# **Chapter 5** : Basic Concept of Reliability

Fault Tolerance and Failure Diagnosis

**Dr. Yeffry Handoko**
**Universitas Komputer Indonesia**

# Definition

- *Fault* is malfunction or deviation from expected behavior

- *Tolerance* as the capacity for enduring

- Putting the words together, **fault tolerance** refers to a system's ability to deal with malfunctions.

# Categories of Faults

- *Transient faults :* These occur once and then disappear
- *Intermittent faults :* Intermittent faults are characterized by a fault occurring, then vanishing again, then reoccurring, then vanishing
- *Permanent faults :* This type of failure is persistent: it continues to exist until the faulty component is repaired or replaced

# Achieving Fault Tolerance

The general approach to building fault tolerant systems is redundancy:

- **Information redundancy** seeks to provide fault tolerance through replicating or coding the data
- **Time redundancy** achieves fault tolerance by performing an operation several times.
- **Physical redundancy** deals with devices, not data. We add extra equipment to enable the system to tolerate the loss of some failed components

# *Redundancy* and *Replication*.

- With **replication**, we have several units operating concurrently and a voting (quorum) system to select the outcome.
- With **redundancy**, only one unit is functioning while the redundant units are standing by to fill in in case the unit ceases to work.

# The Definition of Reliability

A fundamental problem in estimating reliability is whether a system will function in a prescribed manner in a given environment for a given period of time. This depends on a number of factors:

- design of the system
- the parts and components used
- and the environment

*Reliability is the probability that the given system will perform its required function under specified conditions for a specified period of time*.

# Increasing Reliability

- employing the method of worst case design, using high-quality components and imposing strict quality control procedures during the assembly phase
- An alternative approach to reliable system design is to incorporate “redundancy” (i.e. additional resources) into a system with the aim of masking the effects of faults

# Reliability and the Failure Rate

- Let N = identical components under “stress conditions”
- Let *S(t)* be the number of surviving components
- *Let F(t) be* the number of components that have failed

Then Reliability(R(t)) = S(t)/N

# Continuation:

The probability of failure of the components, also known as the unreliability *Q(t),* is:

$Q(t) = F(t)/N$

- Since $S(t) + F(t) = N$, we must have:
- $R(t) + Q(t) = 1$

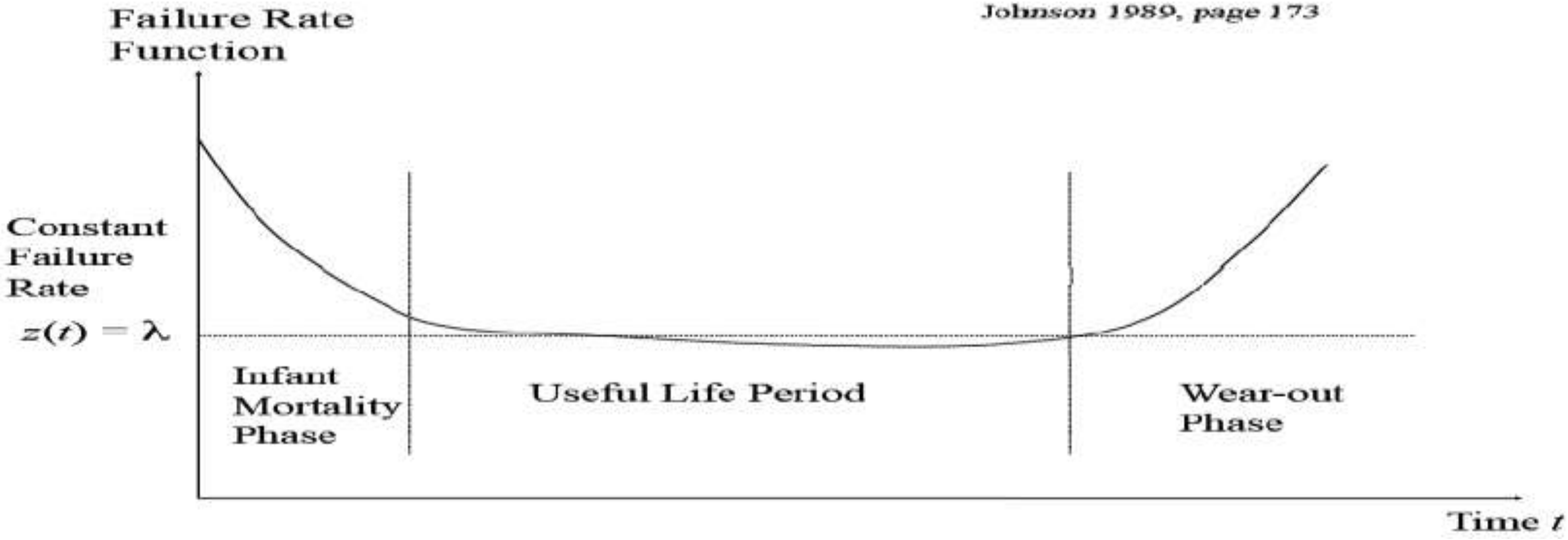
# Continuation:

