Measures of dependability and security

D.M. Nicol, W. Sanders, K.S. Trivedi
Model-Based evaluation: From Dependability to Security
IEEE Transactions on Dependable and Secure Computing, Vol. 1, N. 1, 2004

D. P. Siewiorek R.S. Swarz,
Reliable Computer Systems Prentice Hall, 1998

Outline

Reliability and Availability modelling

- Exponential failure law for the hardware
- Combinatorial models
  - Series/Parallel
  - Fault Trees
- State-based models
  - Discrete time Markov chain
  - Continuous time Markov chain

Security modelling

- Security policy, Vulnerability, Adversary profile
- Combinatorial models
  - Attack trees
- State-based models
  - Attack-state graphs
  - ADVISE

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

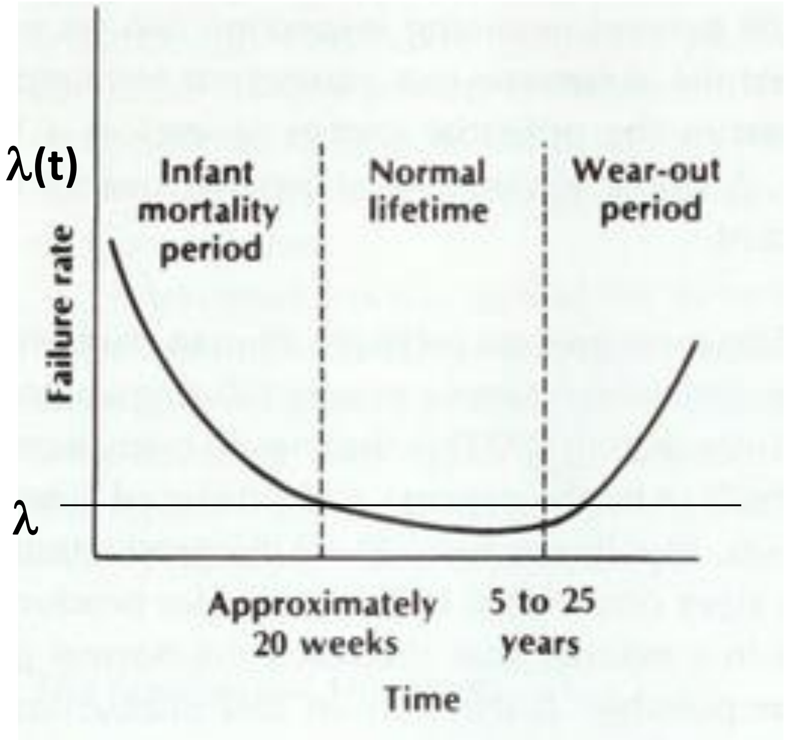
$\lambda(t)$ is a function of time
(bathtub-shaped curve)

$\lambda(t)$ 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

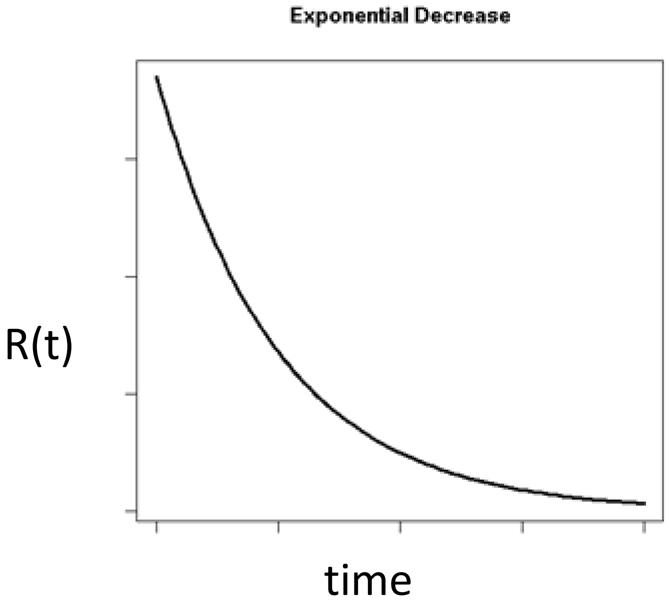
$$\lambda(t) = \lambda \qquad \lambda(t) = \frac{f(t)}{R(t)} = \frac{-\,dR(t)}{dt}\,\frac{1}{R(t)}$$

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)

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

λ = 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)

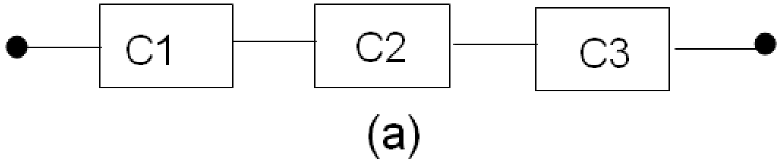
- inadequate to deal with systems that exhibits complex dependencies among components and repairable systems

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



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

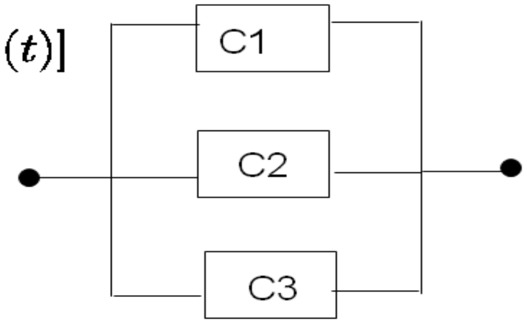
- the failure rate of the system is the sum of the failure rates of the individual components

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

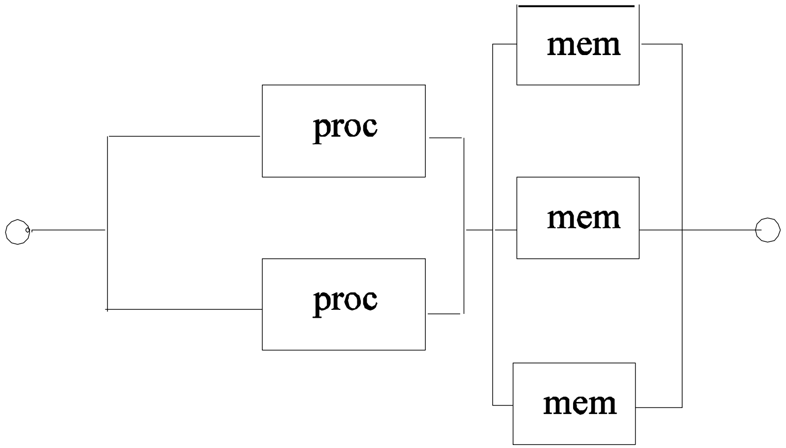
- the system reliability is the reliability of a series/parallel combinatorial model

Combinatorial models

Series/Parallel models

An example:

