University of Southampton

SESA6085 – Advanced Aerospace Engineering Management

Lecture 7

2024-2025

Dr David Toal

Reliability Modelling

Review

- Up until this point we have covered the basic tools:
  - Probability theory
  - Continuous & discrete variations
- Applied these techniques to the study of components
- Now let’s consider the modelling of entire systems

New Products

- An accurate prediction of the reliability of a new product is highly desirable
- Depending on the product and its market, advance knowledge of reliability allows accurate forecasts on support costs, spares requirements, warranty costs, marketability, etc.
- **Reality:** *A reliability prediction can rarely be made with high accuracy or confidence.*

Level of Analysis

- In order to estimate the reliability of a system, we need to consider the reliability contributions of individual parts.
- The lower the level of analysis, the greater is the uncertainty of the reliability prediction.
- Reliability is also affected by human-related factors such as training and motivation of design and test engineers, quality of production, and maintenance skills.

Fundamental Limitations

- Predictions in physics and engineering
  - Mathematical models are used
  - For example:
    - Use Ohm’s law to predict the power consumption of a new electronic system
    - Use Newton’s laws to predict the positions of planets
  - These laws are valid within their domain
    - Ohm’s law is not valid near absolute zero
    - Newton’s laws are not valid at the subatomic level

Fundamental Limitations

- Predictions in reliability:
  - Similar to physics and engineering mathematical models are used for reliability predictions
  - For example: Failure rate models for electronic components based on operating temperature exists
  - Similar failure rate models can be derived for non-electronic components and even for computer software
  - However, *failure* is highly dependent upon human actions and perceptions. This represents a fundamental difficulty of the concept of reliability prediction using mathematical models

Failure depends on your success criteria, what is considered a failure can mean a anything from "everything is pefect" to "it fucking exploded"

Practical Approach

- Reasonably credible reliability predictions can be made if…
  1. The system is similar to systems developed, built and used previously
  2. The new system does not involve significant technological risk
- Credible predictions **must** be made if…
  1. The system will be manufactured in large quantities, or is very complex, or will be used for a long time, or a combination of these
  2. There is a strong commitment to the achievement of the reliability predicted

Needs to be competitive with the market level of risk for that product, because else it wont sell

Credible Reliability Predictions

- We can make credible reliability predictions for a new TV receiver or automobile engine…
  1. No great changes from past practice are involved
  2. Technological risks are low
- We must make such predictions because…
  1. They will be built in large quantities, they are quite complex, and they will be used for a long period
  2. They must compete with established and reliable products in the market

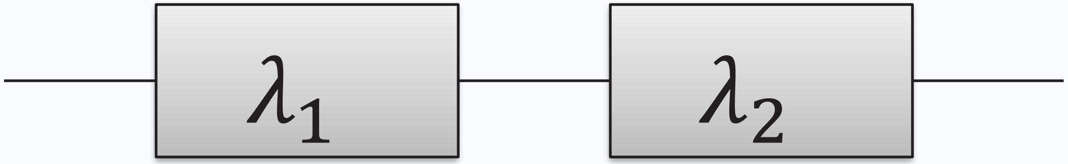
More Complex Systems

- We can make credible reliability predictions for a complete new aircraft or an oil production platform, since they normally use established ‘parts’ with known reliability characteristics
- However, for a new, high technology, weapon system these conditions may not apply

Systems Reliability Models

Basic Series Reliability Model

- For a system composed of two independent components, each having a constant hazard rate.
- If the failure of either component results a system failure, it is called a series model
- The reliability block diagram (RBD) of a series model is



- *Note: A reliability block diagram does not necessarily represent the system's operational logic or functional partitioning!*
- *Note: Hazard rate h(x) is the conditional probability of failure in the interval (x, x+dx), given that there was no failure by x*

A reliability block diagram, shows the path to success. So long as a path exists from the start to the end, it will work. In the event there are no parallel parts, a single failure will block the path and hence the entire system. The order of a RBD doesn't need to reflect the operation structure of the machine.