- The failure rate, also known as the “hazard rate”, *Z(t)* is defined to be the number of failures per unit time compared with the number of surviving components:

$$Z(t) = 1/S(t) * dF(t)/dt$$

# Continuation:

- Study of electronic components show that under normal conditions the failure rate varies as indicated in the figure below (the bathtub curve):



# Continuation:

- In the “useful life” period the failure rate is constant, and therefore:

$$Z(t) = \lambda$$

$$R(t) = \frac{S(t)}{N} = \frac{N - F(t)}{N} = 1 - \frac{F(t)}{N}$$

$$\frac{\mathrm{d}R(t)}{\mathrm{d}t} = -\frac{1}{N} \cdot \frac{\mathrm{d}F(t)}{\mathrm{d}t}$$

$$\frac{\mathrm{d}F(t)}{\mathrm{d}t} = -N \frac{\mathrm{d}R(t)}{\mathrm{d}t}$$

# Continuation:

$$\lambda = -\frac{N}{S(t)} \cdot \frac{\mathrm{d}R(t)}{\mathrm{d}t}$$

$$= -\frac{1}{R(t)} \cdot \frac{\mathrm{d}R(t)}{\mathrm{d}t}$$

$$\lambda \cdot \mathrm{d}t = -\frac{\mathrm{d}R(t)}{R(t)}$$

- The above expression may be integrated giving:

$$\lambda \int_0^t \mathrm{d}t = -\int_1^{R(t)} \frac{dR(t)}{R(t)}$$

# Continuation:

- Integrating, we get:

$$-\lambda t = \ln R(t)$$

$$R(t) = \exp(-\lambda t)$$

- The above relationship is generally known as the *exponential failure law.*
- When the product $\lambda t$ is small:

$$R(t) = 1 - \lambda t$$

# Relation between Reliability and Mean-Time-Between-Failures

- Reliability *R(t)* gives different values for different operating times
- More useful to the user is the average time a system will run between failures; this time is known as the *mean-time-between-failures* (MTBF)
- The MTBF of a system is usually expressed in hours and is given by $\int_0^\infty \mathrm{R(t)dt}$

- For the exponential failure law:

$$\mathrm{MTBF} = \int_0^\infty \exp(-\lambda t)\,dt$$

MTBF = 1/ƛ

- the MTBF of a system is the reciprocal of the failure rate
- If ƛ is the number of failures per hour, the MTBF is expressed in hours

# Example:

- We have 4000 components with a failure rate of 0.02% per 1000 hours. Find the average number of failures per hour and the MTBF.

- Average number is failures is given by the:

  failure rate × total number components

  $= \frac{0.02}{100} * \frac{1}{1000} * 4000 = 8 * 10^{-4} \frac{failure}{hr}$

- MTBF = $\frac{1}{failure\,rate} = 1/8 * 10^{-4}$ = 1250 hrs

- R(t) = $e^{(-t/MTBF)}$
- Again from the exponential failure law, if ƛt <<, then $R(t) = 1 \; -$ ƛt

$$\text{R(t)} = 1 \; - \frac{t}{MTBF}$$

$$\text{MTBF} = \; \frac{t}{1-R(T)}$$

# Example:

- A first-generation computer contains 10,000 thermionic valves each with = 0.5% / (1000 hours). What is the period of 99% reliability?

$$\text{MTBF} = \frac{t}{1 - R(t)}$$

$$= \frac{t}{1 - 0.99}$$

$$t = \text{MTBF} \times 0.01$$

$$= \frac{0.01}{\lambda_{OV}}$$

$$N = \text{No. of valves} = 10{,}000$$

$$\lambda = \text{failure rate of valves} = 0.5\%/(1000\ hours)$$

$$= 0.005/(1000\ hours)$$

$$= 5 \times 10^{-6}/hour$$

$$\lambda_{OV} = N\lambda = 10^{4} \times 5 \times 10^{-6} = 5 \times 10^{-2}/hour$$