Multiprocessor with 2 processors and three shared memories



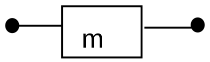
TMR versus Simplex system

Simplex system

λ failure rate of module m

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

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



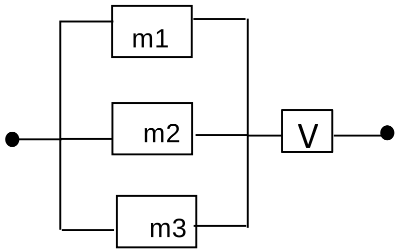
TMR system

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

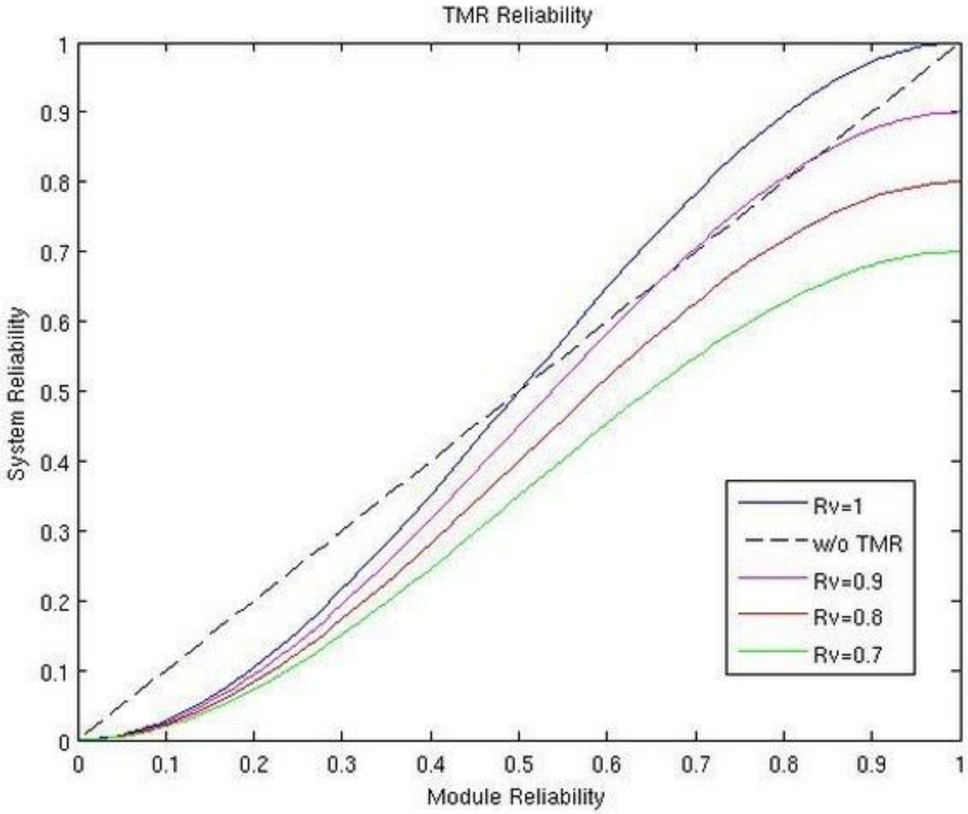
$$\mathbf{R_{TMR}} = \sum_{i=0}^{1} \binom{3}{i} (e^{-\lambda t})^{3-i} (1- e^{-\lambda t})^{i}$$

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

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



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

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

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

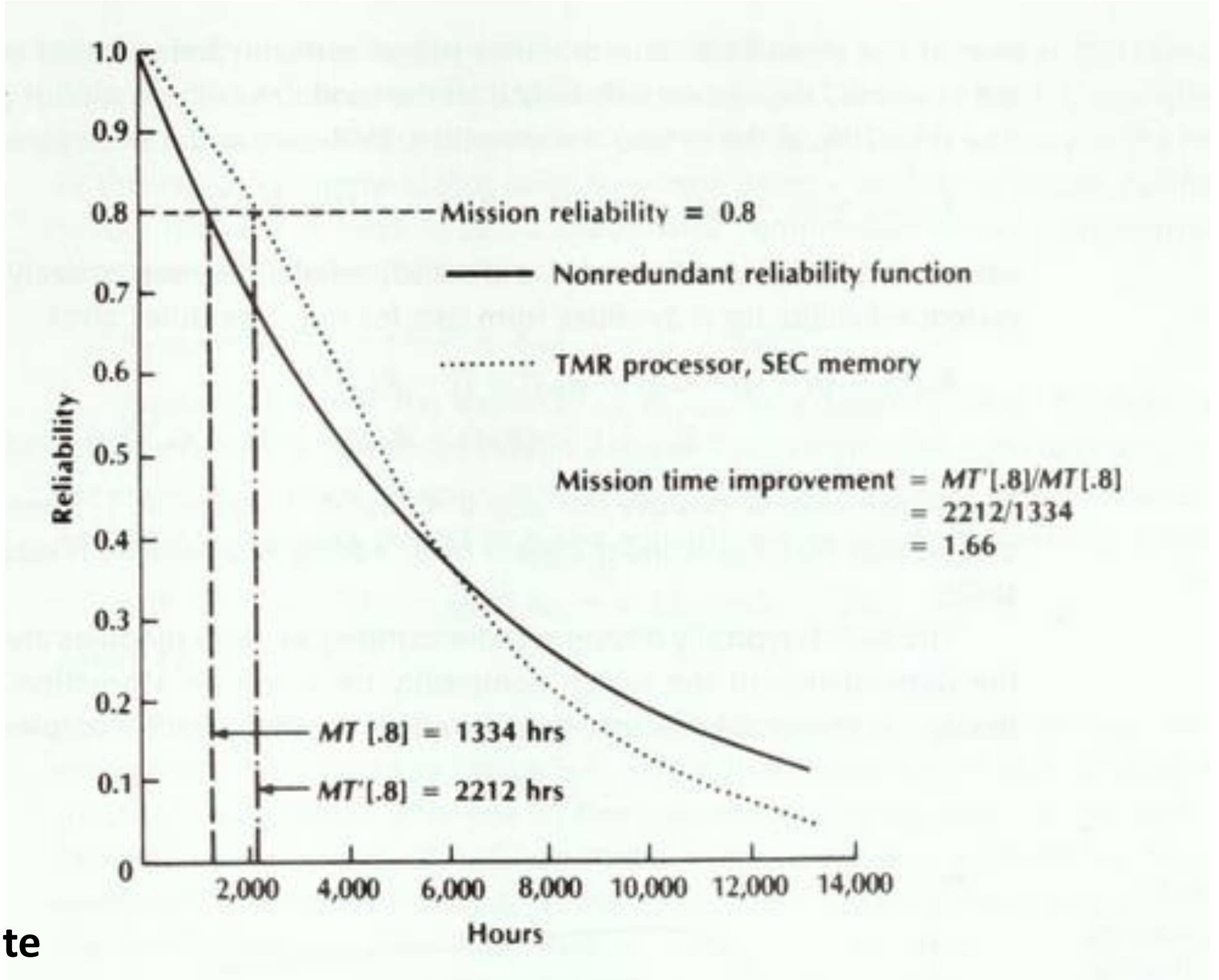
TMR worse than a simplex system

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

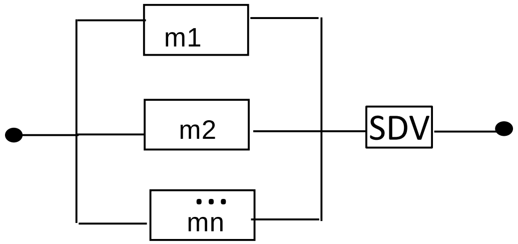
S shape curve is typical of redundant systems: above the knee the redundant system has components that tolerate failures; after the knee the system has exhausted redundancy



Taken from: [Siewiorek et al.1998]

Hybrid redundancy with TMR

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



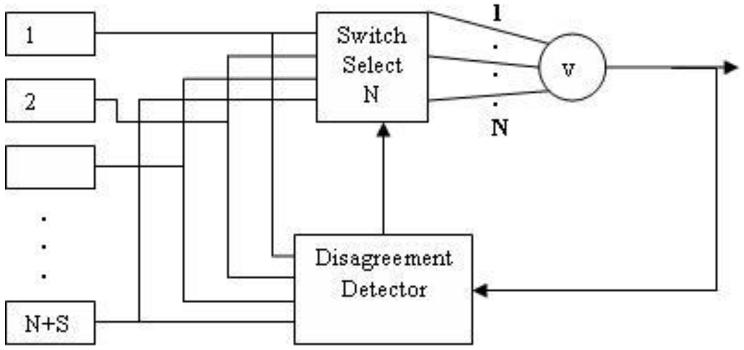
Hybrid system
n=N+S total number of components
S number of spares

