# Reliability of Computer Systems
# Part 3: Reliability Modeling

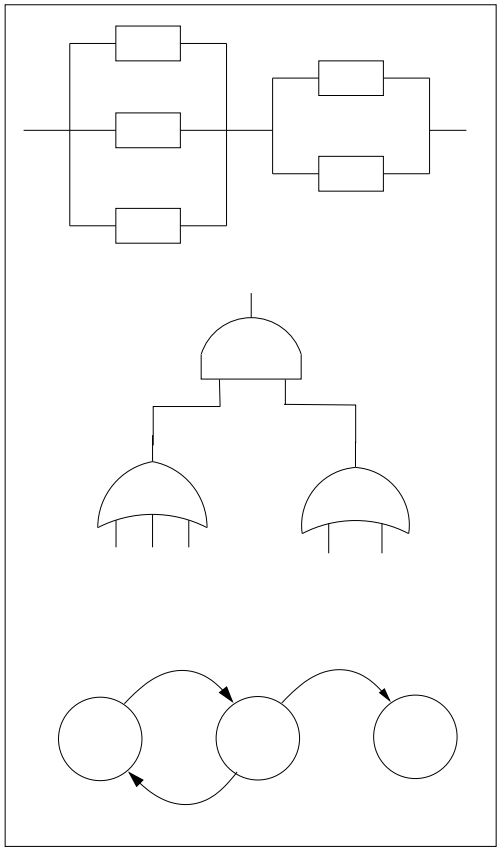
Peter Sobe

HTW Dresden, Germany
Faculty of Computer Science and Mathematics

29th July 2016

# Part 3: Modeling of Fault-tolerant Systems

Overview:



Static system configurations: Without repair

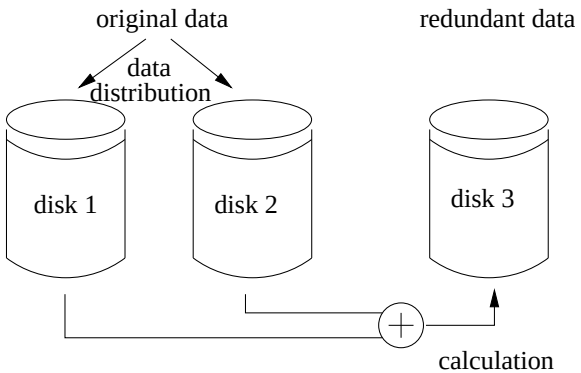
- System structure and Boolean models
- Graphic Presentations: Fault trees and Reliability block diagrams
- Probabilistic quantification

Dynamic Systems:
including repair, reconfiguration

- Modeling: Markov models, birth/death processes

# System Structure

2 out-of 3 system:




Reliability modeling:

Input: system structure, constraints given by fault-tolerance technique, reliability or availability of single components

Output: Reliability, i.e. probability that the system is operational (steady state, or as a function of time)
MTTF (mean time to failure)

Techniques:
Boolean models, Markov chains, stochastic petri nets, simulations

# Boolean Models

Boolean models:

- Switch states 1 and 0 - for operational and failed
- the system is evaluated by means of switching algebra

Example (2 of 3) system: $X$ for operational, $\bar{X}$ for failed

$$X_{2\ of\ 3} = X_1X_2X_3 \vee \bar{X}_1X_2X_3 \vee X_1\bar{X}_2X_3 \vee X_1X_2\bar{X}_3$$

# Other Representations of Boolean Models

Other visual representations:

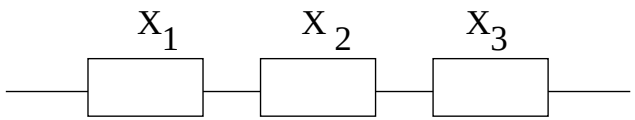
- **Fault Trees:** Tree of logical switching elements (AND, OR, with positive and negated inputs), tree root outputs a logical value for success or for failure
- **Reliability Block Diagrams (RBD):** Digraph with special nodes for input and output. Nodes represent the operational state of a component. Several nodes in the graph can address the same component. RBDs contain serial, parallel and (x of y)-compositions (for example 2 of 3).
- **Binary Decision Diagrams:** Directed acyclic graph that spans the state space, all nodes represent a state $X_i$, except the leaves that represent the result (0 or 1). The $X_i$ nodes are connected to edges that represent their states (0 and 1).

Boolean models are easy to transform into these representations. Their results are equivalent.

