Outline

UNIVERSITÀ DI PISA

- Reliability and Availability modelling
- Exponential failure law for the hardware
- Combinatorial models
  - Series/Parallel
  - Fault Trees
- State based models: Markovian models
  - Discrete time Markov chain
  - Continuus time Markov chain

Quantitative evaluation of Dependability

Faults are the cause of errors and failures. Does the arrival time of faults fit a **probability distribution**?
If so, what are the parameters of that distribution?

Consider the time to failure of a system or component.
It is not exactly predictable - **random variable**.

probability theory

Evaluation of Failure rate, Mean Time To Failure (MTTF), Mean Time To Repair (MTTR), Reliability (R(t)), Availability (A(t)) function

Definition of dependability attributes

Reliability - R(t)

conditional probability that the system performs correctly throughout the interval of time [t0, t], given that the system was performing correctly at the instant of time t0

Availability - A(t)

the probability that the system is operating correctly and is available to perform its functions at the instant of time t

Definitions

Reliability R(t)

$$R(0) = 1 \quad R(\infty) = 0$$

Unreliability Q(t)

$$Q(t) = 1 - R(t)$$

Failure probability density function f(t)

the failure density function f(t) at time t is the number of failures in Δt

$$f(t) = \frac{dQ(t)}{dt} = \frac{-\,dR(t)}{dt}$$

Failure rate function λ(t)

the failure rate λ(t) at time t is defined by the number of failures during Δt in relation to the number of correct components at time t

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{-\,dR(t)}{dt} \frac{1}{R(t)}$$

Hardware Reliability

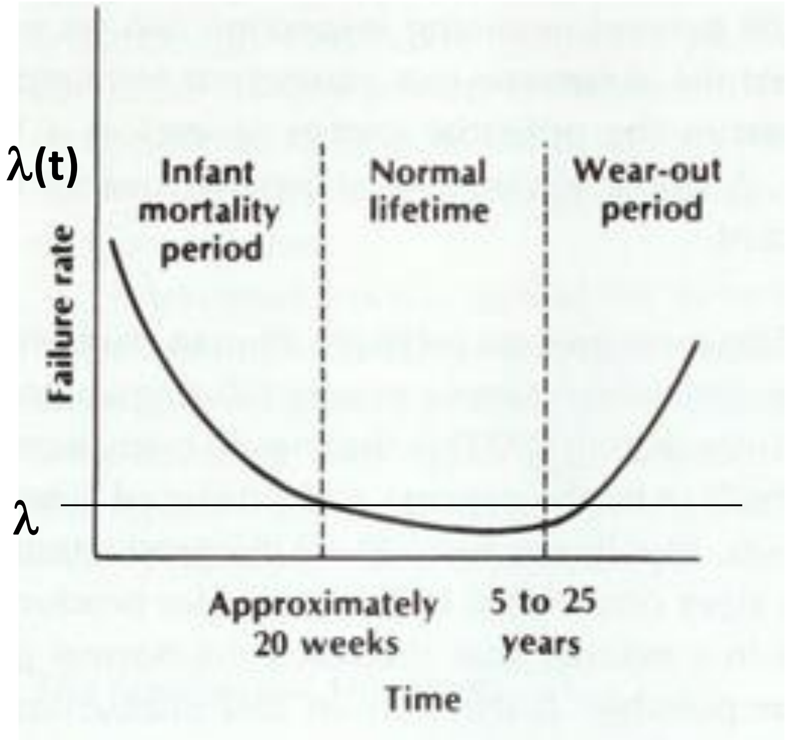
$\lambda(t)$ is a function of time
(bathtub-shaped curve)

$\lambda(t)$ constant > 0
in the operational phase

Constant failure rate λ

(usually expressed in number of failures for million hours)

λ = 1/200 one failure every 2000 hours



Taken from: [Siewiorek et al.1998]

Early life phase: there is a higher failure rate due to the failures of weaker components (result from defetct or stress introduced in the manufacturing process). Wear-out phase: time and use cause the failure rate to increase.

Hardware Reliability

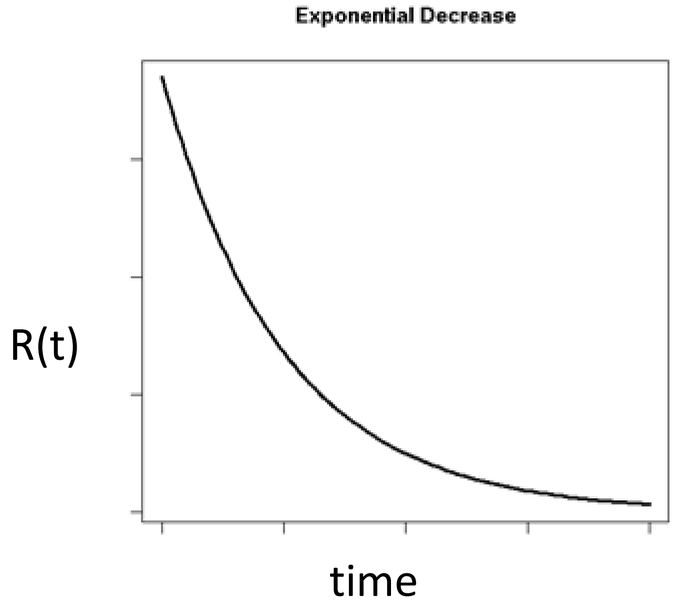
Constant failure rate

$\lambda(t) = \lambda$

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{-\,dR(t)}{dt}\,\frac{1}{R(t)}$$