System's Reliability

- If λ_1 and λ_2 are the hazard rates of the two components, the system hazard rate will be $\lambda_1 + \lambda_2$
- The system reliability will be $R_{SYS} = R_1 R_2 = e^{[-(\lambda_1+\lambda_2)t]}$
- For n components in series

$$R_{SYS} = \prod_{i=1}^{n} R_i$$

- R_i is the reliability of the i^{th} component

Remember a system with constant hazard rate has $R = e^{(-\lambda t)}$

Example

- There are 100 identical components in a system and the failure of any component results in a system failure. What is the individual component reliability in order to reach a 80% reliability of the system?

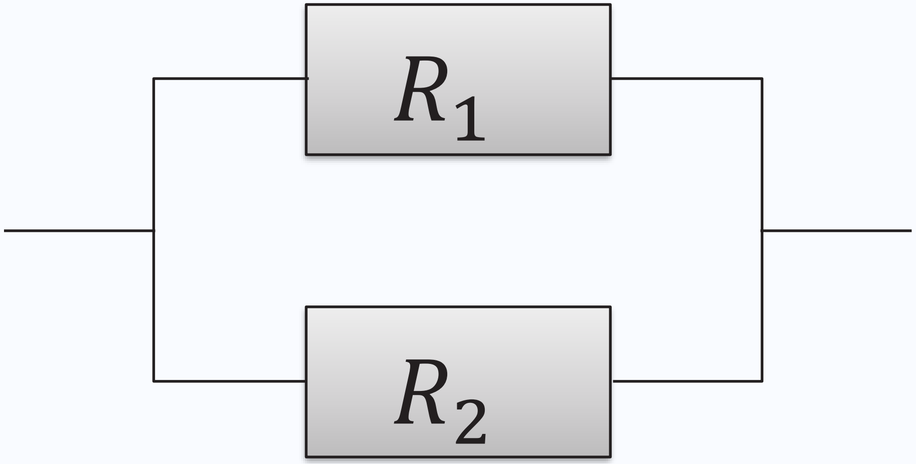
- Solution:

$$R_{SYS} = \prod_{i=1}^{100} R_i = R_1 R_2 \cdots R_{100} = R^{100} = 0.8$$

$$R = \sqrt[100]{0.8} = 0.99777$$

Active Redundancy

- The RBD for the simplest redundant system is as follows



- This system has two s-independent parts with reliabilities R_1 and R_2. The system survives if either or both parts survive.

Active Redundancy

- The system reliability is

$$R_{SYS} = R_1 + R_2 - R_1 R_2 = 1 - \overbrace{(1 - R_1)(1 - R_2)}^{\text{Failure of both items}}$$

- For constant hazard rate

$$R_{SYS} = e^{(-\lambda_1 t)} + e^{(-\lambda_2 t)} - e^{[-(\lambda_1 + \lambda_2)t]}$$

- The general expression is

$$R_{SYS} = 1 - \prod_{i=1}^{n} (1 - R_i)$$

Active Redundancy

- Example: If in a two-unit active redundant system $\lambda_1 = \lambda_2 = 0.1$ failures per 1000h, what is the system reliability at $t = 1000\text{h}$?

$$R_{SYS} = e^{(-\lambda_1 t)} + e^{(-\lambda_2 t)} - e^{[-(\lambda_1 + \lambda_2)t]}$$