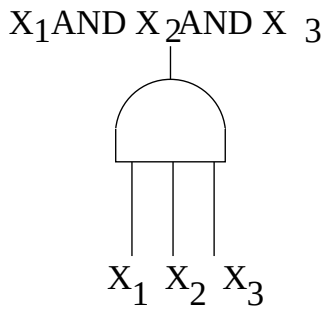
# Fault Trees

Tree of logical switching elements

Serial composition:

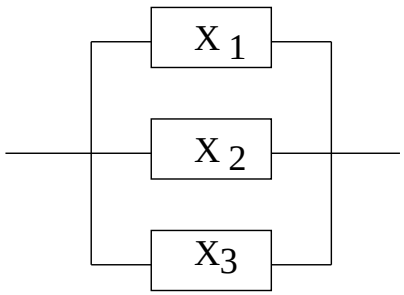



Structural Model

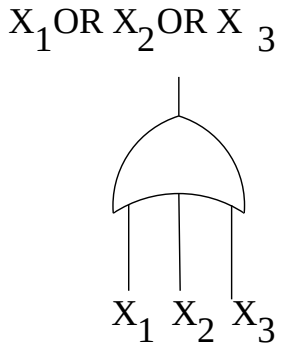



Fault Tree

Parallel composition:



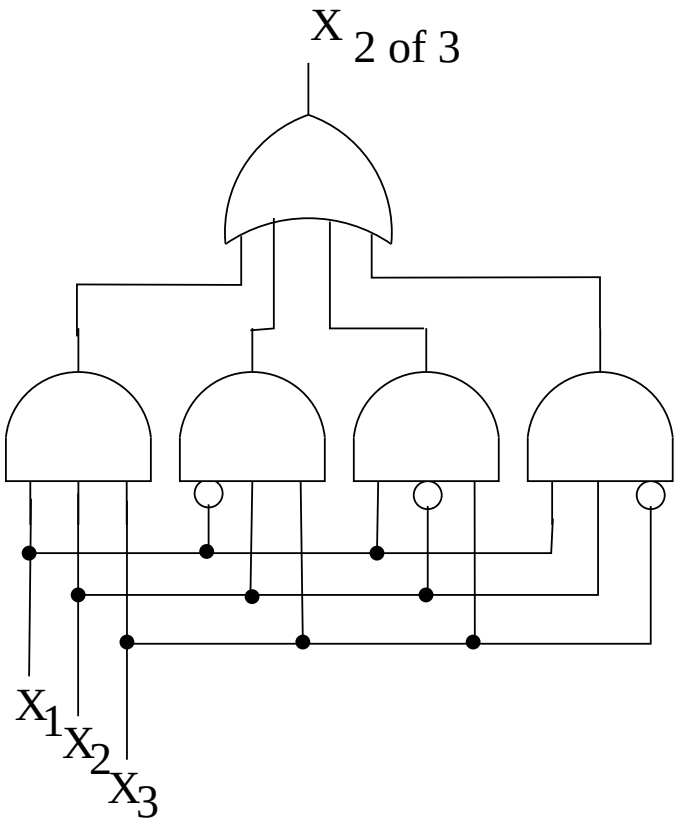

Structural Model




Fault Tree

# Fault Trees

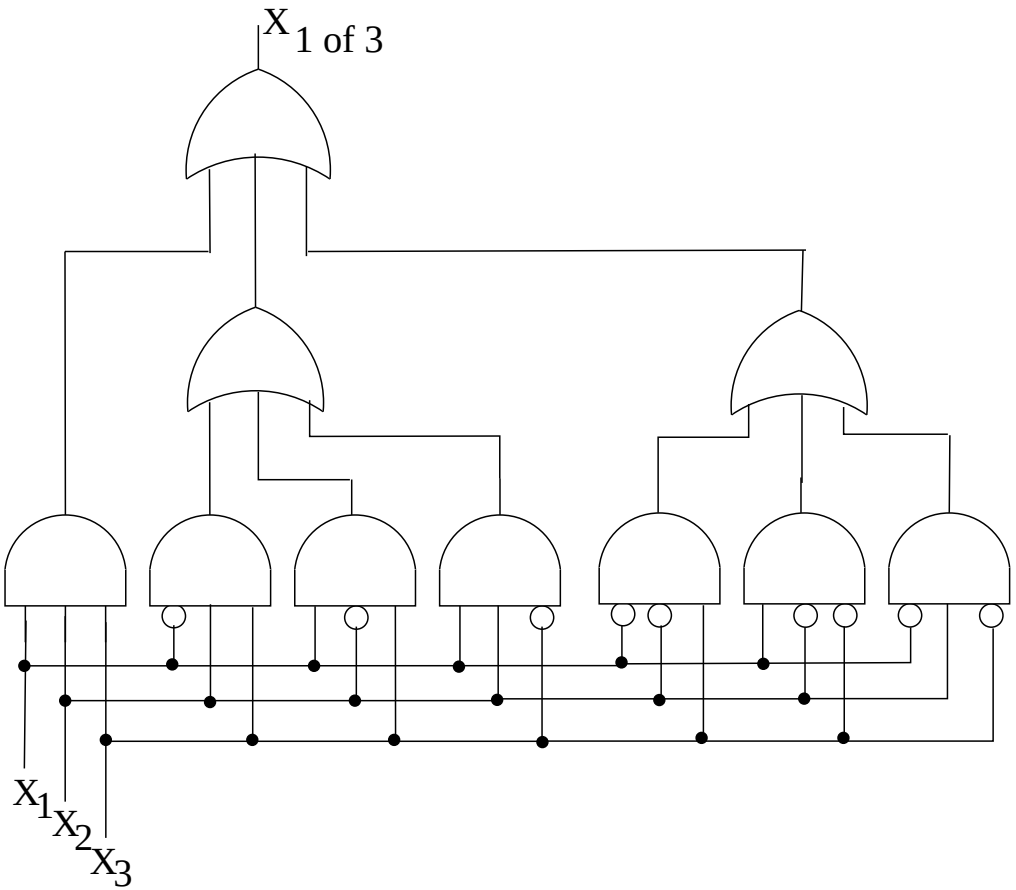
## Example of a fault tree




$$X_{2\ of\ 3} = X_1X_2X_3 \vee \bar{X}_1X_2X_3 \vee X_1\bar{X}_2X_3 \vee X_1X_2\bar{X}_3$$

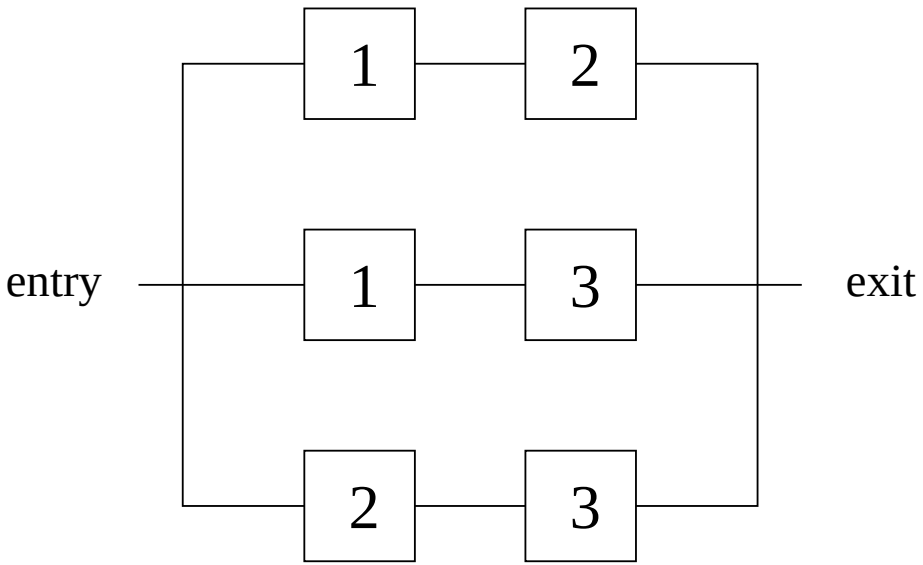
# Fault Trees

## Example of another fault tree




$$X_{1\ of\ 3} = X_1X_2X_3 \vee \bar{X}_1X_2X_3 \vee X_1\bar{X}_2X_3 \vee X_1X_2\bar{X}_3 \vee \bar{X}_1\bar{X}_2X_3 \vee X_1\bar{X}_2\bar{X}_3 \vee \bar{X}_1X_2\bar{X}_3$$

## Reliability Block Diagram (RBD)



# Working with probabilities

States can be translated from $\{0, 1\}$ to probabilities $R \in 0 \ldots 1$,
$F = 1 - R \in 0 \ldots 1$
$R$ ... probability that system operational
$F$ ... probability that system failed

$$X_{2\ of\ 3} = X_1X_2X_3 \vee \bar{X}_1X_2X_3 \vee X_1\bar{X}_2X_3 \vee X_1X_2\bar{X}_3$$

can be transformed to

$$R_{2\ of\ 3} = R_1R_2R_3 + F_1R_2R_3 + R_1F_2R_3 + R_1R_2F_3$$

$$R_{2\ of\ 3} = R_1R_2R_3 + (1 - R_1)R_2R_3 + R_1(1 - R_2)R_3 + R_1R_2(1 - R_3)$$

Another simplification: individual components are operational with the same probability $R$ and fail with the same probability $F$:

$$R_{2\ of\ 3} = R^3 + 3R^2(1 - R), \qquad R = R_1 = R_2 = R_3$$

# Working with probabilities

($k$ of $k+m$)-system:

- $k$ components for base functionality
- $m$ spare components (additionally, not needed for base functionality)
- system is operational, when at least $k$ components (among $k+m$) are faultfree

General expression for any $k$ and $m$:

$$R_{k \text{ of } k+m} = R^{k+m} + \sum_{i=1}^{m} \left( \begin{array}{c} k+m \\ k+m-i \end{array} \right) R^{k+m-i} F^{i})$$

$$F_{k \text{ of } k+m} = 1 - R_{k \text{ of } k+m}$$

# Examples: k of k+m Systems

$$R_{k\ of\ k+m} = R^{k+m} + \sum_{i=1}^{m} \left( \begin{array}{c} k+m \\ k+m-i \end{array} \right) R^{k+m-i} F^{i})$$

$$F_{k\ of\ k+m} = 1 - R_{k\ of\ k+m}$$

Example 1:
Car with 4 wheels and one spare wheel:
4 of 5 system
$R_{wheel} = 0.99$, $R_{4of5wheels} = 0.9990$
$F_{wheel} = 0.01$, $F_{4of5wheels} = 1 - 0.9990 = 0.001$

# Examples: k of k+m Systems

$$R_{k\ of\ k+m} = R^{k+m} + \sum_{i=1}^{m} \left( \begin{array}{c} k+m \\ k+m-i \end{array} \right) R^{k+m-i} F^{i})$$

$$F_{k\ of\ k+m} = 1 - R_{k\ of\ k+m}$$

Example 2:
Storage system consisting of 5 disks, + 2 redundant disks, MDS code:
5 of 7 system
$R_{disk} = 0.9$, $R_{5of7disks} = 0.974308$
$F_{disk} = 0.1$, $F_{5of7disks} = 1 - 0.974308 = 0.025692$

# R and F as functions of time

R and F . . .

- can be interpreted as constant values, in a fixed environment (including time)
- can be modeled as a function of time

$$R(t) = f(t)$$

real $R(t)$ not known, assumptions: $R(0) = 1$, $R(\infty) = 0$

Typical assumption for modeling purposes:

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

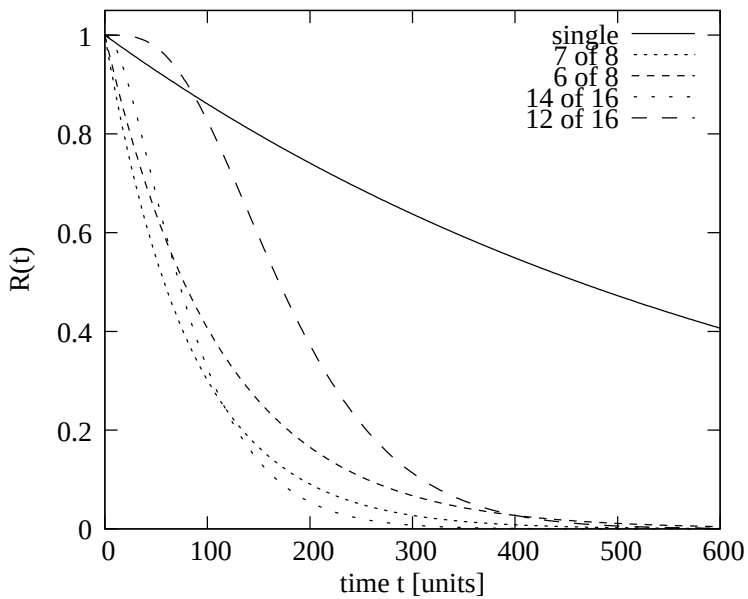
$\lambda$ ... failure rate

Application on a ($k$ of $k + m$)-system:

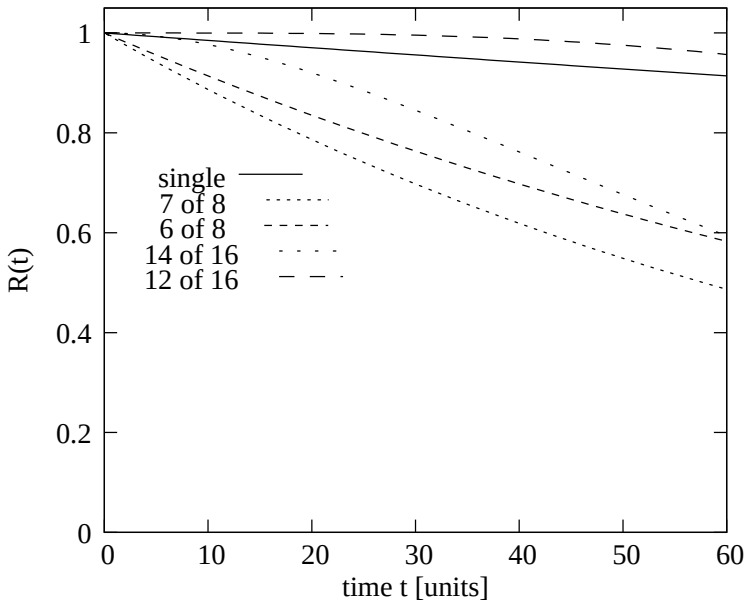
$$R_{k \text{ of } k+m}(t) = R(t)^{k+m} + \sum_{i=1}^{m} \left( \begin{array}{c} k+m \\ k+m-i \end{array} \right) R(t)^{k+m-i} F(t)^{i}$$

# R and F as functions of time

Plots of x of y reliabilities:
big picture:




detail:



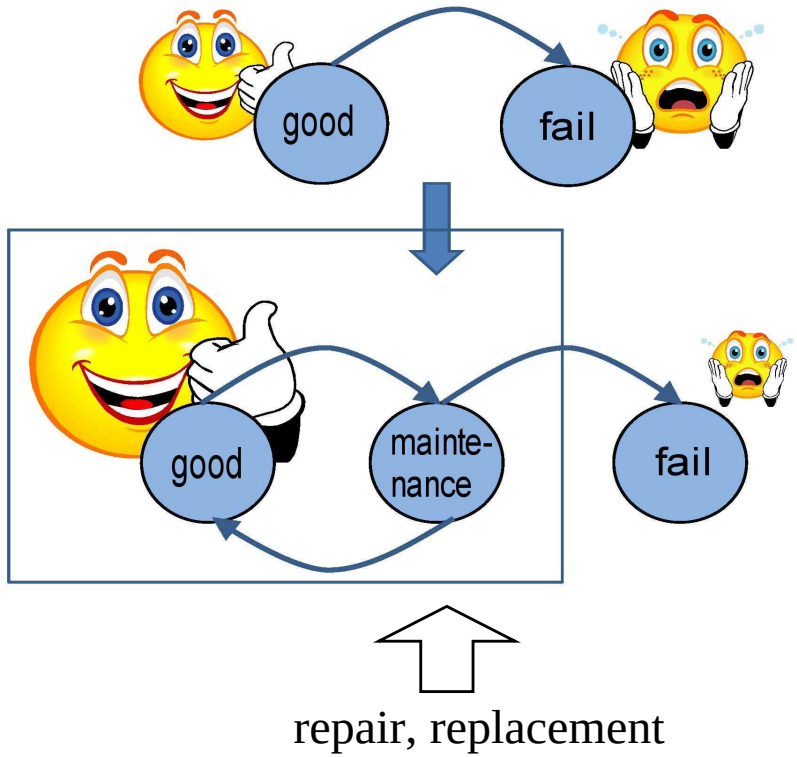
# Preliminary Summary Part 3 : Static system configurations

- Boolean models, fault trees, RBD to represent typical structures of components
- structures: serial, parallel, (k of n) and combinations
- composition without taking time into account
- timely behavior: calculation of component reliabilities as function of time
- What can not be expressed: time aspects of reconfiguration and repair
  $\rightarrow$ modeled using different techniques

# Dynamic Fault-tolerant Systems with Repair

**Overview:**

Reconfiguration during operation, Repair, Rejuvenation



# Repair

Options:

- Without Repair (static system configurations)
  - High reliability must be guaranteed by selection of highly robust and reliable components
  - or ”static” fault-tolerant configurations with fault masking, such as TMR, NMR
- Repair after failure
  - Beneficial for availability (A)
  - Reliability $R(t)$ is not improved, because a failure can not be excluded
- Partly repair during operation
  - Beneficial for reliability R(t) when repair takes place in an operational state

# Repair - Choice of Techniques

**Fail-Stop:**

- duplication (synchronous process duplication), function switch-over, replacement of the failed component, re-synchronization of the new component
- comparable variants can be implemented for a PSR system, and for multiple replicated components

**Arbitrary Faults (including wrong result values):**

- TMR-systems with renewal of the faulty component during operation
- comparable variant also for (k of k+m) systems

