Chap 9: Reliability & Availability Modeling

Reliability Block Diagram using sharpe

\[
\text{block name } \{( \text{param-list} )\} \quad \text{optional}
\]

\[
[ < \text{block line} > \quad \text{end}
\]

can be one of the following:

P.358 Appendix B
1) `comp name exponential-polynomial`

   Referring to the cumulative dist function (cdf)

   \[
   F(t) = 1 - e^{-\lambda t} \quad \text{and} \quad R(t) = e^{-\lambda t}
   \]

   `exp (lambda)` meaning the exponential distribution

   `cdf (component-name{,state}{;arg-list})`

   which has been defined before

   or `gen triple 1, triple 2, ...

   in the form of \((a_j, k_j, b_j)\)

   See p. 352

2) `parallel name name-1 name-2 {name3 name4 ...}`

   The parallel system is assigned to the first name.

3) `series name name-1 name-2 {name3 name4 ...}`

   The series system is assigned to the first name.

4) `kofn name expression-1, expression-2, component-name`

   \[
   F(t) = \sum_{j} a_j \cdot t^{k_j} \cdot e^{b_j t}
   \]
5) \textbf{kofn} \textbf{name k-expression, n-expression, name1 name2 \{name3…\}}

representing a k-out-of-n system
having possibly different components

Components do not have identical failure-time dist.

Ex:

\begin{itemize}
  \item \begin{tikzpicture}
    \node[draw] (cpu1) {CPU1};
    \node[draw] (cpu2) [below of=cpu1] {CPU2};
    \node[draw] (m1) [right of=cpu1] {m1};
    \node[draw] (m2) [below of=m1] {m2};
    \node[draw] (m3) [below of=m2] {m3};
    \draw[->] (cpu1) -- (cpu2);
    \draw[->] (cpu1) -- (m1);
    \draw[->] (cpu2) -- (m2);
    \draw[->] (m1) -- (m2);
    \draw[->] (m1) -- (m3);
    \draw[->] (m2) -- (m3);
  \end{tikzpicture}
  \end{itemize}

Sharing memory: a k-out-of-n device

\begin{itemize}
  \item block system ( k, n, pfrate, mfrate )
  \item comp CPU exp ( pfrate )
  \item comp mem exp ( mfrate )
  \item parallel CPUs CPU CPU
  \item kofn mems k, n, mem
  \item series subsystem CPUs mems
  \item end
\end{itemize}

\textbf{Output}

\begin{itemize}
  \item in semi symbolic form
  \item CDF for system
    \begin{equation}
      1-6e^{-0.00903t}+3e^{-0.0104t}+\ldots
    \end{equation}
  \item (1-out-of-3)
  \item k=1.00
    \begin{itemize}
      \item mean(system;k,3,\ldots) = 2.26*10^2
      \item rel (10,k,3\ldots) = 9.9981*10^{-1}
      \item rel (365,k,3\ldots) = 8.33*10^{-1}
    \end{itemize}
  \item k=2.00
\end{itemize}
Comments: any line starting with the symbol “*”

* printing output.
* printing \( F(t) \) in symbolic form
  \[ \text{cdf} \ (\text{system}; 1, 3, 0.00139, 0.00764) \]
* define reliability function at time \( t \)
  \[ \text{func} \ \text{rel}(t, k, n, \text{pf}, \text{mf}) \]
  \[ 1 - \text{value} \ (t; \text{system}; k, n, \text{pf}, \text{mf}) \]

Returning \( F(t) \) at time \( t \) numerically

\[ \text{loop} \ k, 1, 3, 1 \]
  \[ \text{expr} \ \text{mean} \ (\text{system}; k, 3, 0.00139, 0.00764) \]
  \[ \text{expr} \ \text{rel} \ (10, k, 3, 0.00139, 0.00764) \]
  \[ \text{expr} \ \text{rel} \ (365, k, 3, 0.00139, 0.00764) \]
\[ \text{end} \]
\[ \text{end} \]
Fig. 9.1 p. 156

\[
\begin{array}{c}
\lambda=0.05 \\
A \rightarrow B \\
\lambda=0.01 \\
\lambda=0.3 \\
C \rightarrow C \rightarrow C \\
\lambda=0.25 \\
D \rightarrow D \\
\lambda=0.1 \\
E
\end{array}
\]

\begin{verbatim}
block block1a
  comp A  exp(0.05)
  comp B  exp(0.01)
  comp C  exp(0.3)
  comp D  exp(0.25)
  comp E  exp(0.1)
  parallel threeC  C C C
  parallel twoD  D D
  series sys1  A B threeC twoD E
end