3)

$$t = \frac{0.01}{5 \times 10^{-2}} = \frac{10^{-2}}{5 \times 10^{-2}} = 0.2\ hour = 12\ minutes$$

# Maintainability

- When a system fails, repair action is normally carried out to restore the system to operational effectiveness
- *The probability that a failed system will be restored to working order within a specified time is called the **maintainability** of the system*
- There is therefore a relationship between maintainability and repair rate μ and hence with mean-time-to-repair (MTTR)

- MTTR and μ are always related:

$$\mu = \frac{1}{MTTR}$$

- MTTR and μ are related to maintainability *M(t)* as follows:

$$M(t) = 1 - \exp(-\mu t) = 1 - \exp\left(-\frac{t}{\mathrm{MTTR}}\right)$$

Where *t* is the permissible time constraint for the maintenance action.

- In order to design and manufacture a maintainable system, it is necessary to predict the MTTR for various fault condition that could occur in the system.
- The system repair time consists of two separate intervals – passive repair time and active repair time. The passive repair time is mainly determined by the time taken by service engineers to travel to the customer site. In many cases the cost of travel time exceeds the cost of the actual repair.

The active repair time is directly affected by the system design and may be subdivided as follows:

- The time between the occurrence of a failure and the system user becoming aware that it has occurred.
- The time needed to detect a fault and isolate the replaceable component(s) responsible.
- The time needed to replace the faulty component(s).
- The time needed to verify that the fault has been removed and the system is fully operational

# Availability

- The availability of a system is the probability that the system will be “up”, i.e. functioning according to expectations at any time during its scheduled working period.

$$\text{Availability} = \frac{\text{System uptime}}{\text{System uptime} + \text{System downtime}}$$

$$= \frac{\text{System uptime}}{\text{System uptime} + (\text{No. of failures } \times \text{MTTR})}$$

$$= \frac{\text{System uptime}}{\text{System uptime} + (\text{System up} - \text{time } \times \lambda \times \text{MTTR})}$$

$$= \frac{1}{1 + (\lambda \times \text{MTTR})}$$

$$= \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \text{since} \quad \lambda = \frac{1}{\text{MTBF}}$$

# Series and Parallel Systems

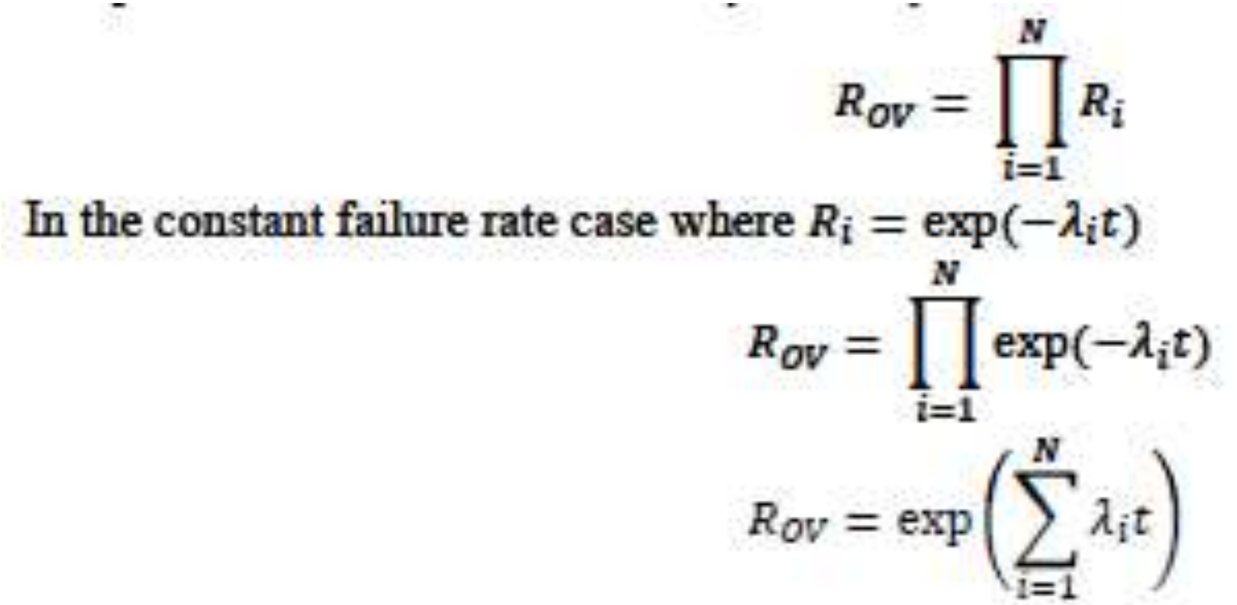
- The reliability of a system can be derived in terms of the reliabilities or the failure rates of the subsystems used to build it
- Two limiting cases of systems design are frequently met in practice:

1. Systems in which each subsystem must function if the system as a whole is to function.

2. Systems in which the correct operation of just one subsystem is sufficient for the system to function satisfactorily. In other words the system consists of redundant subsystems and will fail only if all subsystems fail.

# Case 1: Series System

- Let us consider a system in which a failure of any subsystem would cause a system failure. This can be modeled as a series system. If the subsystem failures are independent and is the reliability of subsystem, then the overall system reliability is:



$$R_{OV} = \prod_{i=1}^{N} R_i$$

In the constant failure rate case where $R_i = \exp(-\lambda_i t)$

$$R_{OV} = \prod_{i=1}^{N} \exp(-\lambda_i t)$$

$$R_{OV} = \exp\left(\sum_{i=1}^{N} \lambda_i t\right)$$

- If the *N* subsystems have identical failure rates $\lambda i = \lambda$ , then $Ri = R$. Hence the overall system reliability is:

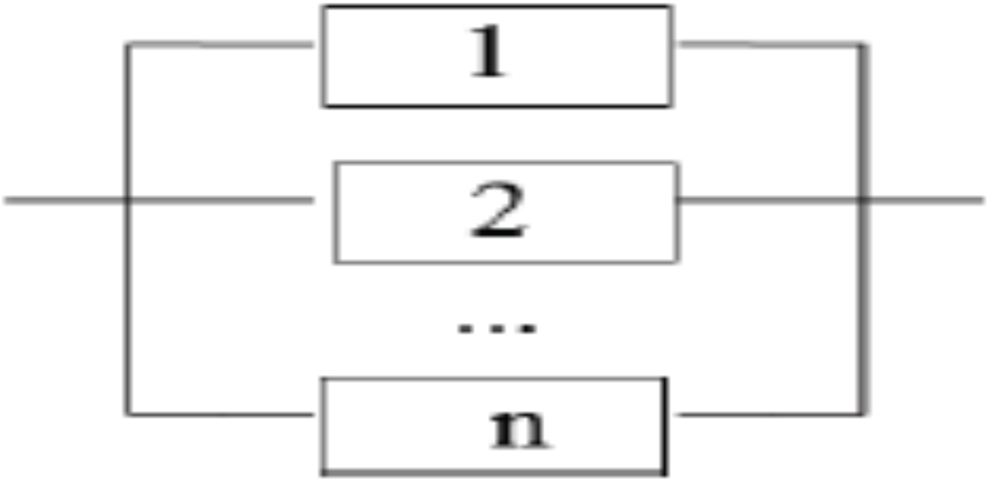
$$\begin{aligned} R_{OV} &= \exp(-N\lambda t) \\ &= R^N \end{aligned}$$

$$\mathrm{MTBF} = \frac{1}{N\lambda}$$

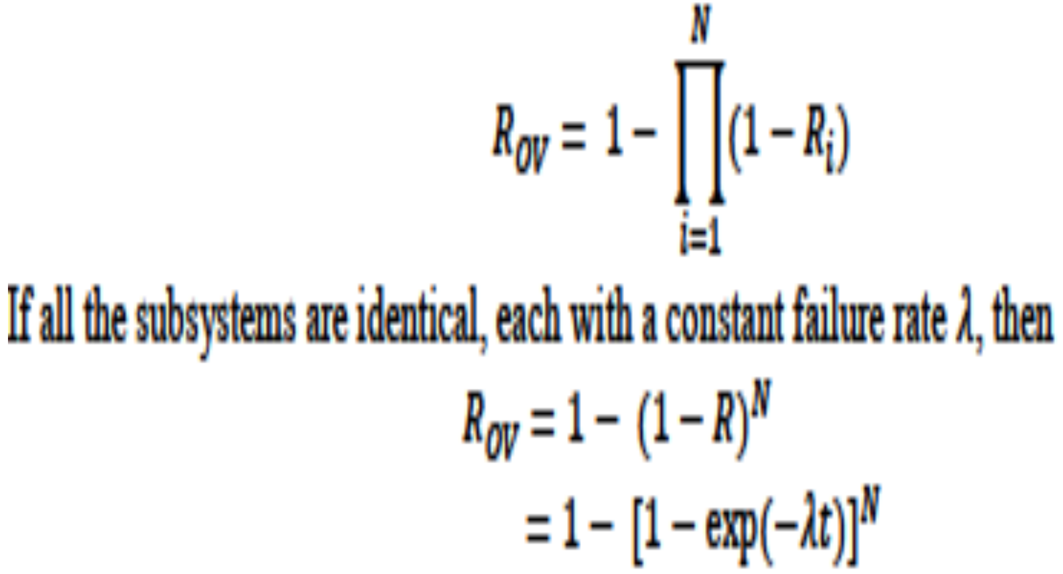
- Note that the overall reliability is decreased *N*-fold while the MTBF is 1/*N* of that of the subsystem