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

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

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



Hybrid Redundancy

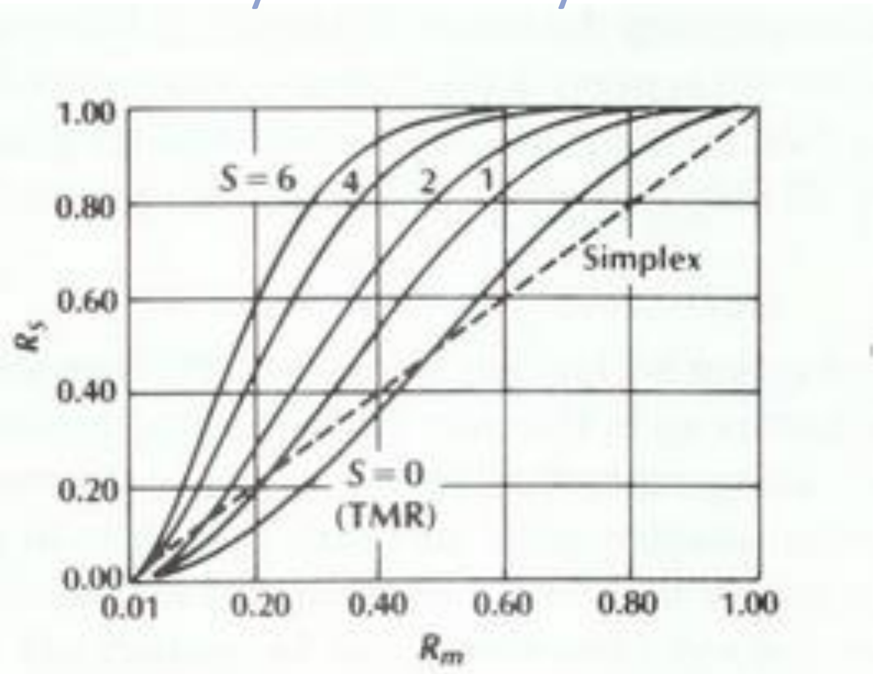
Taken from: [Siewiorek et al.1998]

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

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

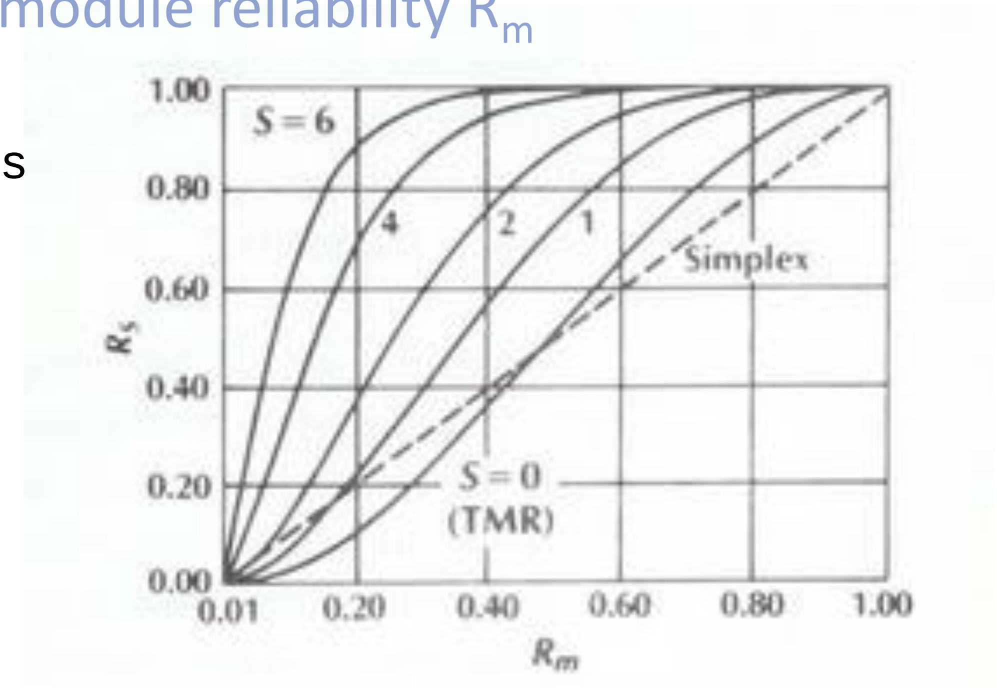


System with standby failure rate equal to on-line failure rate

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

S is the number of spares

R_{SDV} =1



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

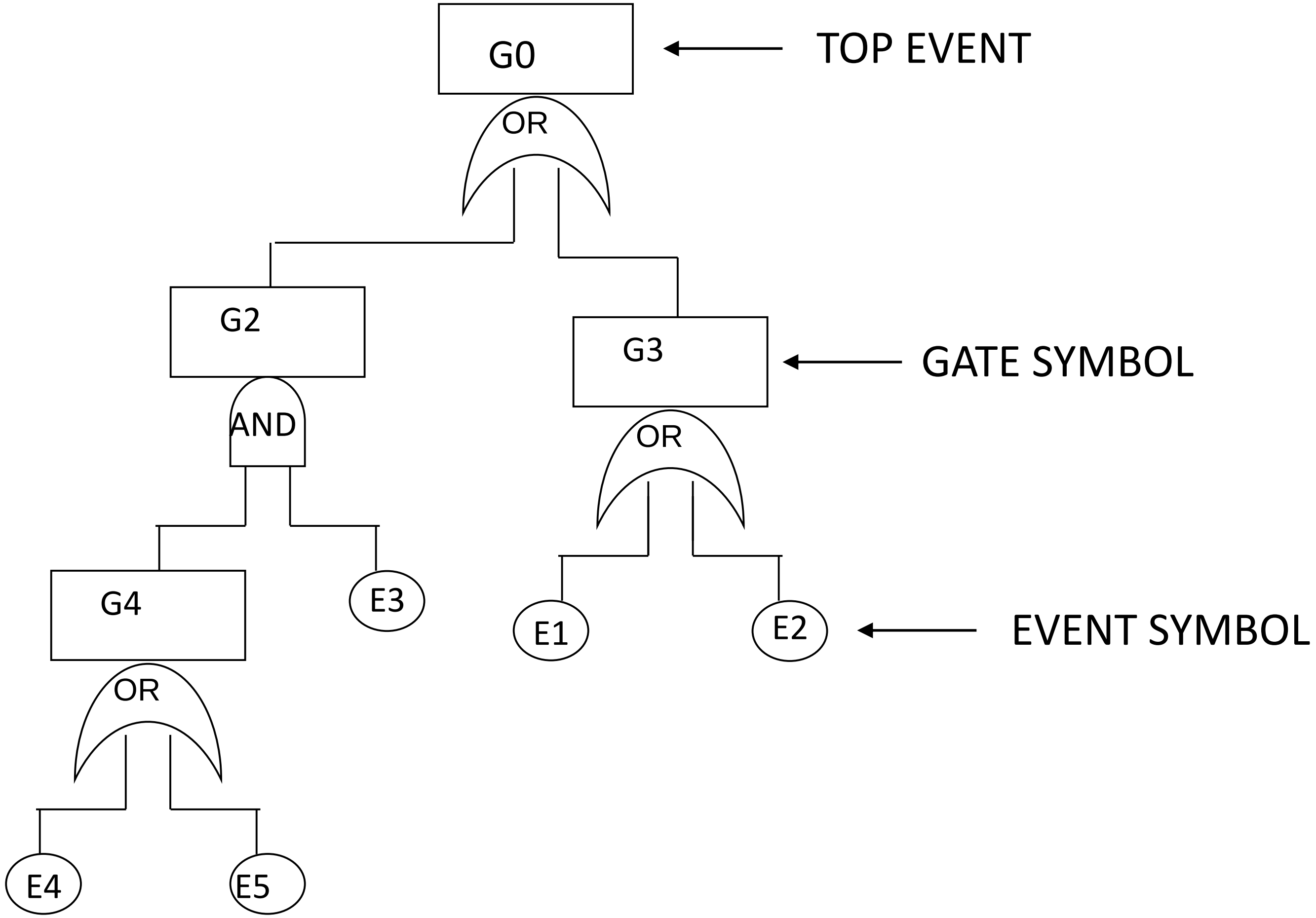
Hierarchy of levels of events linked by logical operators

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)

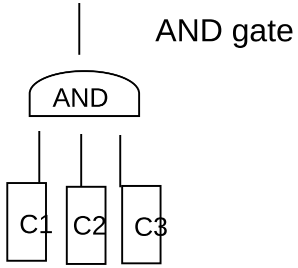


TOP EVENT

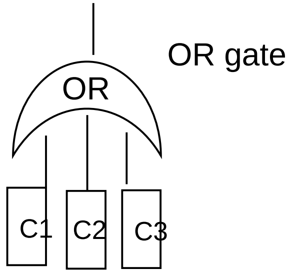
GATE SYMBOL

EVENT SYMBOL

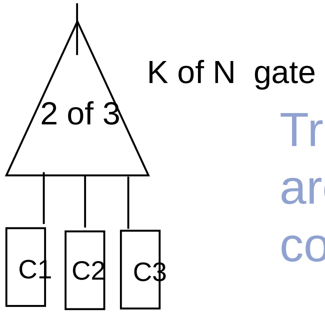
Fault Trees



True if all the components are true (faulty)



