Dependability evaluation

D.P. Siewiorek, R. S. Swarz.
Reliable Computer Systems (Design and Evaluation).
Prentice Hall, 1998.

Chapter 5

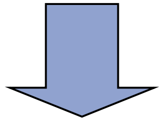
Outline

- Reliability and Availability
- Failure rate and Repair rate
- 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

Evaluation of Dependability

Faults are the cause of errors and failures. Does the arrival time of faults fit a **probability distribution**?
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

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

Evaluation of dependability

Reliability - R(t)

As a function of time, R(t), is the 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)

As a function of time, A(t), is 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)

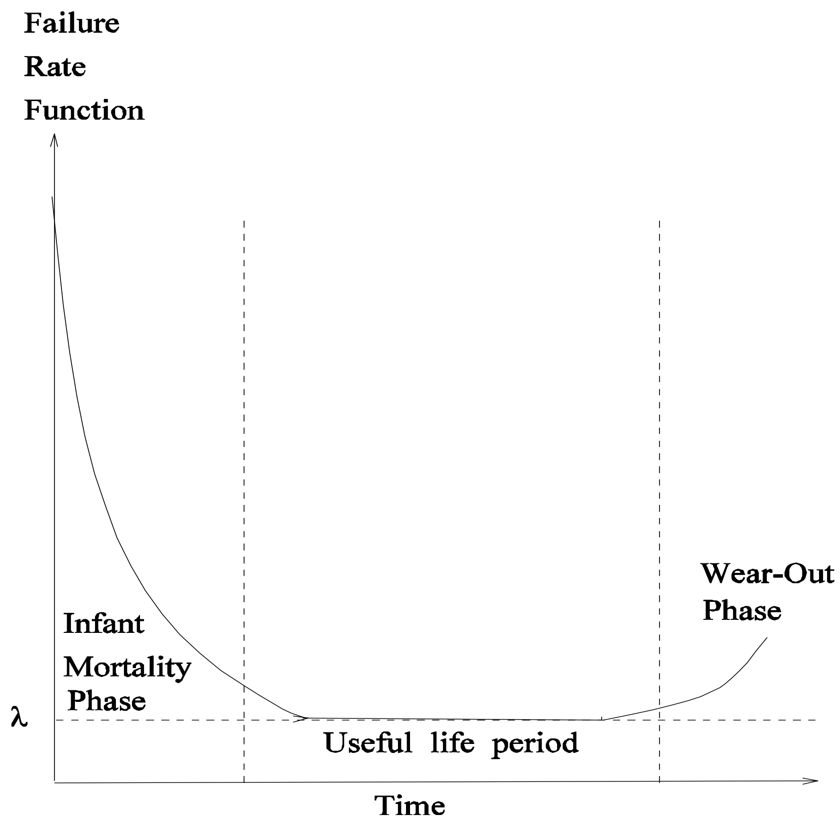
$\lambda(t)$ constant > 0 in the useful life period

Constant failure rate λ

λ = 1/2000 one failure every 2000 hours

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

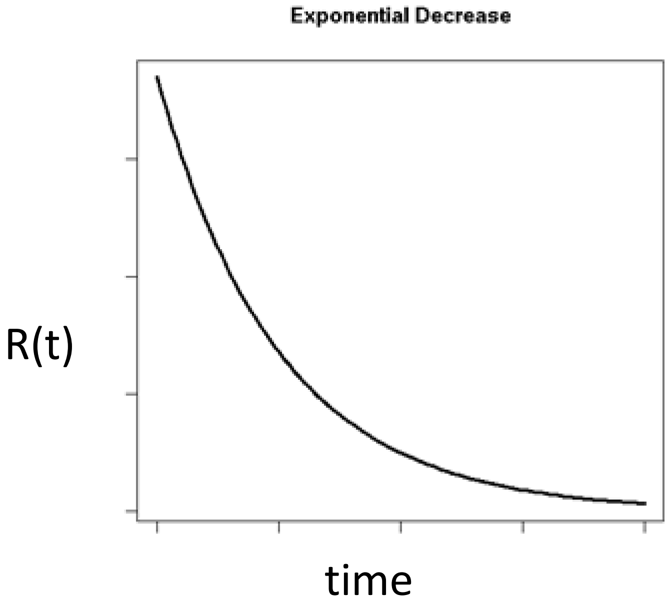
Constant failure rate

$$\lambda(t) = \lambda$$

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

Reliability function

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



Probability density function

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

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)

failure rate usually expressed in number of failures in 1 billion device hours

1 FIT means 1 failure in 10^9 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,
- 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)

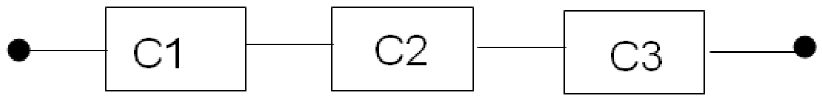
- inadequate to deal with systems that exhibits complex dependencies among components and repairable systems

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:

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

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

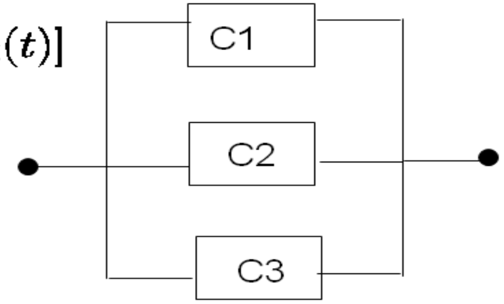
- the failure rate of the system is the sum of the failure rates of the individual components

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

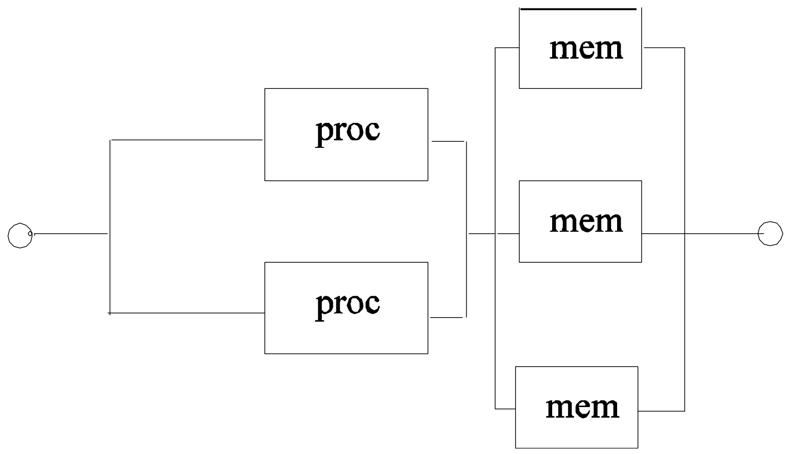
- the system reliability is the reliability of a series/parallel combinatorial model

Combinatorial models

Series/Parallel models

An example:

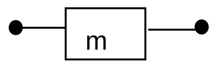
Multiprocessor with 2 processors and three shared memories



TMR versus Simplex system

λ failure rate of module m

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



Simplex system

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

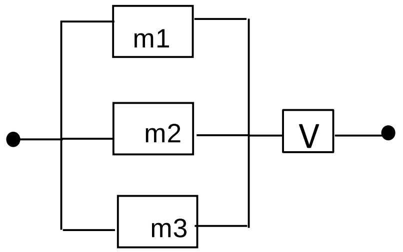
TMR system

$R_V(t) = 1$

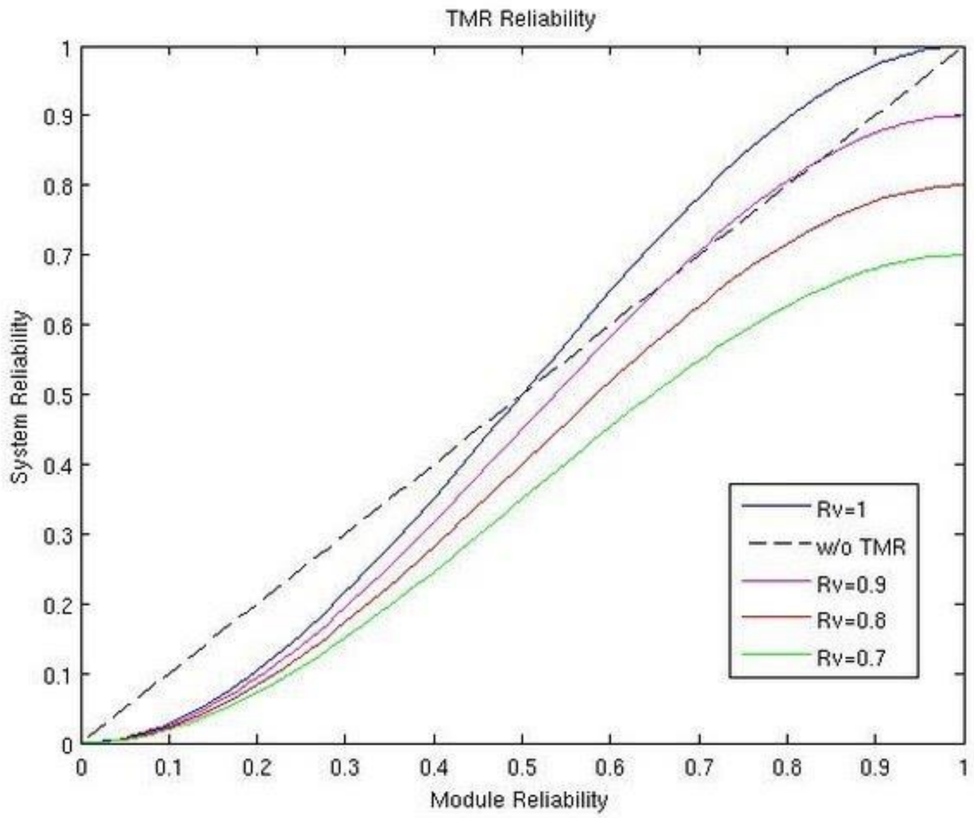
$$R_{TMR} = \sum_{i=0}^{1} \binom{3}{i} (e^{-\lambda t})^{3-i} (1- e^{-\lambda t})^{i}$$

