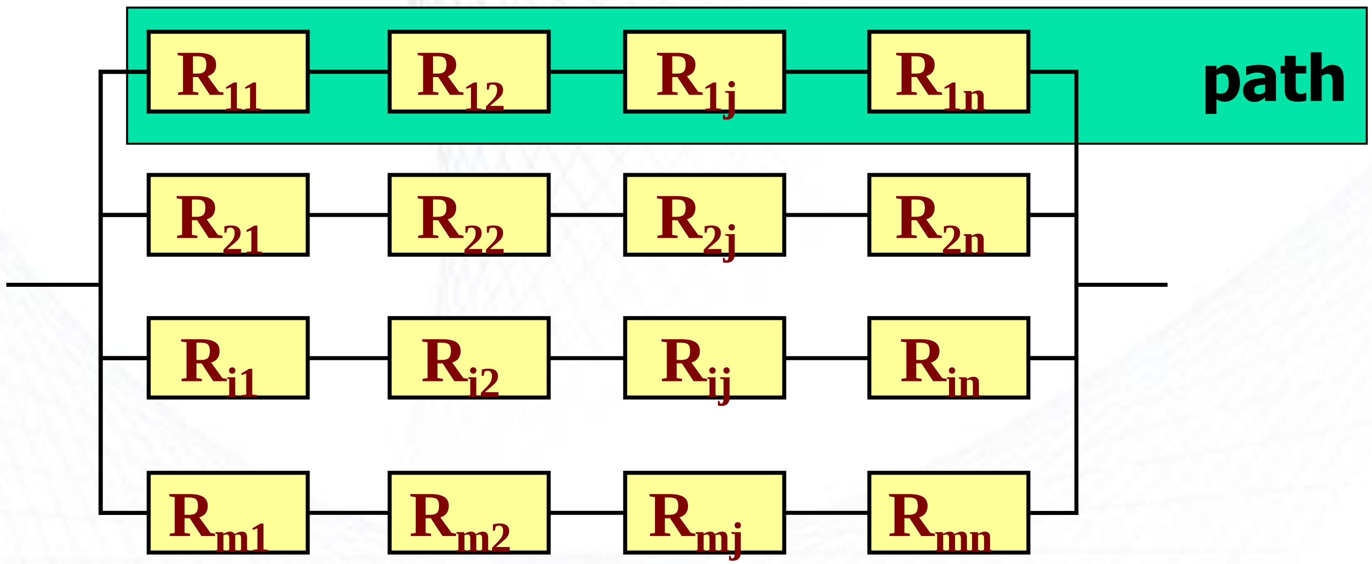


Mixed System Example

- Reliability Block Diagram



Parallel-Series System

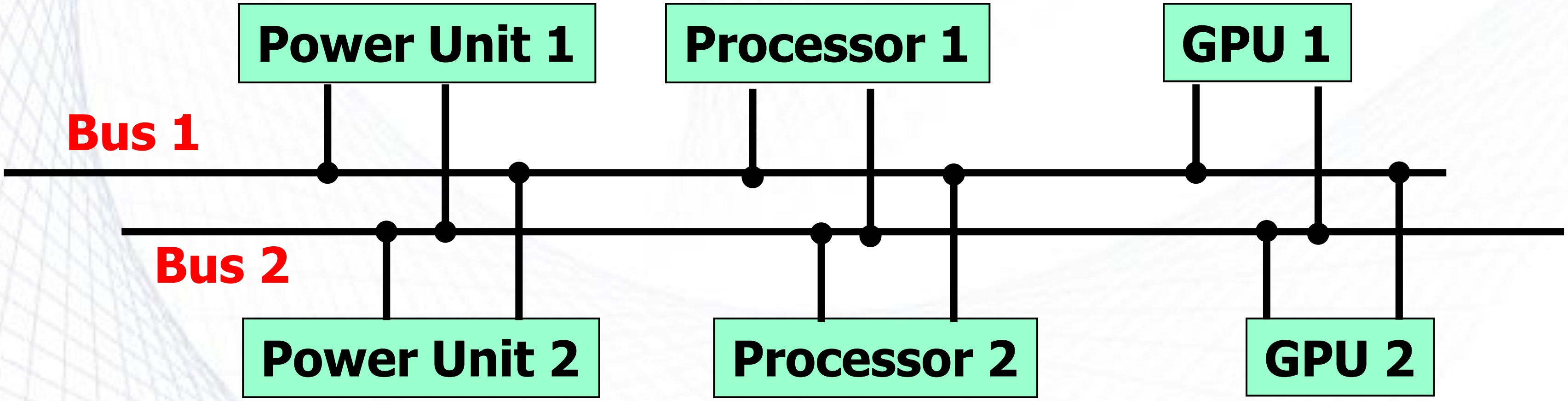


Path reliability $R_i = \prod_{j=1}^{n} R_{ij}$

System reliability $R = 1 - \prod_{i=1}^{m} (1 - R_i) = 1 - \prod_{i=1}^{m} \left(1 - \prod_{j=1}^{n} R_{ij}\right)$