* printing: 5 decimal places
format 5
* cdf
  cdf (block1a)
  expr 1-value(10; block1a)
end
\end{verbatim}

Print 1-F(t)=R(t) at t=10
Availability Modeling

\[ A_i(t) = \frac{\mu_i}{\lambda_i + \mu_i} + \frac{\lambda_i}{\lambda_i + \mu_i} e^{-(\lambda_i + \mu_i)t} \]

To define \(1 - A_i(t)\)

\[ F(t) = \sum_{j} a_j \cdot t^{k_j} \cdot e^{b_j t} \]

See p.354 text on a user-defined distribution syntax:

poly name(param-list) dist. of the form triple

\((a_j, k_j, b_j)\)

* print steady state
* availability \(A(\infty)\)
expr pinf(block1a)

* print instantaneous
* availability at \(t=100\)
expr 1-value(100; block1a)
end
Fault Trees

* A pictorial representation of events that can cause the occurrence of an undesirable event.
* An event at a high level is reduced to a combination of lower level events by means of logic gates
  
  **AND**: when all fail, the failure event occurs.
  **OR**: when one fails, the failure event occurs.
  **K out of n**: when at least k out of n components fail, the failure event occurs.

E.g.

\[
\begin{align*}
\text{failure} & \quad \leftarrow \quad \text{or} \\
\quad \text{AND} & \quad \leftarrow \quad P_1 \quad \text{AND} \quad P_2 \\
\quad \text{AND} & \quad \leftarrow \quad M_1 \quad \text{AND} \quad M_2 \quad \text{AND} \quad M_3
\end{align*}
\]

\[
\begin{align*}
P_1 & \quad \leftarrow \quad \text{AND} \\
P_2 & \quad \leftarrow \quad \text{AND} \\
M_1 & \quad \leftarrow \quad \text{AND} \\
M_2 & \quad \leftarrow \quad \text{AND} \\
M_3 & \quad \leftarrow \quad \text{AND}
\end{align*}
\]
For a fault tree without repeated components:

\[
Q_{\text{ftree}}(t) = \begin{cases} 
\prod_{i=1}^{n} Q_i(t) & \text{AND gate} \\
1 - \prod_{i=1}^{n} (1 - Q_i(t)) & \text{OR gate} \\
\sum_{i=k}^{n} \binom{n}{i} (Q(t))^i (1 - Q(t))^{n-i} & \text{k-out-of-n gate: for } n \text{ identically distributed components} \\
\sum_{|J| \geq k} \left( \prod_{j \in |J|} Q_j(t) \right) \left( \prod_{j \notin |J|} (1 - Q_j(t)) \right) & \text{k-out-of-n gate: for } n \text{ non-identically distributed components}
\end{cases}
\]

Unreliability or failure probability

A set that contains at least \( k \) failed components
The above equation cannot be used when there is a repeated component.

**Example:**

- 2 processors: P₁ & P₂
- 3 memory modules: M₁, M₂ & M₃

- M₃ is shared by P₁ & P₂
- M₁ is private to P₁
- M₂ is private to P₂

the system will operate as long as there is at least one operational processor with access to either a private or shared memory.
i.e. \( \overline{P_i} = 1 \) if Processor i fails at time t and \( \overline{P_i} = 0 \) otherwise.

\[
F_{P_i} = E[\overline{P_i}] \\
(\therefore F_{P_i} = 1 \cdot F_{P_i} + 0 \cdot R_{P_i})
\]

Let \( \overline{P_i} \) represent the failure of processor i, \( \overline{M_i} \) represent the failure of memory i \& \( \phi \) be a boolean variable indicating system failure

\[
\phi = \overline{X_{S1}} \overline{X_{S2}} = \left[1 - \left(1 - \overline{P_1}\right) \left(1 - \overline{M_1M_3}\right)\right] \left[1 - \left(1 - \overline{P_2}\right) \left(1 - \overline{M_2M_3}\right)\right]
\]