$$R_{SYS} = e^{(-0.1)} + e^{(-0.1)} - e^{[-(0.1+0.1)]} = 0.9909$$

- Compare this to a non-redundant system

$$R_{SYS} = R_1 = e^{(-0.1)} = 0.9048$$

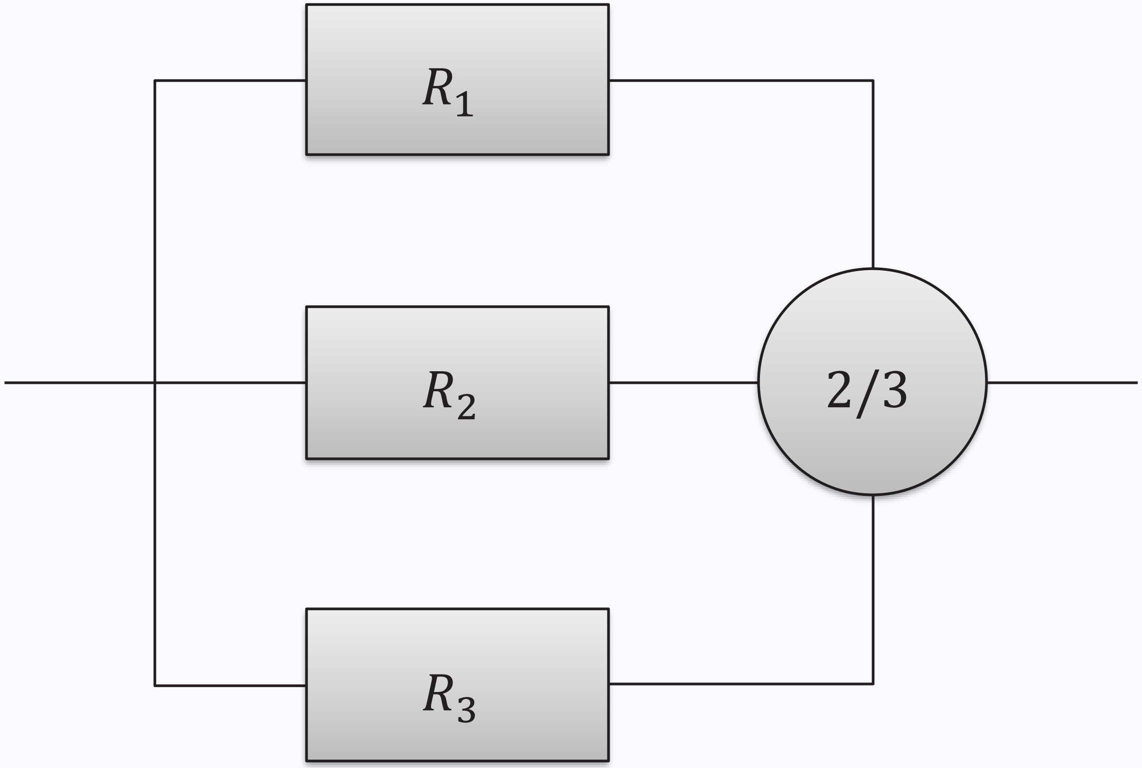
- Quite an impressive improvement!
- This justifies the extra expense of designing redundancy

m-out-of-n Redundancy

- In some active parallel redundant configurations, m out of the n units may be required to be working for the system to function.
- This is called m-out-of-n (or m/n) parallel redundancy
- The reliability of an m-out-of-n system, with n, s-independent components (with **equal** unit reliabilities) the binomial reliability function is used:

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

RBD of an 2-out-of-3 Model



Question

- What is the reliability of the previous 2-out-of-3 configuration for $\lambda_1 = \lambda_2 = \lambda_3 = 0.01$ and $t = 100$?

$$R = e^{(-\lambda t)}$$

- Given
  - $\lambda_1 t = \lambda_2 t = \lambda_3 t = 0.01 \times 100 = 1$
  - $R = e^{-1} = 0.3679$
  - $m = 2$ and $n = 3$

Solution

- Using:

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

- Overall system reliability is:

$$R_{SYS} = 1 - \sum_{i=0}^{2-1} \binom{3}{i} R^i (1-R)^{n-i}$$

$$R_{SYS} = 1 - \binom{3}{0} R^0 (1-R)^{3-0} - \binom{3}{1} R^1 (1-R)^{3-1}$$

$$R_{SYS} = 1 - (1)(1)(1-0.3679)^3 - (3)(0.3679)(1-0.3679)^2$$

$$R_{SYS} = 0.3064$$

Remember: $\dfrac{n!}{x!\,(n-x)!} \equiv \binom{n}{x}$

Question

- What is the reliability of the previous system for a 1-out-of-3 configuration with $\lambda_1 = \lambda_2 = \lambda_3 = 0.01$ and $t = 100$?
- Given
  - $\lambda_1 t = \lambda_2 t = \lambda_3 t = 0.01 \times 100 = 1$
  - $R = e^{-1} = 0.3679$
  - $m = 1$ and $n = 3$
- Will this 1-out-of-3 configuration be more reliable than the 2-out-of-3 configuration?