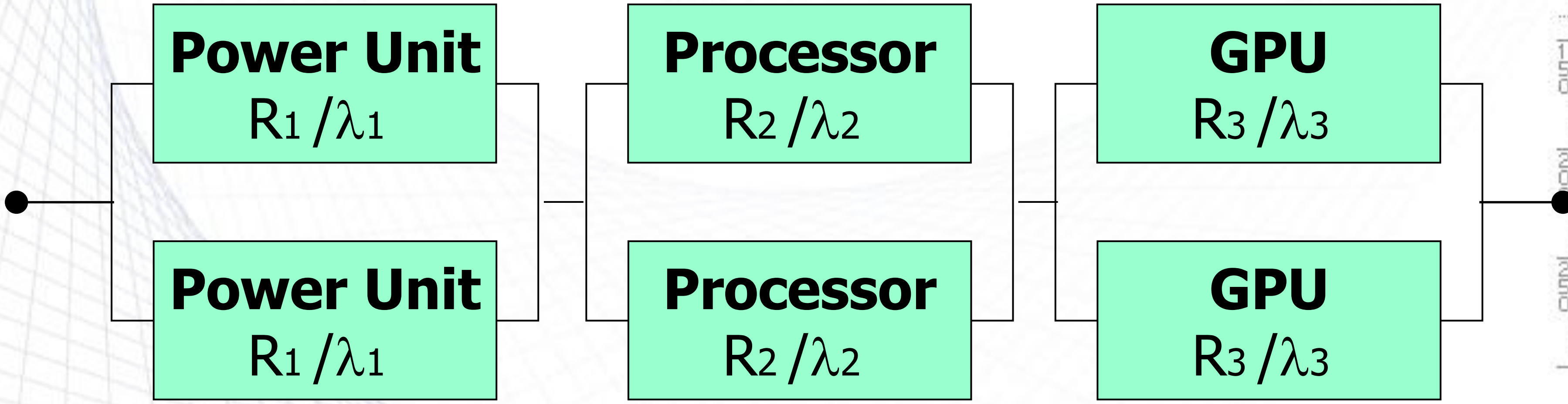
Various Configurations /3

- Series-Parallel configuration

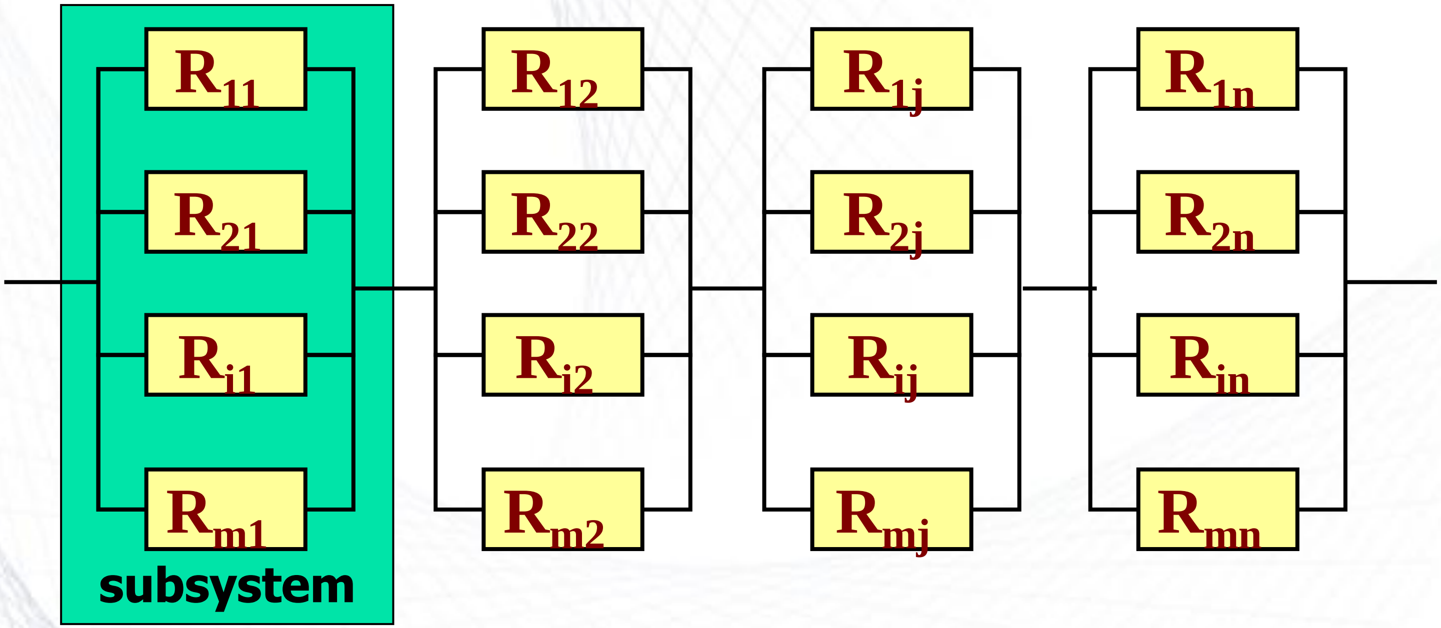


Various Configurations /4

- Reliability Block Diagram for Series-Parallel configuration



Series-Parallel System

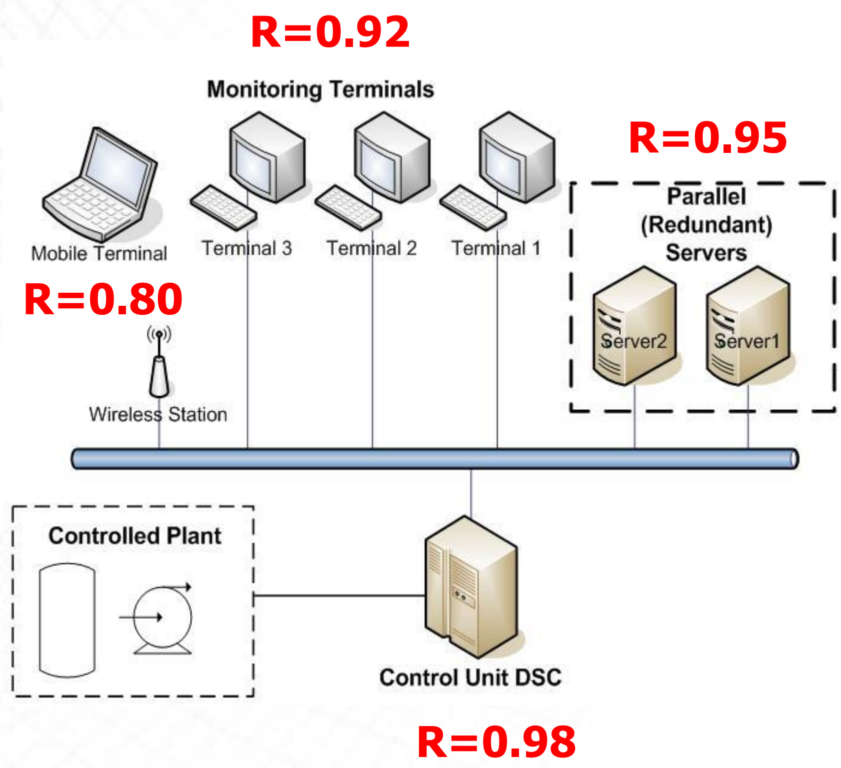


Subsystem reliability $R_j = 1 - \prod_{i=1}^{m}(1 - R_{ij})$

System reliability $R = \prod_{j=1}^{n} R_j = \prod_{j=1}^{n}\left[1 - \prod_{i=1}^{m}(1 - R_{ij})\right]$

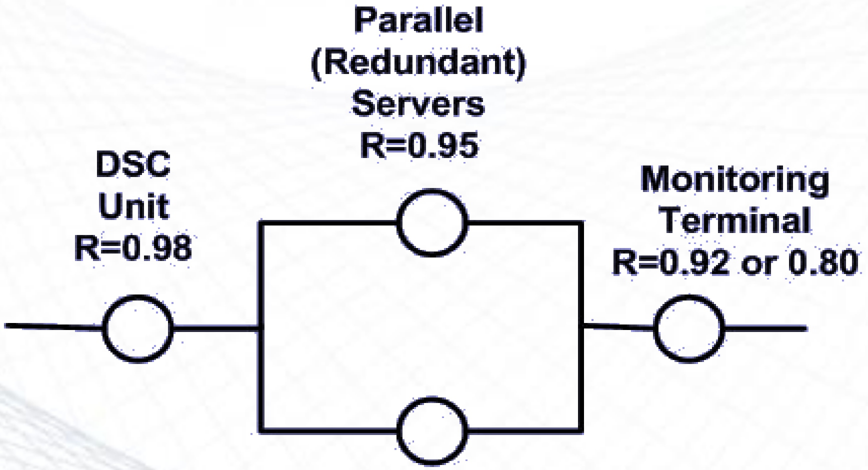
Example

- In this example, control unit DSC is responsible for controlling the plant. The data from the plant is sent to the two database servers. The servers are configured parallel for maximizing system availability. The monitoring terminals (3 stationary and one mobile) are used to monitor the behaviour of the plant. The system is configured that only one monitoring terminal at a time can control the plant. When one of the terminals is connected the other 3 terminals will be cut-off automatically.



Example (cont'd)

- Reliability for 10 hours of operation for DSC, Servers and Terminals are 0.98, 0.95, 0.92, respectively
- For the same 10 hours of operation, the reliability of the wireless station and mobile terminal pair is 0.80
- Draw reliability block diagram for this system



Example (cont'd)

- Calculate the maximum and minimum system reliability

Maximum R_{system} =
$0.98 \times [1 - (1 - 0.95)^2] \times 0.92 = 0.899$

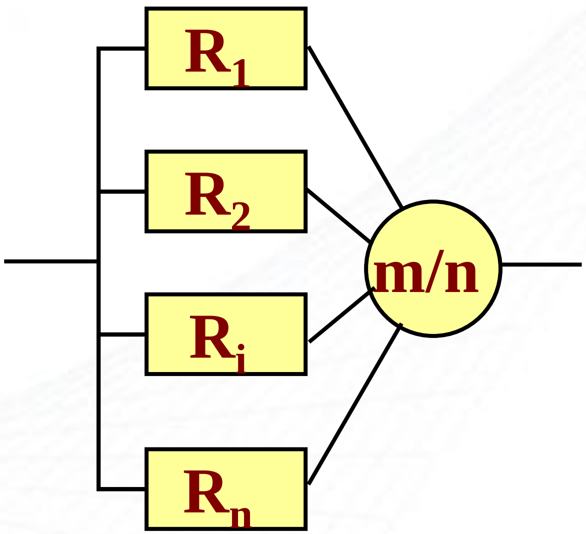
Minimum R_{system} =
$0.98 \times [1 - (1 - 0.95)^2] \times 0.80 = 0.782$