The subsystem fails when either P_1 fails or both (M_1M_3) fail

\[
= \left(\overline{P_1} + \overline{P_1M_1M_3}\right) \ast \left(\overline{P_2} + \overline{P_2M_2M_3}\right) \\
= \overline{P_1P_2} + \overline{P_1P_2M_2M_3} + \overline{P_1P_2M_1M_3} + \overline{P_1P_2M_1M_2M_3}
\]

\[
E[\phi] = Q_{system} = Q_{P_1}Q_{P_2} + Q_{P_1}R_{P_2}Q_{M_2}Q_{M_3} + R_{P_1}Q_{P_2}Q_{M_1}Q_{M_3} \\
+ R_{P_1}R_{P_2}Q_{M_1}Q_{M_2}Q_{M_3}
\]
Fault Tree using Sharpe

e.g.

\[ \begin{align*}
Q(t) &= 1 - Pe^{-a_1t} - (1-P)e^{-a_2t} \\
\text{hyperexponential} & \quad \text{or} \\
\end{align*} \]

\[ Q(t) = 1 - e^{-\lambda t} \]

exponential failure law

```
bind
  a1  0.028
  a2  0.25
  P   0.5
end
ftrace  series (lambda) Failure rate
  basic B  exp (lambda)
  basic A  gen \n  1, 0, 0 \  * for 1
  -P, 0, -a1 \  * for -Pe^{-a_1t}
  -(1-P), 0, -a2 \  * for -(1-P)e^{-a_2t}
or
  top A B
end
* print
cdf'(series; 0.05)
eval (series; 0.05) 0.5 1.5 0.5
end
```

P.172, chapter 9
e.g. Aircraft flight control system

![Diagram of aircraft flight control system]

**bind**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mIRS</td>
<td>0.000015</td>
</tr>
<tr>
<td>mPRS</td>
<td>0.00099</td>
</tr>
<tr>
<td>mSA</td>
<td>0.000037</td>
</tr>
<tr>
<td>mCS</td>
<td>0.00048</td>
</tr>
</tbody>
</table>

* most susceptible to failure

* : use 4 CS components

**end**

* print
  * format 8
  * expr mean(aircraft)
  * eval (aircraft) 1000 10000 1000
  * expr value(10; aircraft) * unreliability

**end**

This means if 3 out of 4 fail then the subsystem fails
Fault Trees using SHARPE with repeated components
Ex: also see the example in Fig. 9.22
Ex:

\[
\text{ftree system}
\]

\[
\text{basic P}_1 \exp (\lambda P_1)
\]

\[
\text{basic P}_2 \exp (\lambda P_2)
\]

\[
\text{basic M}_1 \exp (\lambda M_1)
\]

\[
\text{basic M}_2 \exp (\lambda M_2)
\]

\[
\text{repeat M}_3 \exp (\lambda M_3)
\]

\[
\text{AND M}_1 M_3 \quad M_1 \quad M_3
\]

\[
\text{AND M}_2 M_3 \quad M_2 \quad M_3
\]

\[
\text{OR system}_1 \quad P_1 \quad M_1 M_3
\]

\[
\text{OR system}_2 \quad P_2 \quad M_2 M_3
\]

\[
\text{AND top system}_1 \quad \text{system}_2 \equiv \text{kofn system}_1 1, 2, P_1 M_1 M_3
\]

\[
\text{AND top system}_1 \quad \text{system}_2 \equiv \text{kofn top 2, 2, system}_1 \text{ system}_2
\]

* print reliability at time t

\[
\text{expr 1-value (t; system)}
\]
2.6 **Series-Parallel Block Diagrams with Components in common**
(Also called Network Reliability Models)

e.g. 

```
  1 3 4
  
  2 3 5
```

Can be arranged as

- A parallel connection of series structures
- A series connection of parallel structures

**Definition:** a minimal path is a minimal set of components whose functioning ensures the functioning of the system.

**Definition:** a minimal cut is a minimal set of components whose failure ensures the failure of the system.
Q: how many minimal paths?
A: 4: \{1,3,5\}, \{1,4\}, \{2,5\}, \{2,3,4\}

Q: how many minimal cuts?
A: 4: \{1,2\}, \{4,5\}, \{1,3,5\}, \{2,3,4\}

Use parallel connection

There are series-parallel diagrams with common components
Another example: TMR is a 2-out-of-3 system