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

$R_{TMR} > R_m$ 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

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

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

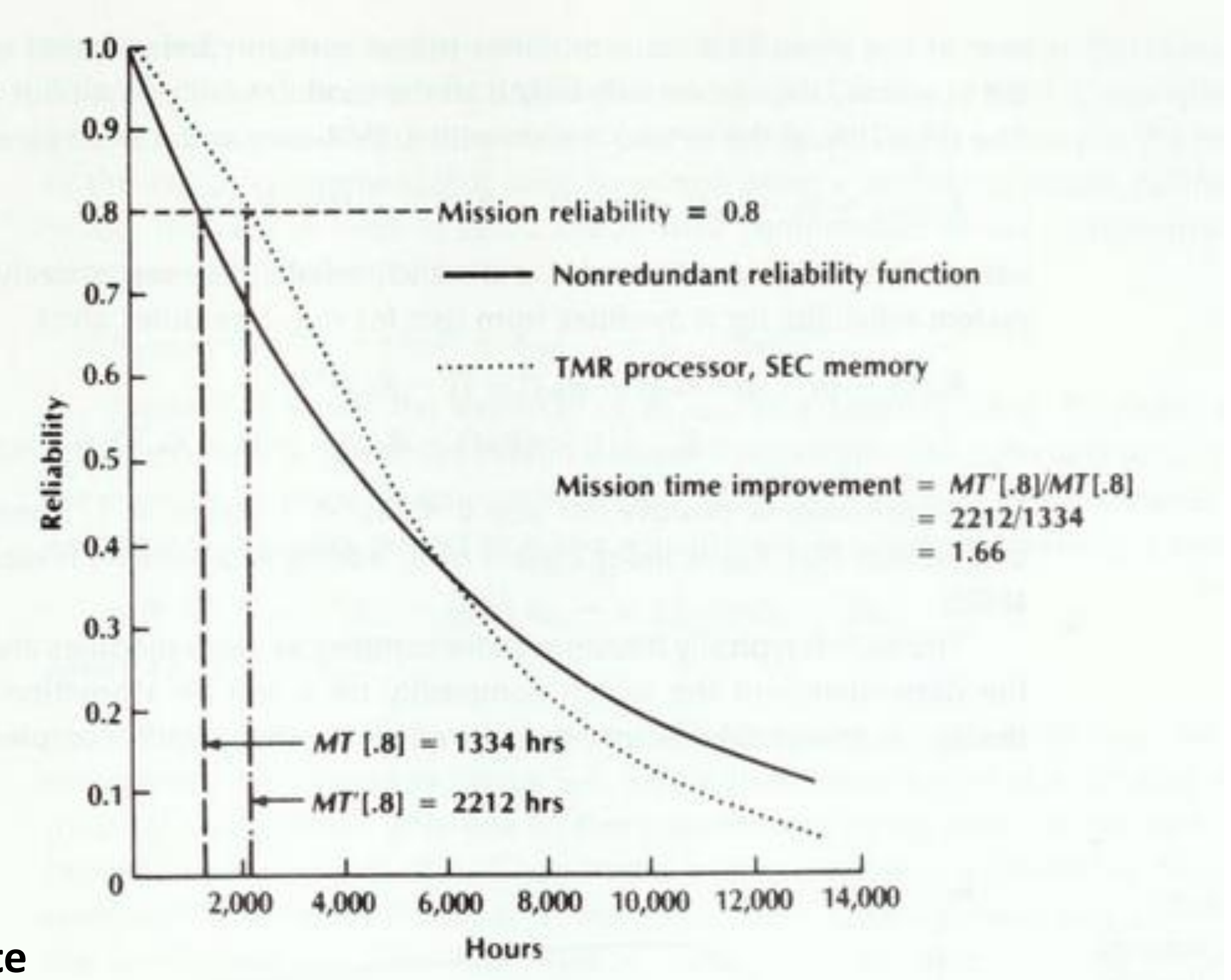
TMR worse than a simplex system

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

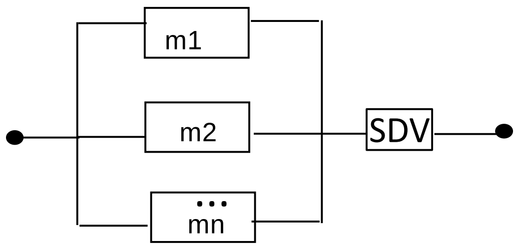
S shape curve is typical of redundant systems: above the knee the redundant system has components that tolerate failures; after the knee the system has exhausted redundancy

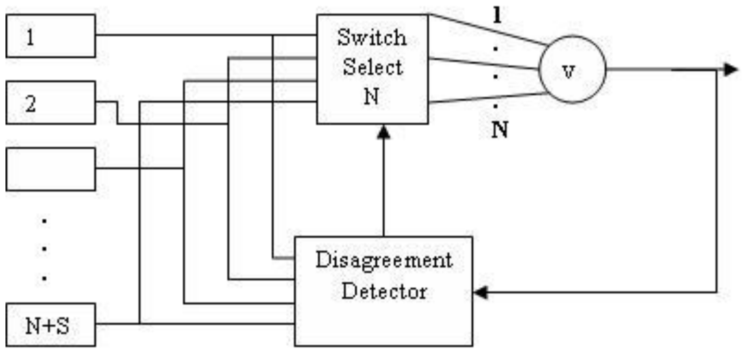


Taken from: [Siewiorek et al.1998]

Hybrid redundancy with TMR

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





Hybrid Redundancy

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

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

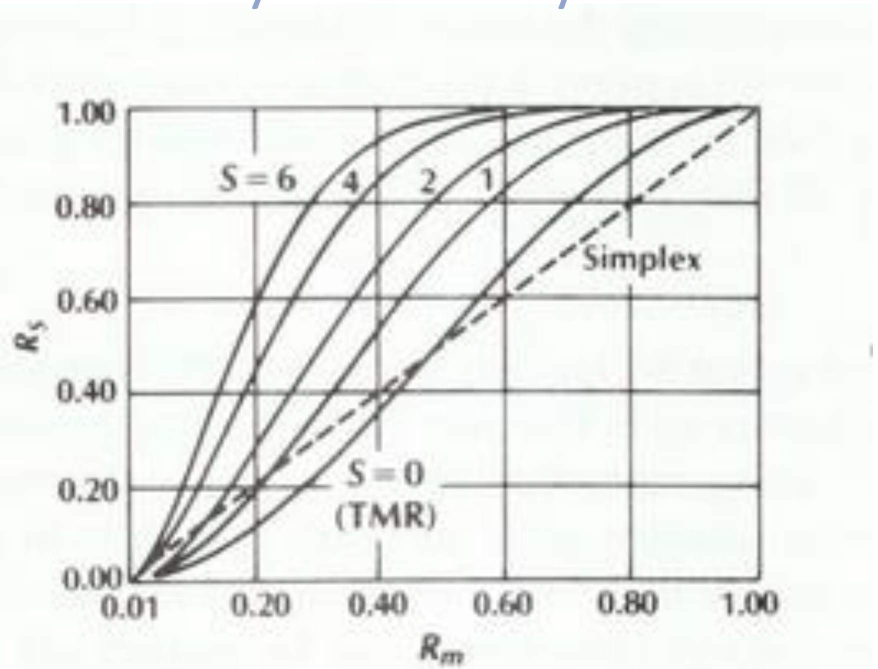
$R_{Hybrid} = (1 – ((1-R_m)^n + n(R_m)(1-R_m)^{n-1}))$

$R_{Hybrid(n+1)} – R_{Hybrid(n)} > 0$

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

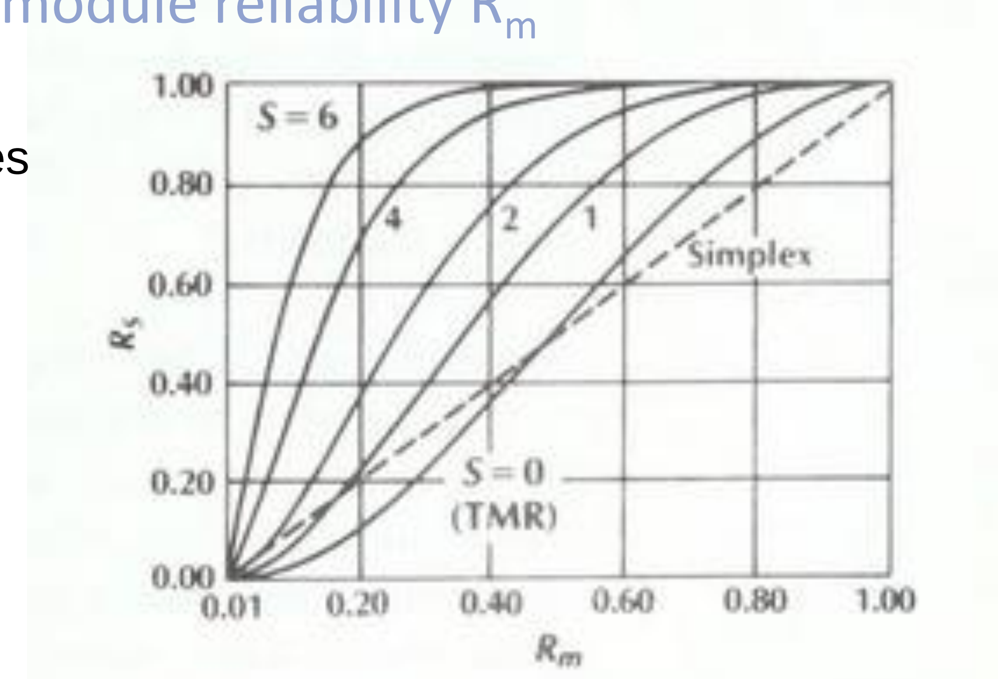


System with standby failure rate equal to on-line failure rate

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

S is the number of spares

R_{SDV} =1

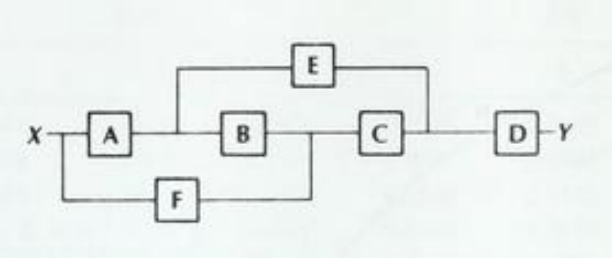


System with standby failure rate equal to 10% of on line failure rate

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

Taken from: [Siewiorek et al.1998]

Non-series/non-parallel models



Succes diagram

System successfully operational for each path from X to Y

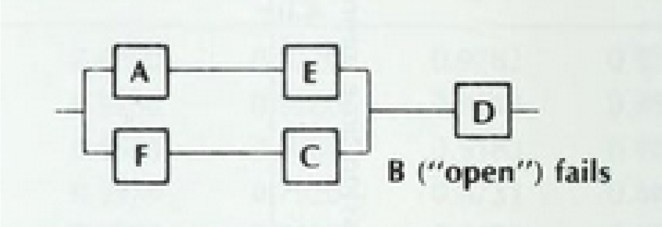
From: D. P. Siewiorek R.S. Swarz, Reliable Computer Systems, Prentice Hall, 1992

Reliability computed expanding around one module m:

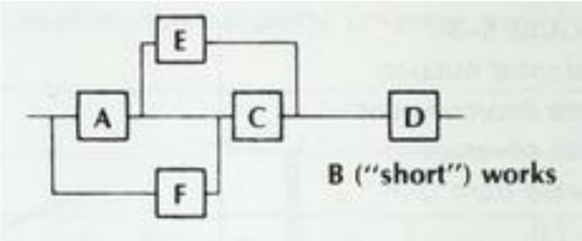
R_{sys} = R_m x P(system works | m works) + (1- R_m) x P(system works | m fails)

Let m = B

R_{sys} = R_B x P(system works | B works) + (1- R_B) x P(system works | B fails)

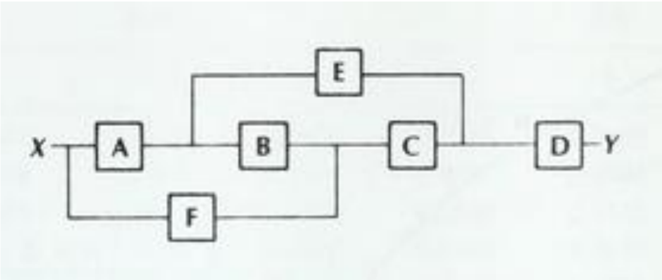


P(system works | B fails) =
{ R_D [1 – (1- $R_A R_E$) (1- $R_F R_C$)]}

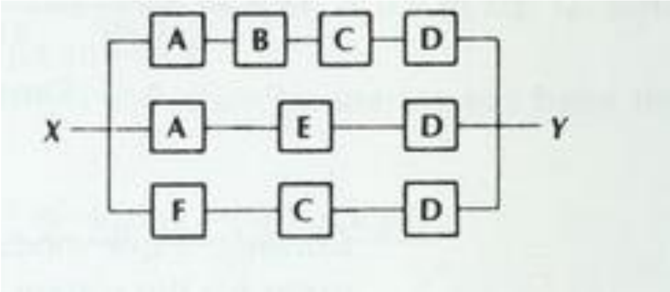


P(system works | B works) must be further reduced

Non-series/non-parallel upper-limit



From: D. P. Siewiorek R.S. Swarz, Reliable Computer Systems, Prentice Hall, 1992



all paths in parallel

Upper-bound:

$$R_{Sys} <= 1- P_i\,(1-R_{path\ i})$$

Upper-bound because paths are not independent, the failure of a single module affects more than one path (close approximation if paths are small)

