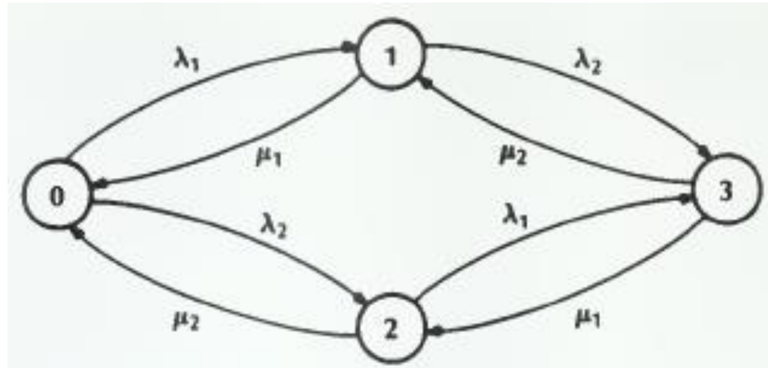
Dual processor system with repair

A, B processors

Rates: λ1, λ2 and μ1, μ2

Identification of states:

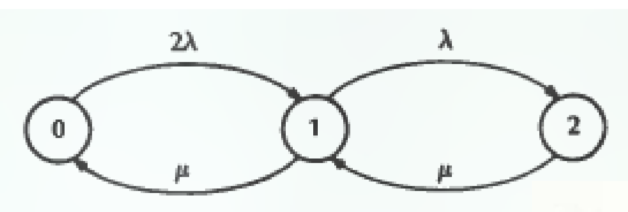
- A, B working
- A working, B failed
- B working, A failed
- A, B failed



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

Collapsed model

Single repair at a time



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

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

Availability

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

Laplace transform

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

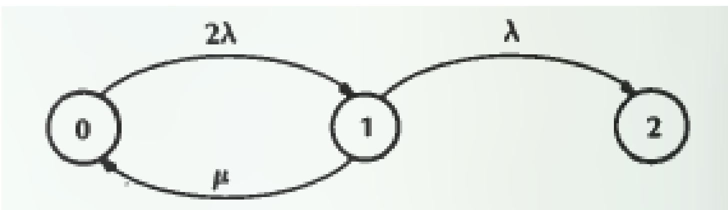
$$A_{ss} = \frac{2\lambda\mu + \mu^2}{2\lambda^2 + 2\lambda\mu + \mu^2}$$

steady-state availability

Reliability modeling

- making state 2 a trapping state

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



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

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

Laplace transform

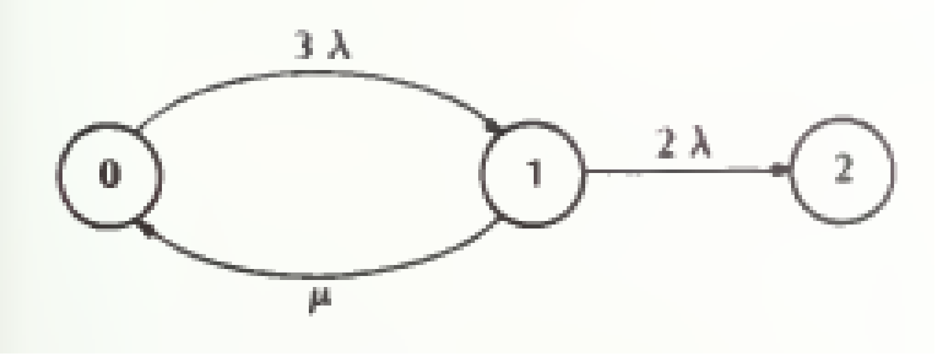
$$R(t) = \frac{4\lambda^2 \exp\left(-(1/2)(3\lambda + \mu - \sqrt{\lambda^2 + 6\lambda\mu + \mu^2})t\right)}{(3\lambda + \mu)\sqrt{\lambda^2 + 6\lambda\mu + \mu^2} - \lambda^2 - 6\lambda\mu - \mu^2} - \frac{4\lambda^2 \exp\left(-(1/2)(3\lambda + \mu + \sqrt{\lambda^2 + 6\lambda\mu + \mu^2})t\right)}{(3\lambda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