Solution 1

- Overall system reliability is

$$R_{SYS} = 1 - \sum_{i=0}^{1-1} \binom{3}{i} R^i (1-R)^{n-i}$$

$$R_{SYS} = 1 - \binom{3}{0} R^0 (1-R)^{3-0}$$

$$R_{SYS} = 1 - (1)(1)(1-0.3679)^3$$

$$R_{SYS} = 0.7474$$

Solution 2

- Overall system reliability for a redundant model with n components is

$$R_{SYS} = 1 - \prod_{i=1}^{n}(1 - R_i)$$

$$R_{SYS} = 1 - (1 - R_1)(1 - R_2)(1 - R_3) = 1 - (1 - R)^3$$

$$R_{SYS} = 1 - (1 - 0.3679)^3$$

$$R_{SYS} = 0.7474$$

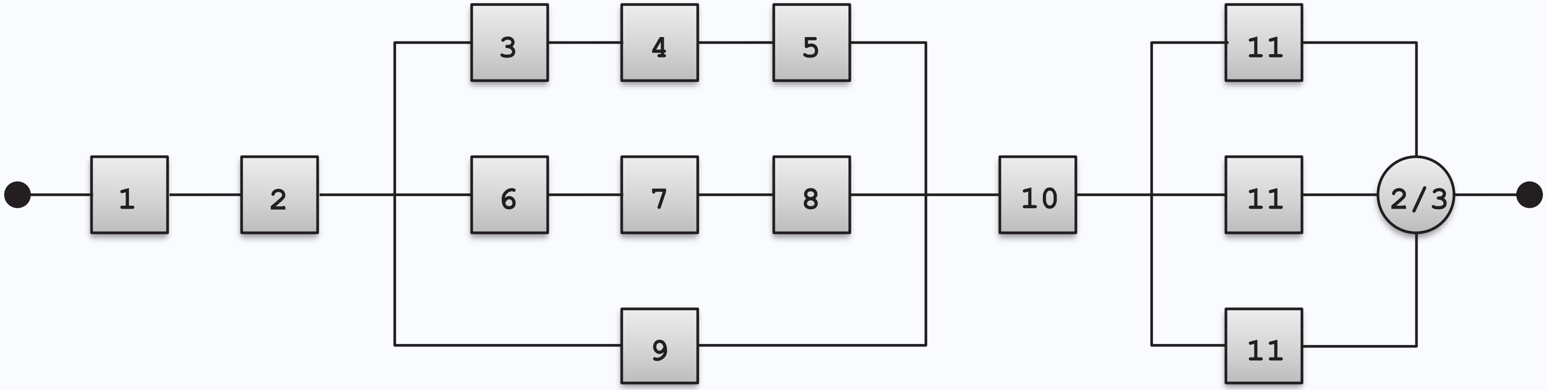
Reliability Block Diagram Decomposition

Reliability Block Diagrams

- So we've seen how to deal with:
  - Series
  - Redundant/Parallel
  - *m* out of *n* redundancy
- These have just been applied to sets of similar components but a system is defined by many different components
- Reliability block diagrams can be quite complex containing all of the above sub-systems in various combinations for different components