Active Redundancy

- Employs parallel systems
- All components are active at the same time
- Each component is able to meet the functional requirements of the system
- Only one component is required to meet the functional requirements of the system
- Each component satisfies the minimum reliability condition for the system
- System only fails if all components fail

m – out of – n System

- System has *n* components
- At least *m* components need to work correctly for the system to function properly ($m \le n$)
  - *m=n:* serial system
  - *m=1:* parallel system
- e.g.: airplane with 4 engines can fly with only 2 engines



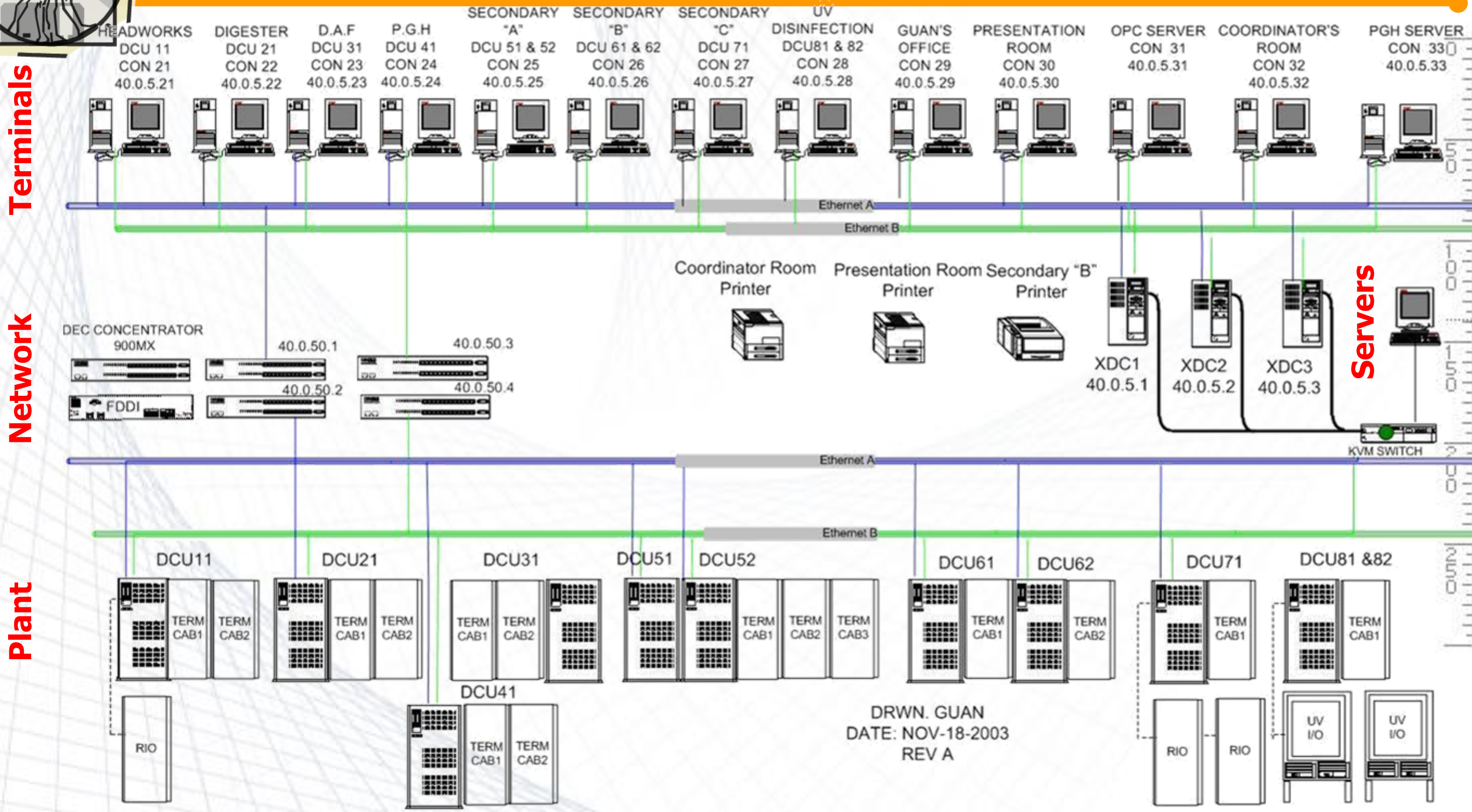
$$R_{sys}(t) = 1 - \sum_{i=0}^{m-1} \binom{n}{i} R(t)^i (1 - R(t))^{n-i}$$

$$\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$$

Assumption:

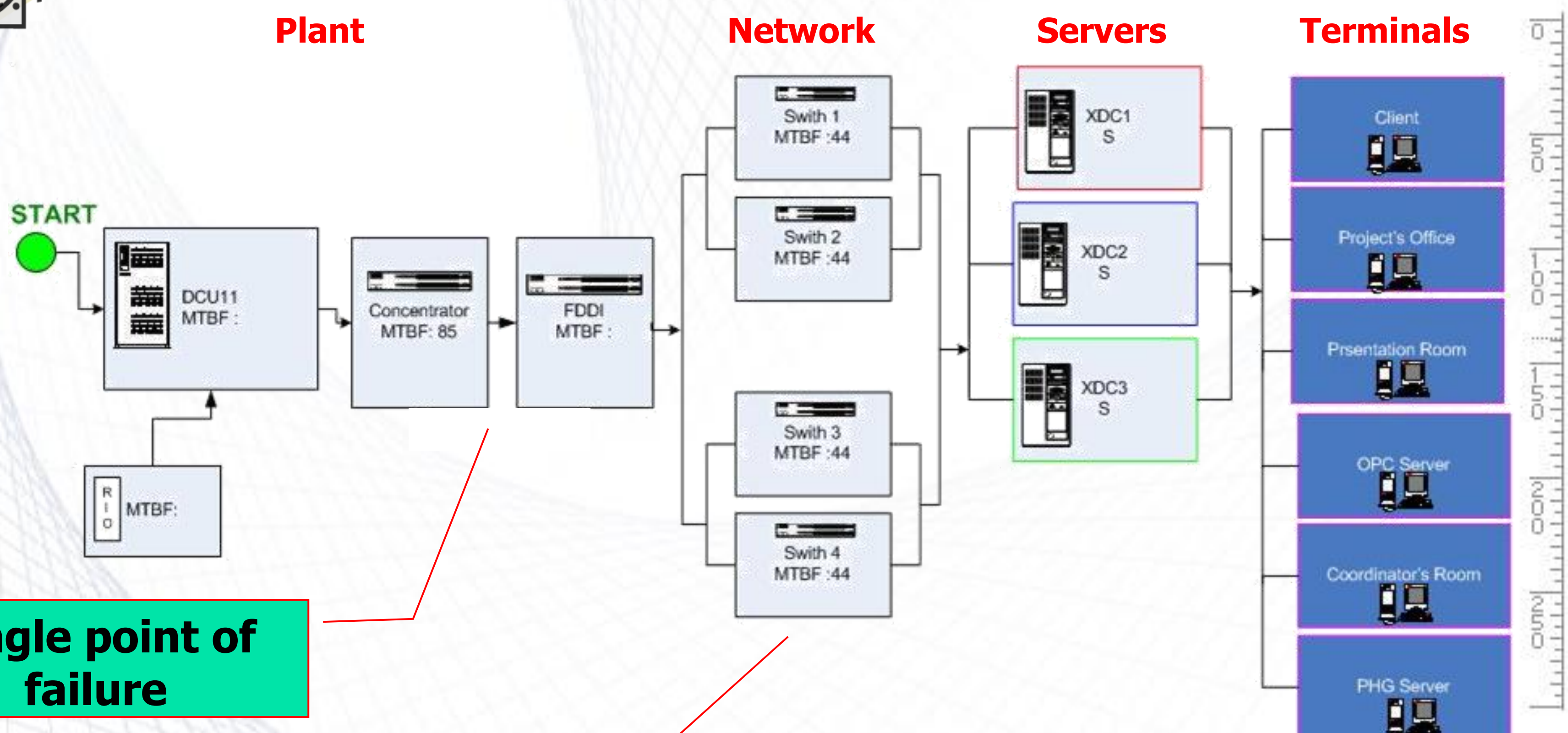
All components have the same reliability