Reliability function

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



Probability density function

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

the exponential relation between reliability and time is known as **exponential failure law**

Time to failure of a component

- Time to failure of a component can be modeled by a **random variable** X

$F_X(t) = P[X<=t]$ (cumulative distribution function)

$F_X(t)$ unreliability of the component at time t

- Reliability of the component at time t

$R(t) = P[X > t] = 1 – P[X <= t] = 1 – F_X(t)$

R(t) is the probability of not observing any failure before time t

Time to failure of a component

Mean time to failure (MTTF)

is the expected time that a system will operate before the first failure occurs (e.g., 2000 hours)

$$\text{MTTF} = \int_0^{\infty} t f(t) dt = \int_0^{\infty} t \lambda e^{-\lambda t} dt = \frac{1}{\lambda}$$

$\lambda = 1/2000$ 0.0005 per hour

MTTF = 2000 time to the first failure 2000 hours

Failure in time (FIT)

measure of failure rate in 109 device hours

1 FIT means 1 failure in 109 device hours

Failure Rate

- Handbooks of failure rate data for various components are available from government and commercial sources.
- Reliability Data Sheet of product

Commercially available databases

- Military Handbook MIL-HDBK-217F
- Telcordia,
- PRISM User's Manual,
- International Eletrotechnical Commission (IEC) Standard 61508
    - …

Distribution model for permanent faults

MIL-HBDK-217 (Reliability Prediction of Electronic Equipment -Department of Defence)

Statistics on electronic components failures studied since 1965 (periodically updated).
Chip failure rates in the range 0.01-1.0 per million hours

$$\lambda = \tau_L \tau_Q (C_1 \tau_T \tau_V + C_2 \tau_E)$$

τ_L = learning factor, based on the maturity of the fabrication process
τ_Q = quality factor, based on incoming screening of components
τ_T = temperature factor, based on the ambient operating temperature
and the type of semiconductor process
τ_E = environmental factor, based on the operating environment
τ_V = voltage stress derating factor for CMOS devices

C_1, C_2 = complexity factors (based on number of gates, or bits for memories and number of pins)

Model-based evaluation of dependability

a model is an abstraction of the system that highlights the important features for the objective of the study

Methodologies that employ combinatorial models:
Reliability Block Diagrams,
Fault tree, ….

State space representation methodologies:
Markov chains, Petri-nets,
SANs, …

Combinatorial models

Combinatorial models

offer simple and intuitive methods of the construction and solutions of models

Assumptions:

- independent components
- each component is associated a failure rate

- model construction is based on the structure of the systems (series/parallel connections of components)

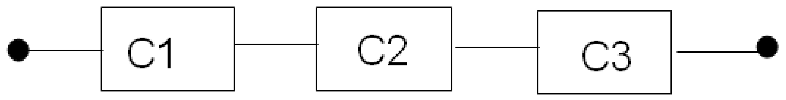
- inadequate to deal with systems that exhibits complex dependencies among components and repairable systems

Combinatorial models

Series: all components must be operational (a)

$R_i(t)$ reliability of module i at time t

$R_{series}(t) = \Pi_{i=1}^{n} R_i(t)$
where Π is the product



(a)

If each individual component i satisfies the exponential failure law with constant failure rate λ_i:

$$R_{series}(t) = e^{-\lambda_1 t} ... e^{-\lambda_n t} = e^{-\sum_{i=1}^{n} \lambda_i t}$$

Unreliability function

$$Q_{series}(t) = 1 - R_{series}(t) = 1 - \Pi_{i=1}^{n} R_i(t) = 1 - \Pi_{i=1}^{n}[1 - Q_i(t)]$$

Combinatorial models

If the system does not contain any redundancy, that is any component must function properly for the system to work, and if component failures are independent, then

- the system reliability is the product of the component reliability, and it is exponential

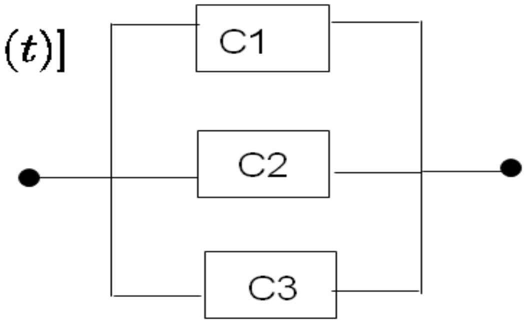
- the failure rate of the system is the sum of the failure rates of the individual components

Combinatorial models

Parallel: at least one of the components must be operational (b)

$$Q_{parallel}(t) = \Pi_{i=1}^{n} Q_i(t)$$
$$R_{parallel}(t) = 1 - Q_{parallel}(t) = 1 - \Pi_{i=1}^{n} Q_i(t) = 1 - \Pi_{i=1}^{n}[1 - R_i(t)]$$

Note the duality between Q and R in the two cases



(b)

M-of-N systems - a generalisation of parallel model
at least M modules of N are required to function

