KUNGL TEKNISKA HÖGSKOLAN

VETENSKAP OCH KONST

International Master Program in System-on-Chip Design

Evaluation Techniques

Two approaches

- Qualitative evaluation
  - aims to identify, classify and rank the failure modes, or event combinations that would lead to system failures
- Quantitative evaluation
  - aims to evaluate in terms of probabilities the attributes of dependability (reliability, availability, safety)

Common dependability measures

- failure rate
- mean time to failure
- mean time to repair
- mean time between failures
- fault coverage

Failure rate

- failure rate
  - expected # of failures per time-unit
  - example
    - 1000 controllers working at t_0
    - after 10 hours: 950 working
    - failure rate for each controller:
      0.005 failures / hour
      (50 failures / 1000 controllers) / 10 hours

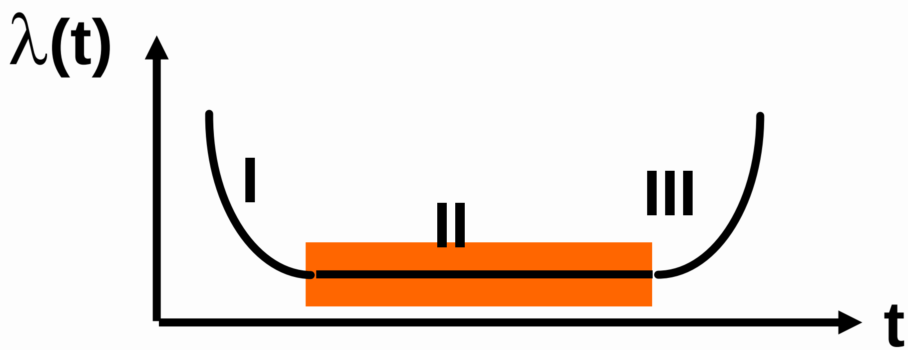
Failure rate and reliability

Reliability R(t) is the conditional probability that the system will perform correctly throughout [0,t], given that it worked at time 0

$$R(t) = \frac{N_{operating}(t)}{N_{operating}(t) + N_{failed}(t)}$$

Failure rate

- typical evolution of λ(t) for hardware:



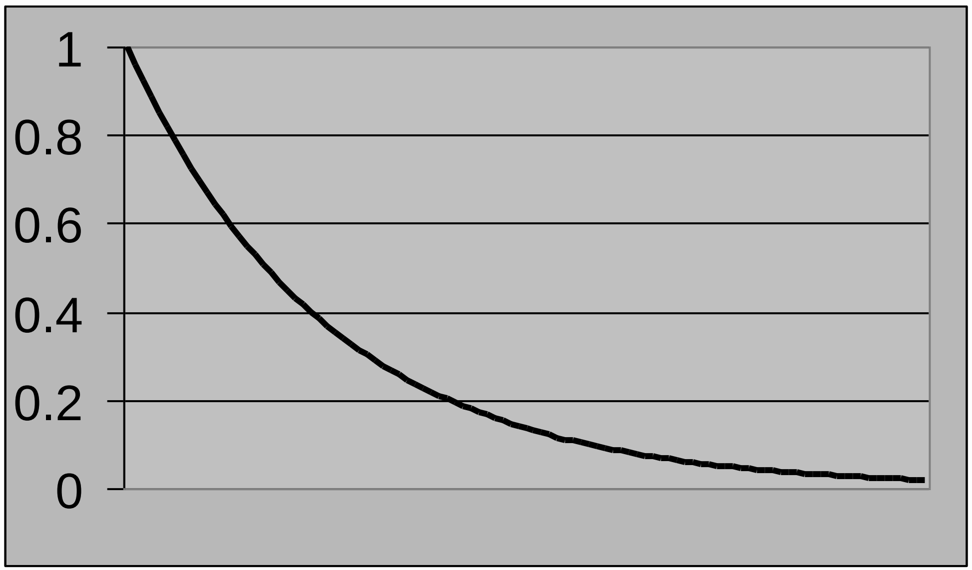
- bathtub: I infant mortality, II useful life, III wear-out
- for useful life period λ = constant, the reliability is given by

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

Exponential failure law

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

If λ is constant, R(t) varies exponentially as a function of time



Time varying failure rate

- Failure rate is not always constant
  - software failure rate decreases as package matures
- Weibull distribution:

$$z(t) = \alpha\lambda(\lambda t)^{\alpha-1}$$

- if α=1, then z(t) = constant = λ
  if α>1, then z(t) increases as time increases
  if α<1, then z(t) decreases as time increases

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

Failure rate calculation

- determined for components
  - systems: combination of components
  - λ of the system = sum of λ of the components
- determine λ experimentally
  - slow
    - e.g. 1 failure per 100 000 hours (=11.4 years)
  - expensive
    - many components required for significance
- use standards for λ