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

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



Transition rate matrix:

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

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

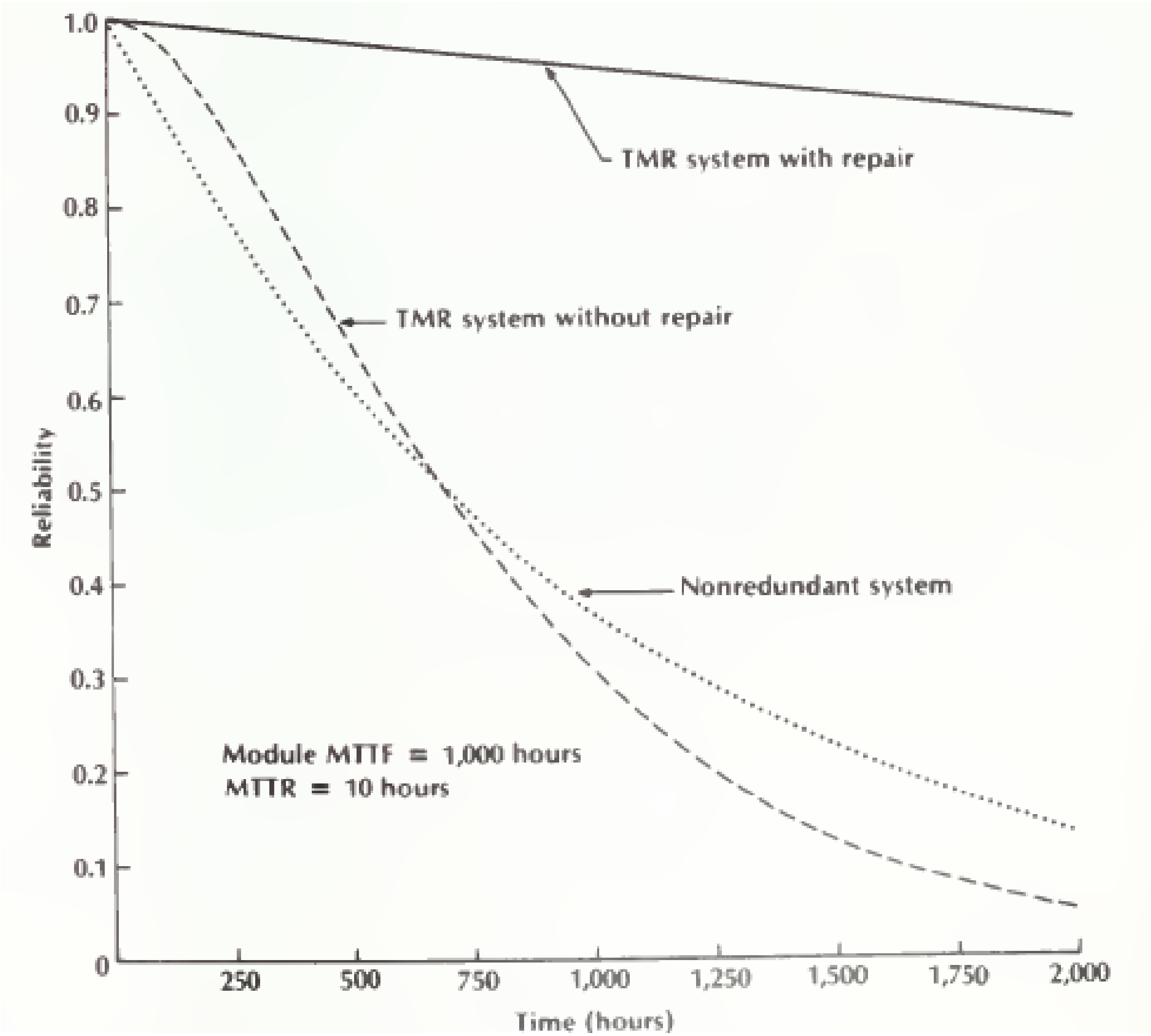
From: D. P. Siewiorek R.S. Swarz, Reliable Computer Systems, Prentice Hall, 1992