Assume N identical modules and M of those are required for the system to function properly, the expression for reliability of M-of-N substems can be written as:

$$R_{M-of-N}(t) = \Sigma_{i=0}^{N-M} \frac{N!}{(N-i)!i!} R^{N-i}(t)(1 - R(t))^i$$

i number of faulty components

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

Binomial coefficient

Combinatorial models

If the system contain redundancy, that is a subset of components must function properly for the system to work, and if component failures are independent, then

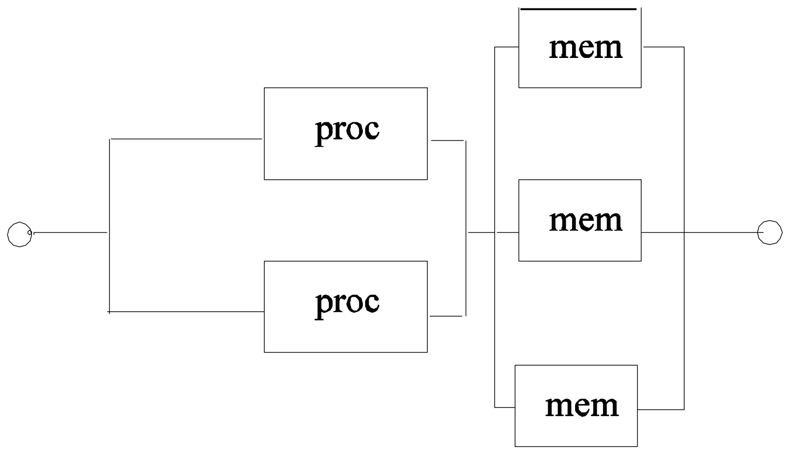
- the system reliability is the reliability of a series/parallel combinatorial model

Combinatorial models

Series/Parallel models

An example:

Multiprocessor with 2 processors and three shared memories



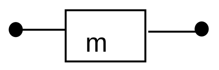
TMR versus Simplex system

Simplex system

λ failure rate of module m

$\mathbf{R_m = e^{-\lambda t}}$

$\mathbf{R_{simplex} = e^{-\lambda t}}$



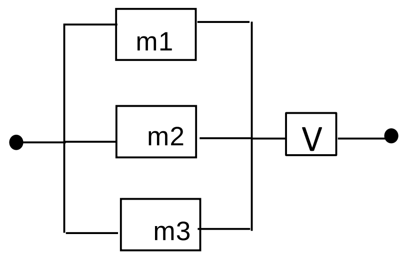
TMR system

$\mathbf{R_V(t) = 1}$

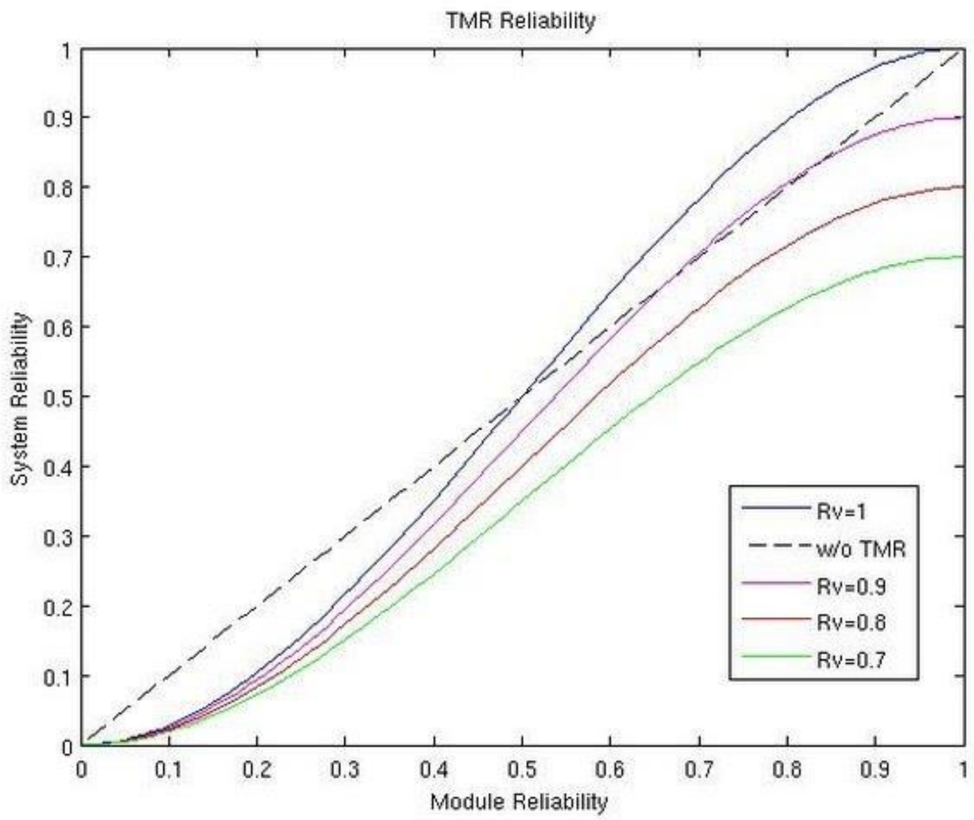
$$\mathbf{R_{TMR} = \sum_{i=0}^{1} \binom{3}{i} (e^{-\lambda t})^{3-i} (1- e^{-\lambda t})^{i}}$$

$$\mathbf{= (e^{-\lambda t})^3 + 3(e^{-\lambda t})^2 (1- e^{-\lambda t})}$$

$\mathbf{R_{TMR} > R_m \text{ if } R_m > 0.5}$



2 of 3



Taken from: [Siewiorek et al.1998]