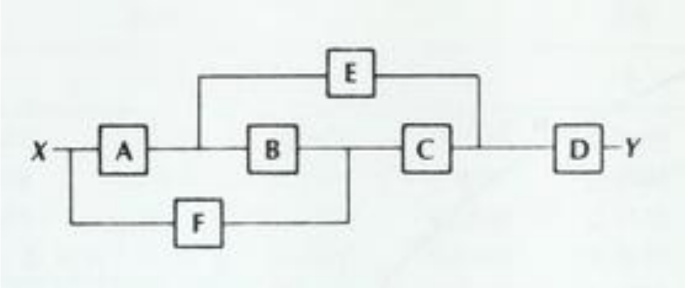
Upper-bound:

$$R_{Sys} <= 1- (1- R_A R_B R_C R_D)\,(1- R_A R_E R_D)\,(1- R_F R_C R_D)$$

Non-series/non-parallel lower-limit

- Minimal cut sets of the system

- Minimal cut set : is a list of components such that removal of any component from the list will cause the system to change from operational to failed



From: D. P. Siewiorek R.S. Swarz, Reliable Computer Systems, Prentice Hall, 1992

Minimal cut sets:
{D}{A,F}{E,C}{A,C}{BEF}

Lower-bound:

$$R_{Sys} >= \Pi_i (1 - Q_{cut\ i}) = \Pi_i\ R_{cut\ i}$$

where $Q_{cut\ i}$ is the probability that the cut i does not occur

Fault tree analysis

Fault tree analysis (FT) is a failure analysis in which an undesired state of the system (e.g., a catastrophic failure) is analyzed using boolean logic to combine a series of lower-level events.

describe the scenarios of occurrence of events at abstract level, linking the hierarchy of levels of events by logical gates

This method allows to study how the system can fail.

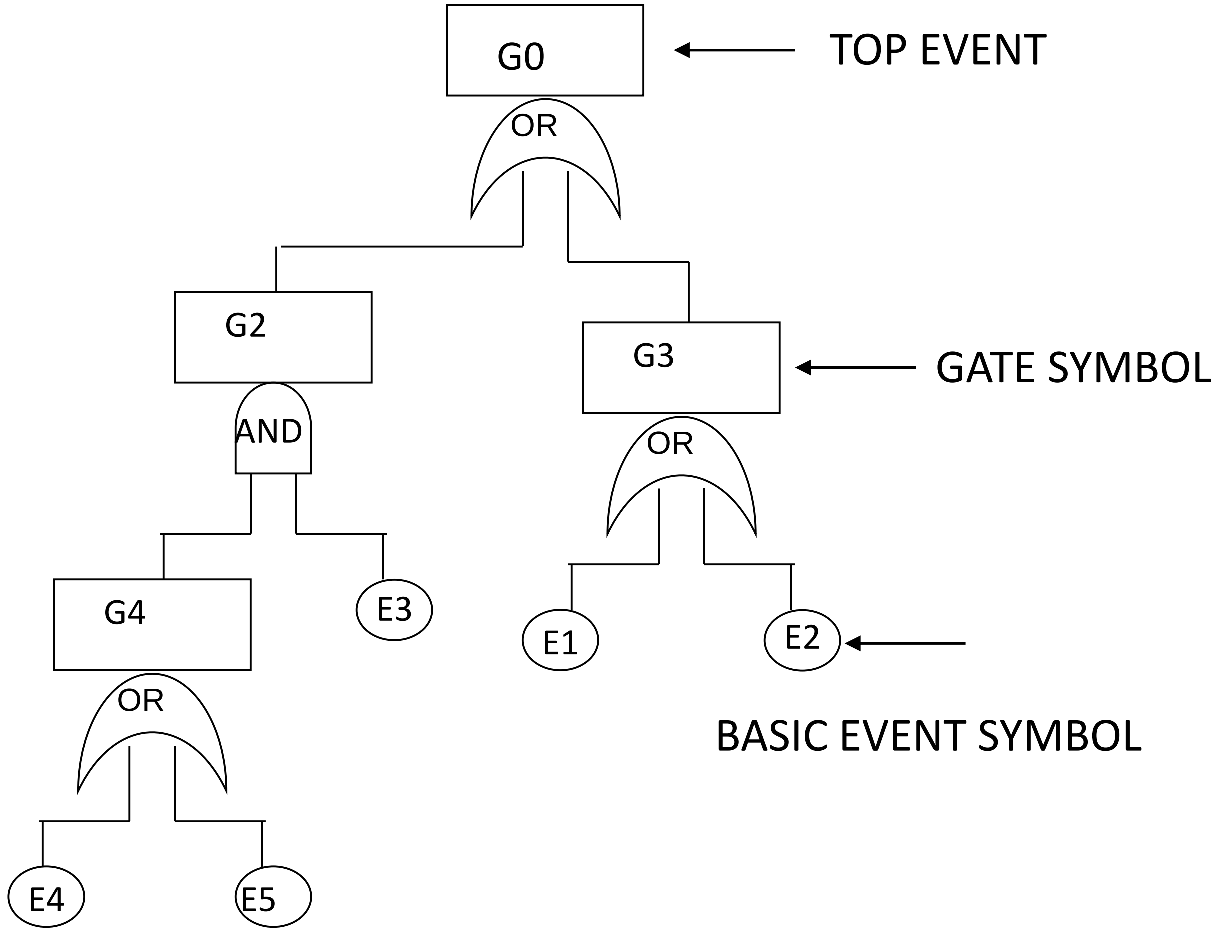
Technique applied in industry

Fault Trees

A fault tree describes the Top Event (status of the system) in terms of the status (faulty/non faulty) of the Basic events.

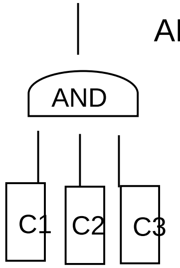
The basic events are the system's components

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)



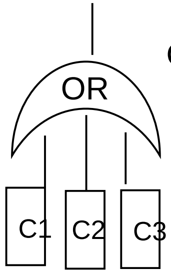
Fault Trees

GATES



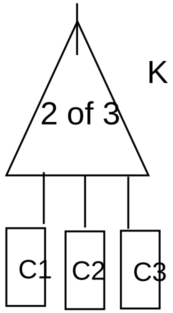
AND gate

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

Faulty component corresponds to logical value **true**, otherwise **false**

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

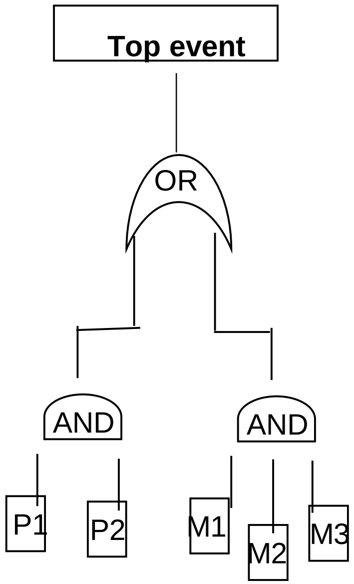
The system fails if the root is true

Fault Trees

Example

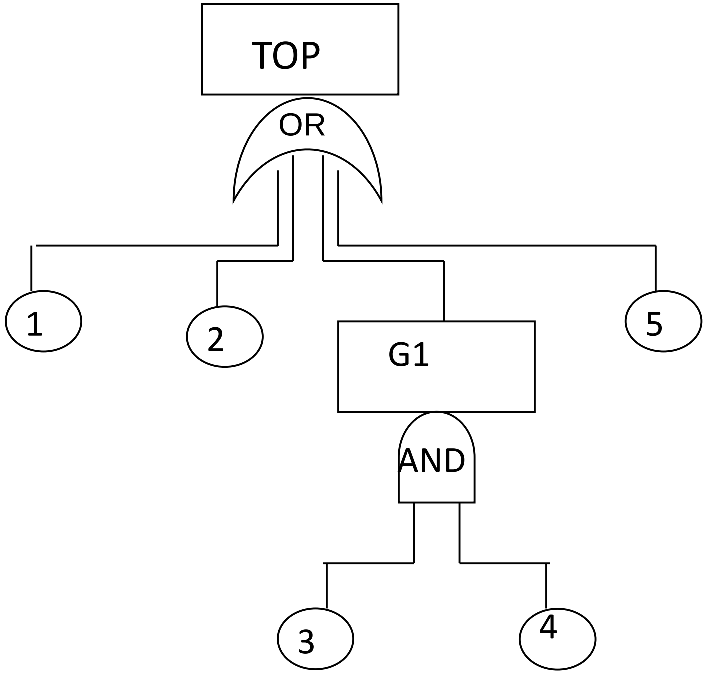
Multiprocessor with 2 processors and three shared memories

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



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

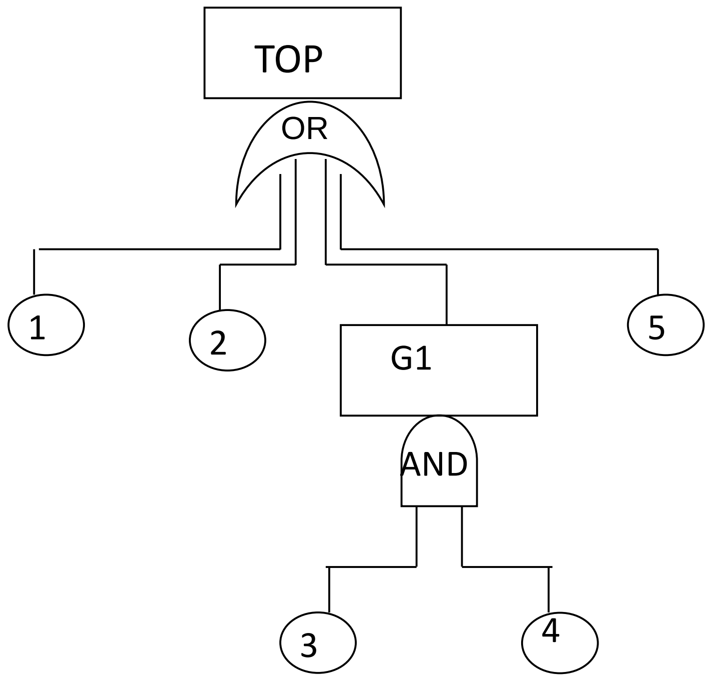
Cut Sets

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}

Assumption: independent faults of the components

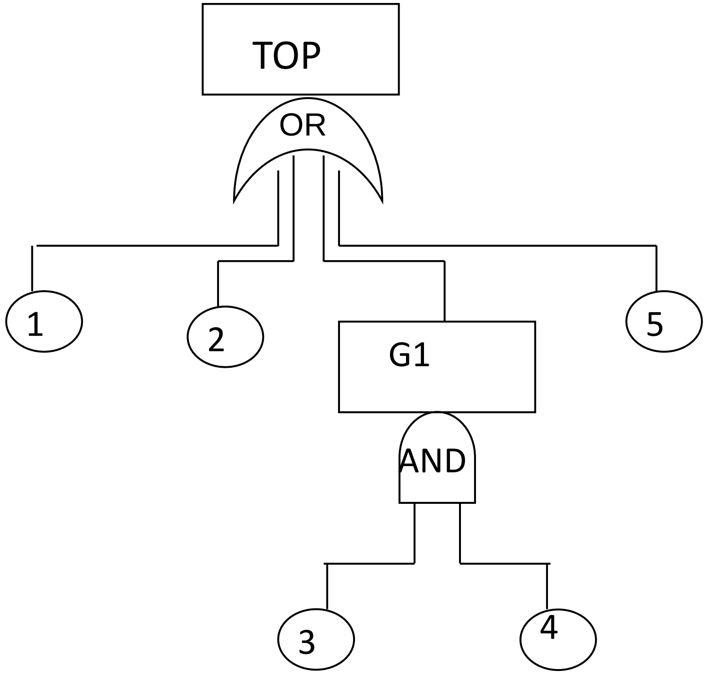
$Q_S(t)$ = probability that all components in the minimal cut set S are faulty