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



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

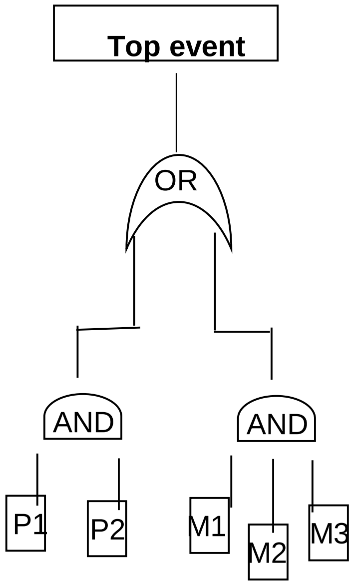
The system fails if the root is true

Fault Trees

Example

Multiprocessor with 2 processors and three shared memories

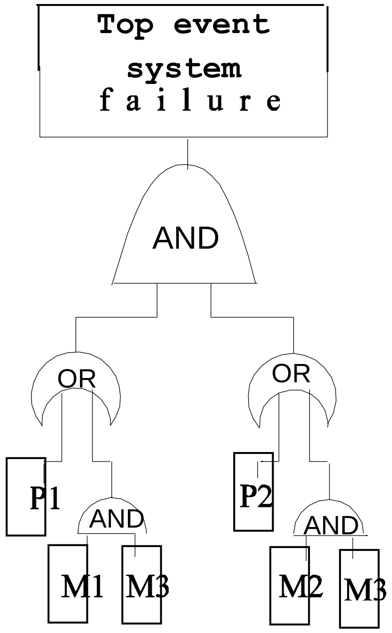
-> the computer fails if all the memories fail or all the processors fail



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

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

where

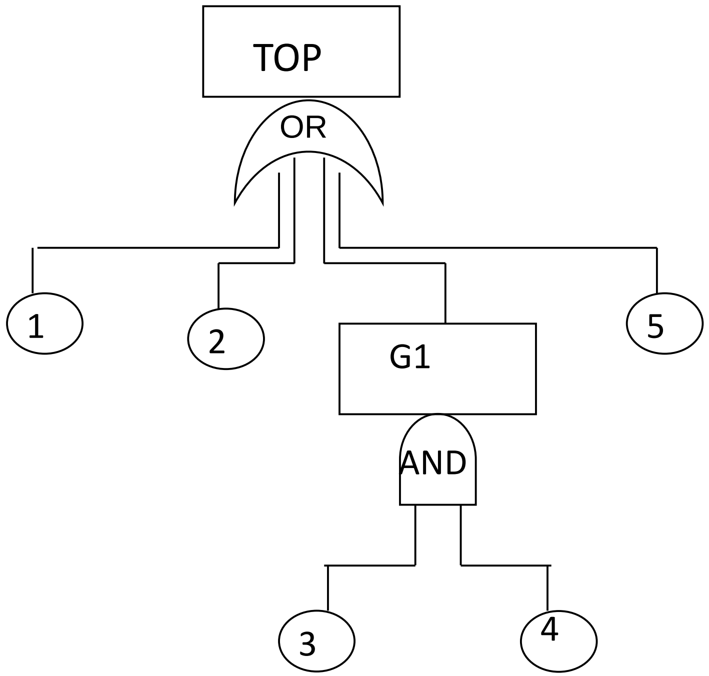
S|C Fails is the system given that C fails

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

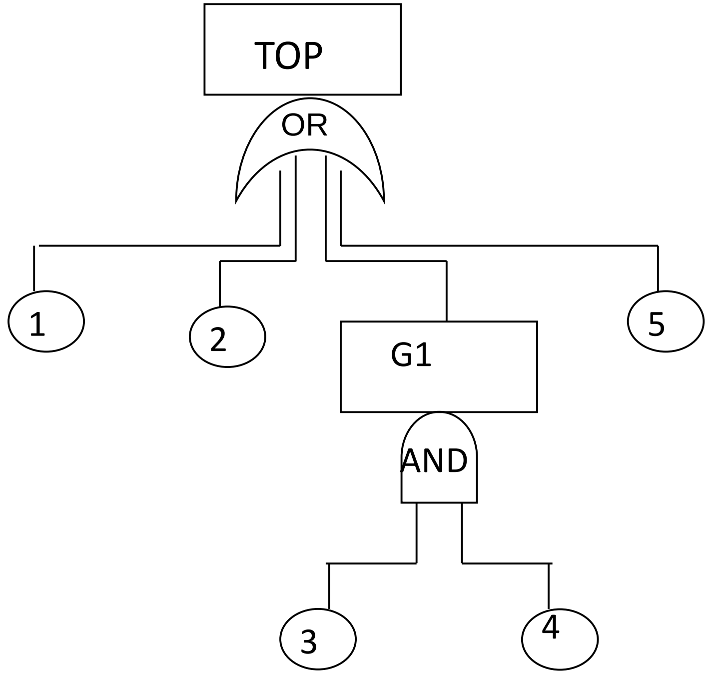
Cut Sets

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

Minimal Cut Sets

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

Minimal cut sets



$Q_{Si}(t)$ = 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 $Si = \{1, 2, \ldots, ni\}$

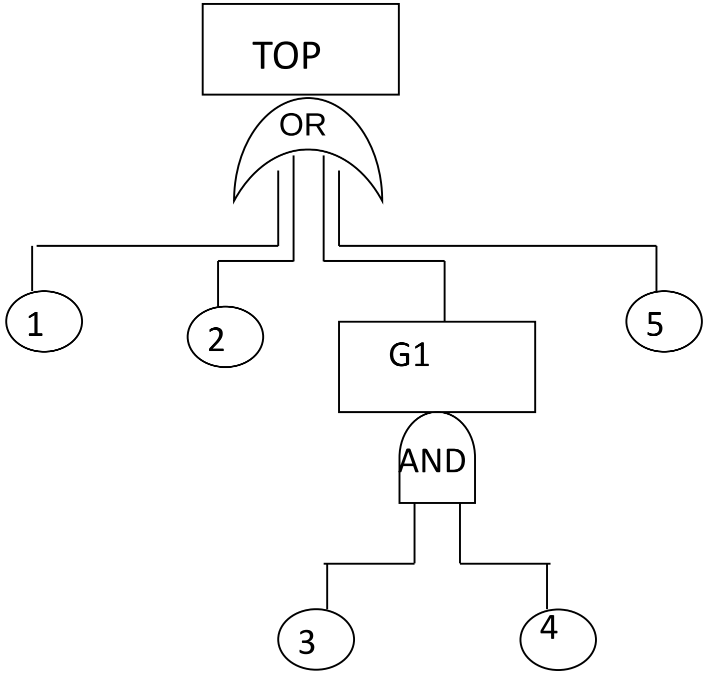
The numerical solution of the FT is performed by computing the probability of occurrence for each of the cuts, and by combining those probabilities to estimate the probability of the root event

Minimal Cut Sets

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

Assumption: independent faults of the components

Minimal cut sets



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

State-based models

State-based models

Characterize the state of the system at time t:

- identification of system states
- identification of transitions that govern the changes of state within a system

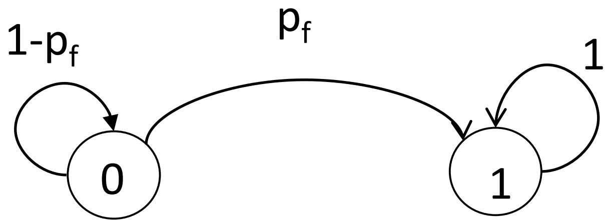
Each state represents a distinct combination of failed and working modules