# **Case 2:** Parallel System

- In this case system failure can occur only when all subsystems have failed. This can be modeled as a parallel system, as shown in the Fig.



- If the failures are independent and is the reliability of subsystem R*i*, then the overall reliability of the system is:



$$R_{OV} = 1 - \prod_{i=1}^{N}(1 - R_i)$$

If all the subsystems are identical, each with a constant failure rate $\lambda$, then

$$\begin{aligned} R_{OV} &= 1 - (1 - R)^N \\ &= 1 - [1 - \exp(-\lambda t)]^N \end{aligned}$$

- For example if a parallel system consists of two subsystems. then:

$$\begin{aligned} R_{OV} &= 1 - \; [1 - \exp(-\lambda t)]^2 \\ &= 2\exp(-\lambda t) - \exp(-2\lambda t) \end{aligned}$$

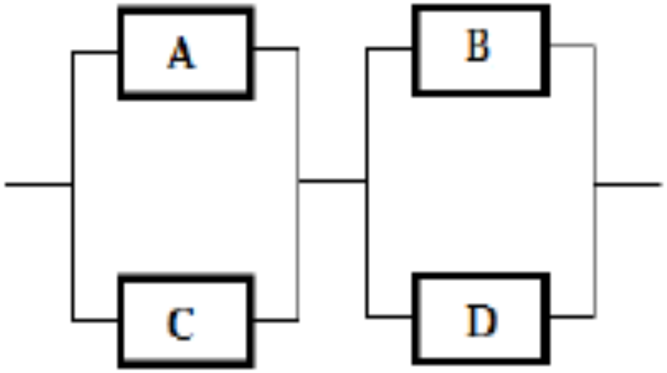
- Therefore the MTBF of the system is:

$$\begin{aligned} &= \int_0^{\infty} [2\exp(-\lambda t) - \exp(-2\lambda t)]\mathrm{d}t \\ &= 3/2\lambda \end{aligned}$$

- In practice a system normally consists of a combination of series and parallel subsystems. These systems are useful when short-circuits or open-circuits are the most commonly expected faults

# Parallel-to-Series Network

- the parallel-to-series network is used when the primary failure mode is an open-circuit



- If subsystems A and C are processors and subsystems B and D are memories, the system in the Fig. can operate if (A, D) or (C, B) or (A, B) or (C, D) works

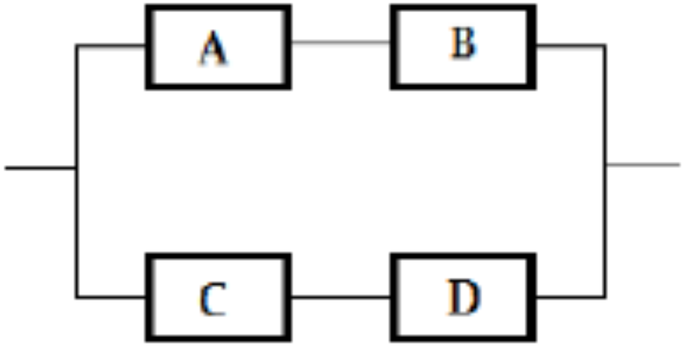
- In this situation the reliability of the parallel-to-series system is:

$$R_{PS} = [1-(1-R_A)(1-R_C)][1-(1-R_B)(1-R_D)]$$

- where $R_A$, $R_B$ , $R_C$ and $R_D$ are the reliabilities of subsystems A, B, C and D respectively

# Series-to-Parallel System

- series-to-parallel network of is used when the primary mode to is a short circuit