3 minimal paths:
\{1,2\} \{2,3\} \& \{1,3\}

Let $\phi(t)$ be a boolean variable indicating if the system is alive at time $t$, i.e.,
\[
\begin{align*}
\phi(t) &= 1 \text{ if alive} \\
\phi(t) &= 0 \text{ if dead}
\end{align*}
\]

Let $X_i(t)$ be a boolean variable indicating if component $i$ is alive at time $t$, i.e.,
\[
\begin{align*}
X_i(t) &= 1 \text{ if alive} \\
X_i(t) &= 0 \text{ if dead}
\end{align*}
\]

\[
\phi(t) = 1 - \left[ \left(1 - X_1X_2 \right) \left(1 - X_2X_3 \right) \left(1 - X_1X_3 \right) \right]
\]
\[
= 1 - \left(1 - X_1X_2 - X_2X_3 - X_1X_3 + X_1X_2X_3 + X_1X_2X_3^2 + X_1^2X_2X_3 - X_1^2X_2^2X_3^2 \right)
\]
\[
= 1 - \left(1 - X_1X_2 - X_2X_3 - X_1X_3 + 2X_1X_2X_3 \right)
\]

Due to $X_i^2 = X_i$ from $X_i$’s definition
Now

\[ E[\phi(t)] = R(t) \]

\[ \therefore E[\phi(t)] = 1 \cdot \{ \text{prob. it is alive at } t \} + 0 \cdot \{ \text{prob. it fails at } t \} = R(t) \]

\[ \Rightarrow E[\phi(t)] = E\left[ X_1X_2 + X_2X_3 + X_1X_3 - 2X_1X_2X_3 \right] \]

Terms each contain only independent components

\[ = E[X_1X_2] + E[X_2X_3] + E[X_1X_3] - 2E[X_1X_2X_3] \]

\[ \therefore R_{\text{system}} = R_1R_2 + R_2R_3 + R_1R_3 - 2R_1R_2R_3 \]

For identical components, \( R_1 = R_2 = R_3 \), \( R_{\text{system}} = 3R^2 - 2R^3 \)
Modeling with a Reliability Graph

* A reliability graph consists of nodes & directed arcs.
  - source node — no arcs enter it
  - target (sink) node — no arcs leave it

* A system represented by a reliability graph fails when there is no path from the source to the sink.

* arcs are associated with failure distribution (in cdf)
e.g.,

\[
\begin{array}{cccccc}
1 & & 2 & & \text{source} & \lambda_1 \\
& 3 & & & b & \lambda_2 \\
4 & & 5 & & c & \lambda_3 \\
& & & & & d & \lambda_4 \\
& & & & & \text{sink} & \lambda_5
\end{array}
\]

Arcs are associated with exponential distributions with rates $\lambda_i$’s.

```
relgraph bridge(v1, v2, v3, v4, v5)
  a  b  exp(v1)
  a  c  exp(v4)
  b  d  exp(v2)
  c  d  exp(v5)
end
```

```
output for pqcdf (bridge; \(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5\)):

\[
1 - (P(0:a,b)*P(1:b,d) + P(2:a,c)*P(3:c,d)*(1-P(0:a,b)*P(1:b,d)) + P(0:a,b)*Q(1:b,d)*Q(2:a,c)*P(3:c,d)*P(4:b,c) + Q(0:a,b)*P(1:b,d)*P(2:a,c)*Q(3:c,d)*P(4:b,c))
\]

meaning

\[
(1 - e^{-\lambda_1 t})
\]

```

The underlying technique for solving the model is minimal path set & minimal cut set.
What is the reliability graph corresponding to the fault tree model on the left?

Ans:

```
relgraph P 2M3shared
src 1 exp(lambda_P 1)
src 2 exp(lambda_P 2)
1         sink    exp(lambda_M1)
2         sink exp(lambda_M2)
share   sink    exp(lambda_M3)
1        share    inf
2        share    inf
end
* print reliability at time t
expr 1-value(t; P_2M_3shared)
end
```

This means
1 → share &
2 → share
links never fail

See p.353 Appendix B
specifying a component having all its mass
at ∞, i.e., F(t)=0
except at F(∞)=1