The system goes from state to state as modules fail and repair

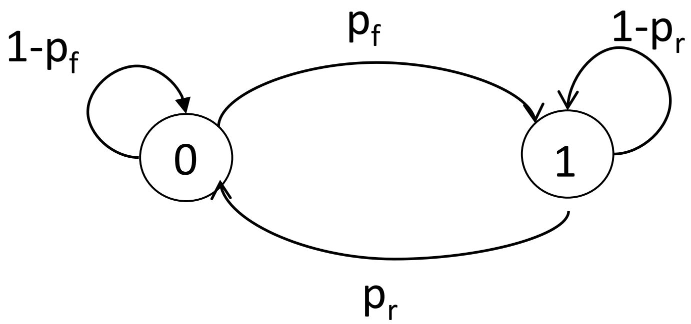
The state transitions are characterized by the probability of failure and the probability of repair

Markov model

graph where nodes are all the possible states and arcs are the possible transitions between states (labeled with a probability function)



Reliability model



Availability model

Markov models

Markov models (a special type of random process) :

Basic assumption: the system behavior at any time instant depends only on the current state (independent of past values)

Main points:

- systems with arbitrary structures and complex dependencies

- assumption of independent failures no longer necessary

- can be used for both reliability and availability modeling

Markov process

In a general random process $\{X_t\}$, the value of the random variable X_{t+1} may depend on the values of the previous random variables

$$X_{t0}\ X_{t1}\ \ldots\ldots\ldots\ldots X_t$$

Markov process

the state of a process at time t+1 depends only on the state at time t, and is independent on any state before t

$$\mathcal{P}\{X_{t+1} = j | X_0 = k_0, \ldots, X_{t-1} = k_{t-1}, X_t = i\} = \mathcal{P}\{X_{t+1} = j | X_t = i\}$$

Markov property: “the current state is enough to determine the future state”

Markov chain

A Markov chain is a Markov process X with discrete state space S

A Markov chain is homogeneous if it has *steady-state transition probabilities*

$$\mathcal{P}\{X_{t+1} = j | X_t = i\} = \mathcal{P}\{X_1 = j | X_0 = i\} \ \forall t \geq 0$$

The probability of transition from state i to state j does not depend by the time. This probability is called p_{ij}

$$p_{ij} = \mathcal{P}\{X_1 = j | X_0 = i\}$$

We consider only *homogeneous* Markov chains

- discrete-time Markov chains (DTMC) / Continuous-time Markov chains (CTMC)

Transition probability matrix

If a Markov process is finite-state, we can define the transition probability matrix P (nxn)

$$P = \begin{bmatrix} p_{11} & \cdots\cdots & p_{1n} \\ \vdots & \ddots & \\ p_{n1} & \cdots\cdots & p_{nn} \end{bmatrix},$$

$$p_{ij} = \mathcal{P}\{X_1 = j | X_0 = i\}$$

pij = probability of moving from state i to state j in one step

row i of matrix P:
probability of make a transition starting from state i

column j of matrix P:
probability of making a transition from any state to state j

Discrete-time Markov chain (DTMC)

State space distribution

State occupancy vector at time t $\pi(t) = [\pi_0(t), \pi_1(t), \pi_2(t) , \ldots]$

Probability that the Markov process is in state i at time-step t $\pi_i(t) = P\{X_t = i\}$

Initial state space distribution $\pi(0) = (\pi_1(0), \ldots, \pi_n(0))$

A single step forward $\pi(1) = \pi(0) P$

State occupancy vector at time t $\pi(t) = \pi(0) P^t$

System evolution in a finite number of steps computed starting from the initial state distribution and the transition probability matrix

Limiting behaviour

A Markov process can be specified in terms of the state occupancy probability vector p and a transition probability matrix P

$$\pi(t) = \pi(0)\ Pt$$

The limiting behaviour of a DTMC (steady-state behaviour)

$$\lim_{t \to \infty} \pi(t)$$

The limiting behaviour of a DTMC depends on the characteristics of its states. Sometimes the solution is simple

Time-average state space distribution

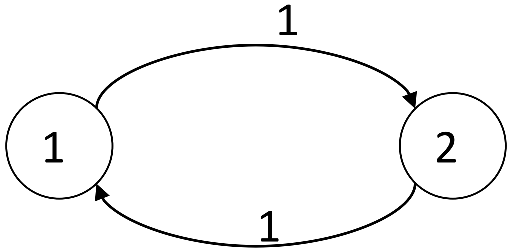
For periodic Markov chains $\lim_{t\to\infty} \pi(t)$

doesn't exist (caused by the probability of the periodic state)

Compute the time-average state space distribution, called π^*

$$\pi^* = \lim_{t\to\infty} \frac{\sum_{i=1}^{t} \pi(i)}{t}$$

$$P = \begin{array}{c|cc} & 1 & 2 \\ \hline 1 & 0 & 1 \\ 2 & 1 & 0 \end{array}$$



$\pi(0) = (1,0)$

state i is periodic with period d=2

$\pi(0) = (1,0)$

$\pi(1) = \pi(0)\ P \qquad \pi(1) = (0,1)$

$\pi(2) = \pi(1)\ P \qquad \pi(2) = (1,0)$

....

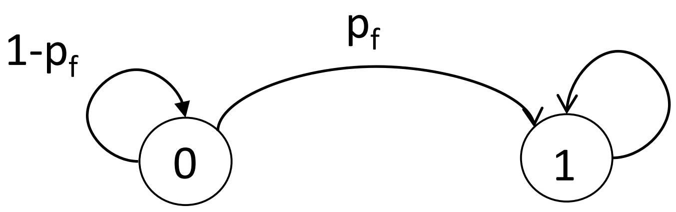
Simplex system

$\{X_t\}$ $t=0, 1, 2, \ldots$ $S=\{0, 1\}$

- all state transitions occur at fixed intervals
- probabilities assigned to each transition
- The probability of state transition depends only on the current state

State 0 : working
State 1: failed

p_f Failure probability



$$P = \begin{array}{c|cc|} & 0 & 1 \\ \hline 0 & 1-p_f & p_f \\ 1 & 0 & 1 \\ \hline \end{array}$$

next state

current state

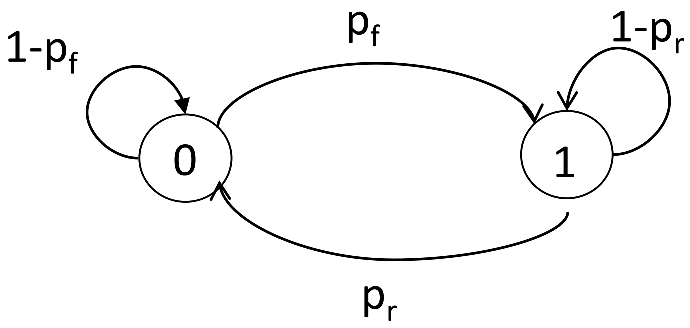
- pij = probability of a transition from state i to state j
- pij >=0
- the sum of each row must be one

Simplex system with repair

State 0 : working
State 1: failed

p_f Failure probability

p_r Repair probability



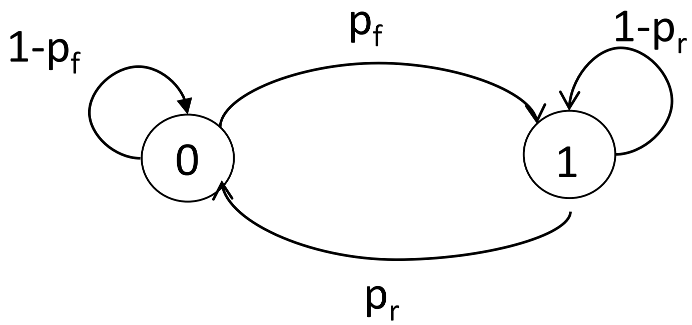
$$P = \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1-p_f & p_f \\ 1 & p_r & 1-p_r \end{array}$$

current state

next state

Simplex system with repair

initial state: working $[p_0(0), p_1(0)] = [1, 0]$

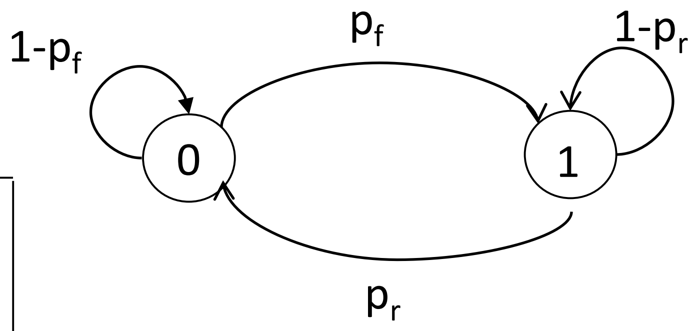


$$[p0(1), p1(1)] = [1, 0] \begin{bmatrix} 0.9 & 0.1 \\ 0.5 & 0.5 \end{bmatrix} = [0.9, 0.1]$$