MTTF

- MTTF: mean time to failure
  - expected time until the first failure occurs
- If we have a system of N identical components and we measure the time t_i before each component fails, then MTTF is given by

$$MTTF = \frac{1}{N} \cdot \sum_{i=1}^{N} t_i$$

MTTF

MTTF is defined in terms of reliability as:

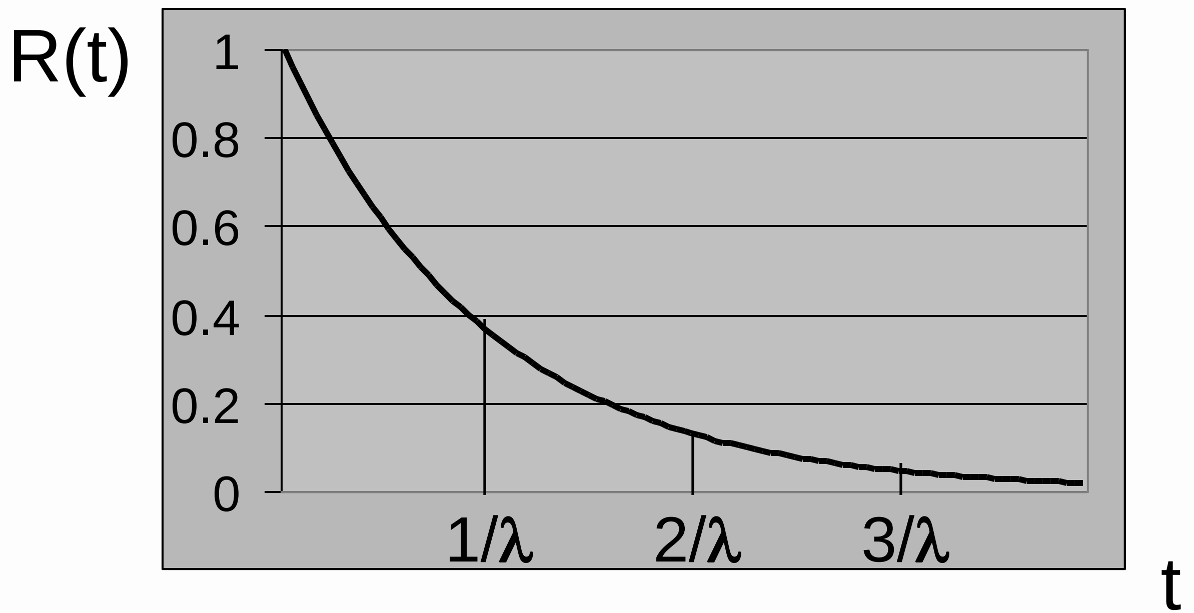
$$MTTF = \int_0^{\infty} R(t)dt$$

If R(t) obeys the exponential failure law, then MTTF is the inverse of the failure rate:

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

MTTF

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



MTTF

- MTTF is meaningful only for systems which operate without repair until they experience a failure
- Most of mission-critical systems a undergo a complete check-up before the next mission
  - all failed redundant components are replaced
  - system is returned to fully operational state
- When evaluating reliability of such system, mission time rather then MTTF is used

MTTR

- MTTR: mean time to repair
  - expected time until repaired
- If we have a system of N identical components and i_{th} component requires time t_i to repair, then MTTR is given by

$$MTTR = \frac{1}{N} \cdot \sum_{i=1}^{N} t_i$$

MTTR

- difficult to calculate
- determined experimentally
- normally specified in terms of repair rate repair rate μ, which is the average number of repairs that occur per time period