TMR: reliability function and mission time

$R_{simplex} = e^{-\lambda t}$

$MTTF_{simplex} = \frac{1}{\lambda}$

TMR system

$R_{TMR} = 3e^{-2\lambda t} - 2e^{-3\lambda t}$

$MTTF_{TMR} = \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6\lambda} < \frac{1}{\lambda}$

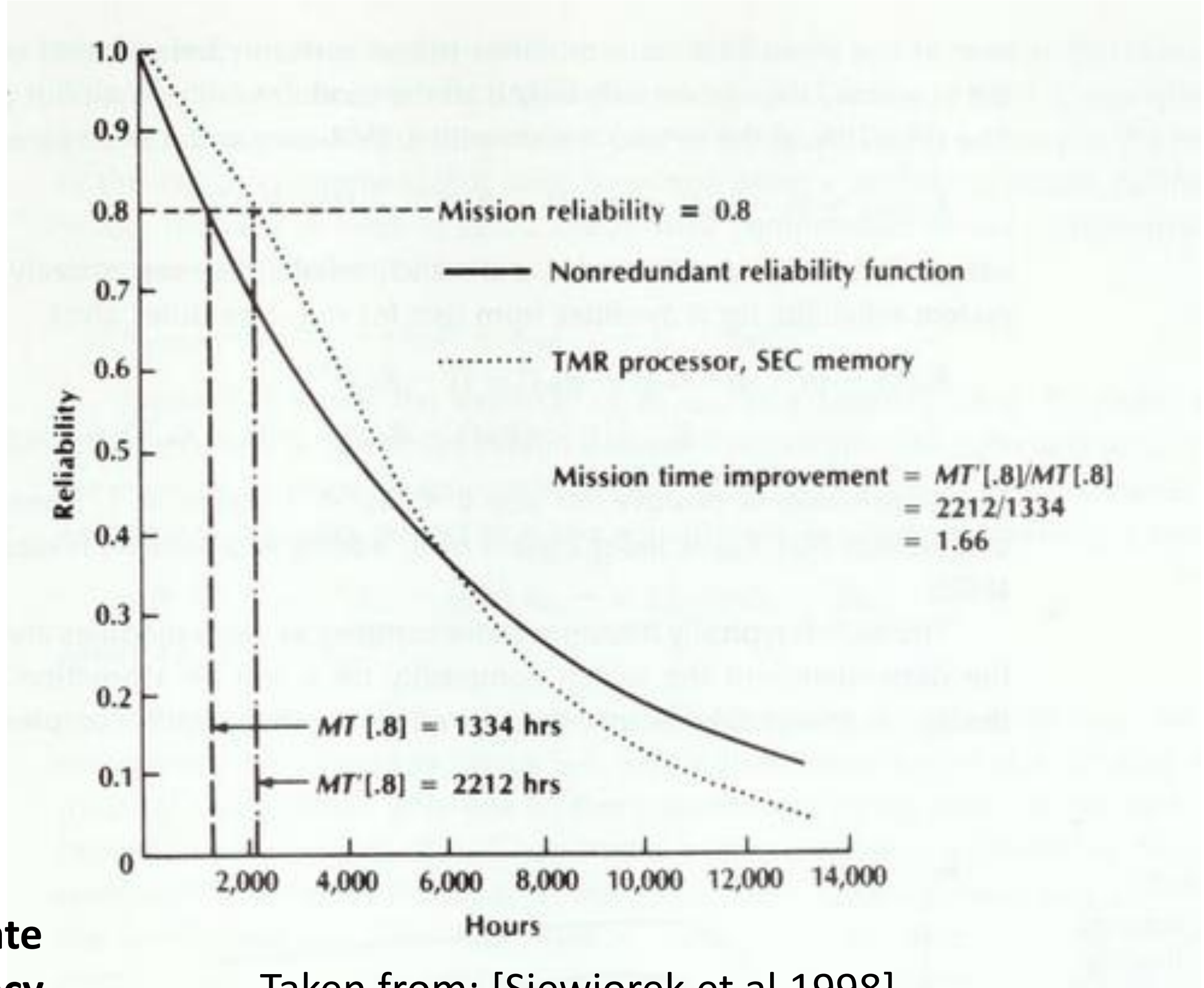
TMR worse than a simplex system

but

TMR has a higher reliability for the first 6.000 hours

TMR operates at or above 0.8 reliability 66 percent longer than the simplex system

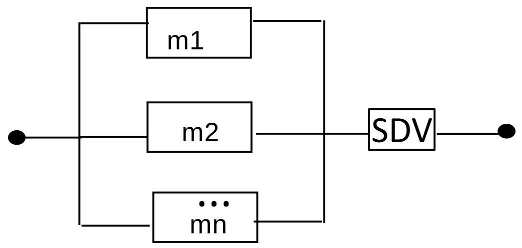
S shape curve is typical of redundant systems: above the knee the redundant system has components that tolerate failures; after the knee the system has exhausted redundancy