State j can be made an trapping state with pjj = 1

Simplex system with repair

probability of being in a state after 1 time-step



$$[p_0(n), p_1(n)] = [p_0(n-1), p1(n-1)] \begin{bmatrix} 1-p_f & p_f \\ p_r & 1-p_r \end{bmatrix}$$

probability of being in a state after n time-steps

$$[p_0(n), p_1(n)] = [p_0(0), p_1(0)] \begin{bmatrix} 1-p_f & p_f \\ p_r & 1-p_r \end{bmatrix}^n$$

Continuous-time Markov model

- state transitions occur at random intervals
- transition rates assigned to each transition

Markov property assumption

the length of time already spent in a state does not influence either the probability distribution of the next state or the probability distribution of remaining time in the same state before the next transition

These assumptions imply that the waiting time spent in any one state is exponentially distributed

Thus the Markov model naturally fits with the standard assumptions that failure rates are constant, leading to exponential distribution of interarrivals of failures

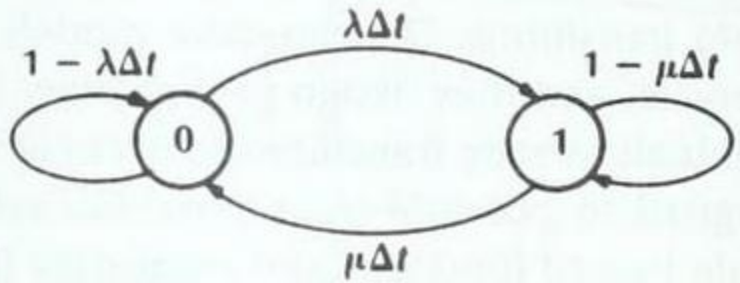
state 0: working
state 1: failed

λ failure rate
μ repair rate

Continuous time

Transition matrix P: transition rate

Probability of being in state 0 or 1 at time t+Δt



$\lambda\Delta t$, $\mu\Delta t$—State transition probabilities
λ, μ—State transition rates

Taken from: [Siewiorek et al.1998]

$$P = \begin{bmatrix} 1-\lambda\Delta t & \lambda\Delta t \\ \mu\Delta t & 1-\mu\Delta t \end{bmatrix}$$

Simplex system with repair

$$[p_0(t+\Delta t), p_1(t+\Delta t)] = [p_0(t), p_1(t)] \begin{bmatrix} 1-\lambda\Delta t & \lambda\Delta t \\ \mu\Delta t & 1-\mu\Delta t \end{bmatrix}$$

↑

probability of being in state 0 at time t+Δt

Performing multiplication, rearranging and dividing by Δt, taking the limit as Δt approaches to 0:

$$\frac{dp_0(t)}{dt} = -\lambda p_0(t) + \mu p_1(t)$$

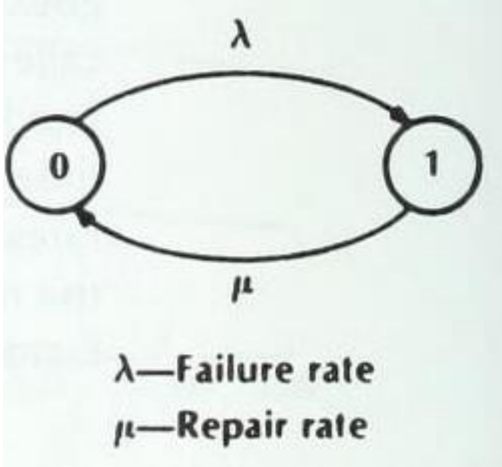
$$\frac{dp_1(t)}{dt} = \lambda p_0(t) - \mu p_1(t)$$

Simplex system with repair

$$\left[\frac{dp_0(t)}{dt}, \frac{dp_1(t)}{dt}\right] = [p_0(t), p_1(t)] \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$

T matrix

Continuous time Markov model graph

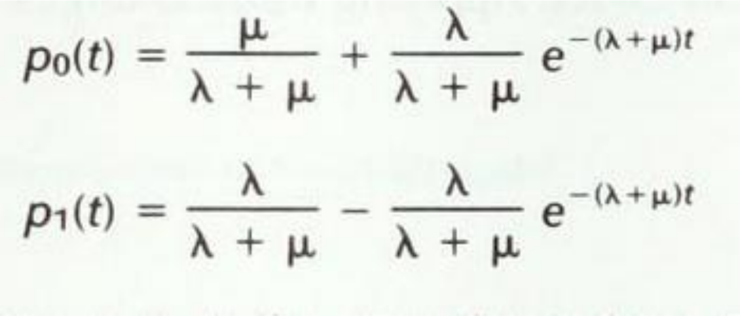


Taken from: [Siewiorek et al.1998]

The change in state 0 is minus the flow out of state 0 times the probability of being in state 0 at time t, plus the flow into state 0 from state 1 times the probability of being in state 1.

The set of equations can be written by inspection of a transition diagram without self-loops and Δt's

Simplex system with repair



$$p_0(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda+\mu)t}$$

$$p_1(t) = \frac{\lambda}{\lambda + \mu} - \frac{\lambda}{\lambda + \mu} e^{-(\lambda+\mu)t}$$

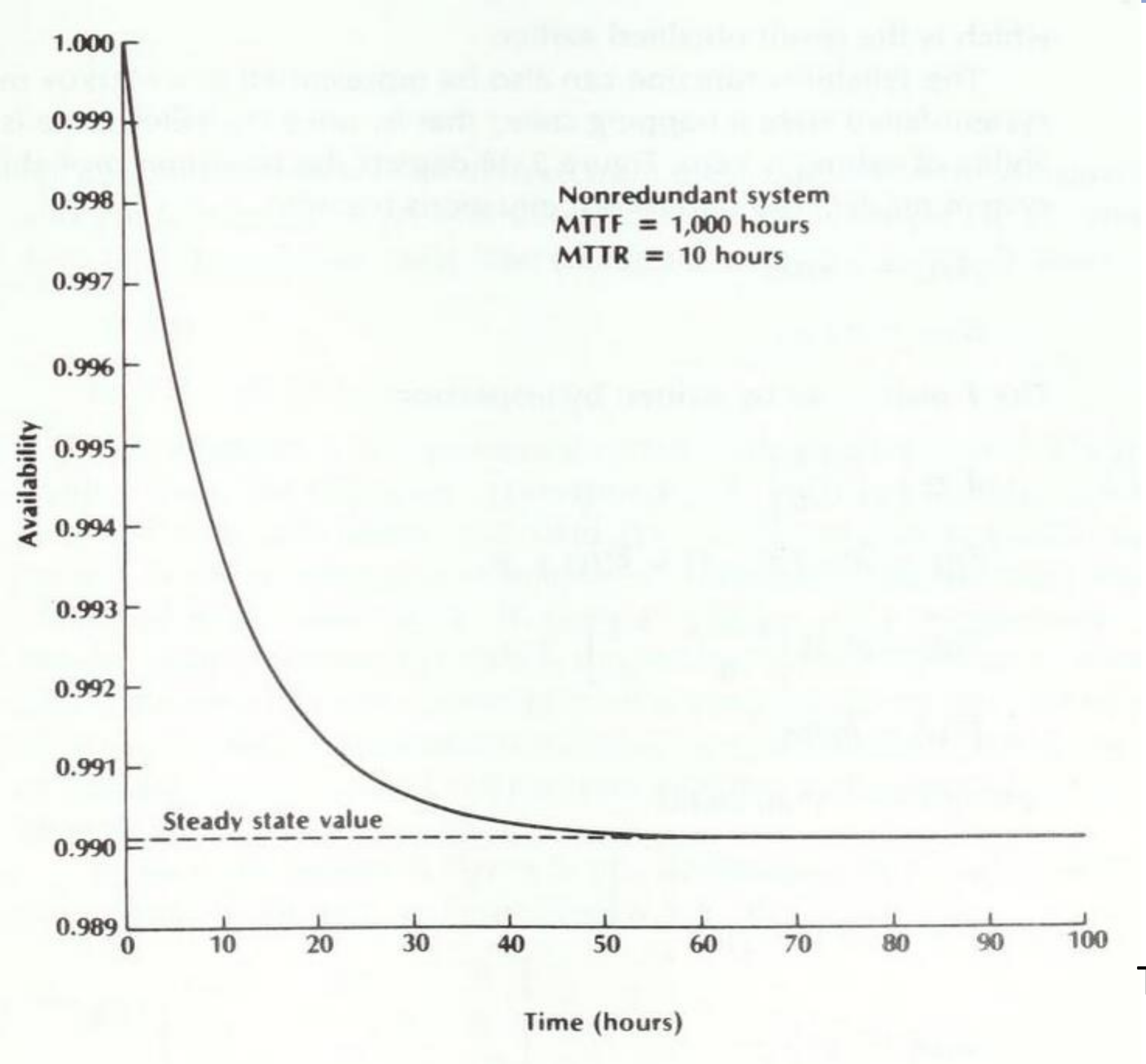
A(t)