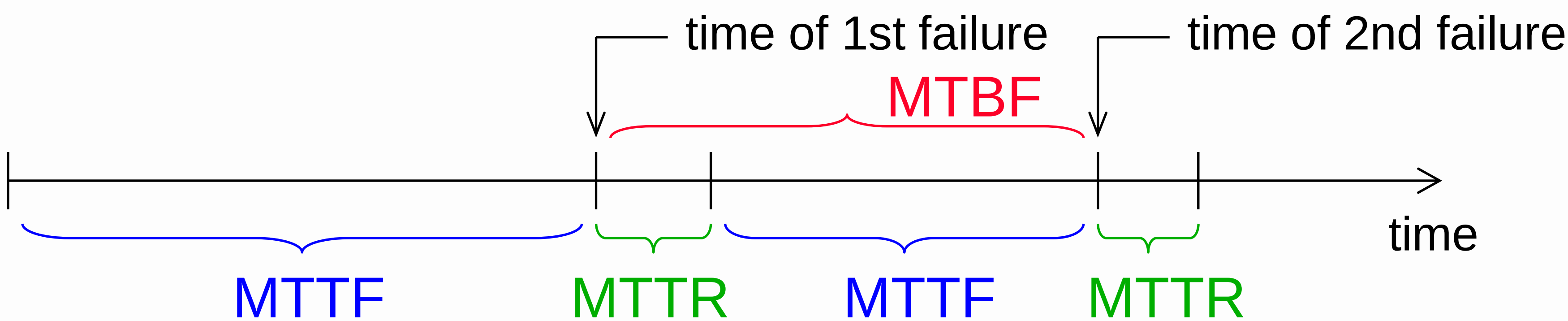
$$MTTR = \frac{1}{\mu}$$

MTTR

- Low MTTR requirement implies high operational cost
  - if hardware spares are kept on cite and the cite is maintained 24hr a day, MTTR=30min
  - if the cite is maintained 8hr 5 days a week, MTTR = 3 days
  - if system is remotely located MTTR = 2 weeks

MTBF

- MTBF: mean time between failures
    - functional + repair
    - MTBF = MTTF + MTTR
  – small time difference: MTBF ≈ MTTF
  – conceptual difference



Fault coverage

- Fault detection coverage is the conditional probability that, given the existence of a fault, the fault is detected
- Difficult to calculate
- Usually computed as

$$C = \frac{\text{number of faults which can be detected}}{\text{total number of faults}}$$

Example

- Suppose your circuit has 10 lines and you use single-stuck at fault as a model
- Then the total number of faults is 20
- Suppose you have 1 undetectable fault
- Then the coverage is

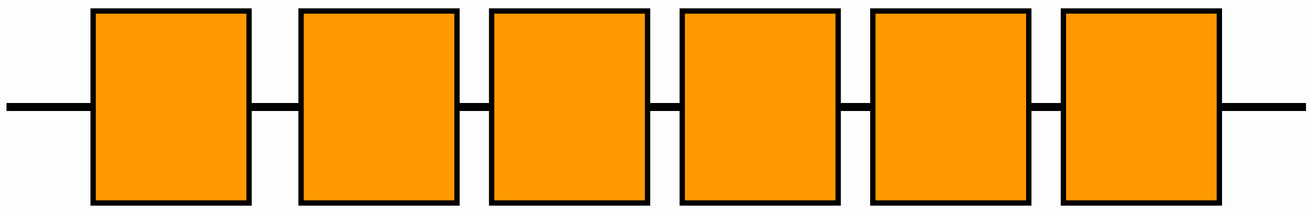
$$C = \frac{19}{20}$$

Dependability modelling

- up to now: λ and R(t) for components
- systems are sets of components
- system evaluation approaches:
  - reliability block diagrams
  - Markov processes

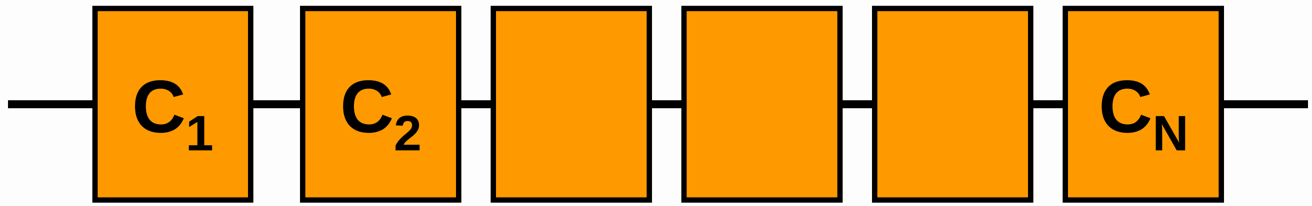
Serial system

- system functions
  if and only if all components function



reliability block diagram (RBD)