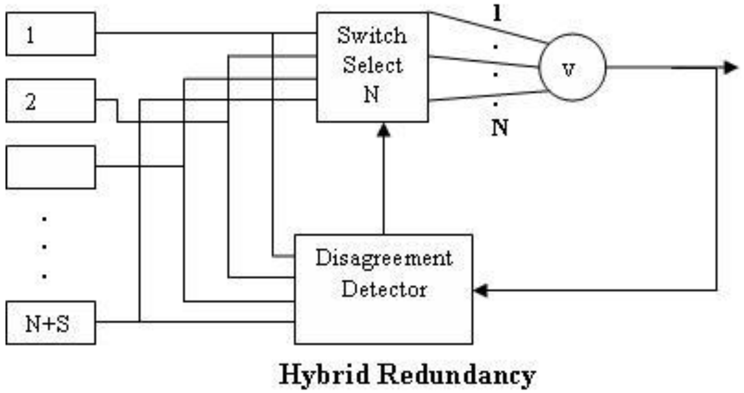


Taken from: [Siewiorek et al.1998]

Hybrid redundancy with TMR

Symplex system
λ failure rate m
$R_m = e^{-\lambda t}$
$R_{sys} = e^{-\lambda t}$





Taken from: [Siewiorek et al.1998]

Hybrid system
n=N+S total number of components
S number of spares

Let N = 3 **$R_{SDV}(t) = 1$**
λ failure rate of on line comp
λ failure rate of spare comp

The first system failure occurs if 1) all the modules fail; 2) all but one modules fail

$$R_{Hybrid} = R_{SDV}(1- Q_{Hybrid})$$

$$R_{Hybrid} = (1 – ((1-R_m)^n + n(R_m)(1-R_m)^{n-1}))$$

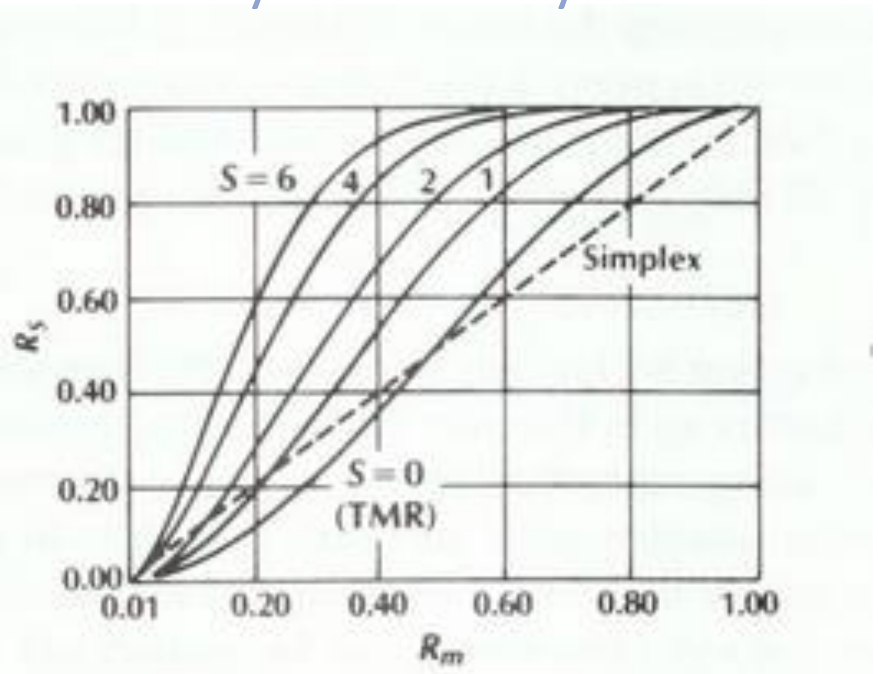
$$R_{Hybrid(n+1)} – R_{Hybrid(n)} > 0$$

adding modules increases the system reliability under the assumption **R_{SDV}** independent of n

Hybrid redundancy with TMR

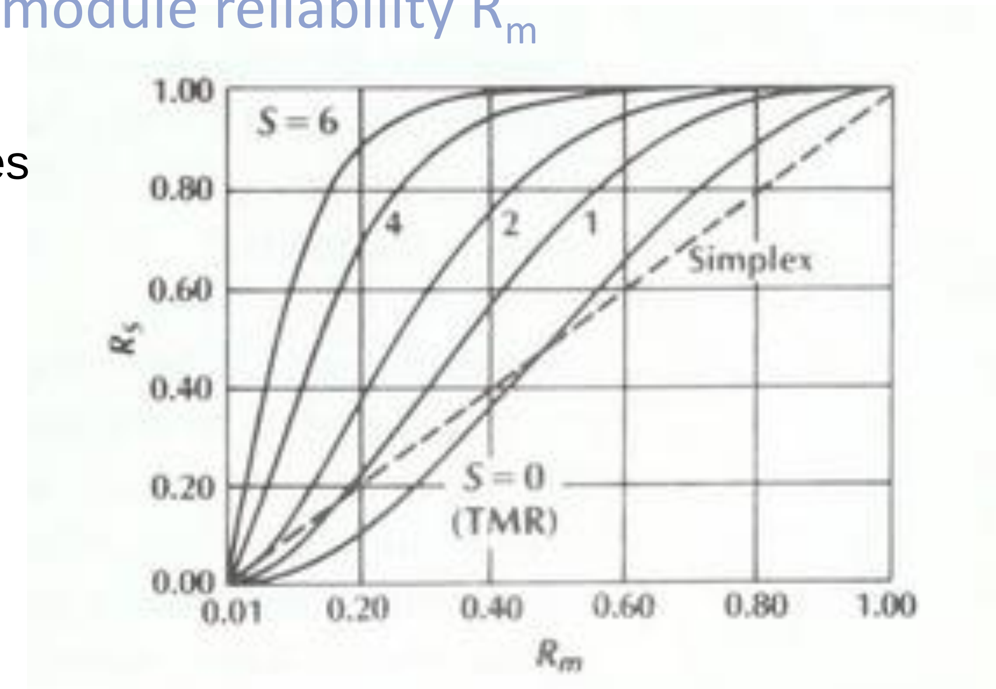
Hybrid TMR system reliability R_S vs individual module reliability R_m