Example: Industrial Control



UNIVERSITY OF CALGARY

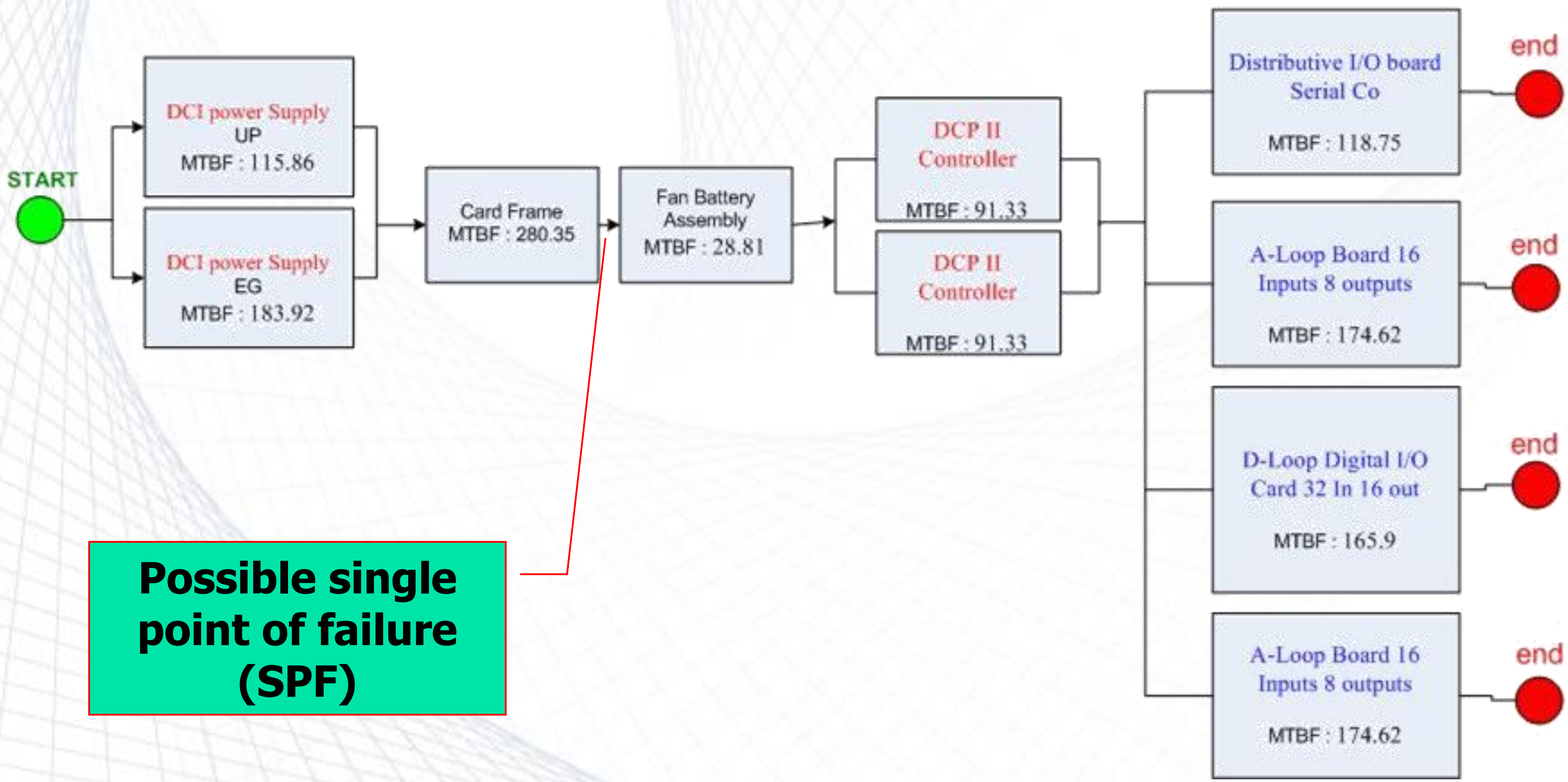
RBD: Example /1



Single point of failure

Possible over redundancy

RBD: Example /2



Possible single point of failure (SPF)

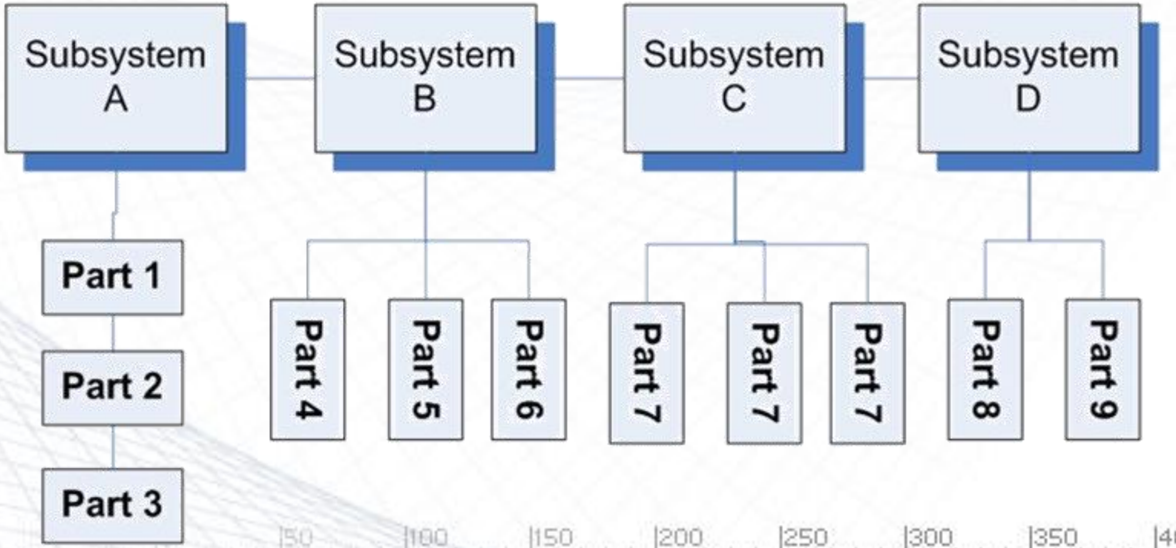
SPF: How to Avoid?

Avoiding Single Point of Failure

- Adopt redundancy ← Use dissimilar methods – consider common-cause vulnerability
- Adopt a fundamental design change
- Use equipment which is **extremely** reliable/robust
- Perform frequent Preventive Maintenance/ Replacement ← repair before failure happens
- Reduce or eliminate service and/or environmental stresses ← extreme stress leads to failure

Exercise 1

- In reliability prediction for an assembled system we usually use a "bottoms-up" approach by estimating the failure rate for each subsystem and then combining the failure rates for the entire assembly. The following figure illustrates a system in which the subsystems A, B, C, and D are in a serial configuration. Each subsystem is composed of several parts which are connected as serial or parallel as shown.