Taken from: [Siewiorek et al.1998]

$p_0(t)$ probability that the system is in the operational state at time t, availability at time t

The availability consists of a steady-state term and an exponential decaying transient term

Availability as a function of time



$\lambda = 0.001$
$\mu = 0.1$

The steady-state value is reached in a very short time

Taken from: [Siewiorek et al.1998]

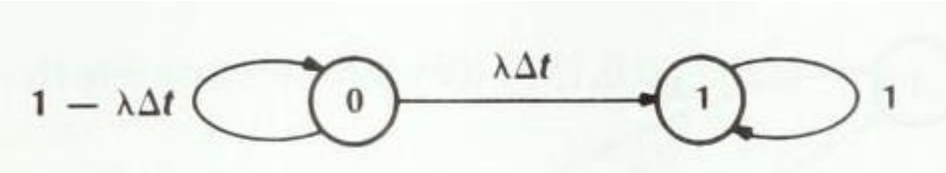
Continuous-time Markov models: Reliability

Single system without repair

failed state as trapping state

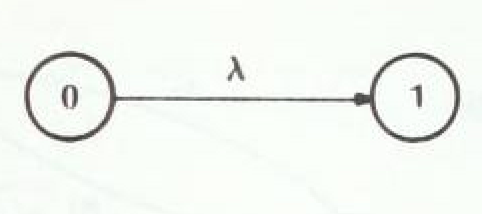
λ = failure rate

$\lambda\Delta t$ = state transition probability



$$T = \begin{bmatrix} -\lambda & \lambda \\ 0 & 0 \end{bmatrix}$$

Continuous time Markov model graph



We can prove that:

$$p_0(t) = e^{-\lambda t}$$

Reliability

$$p_1(t) = 1 - e^{-\lambda t}$$

Unreliability

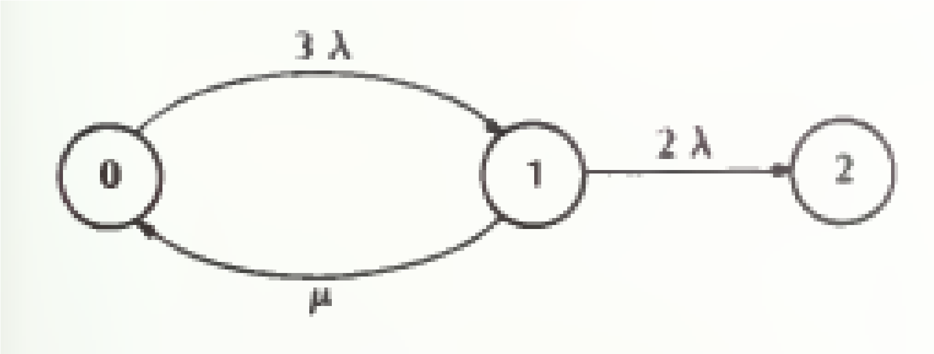
TMR system with repair

Rates: λ and μ

Identification of states:

- 3 processors working, 0 failed
- 2 processors working, 1 failed
- 1 processor working, 2 failed

$p(0) = [1, 0, 0]$

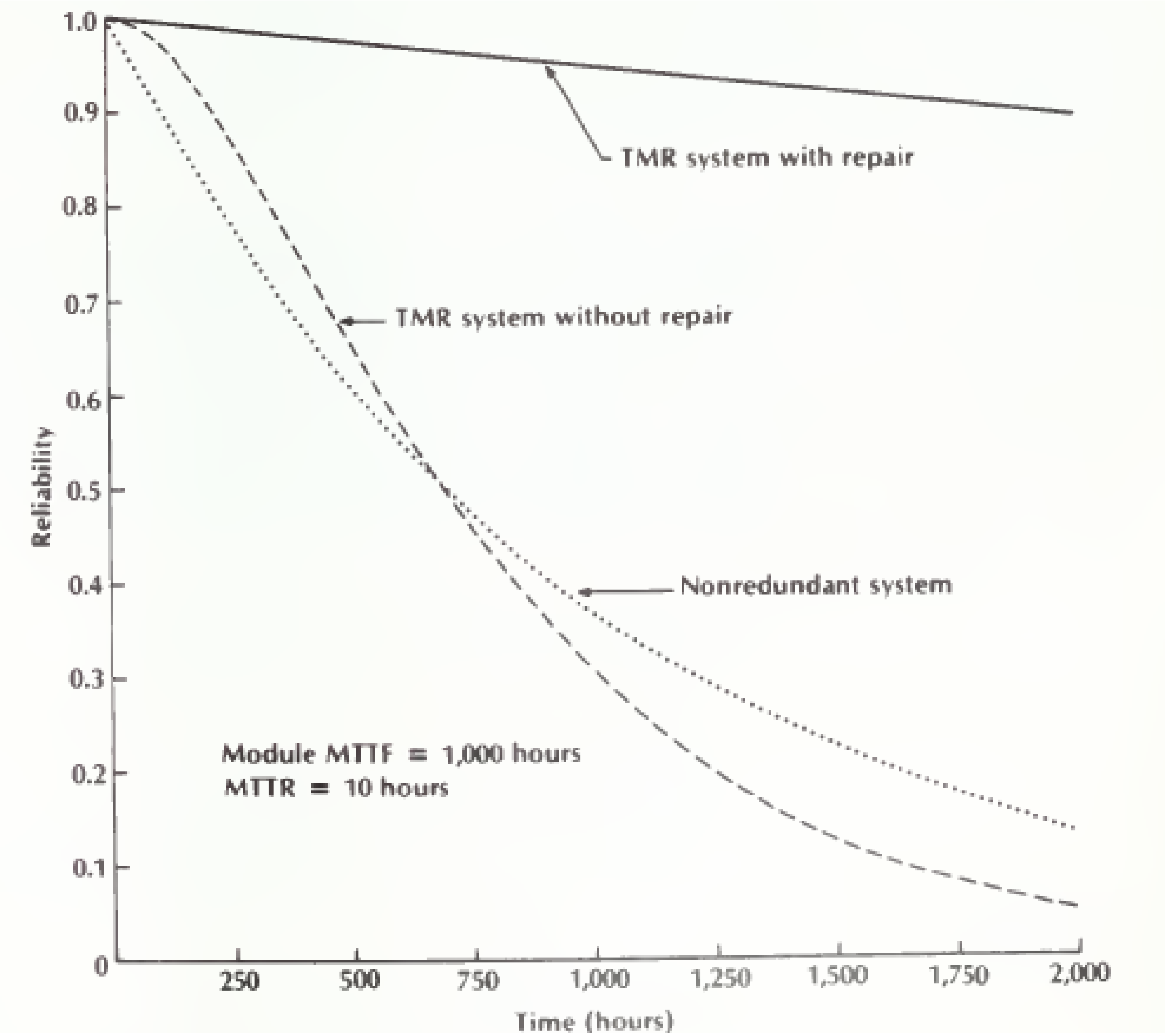


$$T = \begin{bmatrix} -3\lambda & 3\lambda & 0 \\ \mu & -2\lambda-\mu & 2\lambda \\ 0 & 0 & 0 \end{bmatrix}$$