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

Laplace transform

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

Comparison with nonredundant system and TMR without repair



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

MTTF

$$MTTF = \int_{t=0}^{\infty} R(t)\, dt$$

period the system is in a state that correspond to correct behavior

TMR with repair:

$$MTTF = \int_{t=0}^{\infty} p_0(t) + p_1(t)\ dt$$

failure rate $\lambda = 0.001$
repair rate $\mu = 0.1$

$$\text{TMR with repair MTTF} = \frac{5}{6\lambda} + \frac{\mu}{6\lambda^2} = 17{,}5000 \text{ hours}$$

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

MTTF is equal to the MTTF of a TMR system without repair plus an additional term due to the repair activity.

$$\text{Nonredundant MTTF} = \frac{1}{\lambda} = 1000 \text{ hours}$$

$$\text{TMR without repair MTTF} = \frac{5}{6\lambda} = 833 \text{ hours}$$

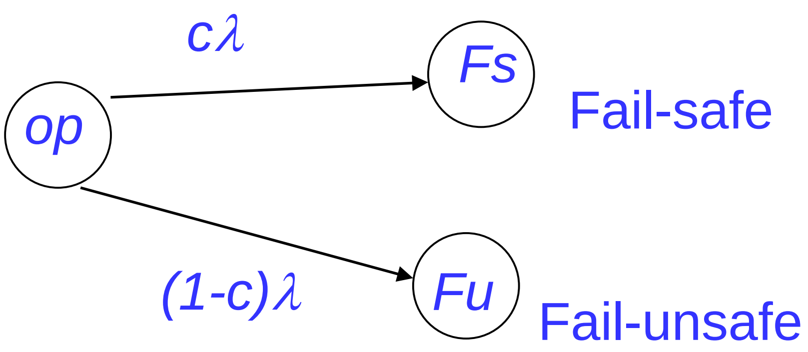
on-line repair allows the system MTTF to increase by a factor of 17

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.

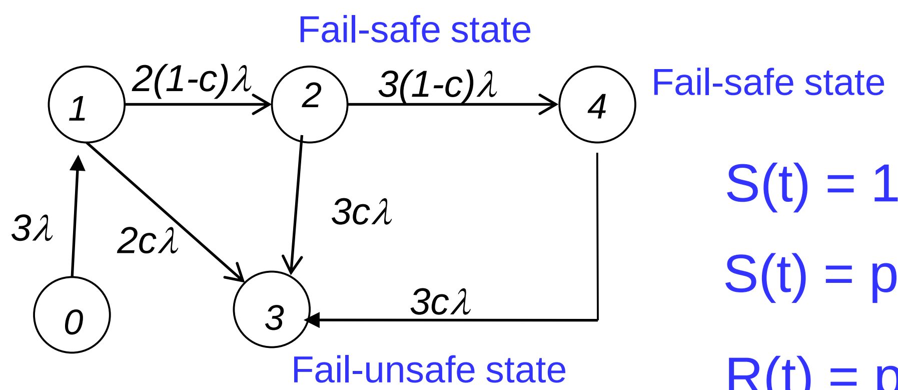
Modeling coverage and safety in a Markov chain means that every unfailed state has two transitions to two different states, one of which is fail-safe, the other is fail-unsafe.



TMR

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)

Observations

Quantitative dependability evaluation:

- guiding design decisions
- assessing systems as built
- mandatory for safety critical systems

Model construction techniques

-> scalability challenge

- **composition approaches**

  build complex models in a modular way through a composition of its submodels

- **decomposition/aggregation approaches**

  (hierarchical decomposition approach)

  The overall model is decoupled in simpler and more tractable submodels, and the measures obtained from the solution of the sub-models are then aggregated to compute those concerning the overall model.