$Q_S(t) = q_1(t)\, q_2(t) \dots q_n(t)$ with S ={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

$\Sigma\, Q_{Si}(t)$

Minimal cut sets



Minimal Cut Sets

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

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

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

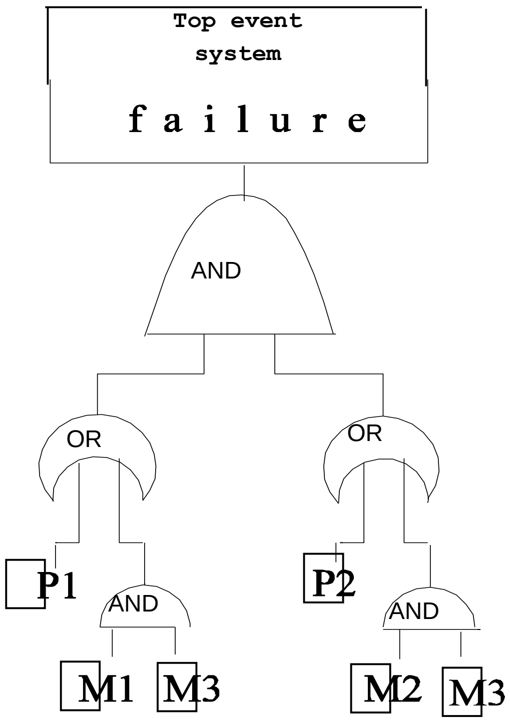
n number of mininal cut sets

- minimal cuts with a single event identify a critical situations

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

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

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

Fault Trees

FT technique allows the identification of critical paths in 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

Failure mode and effects analysis

Failure Mode Effect Analysis (FMEA) is a failure analysis for identifying the risk of failure of a system (or a component)

Vulnerability to single failures is analysed (FMEA does not consider multiple failures)

Combination of knowledge about
all possible failures, the effects, the cause and the possible actions to be taken

Calculate the risk priority number (RPN), in terms of severity of the failure, occurrence of the failure and detectability of the failure

Technique applied in industry

Failure mode and effects analysis

- Identify the **functionality** of the system
- Identify possible failures of the system. In particular, identify all the potential **failure modes.**

Define a Table with the following information :

For each failure mode,

1.1) enumerate the **potential effects of the failure**
identify all the effects (consequences) on the components and on the system.

1.2) rank the **severity (S)** of each effect. Severity is usually rated on a scale from 1 to 10, where 1 is insignificant and 10 is catastrophic.

Failure mode and effects analysis

For each **failure mode**:

2.1 list all possible **causes** of the failure
identify the reasons for the failure

2.2 rank the occurrence (O) of the cause of the failure.
Occurrence is usually rated on a scale from 1 to 10,
where 1 is extremely unlikely and 10 is inevitable.

Failure mode and effects analysis

For each **cause** of the failure:

3.1 list the current **process controls**

tests, procedures or mechanisms that might prevent the cause from happening, reduce the probability that it will happen or detect failure after the cause has already happened but before the customer is affected.

3.2 Rank the **detection rating** (D) of the cause or its failure mode before the customer is affected.

Detection is usually rated on a scale from 1 to 10, where 1 means the control always detects the problem and 10 means the control does not detect the problem (or no control exists).

Failure mode and effects analysis

Build the FMA table with the previous information

Calculate the risk priority number, or RPN

$$RPN = S \times O \times D.$$

Calculate Criticality by multiplying severity by occurrence

$$S \times O$$

An example

FMEA performed by a Bank on ATM (Automated Teller machine) system

Function	Potential failure mode	Potential effects of failure	S	Potential causes of failure	O	Current process control	D	RPN
Dispence amount of cash requested by customer	Does not dispence cash	Customer very dissatisfed	8	Out of cash	5	Internal low-cash alert	5	200
		Incorrect entry to demand deposit system		Machine jams	3	Internal jam alert	10	240
		Discrepancy in cash balancing		Power failure during transaction	2	None	10	160
	Dispense too much cash	Bank loses money	6	Bills stuck together	2	Loading procedure	7	84
		Discrepancy in cash balancing		Denominations in wrong trays	3	Two persons visual veriifcation	4	72
	Takes too long to dispence cash	Customer somewhat annoyed	3	Heavy computer network traffic	7	None	10	210
				Power interruption during transaction	2	None	10	60

From: http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html

Failure mode and effects analysis

FMEA table provides guidance

- for ranking potential failures in the order they should be addressed.

- For identifying recommended actions. These actions may be additional controls to improve detection.

Note that:
FMEA allows to associate a cause, i.e., the failure mode of a simple component, to the system failure event.

Fault Trees / Failure mode and effects analysis

Fault-trees often used in conjunction with FMEA

- FMEA
  vulnerability to single failures is analysed
  (FMEA does not consider multiple failures)

- FT
  allows to describe the case in which the occurrence of an event depends on multiple failures

State-based models

State-based models

"Reliability depends on the frequency of faults and the duration of faults in the system"

Series/Parallel models: relate the reliability of the system to the system structure and to the reliability of its components. If there is a path from the input node to the output node the system behaves correctly. If there is a failed component on a path, the path is broken. Duration of faults is not considered.

State-based models: enumerate the system states. Can be used for Reliability and Availability measures

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

```
 |------------------------------|--    no failures in the interval [t0, t]
t0                              t
```

Availability - A(t)

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

```
|------------XXXXX--------------XXX-------------------------|--    failures and repairs
t0          [t1….t2]           [t3…t4]                      t       in  the interval [t0, t]
             f     r             f    r
```

State-based models

Characterize the state of the system changing over time

1. Each state represents a distinct combination of failed and working modules

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

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

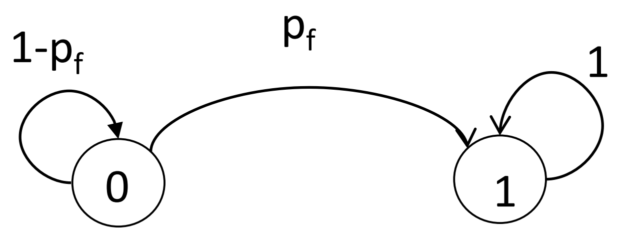
4. The time between a fault and a repair is the duration of the fault inside the system

State-based models

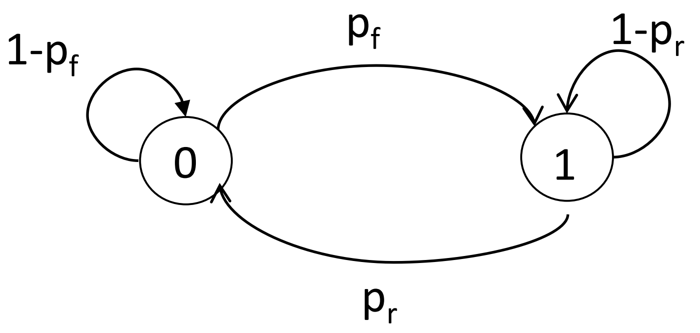
graph where nodes are all the possible states and arcs are the possible transitions between states. Arcs are labeled with a probability function

State: number working and faulty modules

Example:
System that consists of one module



Reliability model



Availability model

The module can be
- working (state 0)
- faulty (state 1)

- pf: probability of failure
- pr: probability of repair

Random process

In probability theory, a **random process** is defined as a family of random variables indexed by numbers expressing points in time

Example of random process: $\{X_t\}$, with time $t = \{0, 1, 2, 3. ...\}$

Let X be the result of tossing a die.
$\{X_t\}$ represents the sequence of results of tossing a die

$P[X_0 = 4] = 1/6$
$P[X_4 = 4 \mid X_2 = 2] = P[X_4 = 4] = 1/6$

$S=\{1,2,3,4,5,6\}$ state space

P probability

Independent random variables

Dependability measures: these variables represent the values of the state of the system randomly changing over time

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 $X_0 X_1 \ldots\ldots\ldots\ldots X_t$

Markov process

$$P\{X_{t+1}=j \mid X_0=j_0, \ldots, X_{t-1}=j_{i-1}, \ldots, X_t=i\} = P\{X_{t+1}=j \mid X_t=i\}$$

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

The conditional probability is called transition probability from state i to state j at time t

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

Markov property: "the current state is enough to determine the future state"

Markov process

Steady-state transition probability: the transition probabilities are steady-state if for any pair of states i and j, the probability of transition between i and j does not depend by the time.

$$P\{X_{t+1}=j \mid X_t=i\} = P\{X_1=j \mid X_0=i\} \quad \text{for all } t >= 0$$

This probability is called p_{ij}

$$p_{i\,j} = P\{X_1=j \mid X_0=i\}$$

Markov process

A stochastic process $\{X_t\}$, with time t = {0, 1, 2, 3. …}, with a numerable set S of states, is called **Markov chain** if satisfies the Markov property

A Markov chain is called **homogeneous** if satisfies the property of steady-state probability, **non-homogeneous** otherwise

A Makov chain is **finite-state** if the set of possible states is finite

A finite-state Markov chain has a representation by a matrix

We consider homogeneous Markov chains

if t = {0, 1, 2, 3. …}, we have discrete time Markov chains (DTMC)

DTMC: Transition probability matrix

The following matrix is called the transition probability matrix P (nxn)

$$
P = \begin{array}{cc} & j \\ i & \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \cdots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} \end{array}
$$

- n number of states of the chain
- i, j are states (numbered starting from 1 to n)
- 0 <= pij <= 1

$p_{i\,j}$ = probability of moving from state i to state j in one step

$$p_{i\,j} = P\,\{X_1 = j \mid X_0 = i\}$$

row i of P: probability of making a transition starting from initial state i
column j of P: probability of making a transition from any state to final state j

DTMC: Transition probability matrix

The transition probability matrix P satisfies the following property

Let $u = [1, 1, 1, ..., 1]^T$

$$P \; u = u$$

$$P = \begin{array}{cc} & \begin{array}{ccc} & j & \end{array} \\ i & \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \cdots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} \end{array}$$

This follows by the condition that the sum of the elements of each raw of the matrix is 1

$$\Sigma_j \; p_{ij} = 1 \;\; \text{for all } i$$

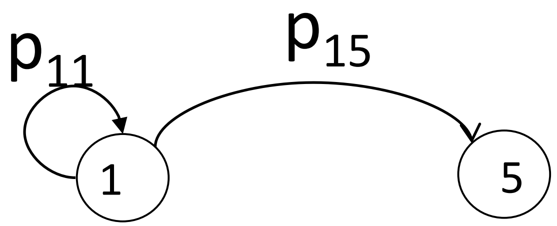
This sum represents the probability of moving from state i into any state in S