Reliability R(t) = 1- p2(t)

$$R(t) = \frac{5\lambda + \mu + \sqrt{\lambda^2 + 10\lambda\mu + \mu^2}}{2\sqrt{\lambda^2 + 10\lambda\mu + \mu^2}} \exp\left(-(1/2)(5\lambda + \mu - \sqrt{\lambda^2 + 10\lambda\mu + \mu^2})t\right) - \frac{5\lambda + \mu - \sqrt{\lambda^2 + 10\lambda\mu + \mu^2}}{2\sqrt{\lambda^2 + 10\lambda\mu + \mu^2}} \exp\left(-(1/2)(5\lambda + \mu + \sqrt{\lambda^2 + 10\lambda\mu + \mu^2})t\right)$$

Comparison with nonredundant system and TMR without repair

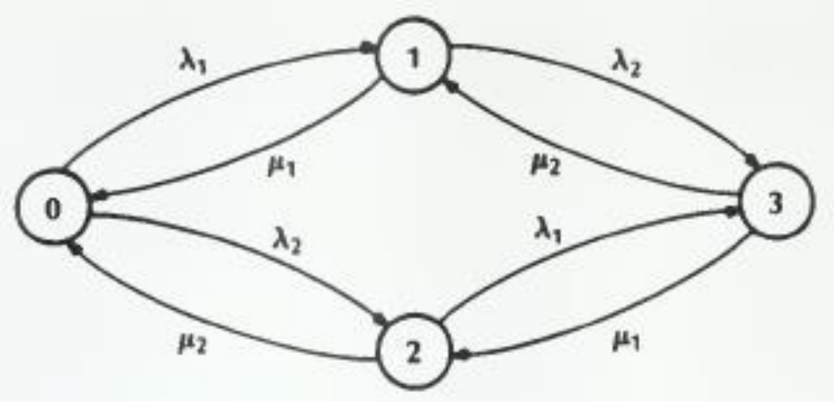


Taken from: [Siewiorek et al.1998]

Dual processor system with repair

A, B processors Rates: $\lambda 1$, $\lambda 2$ and $\mu 1$, $\mu 2$

Identification of states:
- A, B working
- A working, B failed
- B working, A failed
- A, B failed



Availability

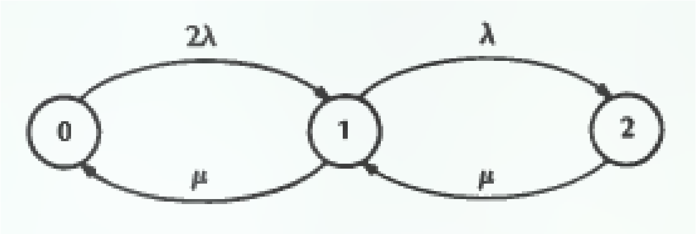
$A(t) = p_0(t) + p_1(t) + p_2(t)$

$A(t) = 1- p_3(t)$

Rates: $\lambda 1 = \lambda 2$ and $\mu 1 = \mu 2$

p(0) = [1, 0, 0]

$$T = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -\lambda-\mu & \lambda \\ 0 & \mu & \mu \end{bmatrix}$$



Taken from: [Siewiorek et al.1998]

Availability

$A(t) = 1- p_2(t)$

Dual processor system with repair

$$A(t) = \frac{2\lambda\mu + \mu^2}{2\lambda^2 + 2\lambda\mu + \mu^2} - \frac{4\lambda^2 \exp\left(-(1/2)[(3\lambda + 2\mu) + \sqrt{\lambda^2 + 4\lambda\mu}]t\right)}{\lambda^2 + 4\lambda\mu + (3\lambda + 2\mu)\sqrt{\lambda^2 + 4\lambda\mu}}$$

$$- \frac{4\lambda^2 \exp\left(-(1/2)[(3\lambda + 2\mu) - \sqrt{\lambda^2 + 4\lambda\mu}]t\right)}{\lambda^2 + 4\lambda\mu - (3\lambda + 2\mu)\sqrt{\lambda^2 + 4\lambda\mu}}$$

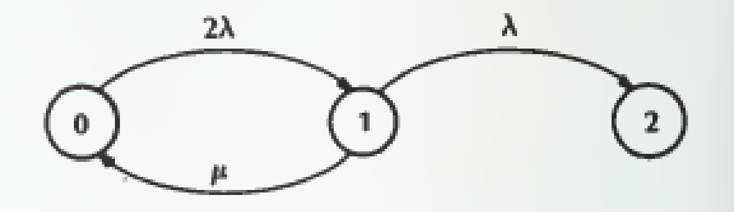
$$A_{ss} = \frac{2\lambda\mu + \mu^2}{2\lambda^2 + 2\lambda\mu + \mu^2}$$

Steady state value

Taken from: [Siewiorek et al.1998]

Reliability model

making state 2 a trapping state



p(0) = [1, 0, 0]

$$T = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -\lambda-\mu & \lambda \\ 0 & 0 & 0 \end{bmatrix}$$

Reliability $R(t) = 1- p_2(t)$ $R(t)=p_0(t) + p_1(t)$

$$R(t) = \frac{4\lambda^2 \exp\left(-(1/2)(3\lambda + \mu - \sqrt{\lambda^2 + 6\lambda\mu + \mu^2})t\right)}{(3\lambda + \mu)\sqrt{\lambda^2 + 6\lambda\mu + \mu^2} - \lambda^2 - 6\lambda\mu - \mu^2} - \frac{4\lambda^2 \exp\left(-(1/2)(3\lambda + \mu + \sqrt{\lambda^2 + 6\lambda\mu + \mu^2})t\right)}{(3\lambda + \mu)\sqrt{\lambda^2 + 6\lambda\mu + \mu^2} + \lambda^2 + 6\lambda\mu + \mu^2}$$

Taken from: [Siewiorek et al.1998]

TMR system with repair

Rates: λ and μ

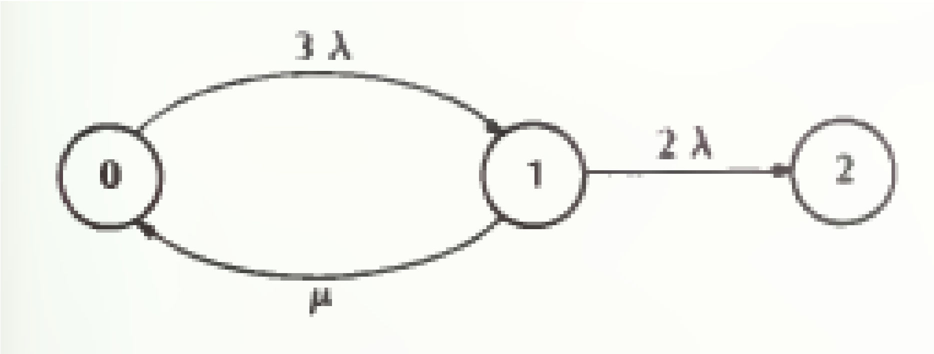
Identification of states:

- 3 processors working, 0 failed
- 2 processors working, 1 failed
- 1 processor working, 2 failed

$p(0) = [1, 0, 0]$

$$T = \begin{bmatrix} -3\lambda & 3\lambda & 0 \\ \mu & -2\lambda-\mu & 2\lambda \\ 0 & 0 & 0 \end{bmatrix}$$

Reliability $R(t) = 1- p2(t)$



$$R(t) = \frac{5\lambda + \mu + \sqrt{\lambda^2 + 10\lambda\mu + \mu^2}}{2\sqrt{\lambda^2 + 10\lambda\mu + \mu^2}} \exp\left(-(1/2)(5\lambda + \mu - \sqrt{\lambda^2 + 10\lambda\mu + \mu^2})t\right) - \frac{5\lambda + \mu - \sqrt{\lambda^2 + 10\lambda\mu + \mu^2}}{2\sqrt{\lambda^2 + 10\lambda\mu + \mu^2}} \exp\left(-(1/2)(5\lambda + \mu + \sqrt{\lambda^2 + 10\lambda\mu + \mu^2})t\right)$$

Taken from: [Siewiorek et al.1998]

Comparison with nonredundant system and TMR without repair