Exercise 1 (cont'd)

- The failure rates of serial parts 1, 2, and 3 are 0.1, 0.3, and 0.5 per hour, respectively
- Determine failure rate and MTTF for subsystem A

$$\lambda_A = \lambda_1 + \lambda_2 + \lambda_3$$

$$\lambda_A = 0.1 + 0.3 + 0.5 = 0.9 \text{ failures per hour}$$

$$MTTF_A = \frac{1}{\lambda} = \frac{1}{0.9} = 1.11 \text{ hours}$$

Exercise 1 (cont'd)

- The failure rates of parallel parts 4, 5, and 6 in subsystem B are 0.2, 0.4, and 0.25 per hour, respectively
- Determine failure rate and MTTF for subsystem B

$$R_B = e^{-\lambda_B t} = 1-(1-R_4)(1-R_5)(1-R_6)$$

$$R_B = e^{-\lambda_B t} = 1-(1-e^{-0.20})(1-e^{-0.40})(1-e^{-0.25})$$

$$R_B = e^{-\lambda_B t} = 0.9868$$

$$\lambda_B = 0.0133 \quad \text{failures per hour}$$

$$MTTF_B = \frac{1}{\lambda_B} = 75.1879 \quad \text{hours}$$

Exercise 1 (cont'd)

- The failure rate of parallel parts 7 is constant and is 0.2 per hour
- Determine failure rate and MTTF for subsystem C in which at least 2 out of 3 items must be working

$$R_C = 1 - \sum_{i=0}^{m-1} \binom{n}{i} R_7^{\,i} (1 - R_7)^{n-i} \qquad R_7 = e^{-0.2} = 0.8187$$

$$R_C = 1 - \left[\binom{3}{0} R_7^{\,0} (1 - R_7)^3 + \binom{3}{1} R_7^{\,1} (1 - R_7)^2 \right] = 1 - \left[(1 - R_7)^3 + 3R_7 (1 - R_7)^2 \right]$$

$$R_C = 1 - \left[(1 - 0.8187)^3 + 3 \times 0.8187 (1 - 0.8187)^2 \right] = 0.9133$$

$$R_C = e^{-\lambda t} = 0.9133 \qquad \lambda_C = 1.004 \quad \text{failures per hour}$$

$$MTTF_C = \frac{1}{\lambda_C} = 0.9960 \quad \text{hours}$$

Exercise 1 (cont'd)

- The failure rates of parallel parts 8 and 9 in subsystem D are 0.25 and 0.2 per hour, respectively
- Determine failure rate and MTTF for subsystem D

$$R_D = e^{-\lambda_D t} = 1-(1-R_8)(1-R_9)$$

$$R_D = e^{-\lambda_D t} = 1-(1-e^{-0.25})(1-e^{-0.20})$$

$$R_D = e^{-\lambda_D t} = 0.9599$$

$$\lambda_D = 0.0409 \quad \text{failures per hour}$$

$$MTTF_D = \frac{1}{\lambda_D} = 24.4498 \quad \text{hours}$$

Exercise 1 (cont'd)

- Determine overall failure rate and MTTF for the whole system

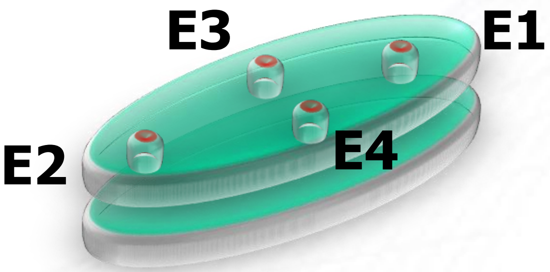
$$\lambda_{system} = \lambda_A + \lambda_B + \lambda_C + \lambda_D = 0.9 + 0.0133 + 1.004 + 0.0409$$

$$\lambda_{system} = 1.9582 \quad \text{failures per hour}$$

$$MTTF_{system} = \frac{1}{\lambda_{system}} = 0.5107 \quad \text{hours}$$

Example 2

The fastening of two mechanical parts in an automobile brake system should be reliable. It is done by means of two flanges which are pressed together with 4 bolt and nut pairs E1 to E4 placed 90 degrees to each other.

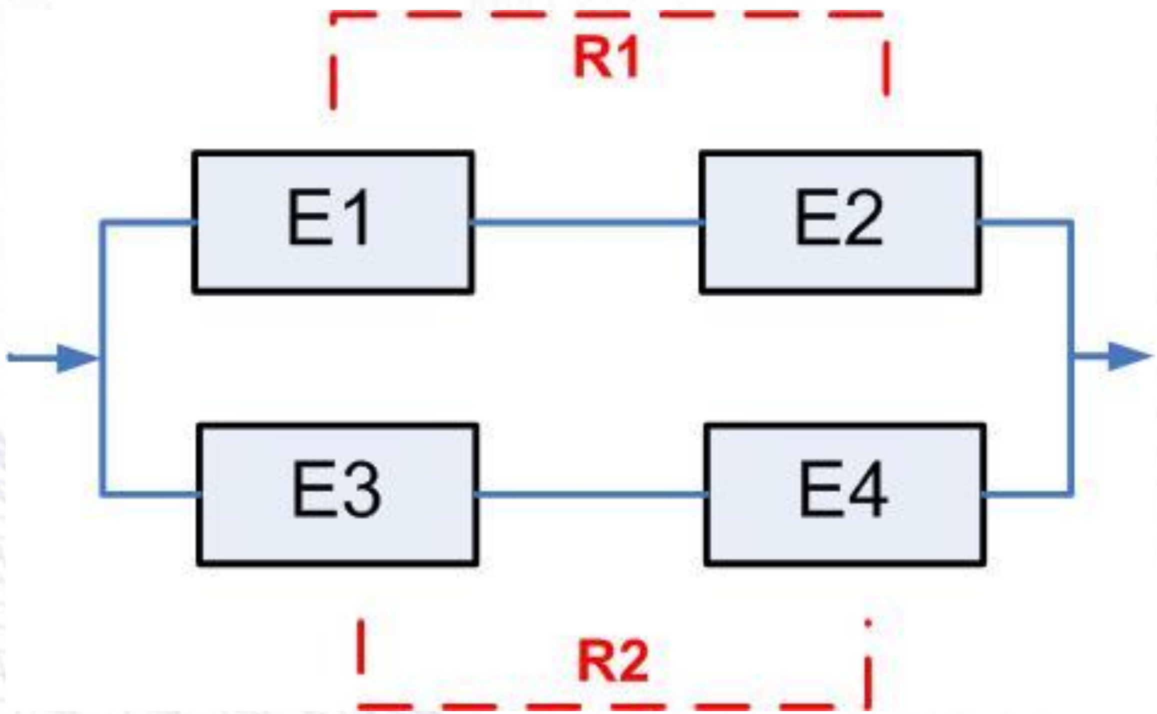


R=0.90
for 50K miles

- Experience shows that the fastening holds when ***<u>at least one bolt and nut pair located opposite to each other</u>*** work, i.e., (E1 and E2) or (E3 and E4)

Example 2 (cont'd)

a) Draw the reliability block diagram (RBD) for this fixation of the system



Example 2 (cont'd)

b) Compute reliability of the fixation described in (a) if all bolt and nut pairs have the reliability of R=0.90 for 50K miles of operation

$R1 = R2 = 0.9 \times 0.9 = 0.81$

$R_{system} = 1 – (1 – R1)\,(1 – R2)$

$= 1 – (1 – 0.81)\,(1 – 0.81) = 0.9639$

Example 2 (cont'd)

c) Name the redundancy type if ***any pair of bolts and nuts*** were sufficient for the required brake function

Two-out-of-four redundancy

Example 2 (cont'd)

d) Compute reliability for case (c) if all bolt and nut pairs have the reliability of R=0.90 for 50K miles of operation

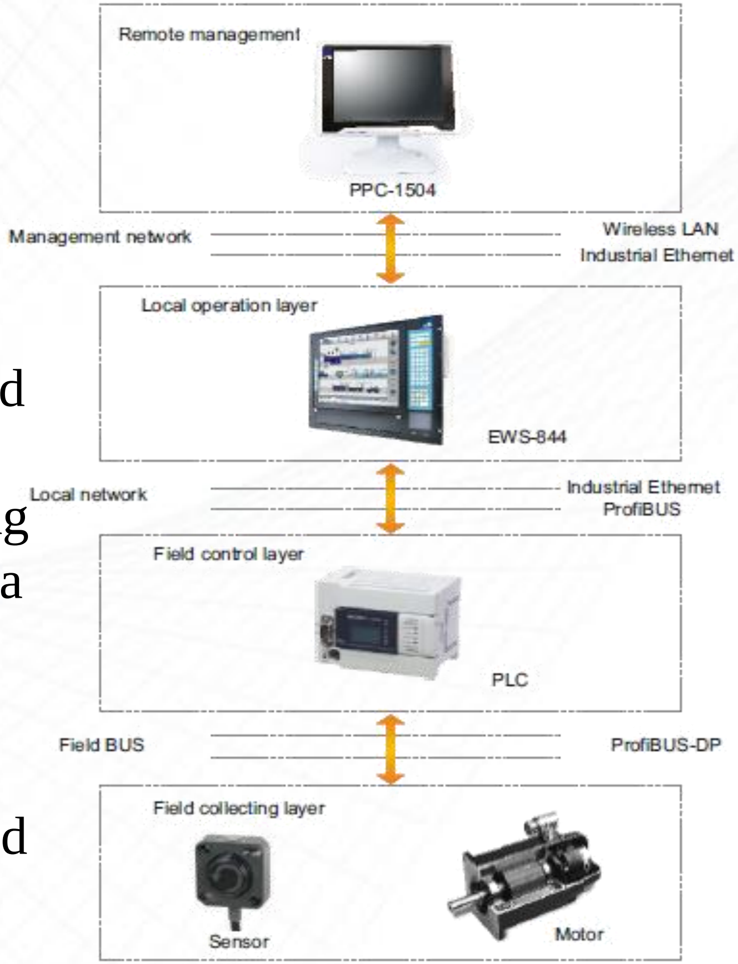
$$R = 1 - \left[\binom{4}{0} (0.9)^0 (1-0.9)^4 + \binom{4}{1} (0.9)^1 (1-0.9)^3 \right] =$$