Serial system



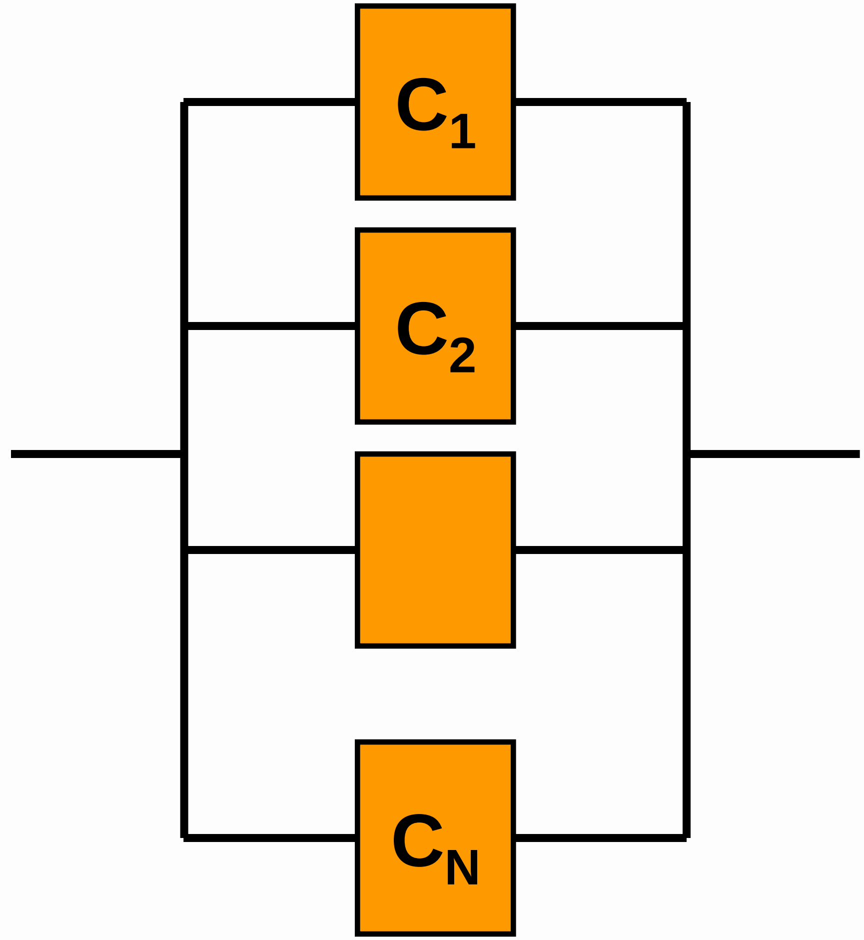
if C_i are independent:

$$R_{series}(t) = \prod R_i(t)$$

$$\lambda_{series} = \sum_{i=1}^{N} \lambda_i$$

Parallel system

- system works as long as one component works



Parallel system

unreliabity: Q(t) = 1 - R(t)

if C_i are independent: $$Q_{parallel}(t) = \prod_{i=1}^{N} Q_i(t)$$

$$R_{parallel}(t) = 1 - \prod_{i=1}^{N} \left(1 - R_i(t)\right)$$

Reliability block diagram

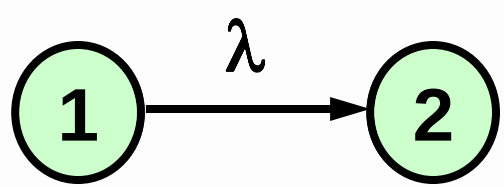
- RBD
  - may be difficult to build
  - equations get complex
  - difficult to take coverage into account
  - difficult to represent repair
  - not possible to represent dependency between components

Markov chains

- Markov chains
  - illustrated by state transition diagrams
- idea:
  - states
    - components working or not
  - state transitions
    - when components fail or get repaired

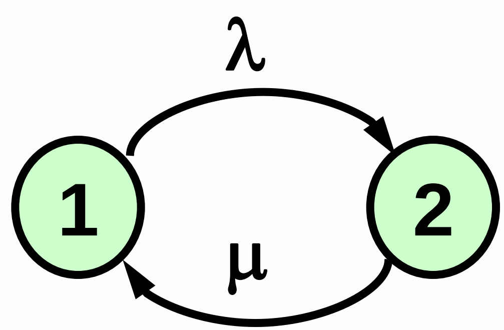
Single-component system, no repair

- Only two states
  - one operational (state 1) and one failed (state 2)
  - if no repair is allow, there is a single, non-reversible transition between the states (used in availability analysis)
  - label λ corresponds to the failure rate of the component



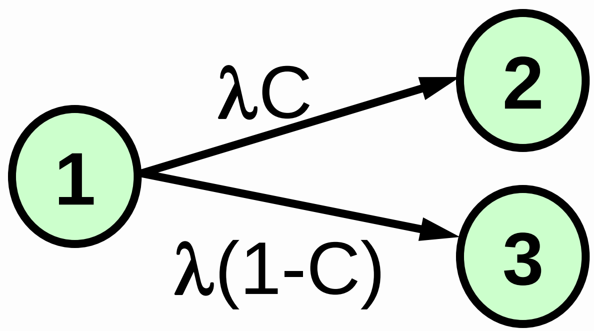
Single-component system with repair

- If repair is allowed (used in availability analysis)
  - then a transition between the failed and the operational state is possible
  - the label is the repair rate μ



Failed-safe and failed-unsafe

- In safety analysis, we need to distinguish between failed-safe and failed-unsafe states
  - let 2 be a failed-safe state and 3 be a failed-unsafe state
  - the transition between the 1 and 2 depends on failure rate and the probability that, if a fault occurs, it is detected and handled appropriately (i.e. fault coverage C)
  - if C is the probability that a fault is detected, 1-C is the probability that a fault is not detected