Non-negative matrices such that Pu=u are called stochastic matrices

DTMC: graph associated to the chain

$$P = \begin{array}{cc} & \begin{array}{ccc} \phantom{p_{11}} & j & \phantom{p_{1n}} \end{array} \\ i & \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \cdots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} \end{array}$$

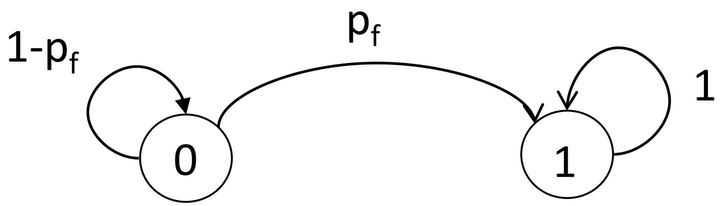
Each state of the Markov chain is a node
Each $p_{i\,j}$ >=0 corresponds to a directed
Edge from node i to node j



Example: simplex system

State 0 : working
State 1: failed

p_f Failure probability



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

- all state transitions occur at fixed intervals
- probabilities assigned to each transition

Transition probability matrix P

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

next state

$$P = \begin{array}{c c} & \begin{array}{cc} 0 & 1 \end{array} \\ \begin{array}{c} 0 \\ 1 \end{array} & \left[\begin{array}{cc} 1-p_f & p_f \\ 0 & 1 \end{array}\right] \end{array}$$

current state

DTMC: transition probability after n steps

Theorem

For each pair of states i and j, and n >= 0:

$$P\{X_{t+n}=j \mid X_t=i\} = P\{X_n=j \mid X_0=i\} \quad \text{for all } t \geq 0$$

Steady-state transition probabilities after n steps :

$$p_{ij}^{(n)} = P\{X_n=j \mid X_0=i\} \quad \text{for all } t \geq 0$$

DTMC: transition probability after n steps

Definitions

$$p_{ij}^{(0)} = P\{X_0=j \mid X_0=i\} = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{otherwise} \end{cases}$$

$$p_{ij}^{(1)} = P\{X_1=j \mid X_0=i\} = p_{ij}$$

$$p_{ij}^{(n)} = P\{X_n=j \mid X_0=i\} \quad \text{for all } t >= 0$$

Properties

$$0 <= p_{ij}^{(n)} <= 1 \quad \text{for all } i,j$$

$$\Sigma_j\, p_{ij}^{(n)} = \Sigma_j\, P\{X_n=j \mid X_0=i\} = 1 \quad \text{for all } i$$

DTMC: transition probability after n steps

Theorem (Chapman-Kolmogorov)

For each pair of states i and j, and for each n, m >= 1:

$$p_{ij}^{(n+m)} = \Sigma_k \, p_{ik}^{(n)} \, p_{kj}^{(m)}$$

$P^{(0)} = I$

$P^{(1)} = P$

$P^{(n)} = P^n$

It can be proved that: $P^{(n+m)} = P^{(n)} P^{(m)}$

Since $P^{(k)} = P^{(k-1)} P^{(1)} = P^{(k-1)} P$

$P^{(n)} = P \, . \, \ldots \, P = P^n$ the n-th power of P

$P^{(n)}$ is a stochastic matrix: $P^{(n)} u = P^{(n-1)} P u = P^{(n-1)} u = \ldots . \, P \, u = u$

DTMC: sojourn time in a state i

Random variable T_i

$$P\{T_i=n\} = p_{ii}^{(n-1)}(1-p_{ii})$$

Probability that, when the system enter the state i, the system remains in state i for n >=1 consecutive steps

Geometric distribution of parameter p_{ii}

$$P\{T_i > n\} = p_{ii}^{(n)}$$

$$E[T_i]= \frac{1}{(1-p_{ii})}$$

DTMC: probability distribution at time t

Probability of being in a given state after a number of time steps

States numbered starting from 0 for readbility

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

where $\pi_i(t)$ is the probability that $\{X_t = i\}$

Initial state occupancy vector $\quad \pi(0) = (\pi_0(0), \pi_1(0), \ldots)$

$\pi(1) = \pi(0)\, P$ state occupancy vector after one step

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

....

$\pi(t) = \pi(t-1)\, P$ state occupancy vector after t step

DTMC: transient analysis

A Markov process can be specified in terms of the **state occupancy vector** π and the transition probability matrix P (transient behavior)

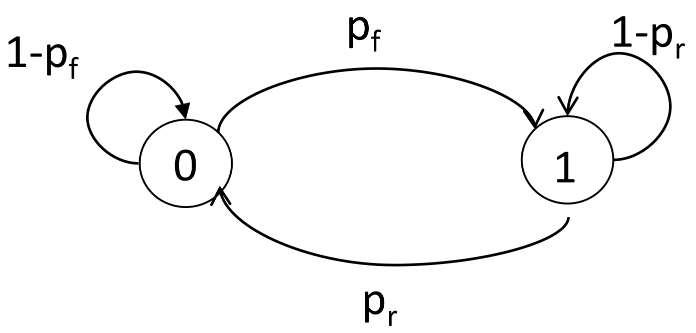
$$\pi(t) = \pi(0)\, \mathrm{P}^t$$

Simplex system with repair

State 0 : working
State 1: failed

p_f Failure probability

p_r Repair probability



$$
P = \begin{array}{c c}
 & \begin{array}{cc} 0 & 1 \end{array} \text{ next state} \\
\begin{array}{c} 0 \\ 1 \end{array} & \begin{bmatrix} 1-p_f & p_f \\ p_r & 1-p_r \end{bmatrix}
\end{array}
$$

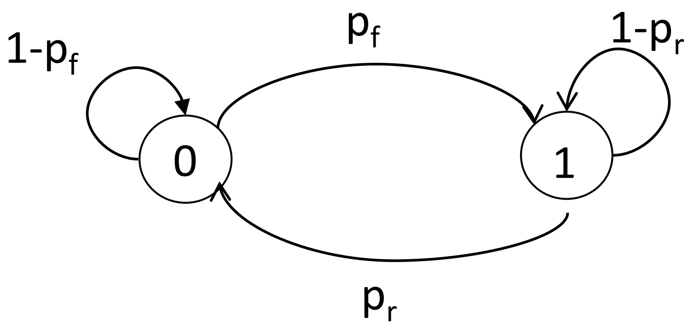
current state

Simplex system with repair

$$\pi(0) = (\pi_0(0), \pi_1(0))$$

probability of being in a state at the beginning

$$\pi(1) = \pi(0) \begin{bmatrix} 1-p_f & p_f \\ p_r & 1-p_r \end{bmatrix}$$



probability of being in a state after 1 time-step

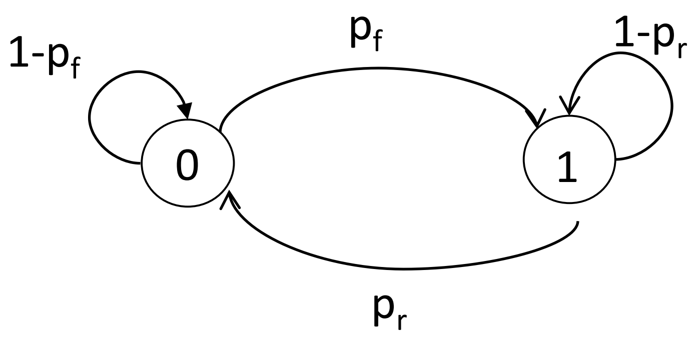
$$\pi(t) = \pi(t-1) \begin{bmatrix} 1-p_f & p_f \\ p_r & 1-p_r \end{bmatrix}$$

probability of being in a state after t time-steps

Simplex system with repair

$\pi(0) = [1, 0]$ initial state: working

$$P = \begin{bmatrix} 0.9 & 0.1 \\ 0.5 & 0.5 \end{bmatrix}$$



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

probability of being in state 0 after 1 time-step is 0.9

DTMC

$S=\{0, 1\}$

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

$X_0 = 0$ prob. 1
$X_0 = 1$ prob. 0

$X_1 = 0$ prob. 0.9
$X_1 = 1$ prob. 0.1

………………………

$X_t = 0$ prob that the system 's state is 0 at time t

$$\pi(2) = [0.9, 0.1] \begin{bmatrix} 0.9 & 0.1 \\ 0.5 & 0.5 \end{bmatrix} = [0.86, 0.14]$$

probability of being in state 0 after 2 time-step is 0.86

$$P^2 = \begin{bmatrix} 0.86 & 0.14 \\ 0.70 & 0.3 \end{bmatrix}$$

DTMC: Limiting behaviour

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.

DTMC: classification of states

A state j is said to be **accessible** from state i if there exists t >0 such that

$$P_{ij}^{(t)} > 0, \qquad \text{we write } i\text{->}j$$

A Markov chain is **irreducible** if for all the states i, j:
- state i is accessible from j in a finite number of time steps
- and state j is accessible from i in a finite number of time steps

for each i, j: i -> j and j -> i

A **irriducible** Markov chain consists of only one equivalence class of communicating states

DTMC: classification of states

A state i is **recurrent** if

for each j: (i->j) implies (j->i)

process moves again to state i with probability 1

A state i is **transient** if

exists (j!=i) such that (i->j) and not (j->i)

A state i is **absorbent** if

$p_{ii}=1$

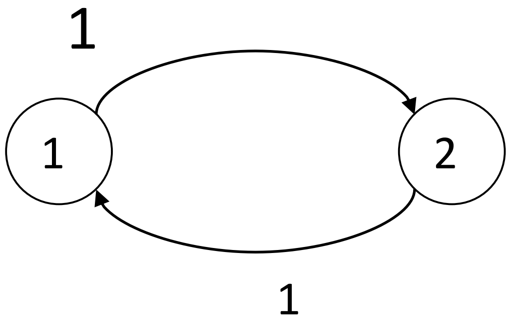
An absorbent state is also a recurrent state

DTMC: classification of states

Given a **recurrent** state, let d be the greatest common divisor of all the integers m such that $P_{ii}^{(m)} > 0$

A recurrent state i is **periodic** if d > 1

A recurrent state i is **aperiodic** if d = 1: it is possible to move to the same state in one step



state 1 is periodic with period d=2

state 2 is periodic with period d=2

If $p_{ii} > 0$ then the state i is **aperiodic**

DTMC: Steady-state behaviour

THEOREM: For **irreducible aperiodic** Markov chain
for each j $\lim_{t \to \infty} \pi_j^{(t)}$

exists and the solution is independent from $\pi^{(0)}$

The **steady-state behaviour** of the Markov chain is given by the fixpoint of the equation:

$$\pi(t) = \pi(t-1)\, P$$

with

$$\Sigma_j\, \pi_j = 1$$

Time-average state space distribution

Markov chains with periodic states

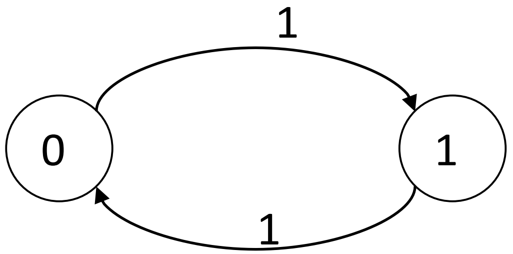
Initial state: working

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

$\pi(1) = \pi(0)\, P = (1,0) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = (0,1)$

$\pi(2) = \pi(1)\, P = (0,1) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = (1,0)$

………..