$$1 - \left[(0.1)^4 + 3.6 \times (0.1)^3 \right] = 0.9963$$

e) What can be concluded?

Example 3

- Control Unit PLC is responsible for controlling the plant via field control layer. Data from the plant is sent to the local operation and remote management layers.
- Between layers, the data is transmitted redundantly using two distinct paths for each, except for the field collecting and field control layers that is only via a single Field BUS. For the rest, we have redundancy. For example, data transmission between local operator and remote management is transmitted via both wired and wireless to ensure maximum reliability.

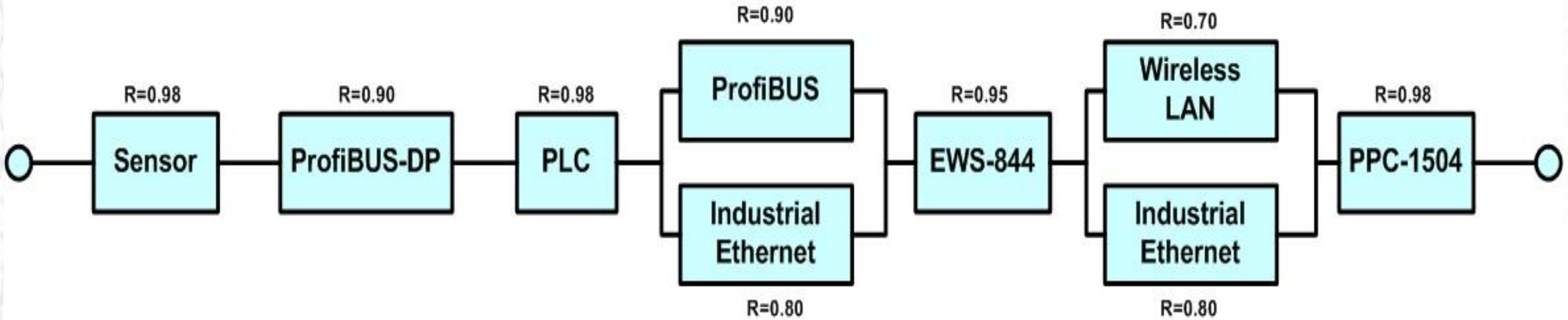


Example 3 (Cont'd)

- Field collecting layer is a single sensor of reliability of 0.98 for 24 hours
- ProfiBUS-DP's reliability is 0.90 for 24 hours
- The PLC's reliability is 0.98 for 24 hours
- Industrial Ethernet and ProfiBUS have reliability of 0.80 and 0.90 for 24 hours, respectively
- Local operator EWS-844's reliability is 0.95 for 24 hours
- Wireless LAN and Industrial Ethernet have reliability of 0.70 and 0.80 for 24 hours, respectively
- Remote manager PPC-1504 has reliability of 0.98 for 24 hours

Example 3 (Cont'd)

- Draw reliability block diagram for this system



- Calculate system reliability for 24 hours of operation

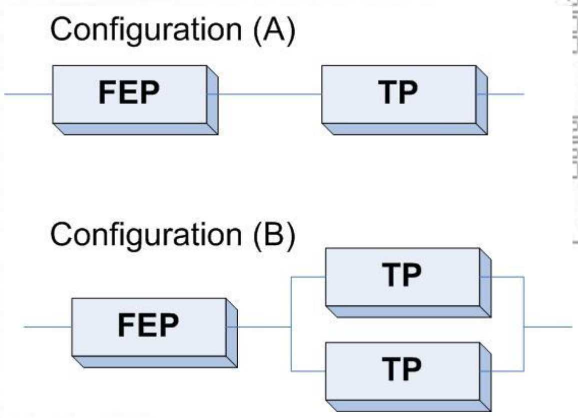
R = 0.98 x 0.90 x 0.98 x (1-(1-0.90)(1-0.80)) x 0.95 x (1-(1-0.70)(1-0.80)) x 0.98

R = 0.7413

Example 4

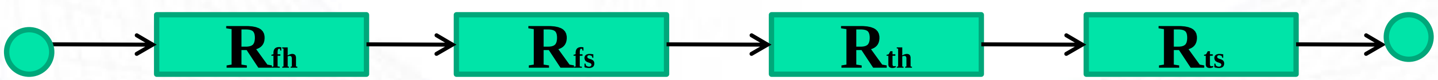
A bank is going to set up a computerized transaction system with a target reliability objective of 0.90 per shift (8 hours of operation). There are two system configurations considered for this job as shown below. Each configuration consists of a front-end-processor (FEP) and one or more transaction processors (TP). The 8-hours reliability and utilization rate for the FEP and TPs are given below.

	Front-end processor (FEP)	*Transaction processors (TP)*
Hardware reliability (for 8 hours)	$R_{fh} = 0.99$	$R_{th} = 0.98$
Software reliability (for 8 hours)	$R_{fs} = 0.95$	R_{ts}
Hardware failure intensity	$\lambda_{fh} = 0.00126$ failures/hour	$\lambda_{th} = 0.00253$ failures/hour
Software failure intensity	$\lambda_{fs} = 0.00641$ failures/hour	λ_{ts}
Utilization rate	%100	%40



Example 4 (Cont'd)

- For configuration (A) draw the reliability block diagram (RBD) and calculate the 8-hours reliability of the transaction processor (R_{ts}) and software failure intensity λ_{ts}



As the two components are in serial, we have:

$$R = R_{fh} \times R_{fs} \times R_{th} \times R_{ts}$$

$$0.90 = 0.99 \times 0.95 \times 0.98 \times R_{ts}$$

$$R_{ts} = 0.976$$

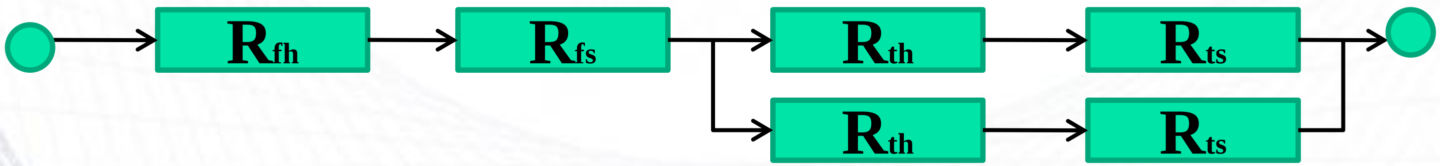
As utilization of TP is 40% then $t = 8 \times 0.4 = 3.2$

$R_{ts} = \exp(-\lambda_{ts}\ t) = \exp(-3.2\ \lambda_{ts})$ **therefore**

$\lambda_{ts} = 0.0076$ **failure/CPU hour**

Example 4 (Cont'd)