Two-component system

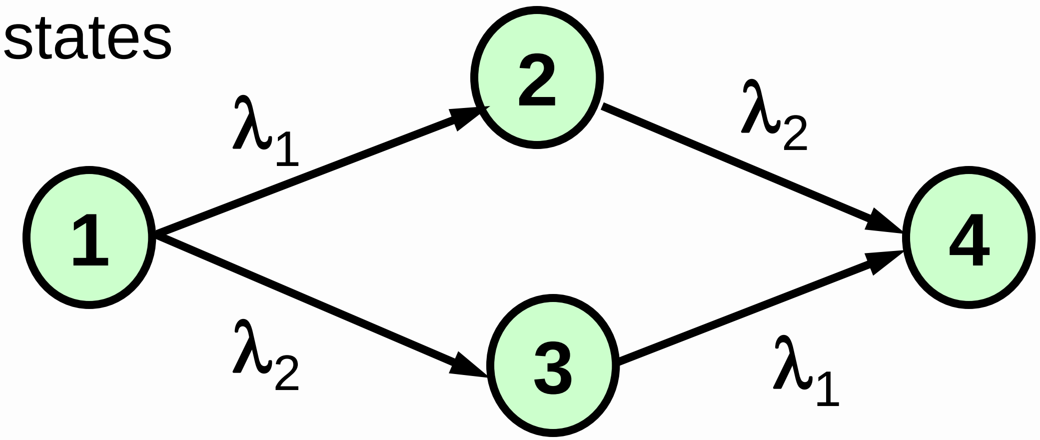
- Has four possible states

  O O state 1

  F O state 2

  O F state 3

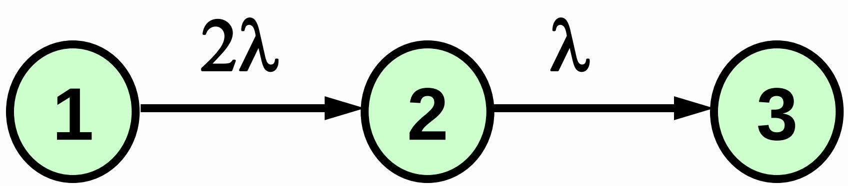
  F F state 4



- Components are assumed to be independent and non-repairable
- If components are in serial
  – state 1 is operational state, states 2,3,4 are failed states
- If components are in parallel
  – states 1,2,3 are operational states, state 4 is failed state

State transition diagram simplification

- Suppose two components are in parallel
- Suppose $\lambda_1 = \lambda_2 = \lambda$
- Then, it is not necessary to distinguish between between the states 2 and 3
  - both represent a condition where one component is operational and one is failed
  - since components are independent events, transition rate from state 1 to 2 is the sum of the two transition rates



Markov chain analysis

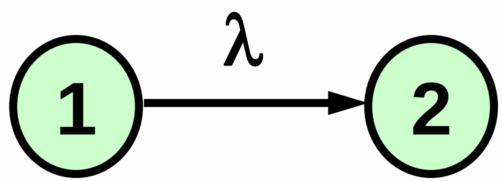
- The aim is to compute $P_i(t)$, the probability that the system is in the state i at time t
- Once $P_i(t)$ is known, the reliability, availability or safety of the system can be computed as a sum taken over all operating states
- To compute $P_i(t)$, we derive a set of differential equations, called state transition equations, one for each state of the system

Transition matrix

- State transition equations are usually presented in matrix form
- Transition matrix M has entries m_{ij}, representing the rates of transition between the states i and j
  – index i is used for the number of columns
  – index j is used for the number of rows

$$M = \begin{bmatrix} m_{11} & m_{21} \\ m_{12} & m_{22} \end{bmatrix}$$

Single-component system, no repair

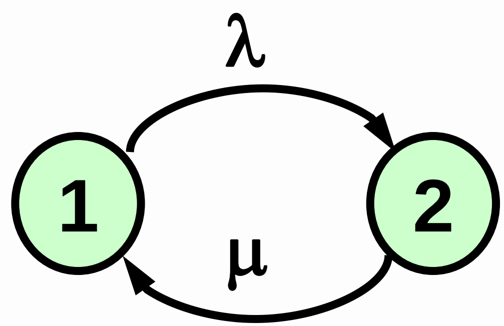


- Transition matrix M has the form:

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

- entries in each columns must sum up to 0
  - entries m_{ii}, corresponding to self-transitions, are computed as –(sum of other entries in this column)

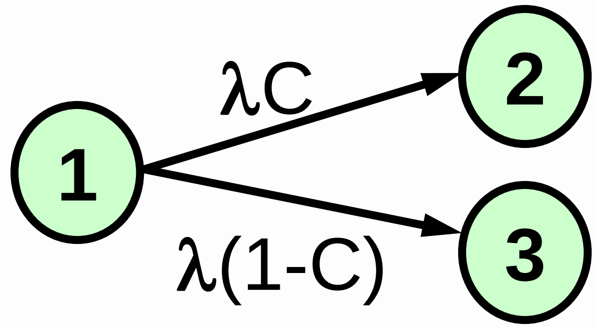
Single-component system with repair



- Transition matrix M has the form:

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

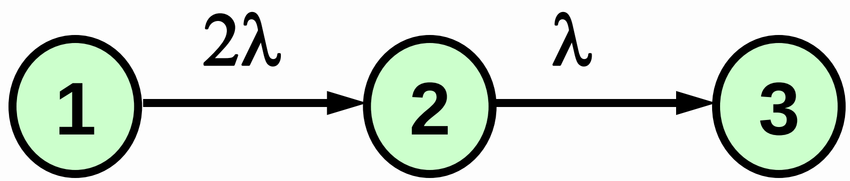
Single-component system, safety analysis



- Transition matrix M has the form:

$$M = \begin{bmatrix} -\lambda & 0 & 0 \\ \lambda C & 0 & 0 \\ \lambda(1-C) & 0 & 0 \end{bmatrix}$$

Two-component parallel system



- Transition matrix M has the form:

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

Important properties of matrix M

- Sum of the entries in each column is 0
- Positive sign of an ij_{th} entry indicates that the transition originates from the i_{th} state
- In reliability analysis, M allows us to distinguish between the operational and failed states
  - each failed state i has a zero diagonal element m_{ii} (a failed state cannot leaved)

State transition equations

- Let P(t) be a vector whose i_{th} element is the probability $P_i(t)$, the probability that the system is in the state i at time t
- The matrix representation of a system of state transition equations is given by

$$\frac{d}{dt} P(t) = M \cdot P(t)$$

Two-component parallel system

- Using transition matrix derived earlier, we get:

$$\frac{d}{dt}\begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \end{bmatrix} = \begin{bmatrix} -2\lambda & 0 & 0 \\ 2\lambda & -\lambda & 0 \\ 0 & \lambda & 0 \end{bmatrix} \cdot \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \end{bmatrix}$$

- This represents the following system of equations

$$\begin{cases} \frac{d}{dt}P_1(t) = -2\lambda P_1(t) \\ \frac{d}{dt}P_2(t) = 2\lambda P_1(t) - \lambda P_2(t) \\ \frac{d}{dt}P_3(t) = \lambda P_2(t) \end{cases}$$

Solving state transition equations

- By solving these equations, we get

$$P_1(t) = e^{-2\lambda t}$$

$$P_2(t) = 2e^{-\lambda t} - 2e^{-2\lambda t}$$

$$P_3(t) = 1 - 2e^{-\lambda t} + e^{-2\lambda t}$$

- Since the $P_i(t)$ are known, we can compute the reliability of the system as a sum of probabilities taken over all operating states

$$R_{parallel}(t) = P_1(t) + P_2(t) = 2e^{-\lambda t} - e^{-2\lambda t}$$

Comparison to RBD result

- Since $R = e^{-\lambda t}$, the previous equation can be written as

$$R_{parallel}(t) = 2R - R^2$$

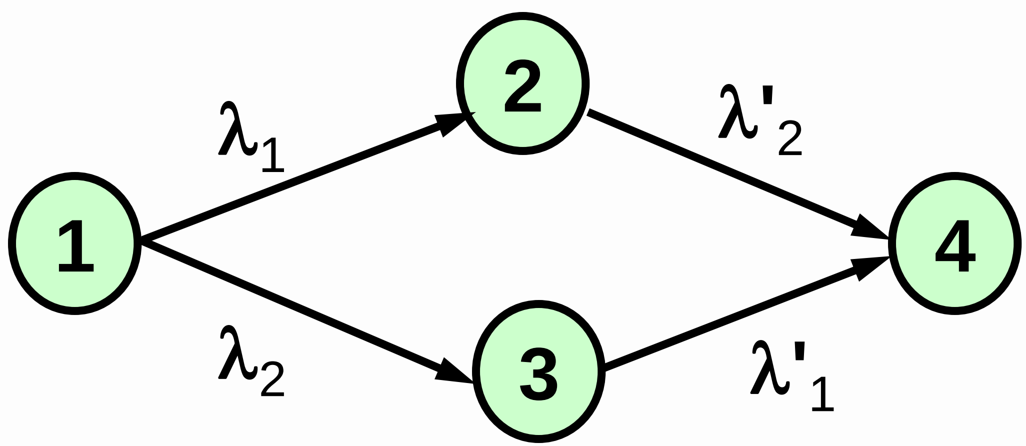
- which agrees with the expression derived using RBD
- two results are the same because we assumed that the failure rates of the two components are independent

Dependant component case

- The value of Markov chains become evident when component failures cannot be assumed to be independent
  - load-sharing components
  - examples: electrical load, mechanical load, information load
- If two components share the same load and one fails, the additional load on the second component increases its failure rate