# Repair - Choice of Techniques

Needed building blocks:

- failure detector (crash) or agreement/masking protocol
- synchronous duplication/replication, communication protocol for atomicy and consistent message order
- checkpoints/snapshots, rollback or roll-forward for re-synchronization

# Markov models

- A model that represents all states of the entire system that can be combined from the (0,1) states of the individual components.
- Transitions between the states are expressed by rates: $\lambda$ failure rate, $\mu$ repair rate
- rates are constant over time, but different rates can be applied, depending on the start and end state, e.g. $\lambda_1$, $\lambda_2$
- States are present with a probability, rates express a probability flow
- States that represent comparable situations (e.g. a single fault, a double fault) can be combined, combination of the rates

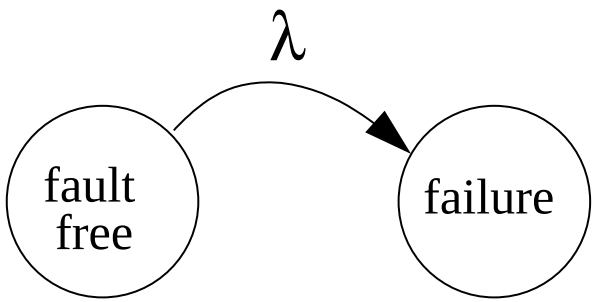
# Markov models

A model analysis reveals

- state probabilities in a steady state situation
- or probabilities of states as a function of time $t$: $P_{state-X}(t)$.

# Markov models

A single component without repair:




Differential equation:

$$P_{faultfree}(t)' = -\lambda P_{faultfree}(t)$$

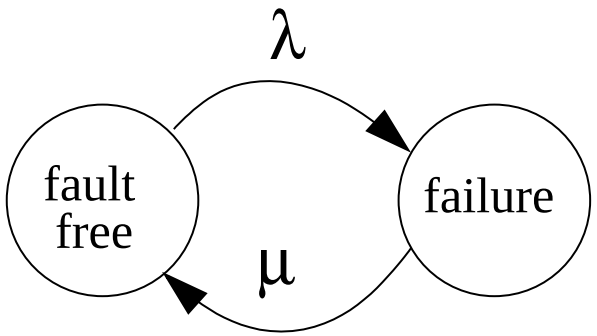
Solution:

$$P_{faultfree} = e^{-\int_0^t \lambda dt} = e^{-\lambda t}$$

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

# Markov models

A single component with repair:



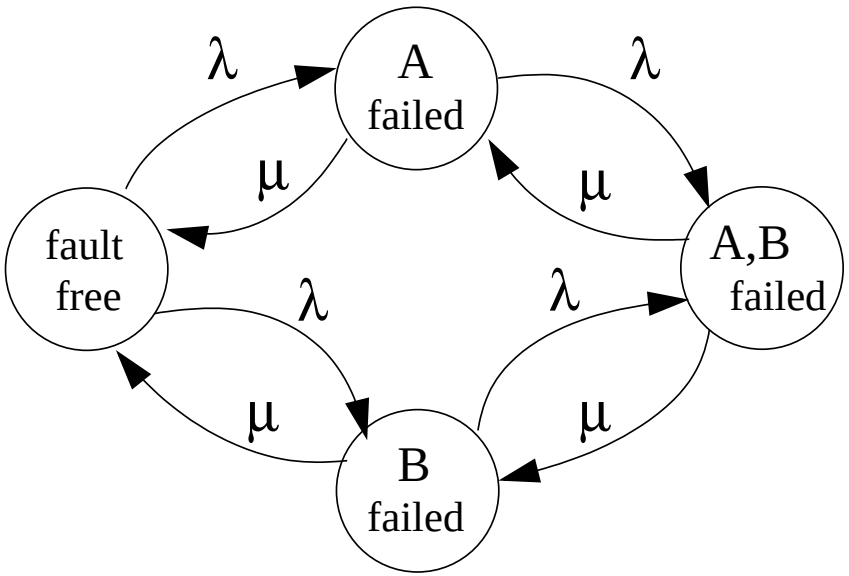

$$
\begin{aligned}
P_{faultfree}(t)' &= +\mu P_{failure}(t) - \lambda P_{faultfree}(t) \\
P_{failure}(t)' &= -\mu P_{failure}(t) + \lambda P_{faultfree}(t)
\end{aligned}
$$

Solution:

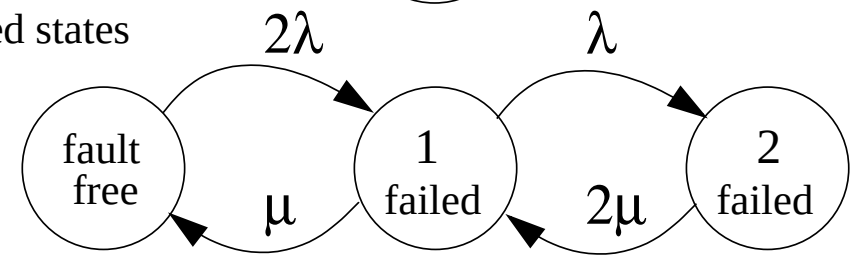
$$
A(t) = P_{faultfree}(t) = \frac{\mu}{\lambda+\mu} + (P_{faultfree}(0) - \frac{\mu}{\lambda+\mu}) \cdot e^{-(\lambda+\mu)t}
$$

# Markov models

General Markov model of a two component system:



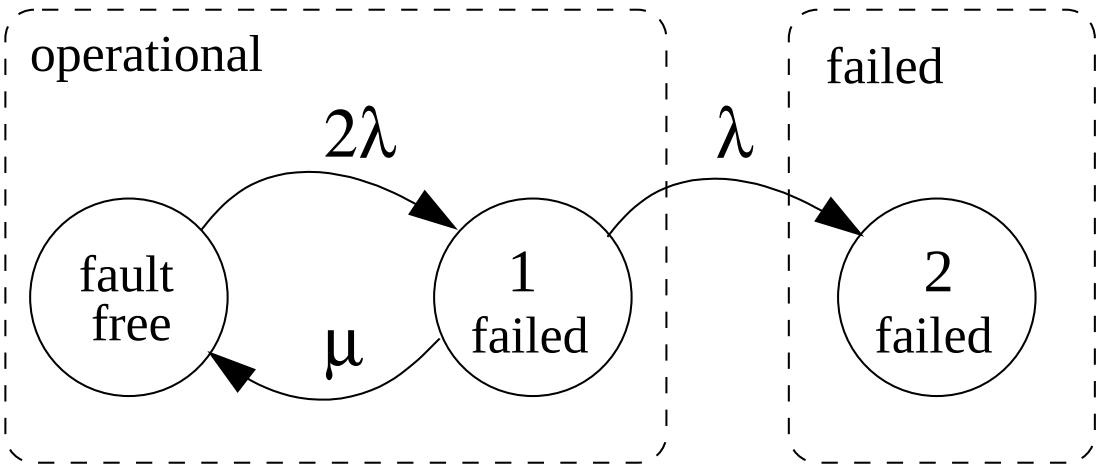

with combined states



# Markov models

A process pair where one process is able to substitute the other one, and the failed process can be repaired (e.g. restarted).

This is modeled by a (1 of 2) system with repair

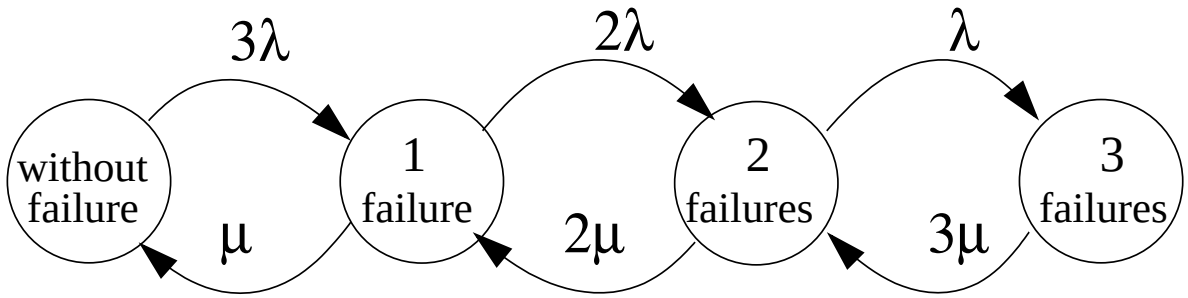



$$
\begin{aligned}
R(t) &= P_{faultfree}(t) + P_{1failed}(t) \\
F(t) &= P_{2failed}(t)
\end{aligned}
$$