- For configuration (B) draw the reliability block diagram (RBD) and repeat calculation for 8-hours reliability of the transaction processor (R_{ts}) and software failure intensity λ_{ts}



$$R = R_{fh} \times R_{fs} \times [1-(1-(R_{th} \times R_{ts}))^2]$$
$$0.90 = 0.99 \times 0.95 \times [1-(1-(0.98 \times R_{ts}))^2]$$

$R_{ts} = 0.809$ and
$\lambda_{ts} = 0.0662$ failure/CPU hour

RBD: When and How

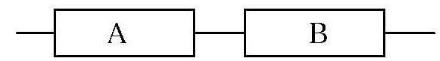
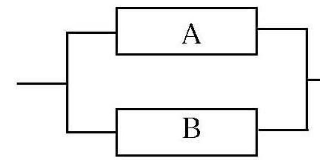
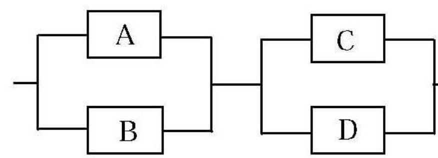
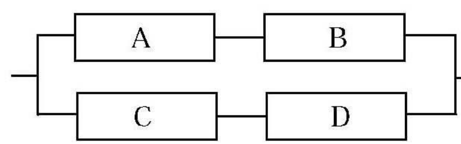
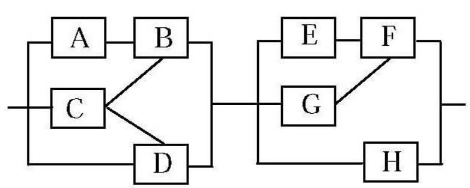
- When to use RBD?
  - When reliability of a complex system must be calculated and the reliability-wise weaknesses of the system must be identified
- How to use RBD?
  - Draw the RDB diagram ← sometimes not that simple!
  - Calculate the system reliability using the RBD diagram
  - Perform calculation such as availability and downtime
- There are a number of automated tools, integrated with the other methods, such as Fault Tree Analysis (FTA), to generate the diagram and to analyze it

RBD: Benefits & Limitations

- RBD is the simplest way of visualizing the reliability of the complex systems
- The benefits of the RBD are:
  - Establishes reliability goals; Evaluates component failure impact on overall system safety; Provides a basis for "what if" analysis; Allocates component reliability by calculating system MTBF; Provides cost savings in large system trouble-shooting; Estimates system reliability; Analyzes various system configurations in trade-off studies; Identifies potential design problems; Determines system sensitivity to component failures
- Disadvantages are that some complex constructs, such as standby, branching and load sharing, etc., cannot be clearly represented using the traditional RBD constructs

RBD: Conclusion

- Restricting assumptions:
  - Statistical independence
  - Failures independence
  - Repairs independence

Type Branch	Block Diagram Representation	System Reliability #
Series		$R_S = R_A * R_B$
Parallel		$R_S=1-(1-R_A)(1-R_B)$
Series-parallel		$R_S=1-(1-R_A)(1-R_B))$ $* (1-(1-R_C)(1-R_D))$
Parallel-series		$R_S=1-(1-(R_A*R_B))$ $* (1-(R_C*R_D))$
Complex		

Hazard Analysis

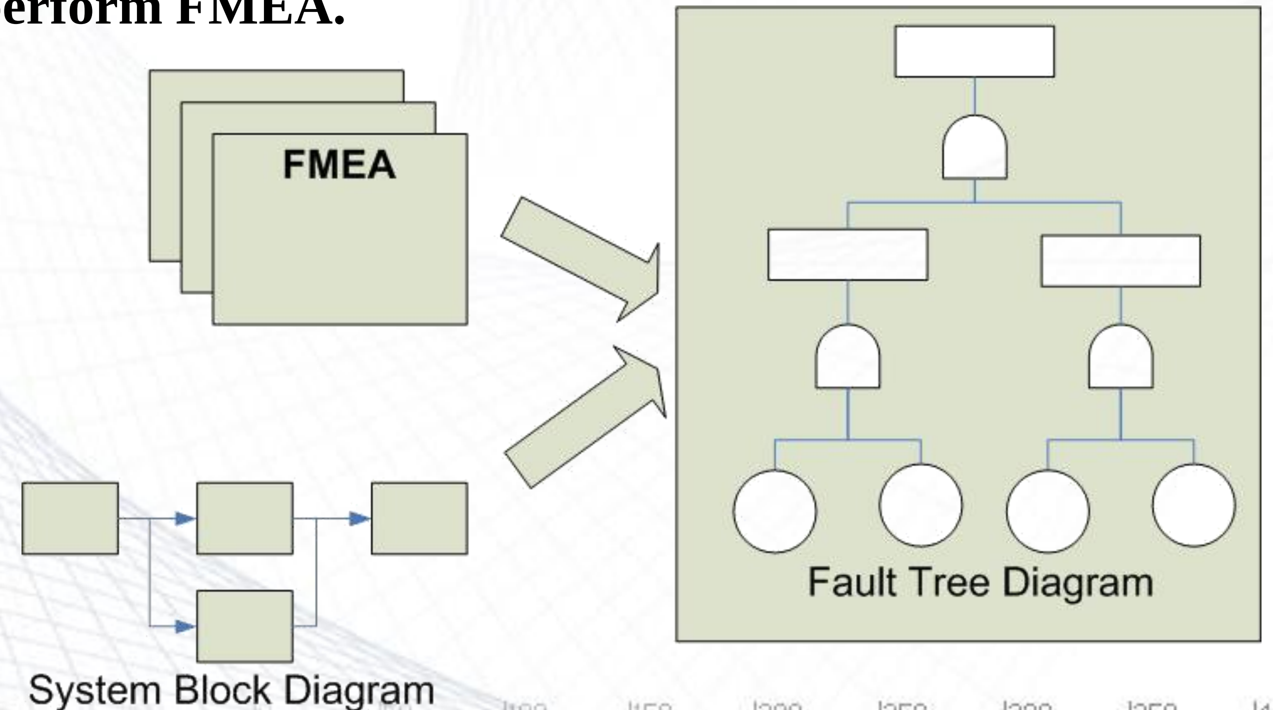
- **Goal**
  - Identify events that may eventually lead to accidents
  - Determine impact on system
- **Techniques**
  - **FMEA:** Failure Modes and Effects Analysis
  - **FMECA:** Failure Modes, Effects and Criticality Analysis
  - **ETA:** Event Tree Analysis
  - **FTA:** Fault Tree Analysis ← **Our focus here**
  - **HAZOP:** HAZard and OPerability studies

Fault Tree Analysis (FTA)

- **Fault tree** analysis is a graphical representation of the major faults or critical failures associated with a product, the causes for the failures, and potential countermeasures. FTA helps identify areas of concern for new system design or for improvement of existing systems. It also helps identify corrective actions to correct or mitigate problems.
- FTA can also be defined as a graphic “model” of the pathways within a system that can lead to a foreseeable, undesirable event. The pathways interconnect contributory events and conditions, using standard logic symbols.
- Fault tree analysis is useful both in designing new systems, products or services or in dealing with identified problems in existing products/services. As part of process improvement, it can be used to help identify root causes of failure and to design remedies and/or countermeasures.