Parallel system with load sharing

- As before, we have four states, but after the 1st component failure, the failure rate of the 2nd component increases



Parallel system with load sharing

- State transition equations are:

$$\frac{d}{dt}\begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \end{bmatrix} = \begin{bmatrix} -\lambda_1-\lambda_2 & 0 & 0 & 0 \\ \lambda_1 & -\lambda'_2 & 0 & 0 \\ \lambda_2 & 0 & -\lambda'_1 & 0 \\ 0 & \lambda'_2 & \lambda'_1 & 0 \end{bmatrix} \cdot \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \end{bmatrix}$$

$$\begin{cases} \frac{d}{dt}P_1(t) = (-\lambda_1-\lambda_2)P_1(t) \\ \frac{d}{dt}P_2(t) = \lambda_1 P_1(t) - \lambda'_2 P_2(t) \\ \frac{d}{dt}P_3(t) = \lambda_2 P_1(t) - \lambda'_1 P_3(t) \\ \frac{d}{dt}P_4(t) = \lambda'_2 P_2(t) + \lambda'_1 P_3(t) \end{cases}$$

Effect of the load

- If $\lambda'_1 = \lambda_1$ and $\lambda'_2 = \lambda_2$, the equation of load sharing parallel system reduces to well-known

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

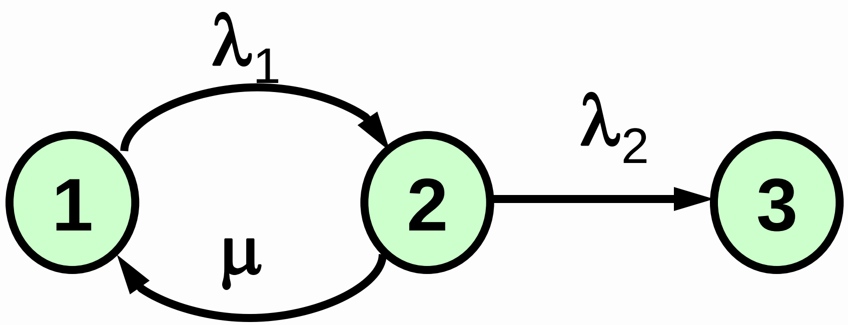
Availability evaluation

- Difference with reliability analysis:
  - in reliability analysis components are allowed to be repaired as long as the system has not failed
  - in availability analysis components can also be repaired after the system failure

Two-component standby system

- First component is primary
- Second is held in reserve and only brought to operation if the first component fails
- We assume that
  - fault detection unit which detect failure of the primary component are replace is with standby is perfect
  - standby component cannot fail while in the standby mode

State transition diagram for reliability analysis with repair



$$M = \begin{bmatrix} -\lambda_1 & \mu & 0 \\ \lambda_1 & -\lambda_2-\mu & 0 \\ 0 & \lambda_2 & 0 \end{bmatrix}$$

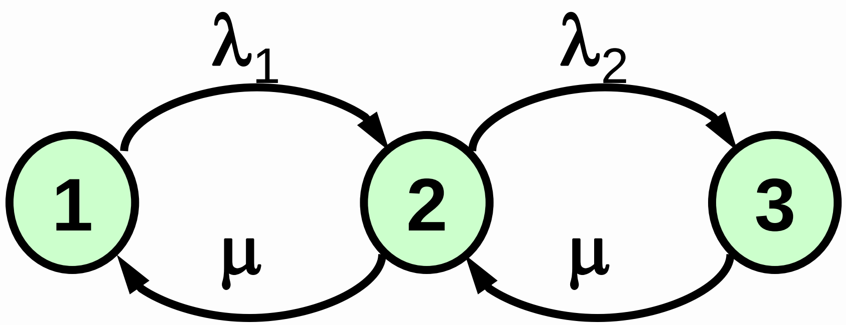
state 1: both OK

state 2: primary failed and replaced by spare

state 3: both failed

Repair replaces a broken component by a working one.

State transition diagram for availability analysis with repair

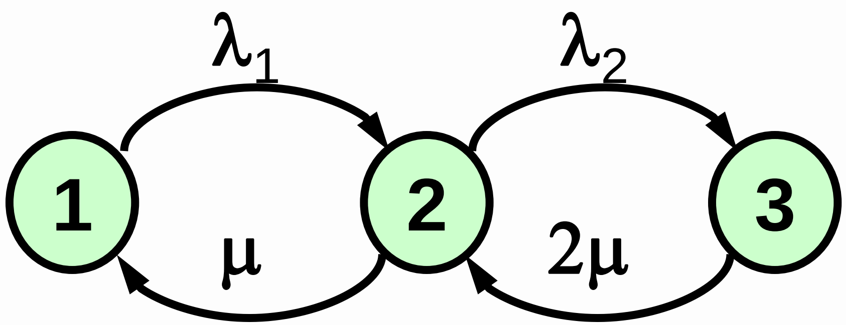


$$M = \begin{bmatrix} -\lambda_1 & \mu & 0 \\ \lambda_1 & -\lambda_2-\mu & \mu \\ 0 & \lambda_2 & -\mu \end{bmatrix}$$

States are the same.