S is the number of spares
R_{SDV} =1



System with standby failure rate equal to on-line failure rate

TMR with one spare is more reliable than simplex system if R_m>0.23



System with standby failure rate equal to 10% of on line failure rate

TMR with one spare is more reliable than simplex system if R_m>0.17

Taken from: [Siewiorek et al.1998]

Fault Trees

Consider the combination of events that may lead to an undesirable situation of the system

Describe the scenarios of occurrence of events at abstract level

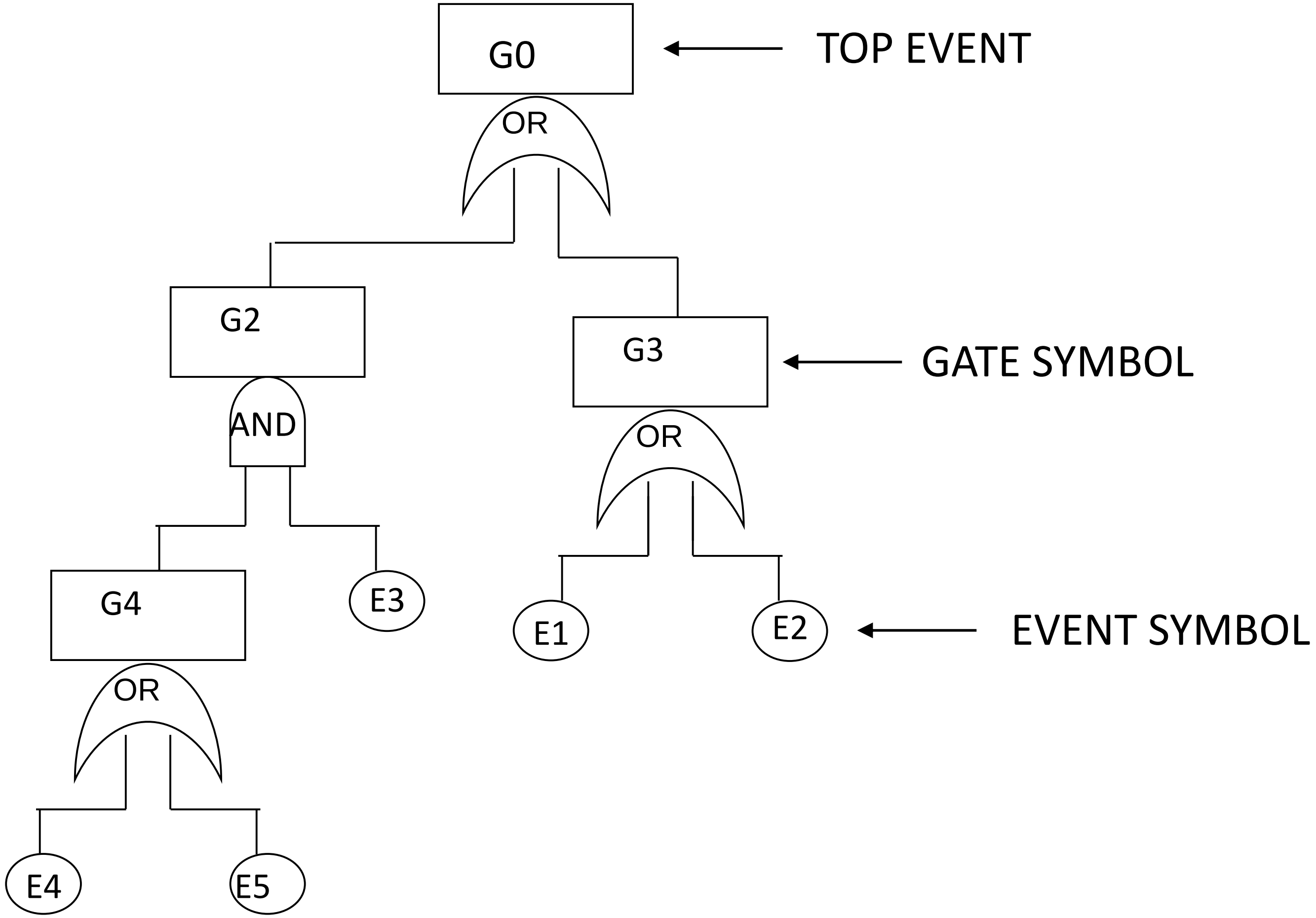
Hierarchy of levels of events linked by logical operators