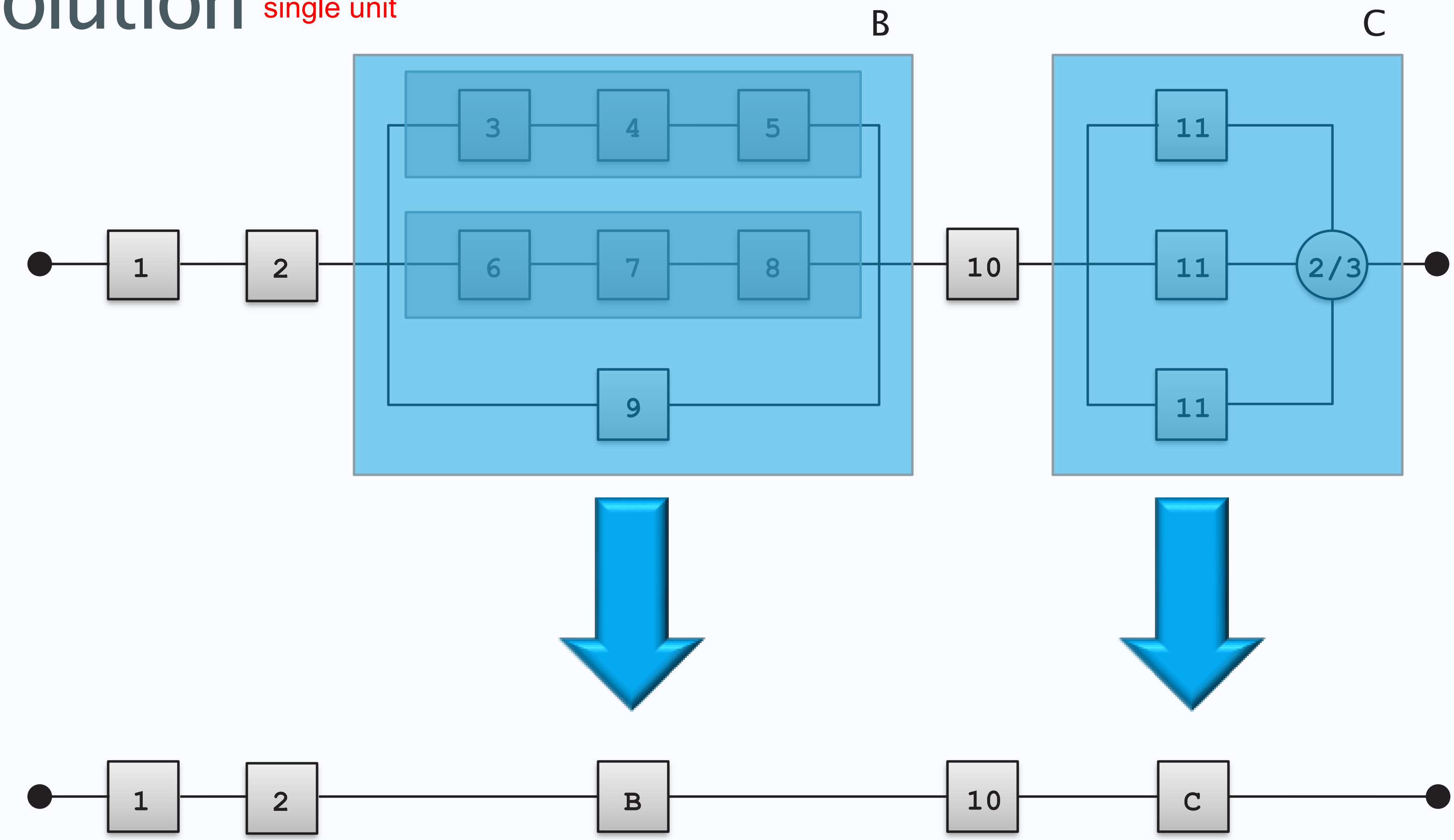
Reducing the Overall RBD

- When possible, complex parts of a RBD can be reduced to a simpler system which can then be analysed using the formulae for series and parallel (redundant) configurations.
- This technique is also called block diagram decomposition.
- Example:



Solution

We can work out the reliability of the series systems to make it a simple parallel system, then calculate that systems reliability and convert the entire thing into a single unit