# Markov models

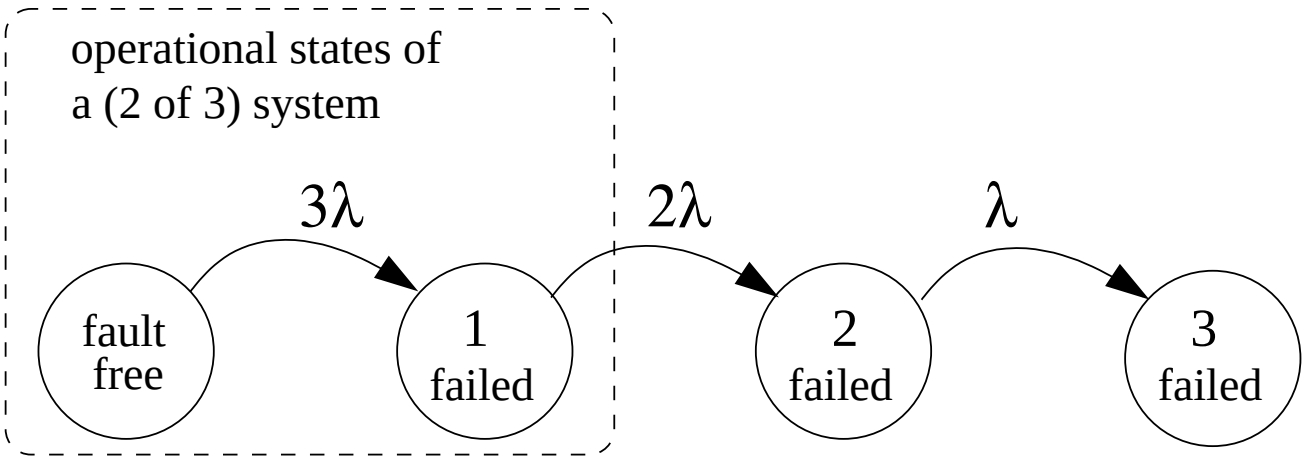
General Markov chain for a 3 component system:

3 components: $2^3 = 8$ different system states



# Markov models

A static TMR system, or a group of three processes with voting can be modeled by a (3 of 2) system without repair

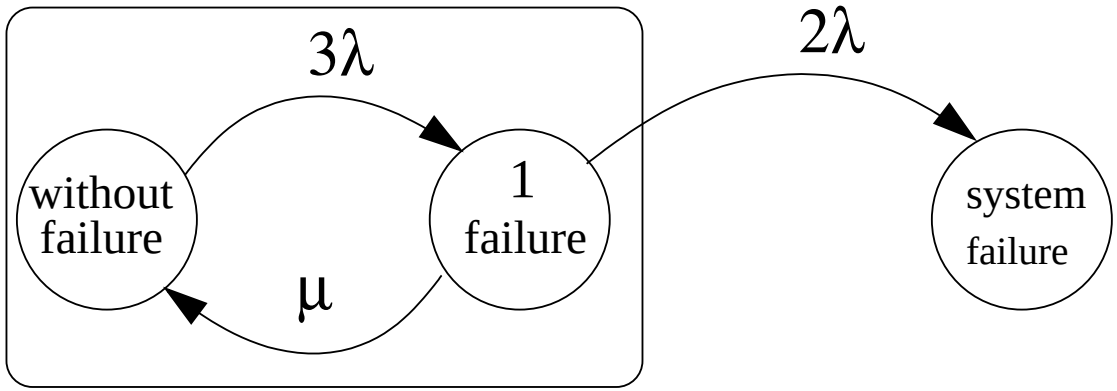



Note: This can be handled by a simple reliability calculation:

$$R_{2of3} = R^3 + 3R^2F$$

# Markov models

2 out-of 3 system with repair:



# Markov models

## Markov chain simulator

- mm_solve[1]
- Monte Carlo simulation of a Markov chain model
- Definition of states and transitions in a parameter file
- One specific state is assumes as the failure state (specific of the simulator related to general Markov chains)
- Simulation run with specification of a mission time
- Output:
  MTTF of the system
  $R(t)$: Reliability of the system within the mission time

[1] Kevin M. Greenan, High-Fidelity Reliability (HFR) Simulator, http://users.soe.ucsc.edu/ ∼kmgreen/

# Summary Part 3

- Static system configurations modeled by Boolean models
- Graphical expressions: fault trees (success trees), RBD
- Many regularly structured systems can be described as a (k of k+m) system:

  | | |
  |---|---|
  | serial system, s components: | (s of s) |
  | parallel system, p components: | (1 of p) |
  | k primary components, k redundant: | (k of k+m) |

- Time t is expressed by R(t) and F(t) values that can be applied in the context of a (k of k+m) system

# Summary Part 3 (cont.)

- Dynamic systems: modeled by Markov models
  - time aspects expressed by rates ($\lambda$, $\mu$)
  - different systems states are expressed in model
  - solutions of the model deliver the probabilities for states and allow the assessment of $R(t)$, $F(t)$ and $A(t)$