Steps in FTA

- ***FMEA (Failure Modes and Effects Analysis)*** determines the failure modes that are likely to cause failure events. Then it determines what single or multiple point failures could produce those top level events. FMEA asks the question, "What can go wrong?" even if the product meets specification. **In order to perform FTA one first needs to perform FMEA.**



FTA: Example

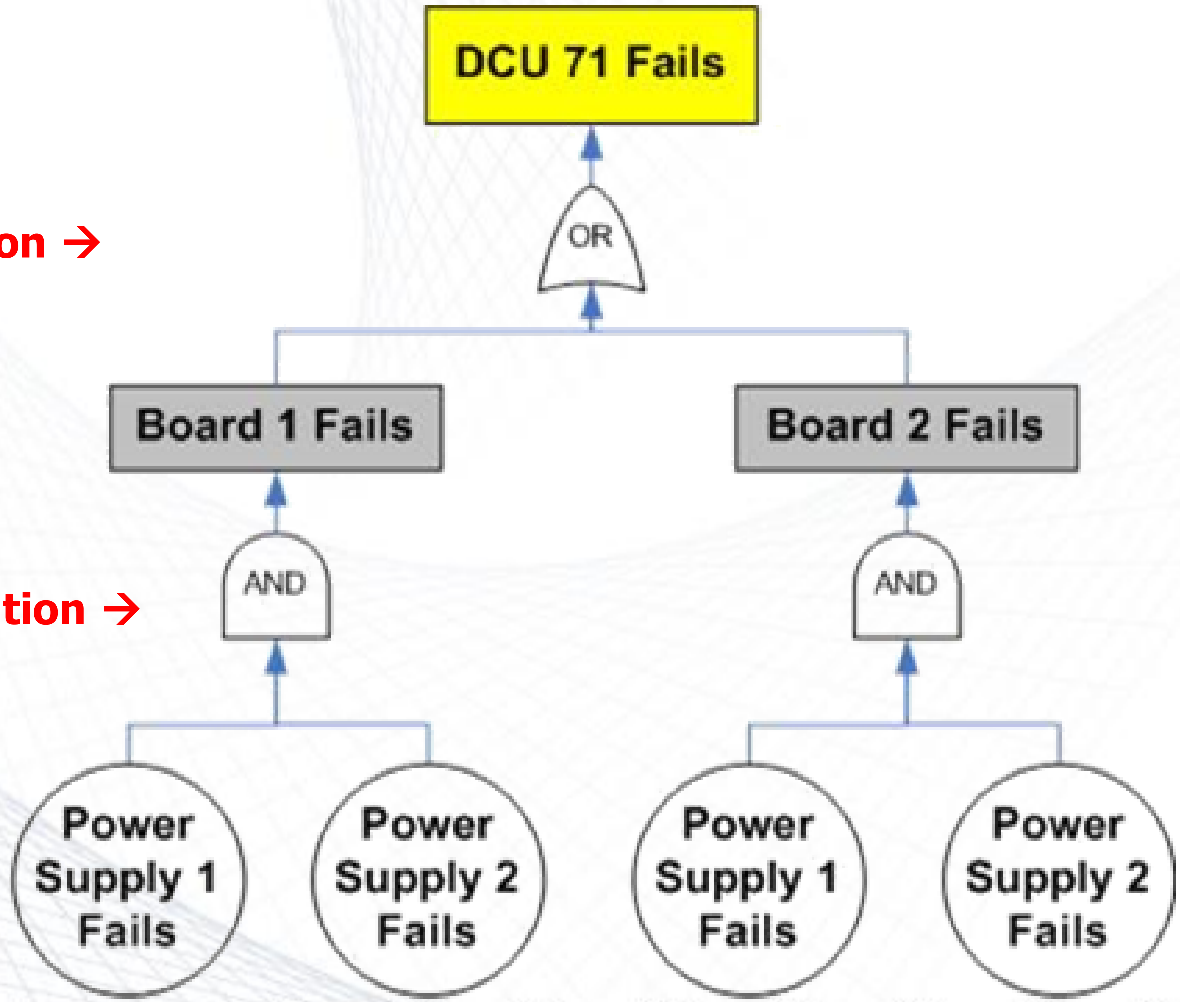
Event →

Serial configuration →

Event →

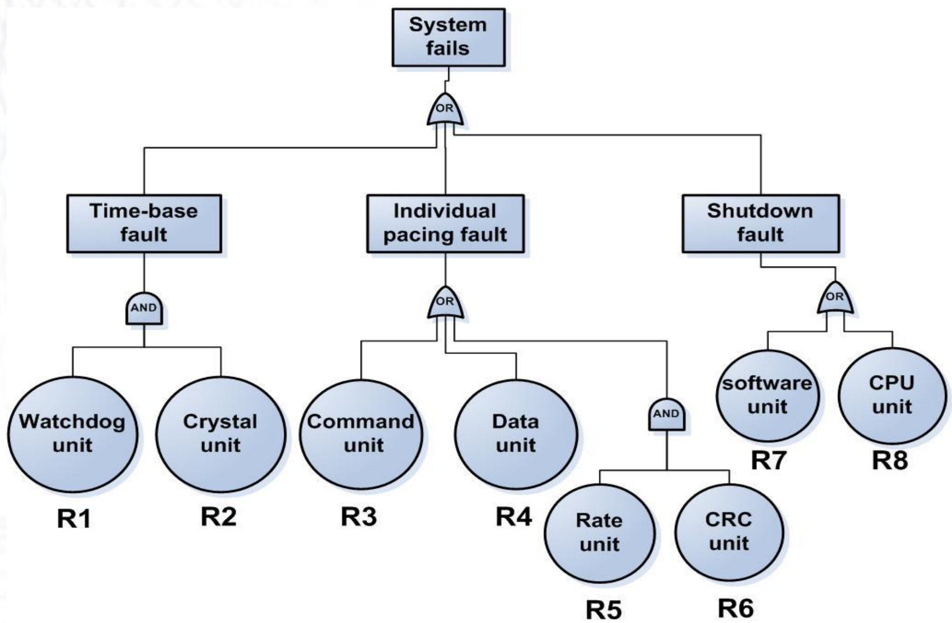
Parallel configuration →

Failure mode →



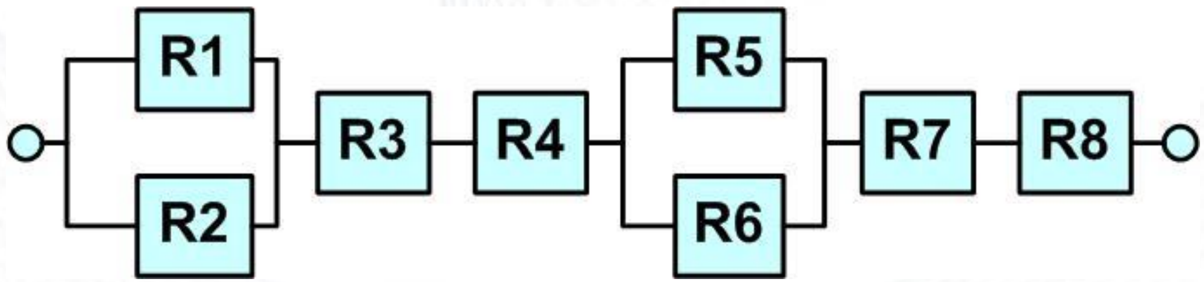
Converting Fault Tree to RBD

- Fault tree for a heart pacemaker system composed of 8 units is shown
- Let's assume that the reliability of all units R1-R8 is 0.95 for 100 hours of operation



Converting Fault Tree to RBD

- Draw the Reliability Block Diagram (RBD) for this system



- Calculate the system overall reliability for 100 hours of operation

R1 and R2 are parallel → R = 1-(1-0.95)^2 = 0.9975
R5 and R6 are parallel → R = 1-(1-0.95)^2 = 0.9975
R_{system} = 0.9975 x 0.95 x 0.95 x 0.9975 x 0.95 x 0.95 = 0.81

FTA: Benefits & Limitations

- **Benefits:**
  - Producing meaningful data for evaluation and improvement of the overall reliability of the system
  - Evaluating effectiveness of and need for redundancy
- **Limitation:**
  - Undesired event evaluated must be foreseen and all significant contributors to the failure must be anticipated
  - This effort may be very time consuming and expensive
  - Overall success of the process depends on the skill of the analyst involved

FTA: Summary

- **Method**: trace faults stepwise back through system design to possible causes
  - a tree with a *top event* at the root
  - *logic gates* at branches, linking each event with its “immediate” causes
  - *initiating faults* at leaves (eventually)
- Good for tracing system hazards to component failures, and allocating safety requirements
- Good for systems with multiple failures
- Good for checking completeness of safety requirements
- Can be difficult, time-consuming, hard to maintain

Conclusions

- We have learnt to calculate system reliability knowing the reliability of its components and their configuration through RBD and FTA analysis
- This is general and can be used for any hardware, software, electrical, mechanical system or combination of them