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

state i is periodic with period d=2

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

Limiting behaviour: time-average space distribution

Irreducible Markov chain with **periodic** states: the periodic state oscillates periodically. The limiting behaviour does not exist (caused by the probability of the periodic state)

We calculate the time-average state space distribution

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

From discrete-time to continuous-time Markov chain (CTMC)

- state transitions may occur at any time (random intervals)
- transitions are assigned **transition rates**

$\{X_t\}$, with t in T (an interval of real numbers)

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

From discrete-time to continuous-time Markov chain (CTMC)

$\{X_t\}$, with t in $\mathcal{T}$ =\{t1, t2, …\} ($\mathcal{T}$ is an interval of real numbers)

We consider steady-state transition probability (homogeneous chain)
for each t1, t2, … and for all $\tau >= 0$

$$P\{X_{t+\tau}=j \mid X_t=i\} = P\{X_\tau=j \mid X_0=i\}$$

The chain has a transition probability matrix.

Continuous-time Markov chain (CTMC)

T_i the time spent in a state

For the Markov property assumption,
T_i is a continuous random variable with exponential distribution

The value of this variable characterizes the behaviour of the CTMC

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

Continuous-time Markov chain (CTMC)

T_i the time spent in a state

The value of this variable characterizes the behaviour of the CTMC

For each state i, $T_i = e^{(-ai)}$

if $ai=0$, the state is **absorbent**

if $ai = \infty$, the state is **instantaneous**

if $0 < ai < \infty$, the state is **stable**

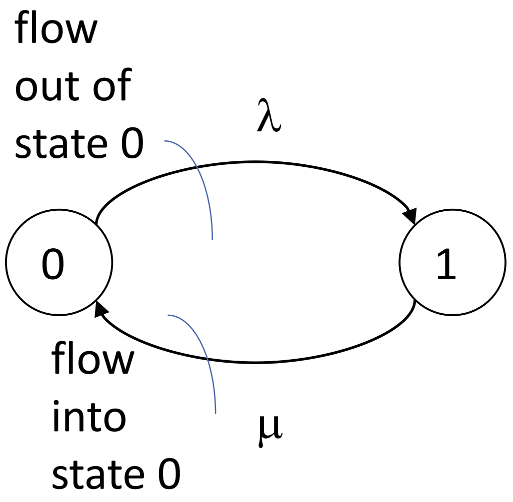
Continuous-time Markov chain (CTMC)

A CTMC can be specified in terms of the occupancy probability vector π and the state-transition-rate matrix Q

Simplex system with repair

state 0: working
state 1: failed

λ failure rate
μ repair rate



$\pi(t0) = [1, 0]$

$$Q = \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$

Flow
- out of a state
- into a state

Self-loops are not shown in the graph

$\pi(t1) = [?, \ ?]$

Probability of being in state 0 at time t1:
- minus the flow out of state 0 times the probability of being in state 0 at time t0,
- plus the flow into state 0 from state 1 times the probability of being in state 1 at time t0.
Similarly for state 1.

State-transition rate matrix Q

The matrix Q is defined as follows

$$
q_{ij} = \begin{cases} \text{rate of going from state } i \text{ to state } j & \text{if } (i \mathrel{!=} j) \\ -\sum_{k!=i} q_{ik} & \text{otherwise} \end{cases}
$$

the sum of each row must be zero

CTMC: transient and steady-state analysis

Mobius provides simulation and numerical solvers

- Simulation solver (to solve all models)

  statistically accurate solutions within a confidence interval

- Numerical solver (to solve models with exponential/deterministic distribution)
  limited to models that have small state-space
  numerical solvers provide exact solutions

Simplex system with repair: Availability

$\pi(t) = (\pi_0(t), \pi_1(t))$

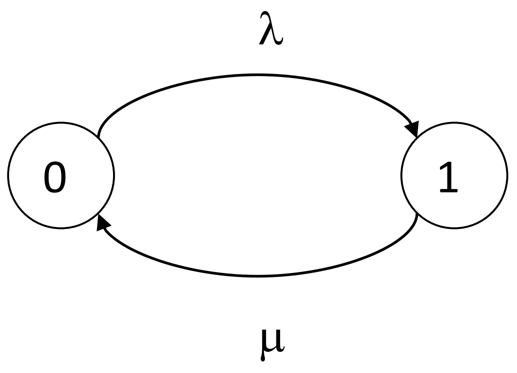
$\pi_0(t)$ is the probability that the system is in the operational state at time t, availability at time t

$A(t) = \pi_0(t)$

steady-state term

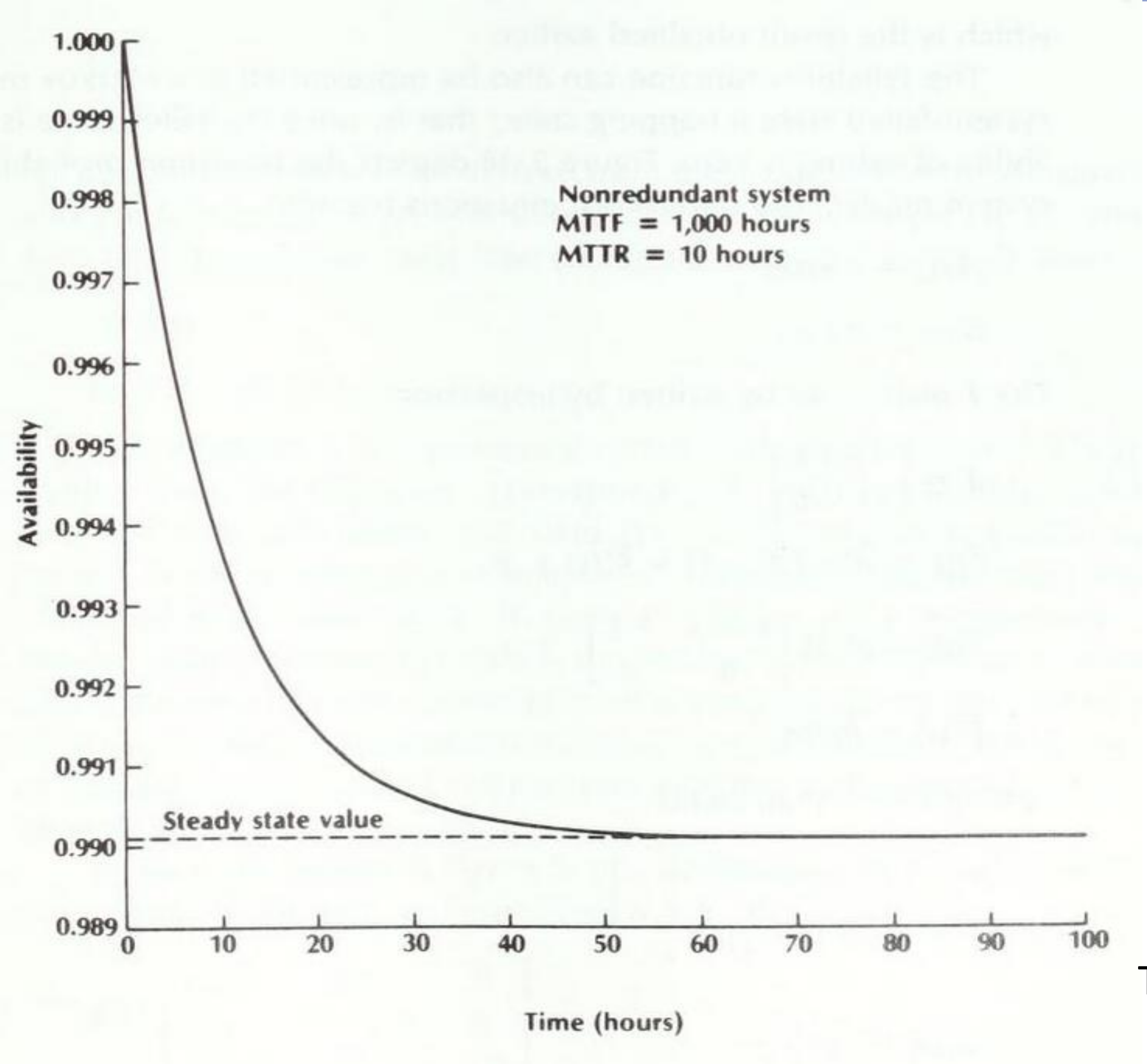
$$\boxed{\pi_0(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu) t}}$$

$$\pi_1(t) = \frac{\lambda}{\lambda + \mu} - \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu) t}$$



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

Availability as a function of time



$\lambda = 0.001$ (1/1000)
$\mu = 0.1$ (1/10)

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

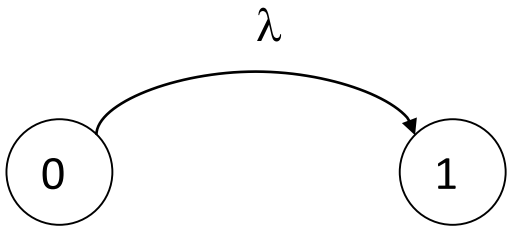
Taken from: [Siewiorek et al.1998]

Continuous-time Markov models: Reliability

Single system without repair

failed state as trapping state

λ = failure rate



$\pi(t0) = [1, 0]$

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

Reliability $R(t) = \pi_0(t) = e^{-\lambda t}$

Unreliability $Q(t) = \pi_1(t) = 1 - e^{-\lambda t}$

TMR system with repair

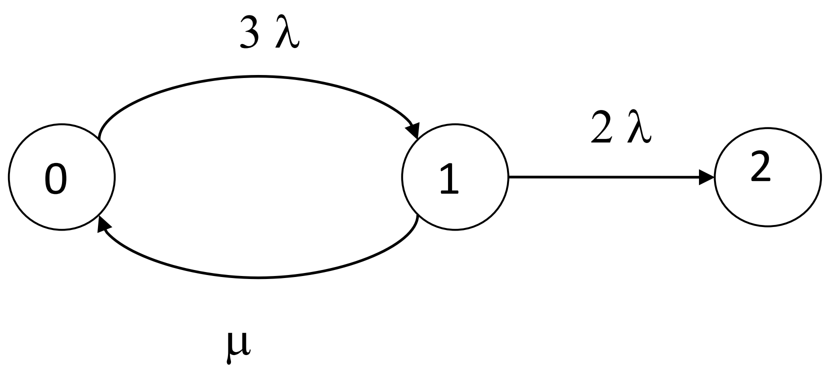
Rates: λ and μ

Identification of states:

3 processors working, 0 failed

2 processors working, 1 failed

1 processor working, 2 failed

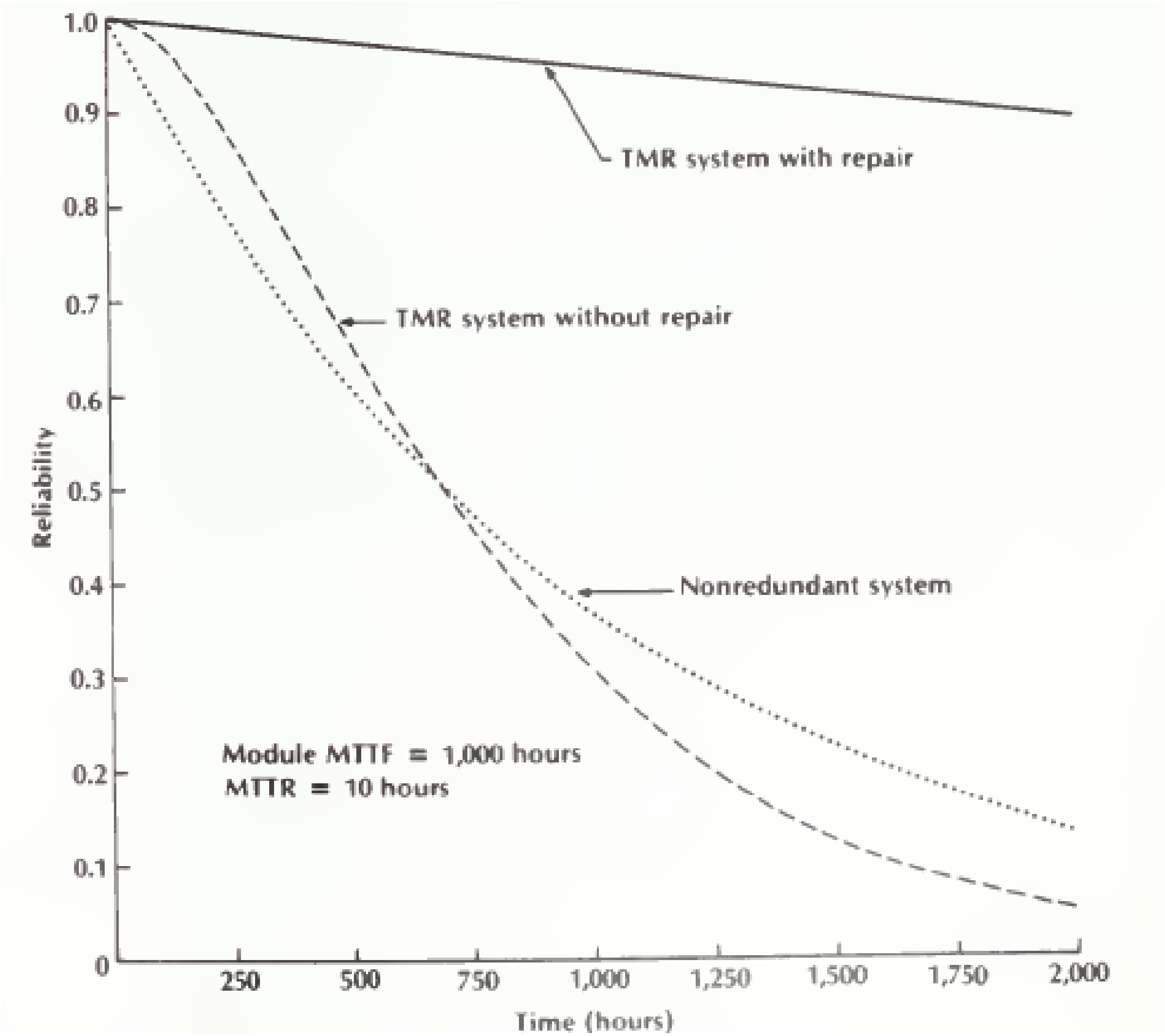


$\pi(0) = [1, 0, 0]$

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

Reliability $R(t) = 1- \pi_2(t)$

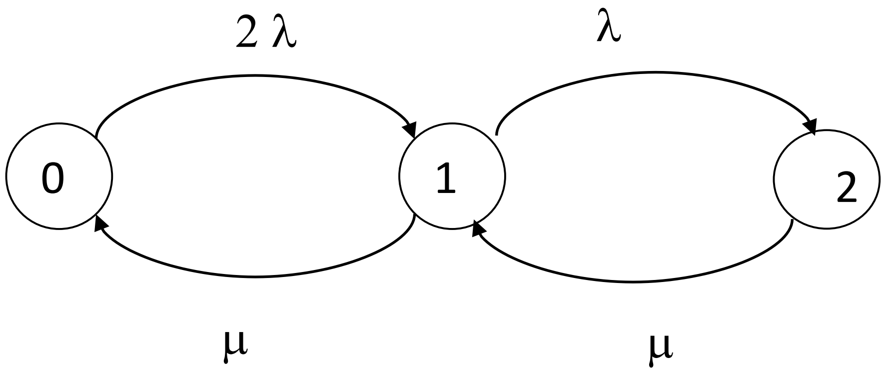
Comparison with nonredundant system and TMR without/with repair



Taken from: [Siewiorek et al.1998]

Dual processor system with repair: Availability model

A, B processors
Failure rates: λ
Repair rate: μ



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

$$Q = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & \mu & -\mu \end{bmatrix}$$

Identification of states:
- A, B working: state 0
- B working, A failed: state 1
- A working, B failed: state 1
- A, B failed: state 2

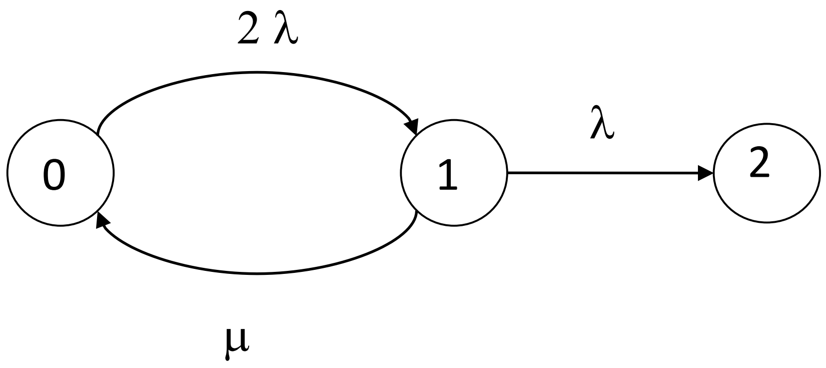
Availability $\quad A(t) = 1- \pi_2(t)$

Steady-state Availability $\quad Ass = \dfrac{2\lambda\mu + \mu^2}{2\lambda^2 + 2\lambda\mu + \mu^2}$

Build the model assuming different failure/repair rates for A and B

Dual processor system with repair: Reliability model

making state 2 a trapping state



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

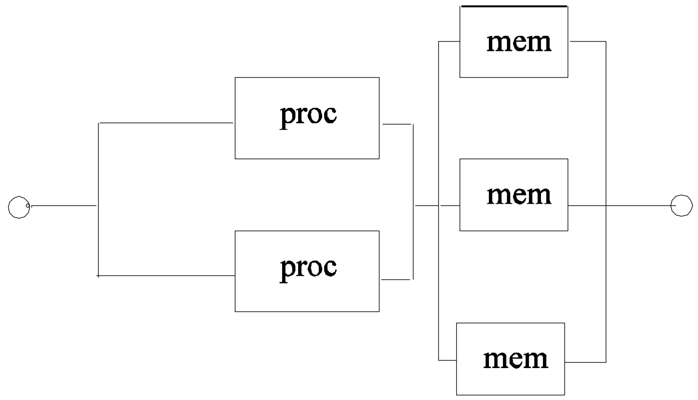
$$Q = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & 0 & 0 \end{bmatrix}$$

Reliability $R(t) = 1 - \pi_2(t)$

$R(t) = \pi_0(t) + \pi_1(t)$

Another example of modelling (CTMC)

Multiprocessor system with 2 processors and 3 shared memories system.
System is operational if at least one processor and one memory are operational.



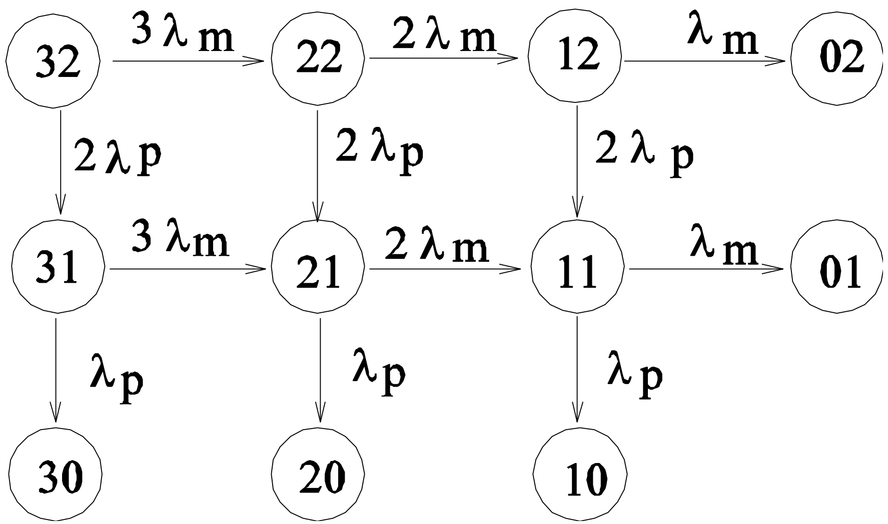
λ_m failure rate for memory
λ_p failure rate for processor

X random process that represents the number of operational memories and the number of operational processors at time t

Given a state (i, j):
i is the number of operational memories;
j is the number of operational processors

S = {(3,2), (3,1), (3,0), (2,2), (2,1), (2,0), (1,2), (1,1), (1,0), (0,2), (0,1)}

A example of modelling (CTMC): Reliability



λ_m failure rate for memory

λ_p failure rate for processor

(3, 2) -> (2,2) failure of one memory

(3,0), (2,0), (1,0), (0,2), (0,1) are absorbent states

A example of modelling (CTMC): Availability

Assume that faulty components are replaced and we evaluate the probability that the system is operational at time t

Constant repair rate μ (number of expected repairs in a unit of time)

Strategy of repair:

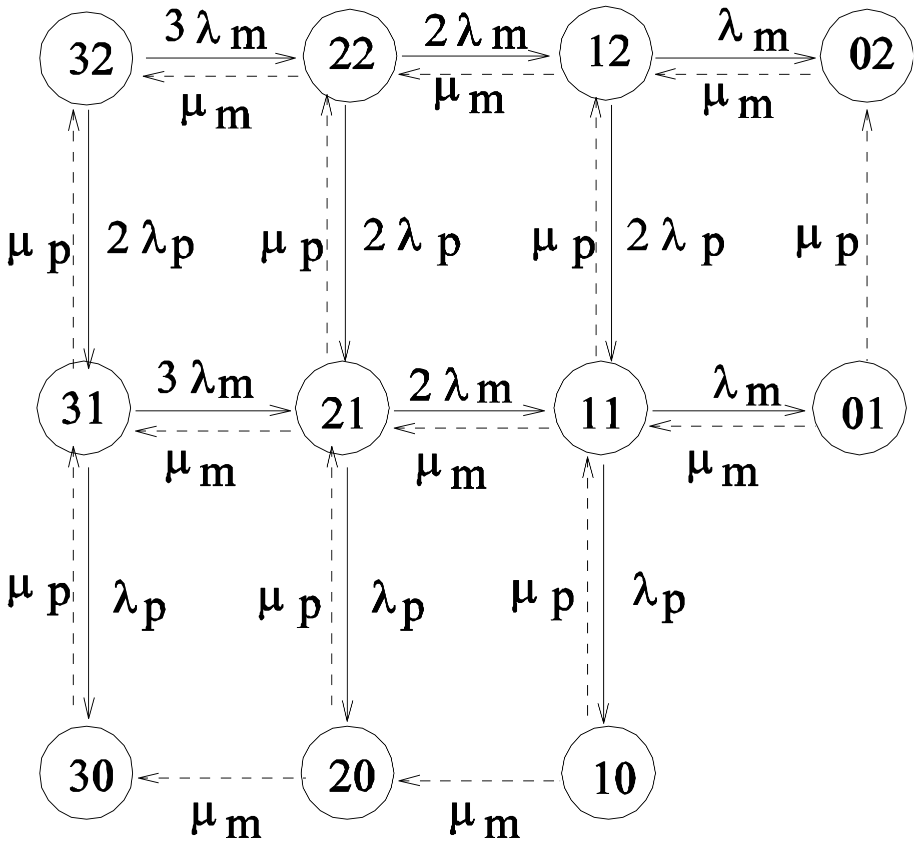
only one processor or one memory at a time can be substituted

The behaviour of components (with respect of being operational or failed) is not independent: it depends on whether or not other components are in a failure state.