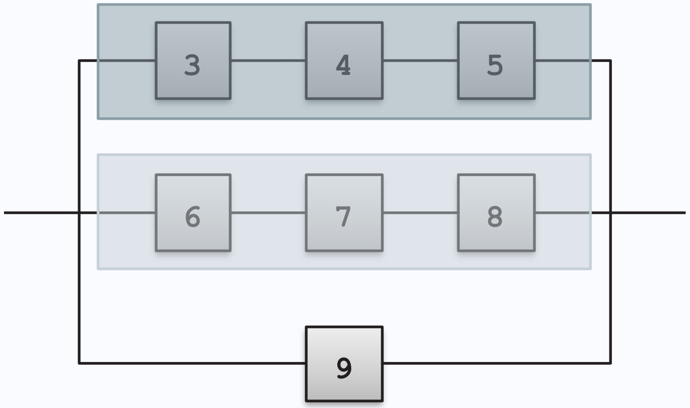


Solution

$$R_{SYS} = R_1 \times R_2 \times R_B \times R_{10} \times R_C$$

$$R_B = 1 - \prod_{i=1}^{3} (1 - R_i)$$

$$R_B = 1 - [1 - (R_3 R_4 R_5)][1 - (R_6 R_7 R_8)]\ [1 - (R_9)]$$

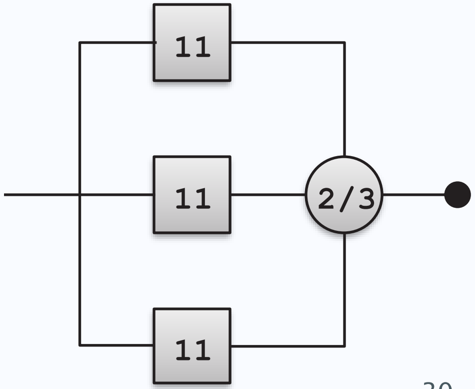


Solution

$$R_C = 1 - \sum_{i=0}^{2-1} \binom{3}{i} (R_{11})^i \ (1 - R_{11})^{3-i}$$

$$R_C = 1 - \binom{3}{0} (R_{11})^0 \ (1 - R_{11})^3 - \binom{3}{1} (R_{11})^1 \ (1 - R_{11})^2$$

$$R_C = 1 - (1 - R_{11})^3 - 3R_{11}(1 - R_{11})^2$$



Common Mode Failures

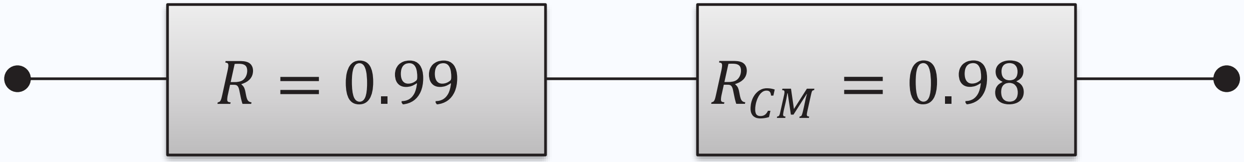
Common Mode Failures

- A common mode failure is one which can lead to the failure of all paths in a redundant configuration
- In the design of redundant systems it is vital to identify and eliminate sources of common mode failures!
- Practical examples:
  - A technician fails to replace seals on aircraft engine oil sampling plugs, causing all of the engines to fail
  - The Chernobyl nuclear reactor accident was caused by the operators conducting an unauthorised test. Ironically, the purpose of the test was to see how the reactor would function in the event of a power shutdown

Example

- Consider a system in which each path has a reliability $R = 0.99$ and a common mode failure with a probability of non-occurrence $R_{CM} = 0.98$
- The system can be designed as
  a) a single unit
  b) a dual redundant configuration
- Compare the overall system reliability for both cases

Scenario a)

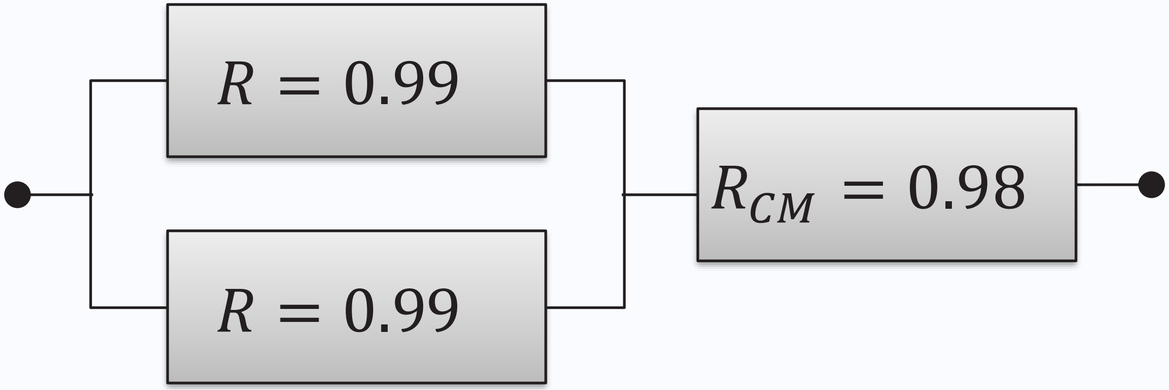


$R = 0.99$

$R_{CM} = 0.98$

$$R_{SYS} = R \times R_{CM} = (0.99) \times (0.98) = 0.9702$$

Scenario b)



$$R_{SYS} = [1 - (1 - R)^2] \times R_{CM} = [1 - (1 - 0.99)^2] \times (0.98)$$

$$R_{SYS} = 0.9799$$

But scenario a gave $R_{SYS} = 0.9702$

- *The common mode failure practically eliminates the advantage of the redundant configuration*

University of
Southampton