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

- 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

$$X_{2\text{ of } 3} = X_1X_2X_3 \lor \bar{X}_1X_2X_3 \lor X_1\bar{X}_2X_3 \lor X_1X_2\bar{X}_3$$
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 \((x \text{ of } y)\)-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:

Parallel composition:
Example of a fault tree

\[ X_{2 \text{ of } 3} = X_1 X_2 X_3 \lor \bar{X}_1 X_2 X_3 \lor X_1 \bar{X}_2 X_3 \lor X_1 X_2 \bar{X}_3 \]
Fault Trees

Example of another fault tree

\[ X_{\text{1 of 3}} = X_1 X_2 X_3 \vee \bar{X}_1 X_2 X_3 \vee X_1 \bar{X}_2 X_3 \vee X_1 X_2 \bar{X}_3 \vee \bar{X}_1 \bar{X}_2 X_3 \vee X_1 \bar{X}_2 \bar{X}_3 \vee \bar{X}_1 X_2 \bar{X}_3 \]
Reliability Block Diagram (RBD)
Working with probabilities

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

\[ X_{2 \text{ of } 3} = X_1 X_2 X_3 \lor \bar{X}_1 X_2 X_3 \lor X_1 \bar{X}_2 X_3 \lor X_1 X_2 \bar{X}_3 \]

can be transformed to

\[ R_{2 \text{ of } 3} = R_1 R_2 R_3 + F_1 R_2 R_3 + R_1 F_2 R_3 + R_1 R_2 F_3 \]

\[ R_{2 \text{ of } 3} = R_1 R_2 R_3 + (1 - R_1) R_2 R_3 + R_1 (1 - R_2) R_3 + R_1 R_2 (1 - R_3) \]

Another simplification: individual components are operational with the same probability \( R \) and fail with the same probability \( F \):

\[ R_{2 \text{ of } 3} = R^3 + 3R^2(1 - R), \quad R = R_1 = R_2 = R_3 \]
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:

\[ R_{k \text{ of } k+m} = R^{k+m} + \sum_{i=1}^{m} \binom{k+m}{k+m-i} R^{k+m-i} F^i \]

\[ F_{k \text{ of } k+m} = 1 - R_{k \text{ of } k+m} \]
Examples: $k$ of $k+m$ Systems

\[ R_{k \text{ of } k+m} = R^{k+m} + \sum_{i=1}^{m} \binom{k+m}{k+m-i} R^{k+m-i} F^i \]

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

Example 1:
Car with 4 wheels and one spare wheel:
4 of 5 system
\[ R_{\text{wheel}} = 0.99, \quad R_{4\text{of5wheels}} = 0.9990 \]
\[ F_{\text{wheel}} = 0.01, \quad F_{4\text{of5wheels}} = 1 - 0.9990 = 0.001 \]
Examples: $k$ of $k+m$ Systems

\[ R_{k \text{ of } k+m} = R^{k+m} + \sum_{i=1}^{m} \binom{k+m}{k+m-i} R^{k+m-i} F^i \]

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

Example 2:
Storage system consisting of 5 disks, + 2 redundant disks, MDS code:
5 of 7 system
\[ R_{\text{disk}} = 0.9, \quad R_{5 \text{ of } 7 \text{ disks}} = 0.974308 \]
\[ F_{\text{disk}} = 0.1, \quad F_{5 \text{ of } 7 \text{ disks}} = 1 - 0.974308 = 0.025692 \]
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 \((k \text{ of } k + m)\)-system:

\[ R_{\text{k of } k+m}(t) = R(t)^{k+m} + \sum_{i=1}^{m} \binom{k+m}{k+m-i} R(t)^{k+m-i} F(t)^i \]
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 → modeled using different techniques
Overview:

Reconfiguration during operation, Repair, Rejuvenation

repair, replacement
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
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 atomicity 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
A model analysis reveals

- state probabilities in a steady state situation
- or probabilities of states as a function of time $t$: $P_{state-x}(t)$. 
A single component without repair:

Differential equation:

\[ P_{\text{fault free}}(t)' = -\lambda P_{\text{fault free}}(t) \]

Solution:

\[ P_{\text{fault free}} = e^{-\int_0^t \lambda dt} = e^{-\lambda t} \]

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

A single component with repair:

\[ \lambda \]

\[ \mu \]

\[ P_{\text{faultfree}}(t) \]

\[ P_{\text{failure}}(t) \]

\[
P_{\text{faultfree}}(t)' = +\mu P_{\text{failure}}(t) - \lambda P_{\text{faultfree}}(t)
\]

\[
P_{\text{failure}}(t)' = -\mu P_{\text{failure}}(t) + \lambda P_{\text{faultfree}}(t)
\]

Solution:

\[ A(t) = P_{\text{faultfree}}(t) = \frac{\mu}{\lambda + \mu} + \left( P_{\text{faultfree}}(0) - \frac{\mu}{\lambda + \mu} \right) \cdot e^{-(\lambda+\mu)t} \]
General Markov model of a two component system:

- **A**
  - Failed
  - Transition rates: $\lambda$, $\mu$

- **B**
  - Failed
  - Transition rates: $\lambda$, $\mu$

States:
- Fault free
- Failed

Combined states:
- $A, B$ failed

Transition rates:
- $2\lambda$
- $\lambda$
- $2\mu$
- $\mu$

With combined states.
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

\[
R(t) = P_{\text{fault free}}(t) + P_{\text{1 failed}}(t)
\]
\[
F(t) = P_{\text{2 failed}}(t)
\]
Markov models

General Markov chain for a 3 component system:

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

![Diagram of Markov chain with 3 components and transition rates $3\lambda$, $2\lambda$, $\lambda$, $\mu$, $2\mu$, $3\mu$.]
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:

\[ R_{2of3} = R^3 + 3R^2F \]
2 out-of 3 system with repair:
Markov chain simulator

- `mm_solve`
- Monte Carlo simulation of a Markov chain model
- Definition of states and transitions in a parameter file
- One specific state is assumed 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/
Static system configurations modeled by Boolean models

Graphical expressions: fault trees (success trees), RBD

Many regularly structured systems can be described as a \((k \text{ of } k+m)\) system:

- Serial system, \(s\) components: \((s \text{ of } s)\)
- Parallel system, \(p\) components: \((1 \text{ of } p)\)
- \(k\) primary components, \(k\) redundant: \((k \text{ of } k+m)\)

Time \(t\) is expressed by \(R(t)\) and \(F(t)\) values that can be applied in the context of a \((k \text{ of } k+m)\) system.
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 $A(t)$