The analysis of the fault tree evaluates the probability of occurrence of the root event, in terms of the status of the leaves (faulty/non faulty)

Applicable both at design phase and operational phase

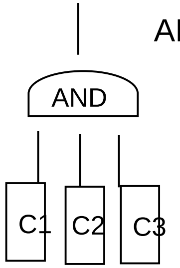
Fault Trees

Describes the Top Event
(status of the system)
in terms of the status
(faulty/non faulty) of the Basic
events (system's components)



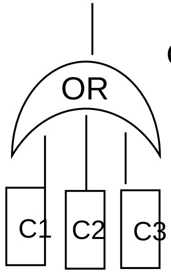
Fault Trees

AND gate



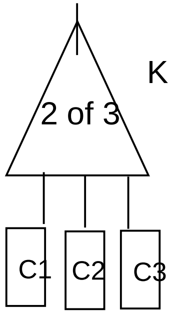
True if all the components are true (faulty)

OR gate



True if at least one of the components is true (faulty)

K of N gate



True if at least k of the components are true (two or three components) (faulty)

Components are leaves in the tree

Component faulty corresponds to logical value **true**, otherwise **false**

Nodes in the tree are boolen AND, OR and k of N gates

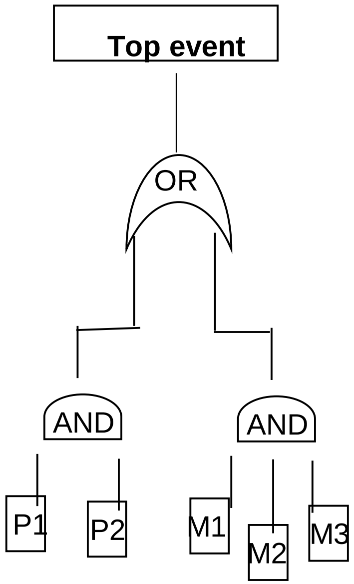
The system fails if the root is true

Fault Trees

Example

Multiprocessor with 2 processors and three shared memories

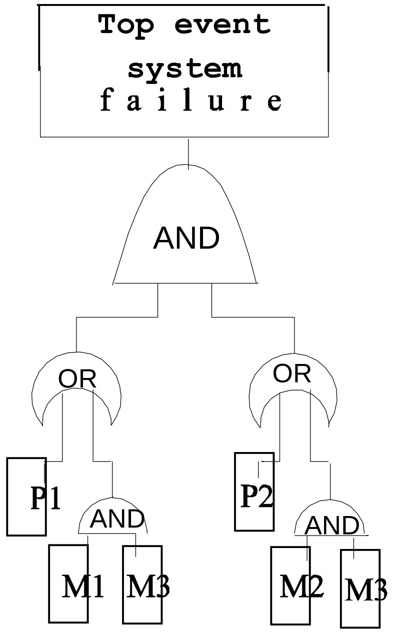
-> the computer fails if all the memories fail or all the processors fail



Conditional Fault Trees

Example

Multiprocessor with 2 processors and three memories:
M1 private memory of P1, M2 private memory of P2, M3 shared memory.



- Assume every process has its own private memory plus a shared memory
- Operational condition: at least one processor is active and can access to its private or shared memory

repeat instruction: given a component C whether or not the component is input to more than one gate, the component is unique

Conditional Fault Trees

If the same component appears more than once in a fault tree, the independent failure assumption. We use conditioned fault tree is violated

If a component C appears multiple times in the FT

$$Q_s(t) = Q_{S|C\ Fails}(t)\ Q_C(t) + Q_{S|C\ not\ Fails}(t)\ (1-Q_C(t))$$

where

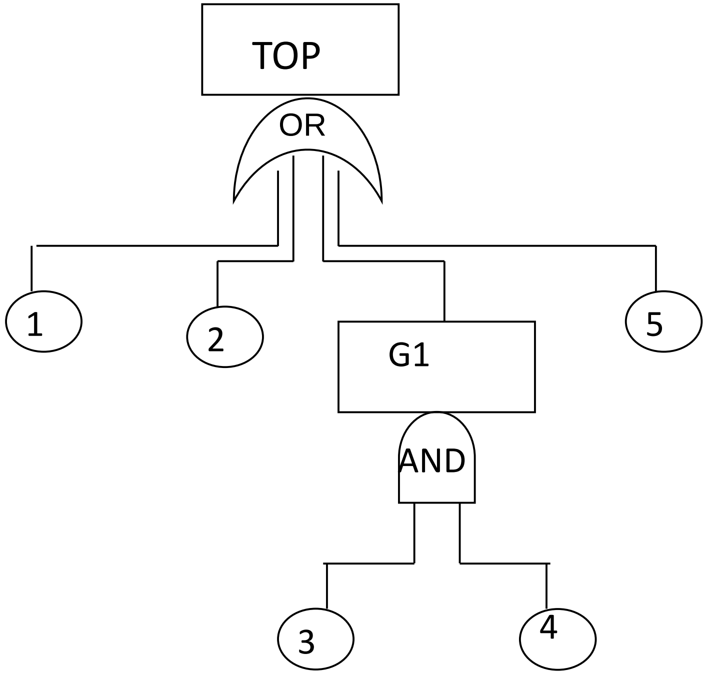
S|C Fails is the system given that C fails

and

S|C not Fails is the system given that C has not failed

Minimal cut sets

1. A cut is defined as a set of elementary events that, according to the logic expressed by the FT, leads to the occurrence of the root event.