Repair replaces a broken component by a working one. Here we assume that there is only one repair team.

State transition diagram for availability analysis with repair



If we assume that there are two independent repair teams, then **μ** on the edge from 3 to 2 gets the coefficient 2 (the rate doubles).

$$M = \begin{bmatrix} -\lambda_1 & \mu & 0 \\ \lambda_1 & -\lambda_2-\mu & 2\mu \\ 0 & \lambda_2 & -2\mu \end{bmatrix}$$

Availability analysis

- None of the diagonal elements of M are 0
- By solving the system, we can get $P_i(t)$ are compute the availability as a sum of probabilities taken over all operating states
- Usually steady-state availability rather than time dependent one is of interest
- As time approaches infinity, the derivative of the right-hand side of the equation d/dt P(t) = M • P(t) vanishes and we get time-independent relationship

$$M \bullet P(\propto) = 0$$

Two-component standby system

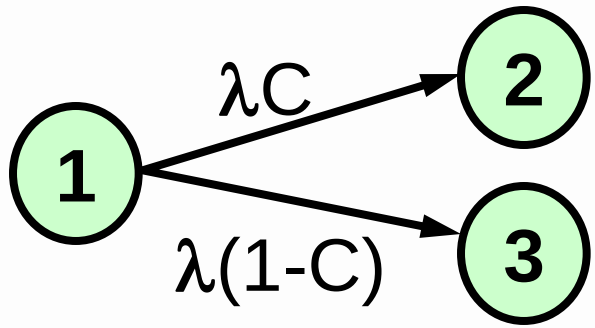
- Using transition matrix derived earlier, we get the following system of equations

$$\begin{cases} -\lambda_1 P_1(\infty) + \mu P_2(\infty) = 0 \\ \lambda_1 P_1(\infty) - (\lambda_2 + \mu) P_2(\infty) + \mu P_3(\infty) = 0 \\ \lambda_2 P_2(\infty) - \mu P_3(\infty) = 0 \end{cases}$$

- By solving the equations, we get

$$A(\infty) \approx 1 - (\lambda/\mu)^2$$

Safety evaluation



- The state transition equations are:

$$\frac{d}{dt}\begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \end{bmatrix} = \begin{bmatrix} -\lambda & 0 & 0 \\ \lambda C & 0 & 0 \\ \lambda(1-C) & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \end{bmatrix}$$

Safety evaluation

- By solving these equations, we get

$$P_1(t) = e^{-\lambda t}$$

$$P_2(t) = C(1- e^{-\lambda t})$$

$$P_3(t) = (1-C) – (1-C)e^{-\lambda t}$$

- Since the $P_i(t)$ are known, we can compute the reliability of the system as a sum of probabilities of neing the operational and fail-safe states

$$R(t) = P_1(t) + P_2(t) = C + (1-C)e^{-\lambda t}$$

- At time t=0, the safety is 1. As time approaches infinity, the safety approaches C

How to deal with cases of systems with "k out of n choices"

- Suppose we want to solve the following task:

  What is the probability that more than two engines in a 4-engine airplane will fail during a t-hour flight if the failure rate of a single engine is λ per hour?

- The probability that more than two engines fail can be expressed as:

$$P_{>2 \text{ failed}} = \binom{4}{1} P_{1 \text{ works } 3 \text{ failed}} + P_{4 \text{ failed}}$$

$$= 1 - \left(P_{4 \text{ work}} + \binom{4}{3} P_{3 \text{ work } 1 \text{ failed}} + \binom{4}{2} P_{2 \text{ work } 2 \text{ failed}}\right)$$

- Only probabilities of mutually exclusive events can be summed up like this

"k out of n choices"

- "k out of n choices" can be computed as

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$$

- For example

$$\binom{4}{2} = \frac{4!}{(4-2)!\,2!} = 6$$

Example cont.

So, we get

$$P_{>2 \text{ failed}} = 4\, P_{1 \text{ works } 3 \text{ failed}} + P_{4 \text{ failed}}$$

where

$$P_{1 \text{ works } 3 \text{ failed}} = R\,(1-R)^3$$

$$P_{4 \text{ failed}} = (1-R)^4$$

where R is the reliability of a single engine computed as $R = e^{-\lambda t}$

Summary

- Methods for evaluating the reliability, availability and safety of a system
  - RBDs
  - Markov chains

Next lecture

- Hardware redundancy

Read chapter 4

of the text book