- the system of the Fig. can operate only if either (A, B) or (C, D) works

- The reliability of the series-to-parallel system is given by:

$$R_{SP} = [1 - (1 - R_A R_B)(1 - R_C R_D)]$$

- where $R_A$, $R_B$ , $R_C$ and $R_D$ are the reliabilities of subsystems A, B, C and D respectively

Assuming

$$R_A = R_B = R_C = R_D = R$$

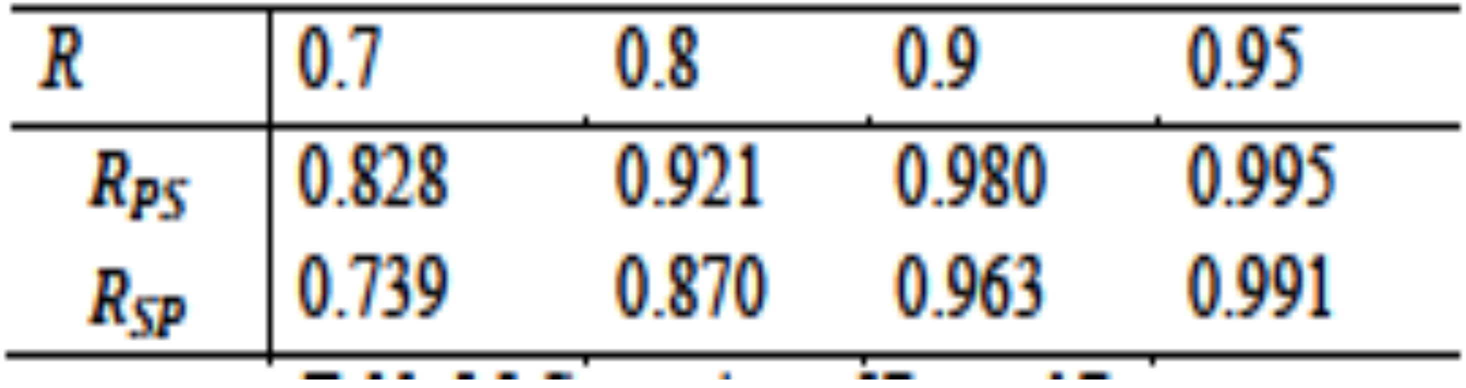
Then

$$R_{PS} = R^4 - 4R^3 + 4R^2$$

and

$$R_{SP} = 2R^2 - R^4$$

- Some indication of the effectiveness of the series-to-parallel and parallel-to-series schemes is shown by assigning a range of values to R, as in the Table below. The figures in the show clearly that $R_{PS} > R_{SP}$.



| $R$ | 0.7 | 0.8 | 0.9 | 0.95 |
|---|---|---|---|---|
| $R_{PS}$ | 0.828 | 0.921 | 0.980 | 0.995 |
| $R_{SP}$ | 0.739 | 0.870 | 0.963 | 0.991 |

# M out of N Systems

- An M-of-N system is one which consists of N identical components, with failure occurring if fewer than M components are still functional
- Best-known example - The Triplex (TMR) is three identical components whose outputs are voted on. This is a 2-of-3 system: as long as a majority of the processors produce correct results, the system will be functional

# *Reliability of M out of N Systems*

- For N identical components, R(t) is the reliability of an individual components. The reliability of the system is the probability that N-M or fewer components have failed

$$R_x(t) = \sum_{i=0}^{N-M} C(N,i)\big(1 - R(t)\big)^i R(t)^{N-i}$$

$C(N,i) = \frac{N!}{[i!(N-i)!]}$and$R_x(t)$ is the reliability of M-out-of-N.

- Consider a TMR - Triple Modular Redundant Cluster which is perhaps the most important M-of-N system where M=2, N=3 - system is good if at least two components are operational
- A voter picks the majority output but a Voter can fail. Let the Voter reliability be Rvot(t).

$$R_{tmr}(t) = R_{vot}(t) \sum_{i=0}^{1} C(3,1)\big(1 - R(t)\big)^{i} R(t)^{3-1}$$

$$R_{tmr}(t) = R_{vot}(t)\big(3R^{2}(t) - 2R^{3}(t)\big)$$

*TMR – Constant Failure Rates*

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

Assume no Voter failures i.e. $R_{vot}(t) = 1$

$$R_{tmr}(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

and

$$MTTF_{tmr} = \int_{0}^{\infty} R_{tmr}(t)dt = \tfrac{5}{6\lambda} < \tfrac{1}{\lambda} = MTTF_{simplex}$$