2. To estimate the probability of the root event, compute the probability of occurrence for each of the cuts and combine these probabilities

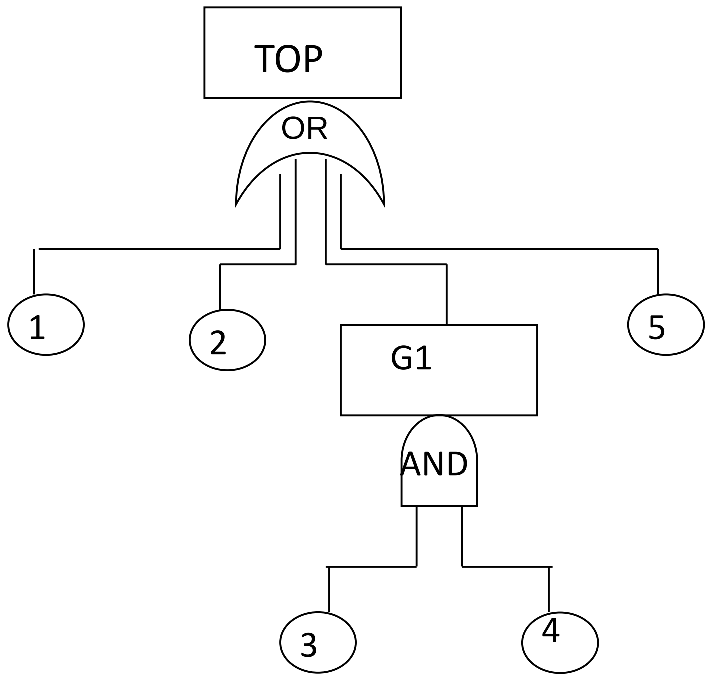
Cut Sets

Top = {1}, {2} , {G1} , {5} = {1}, {2} , {3, 4} , {5}

Minimal Cut Sets

Top = {1}, {2} , {3, 4} , {5}

Minimal cut sets



Minimal Cut Sets

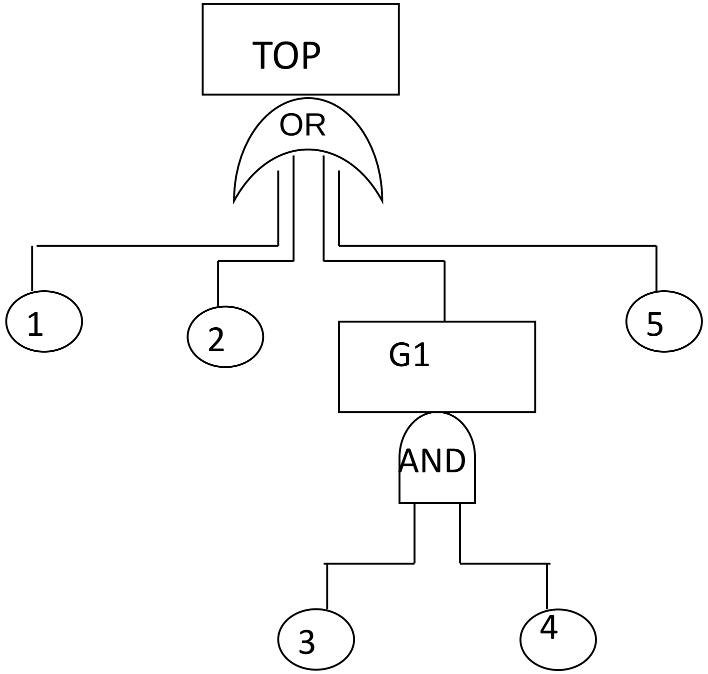
Top = {1}, {2} , {3, 4} , {5}

$Q_{Si}(t)$ = probability that all components in the minimal cut set Si are faulty

$Q_{Si}(t) = q_1(t)\, q_2(t) \ldots q_{ni}(t)$ with Si ={1, 2, …, ni }

The numerical solution of the FT is performed by computing the probability of occurrence for each of the cuts, and by combining those probabilities to estimate the probability of the root event

Assumption: independent faults of the components



Minimal Cut Sets

Top = {1}, {2} , {3, 4} , {5}

$S_1 = \{1\}$ $S_2 = \{2\}$ $S_3 = \{3, 4\}$ $S_4 = \{5\}$

$$Q_{Top}(t) = Q_{S1}(t) + \ldots + Q_{Sn}(t)$$

n number of mininal cut sets

Fault Trees

Identification of critical path of the system

- Definition of the Top event
- Minimal cut set (minimal set of events that leads to the top event)

Analysis:

- Failure probability of Basic events
- Failure probability of minimal cut sets
- Failure probability of Top event
- Single point of failure of the system: minimal cuts with a single event