A example of modelling (CTMC): Availability

Strategy of repair:

only one component can be substituted at a time



λm failure rate for memory

λp failure rate for processor

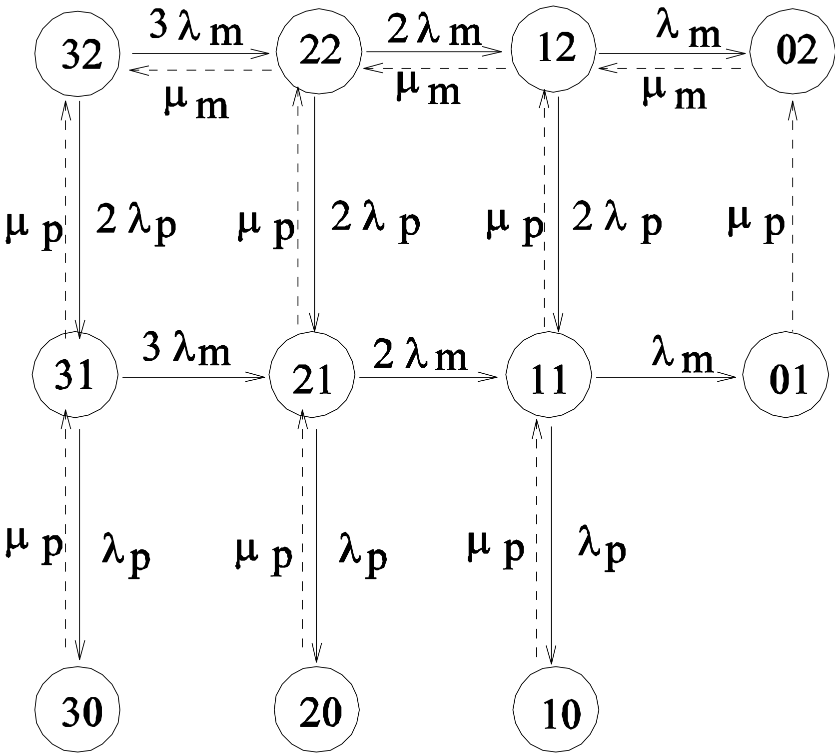
μm repair rate for memory

μp repair rate for processor

A example of modelling (CTMC): Availability

An alternative strategy of repair:

- only one component can be substituted at a time and processors have higher priority
- exclude the lines μm representing memory repair in the case where there has been a process failure

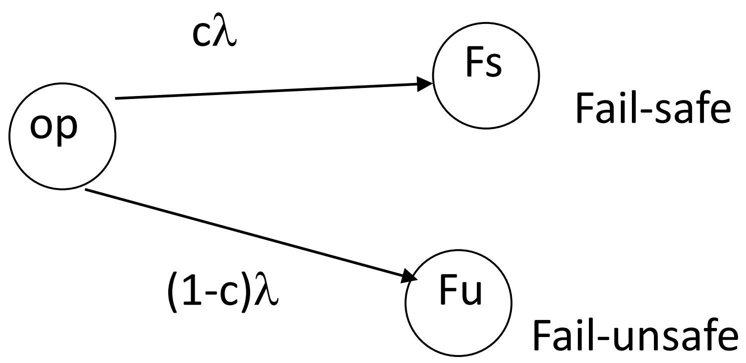


Safety

Safety - avoidance of catastrophic consequences -

As a function of time, S(t), is the probability that the system either behaves correctly or will discontinue its functions in a manner that causes no harm (operational or Fail-safe)

Coverage – The coverage is the measure **c** of the system ability to reach a fail-safe state after a fault.

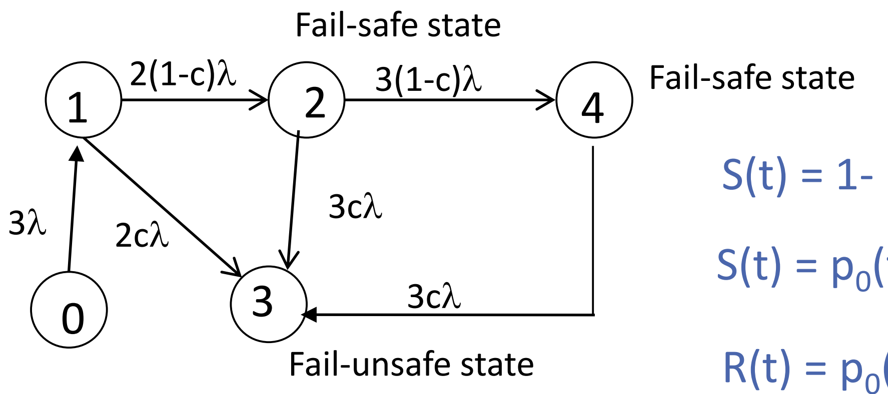


Modeling coverage in a Markov chain means that every un-failed state has two transitions to two different states, one of which is fail-safe, the other is fail-unsafe.

A example of modelling (CTMC): Safety

the system can be in a safe state although the failures of two components, if the output of the three components disagree

c = probability of coincident failures of two components



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

$S(t) = p_0(t) + p_1(t) + p_2(t) + p_4(t)$

$R(t) = p_0(t) + p_1(t)$

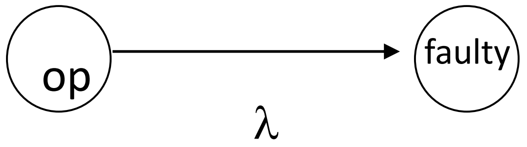
0 three correct components
1 one faulty component
2 two faulty components (no coincident failures)
3 two faulty component coincident failures
4 three faulty components (no coincident failures)

Summary

Reliability - R(t), is the conditional probability that the system performs correctly throughout the interval of time [0, t], given that the system was performing correctly at time 0

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

with λ constant failure rate.



Failure rate - The failure rate is the expected number of failures of a type of device per a given time period (e.g. $\lambda = 1/1000$, one failure per 1000 hours)

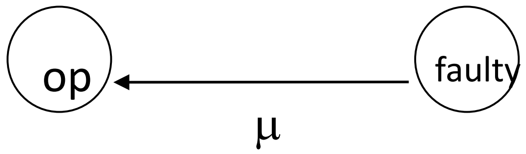
MTTF – The Mean Time To Failure is the expected time that a system will operate before the first failure occurs (e.g., 1000 hours)

$$MTT = 1/\lambda$$

Summary

MTTR - The Mean Time To Repair is the average time required to repair the system.
MTTR is expressed in terms of a repair rate m which is the average number of repairs that occur per time period, generally number of repairs per hours

$$\mu = 1/MTTR$$



Maintenability - M(t) is the conditional probability that the system is repaired throughout the interval of time [0, t], given that the system was faulty at time 0

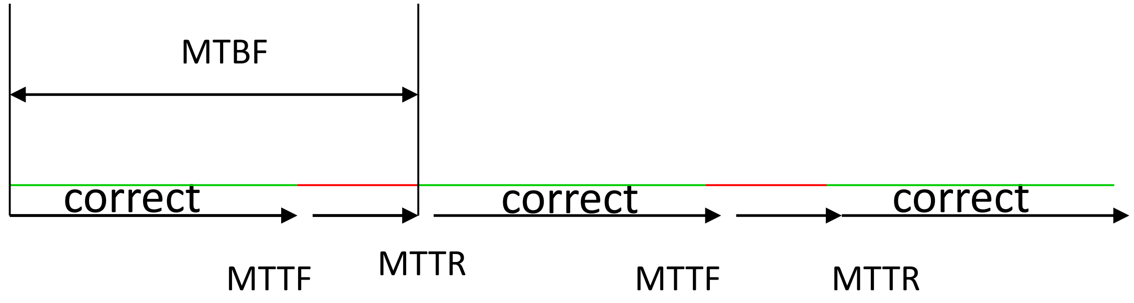
$$M(t) = 1 - e^{-\mu t}$$

with μ constant repair rate.

Summary

Mean Time Between Failures - The MTBF is the average time between failures of the system, including the time required to repair the system and place it back into an operational status

$$MTBF = MTTF + MTTR$$



Steady-state Availability: Simplex system

$$A(\infty) = \frac{\mu}{(\lambda + \mu)} \qquad A(\infty)=0 \quad \text{if } \mu = 0$$

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

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

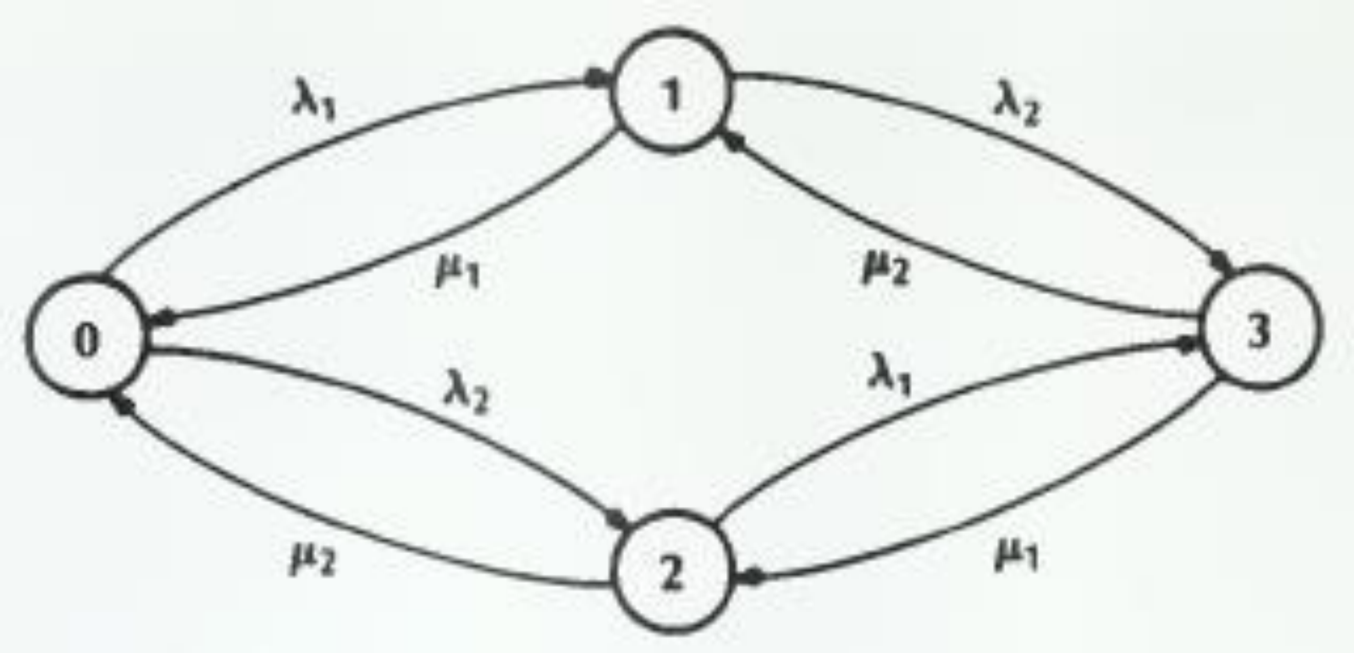
Identification of states:

A, B working: state 0

B working, A failed: state 1

A working, B failed: state 2

A, B failed: state 3



Availability

$A(t) = \pi_0(t) + \pi_1(t) + \pi_2(t)$

$A(t) = 1- \pi_3(t)(t)$