Chapter 8.
Calculation of PFD using Markov

Mary Ann Lundteigen Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1)

NTNU – Trondheim
Norwegian University of
Science and Technology

Learning Objectives

The main learning objectives associated with these slides are to:

- Study how Markov analysis can be used to calculate the PFD
- Become familiar with how CCFs and the effects of DU and DD failures are included
- Understand how Markov model can be used to incorporate the effects of demand rate and demand duration

The slides include topics from Chapter 8 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

Outline of Presentation

Markov Approach in Brief

Some keywords:

- Suitable for multistate and dynammic systems
- Must satisfy the Markov properties
- Can model system states, beyond failure states
- Can be used to find analytical formulas and calculate steady state and time-dependent probabilities
- Can be used to determine mean time to first failure (MTTF_S)

Figure: Russian mathematician Andrei Markov (1856-1922)

The Markov approach - step by step

1. Define system states (table format)
2. Set up the transition diagram (“Markov model”)
3. Include the transition rates
4. Set up the transition matrix
5. Do your calculations, either in terms of time dependent analysis or in terms of steady state

The Markov approach - example

Consider a 2oo3 voted system of identical components.

- Step 1: Set up the system states, first assuming no common cause failures.

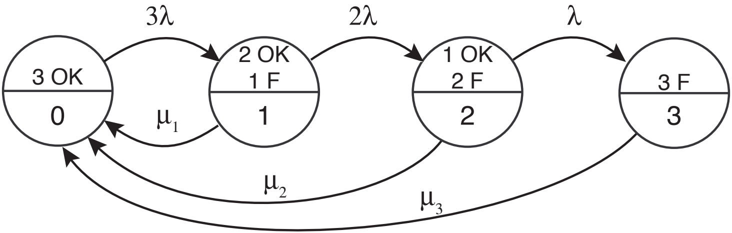
State	State description
0	Three channels are functioning
1	Two channels are functioning and one is failed
2	One channel is functioning and two are failed
3	Three channels are failed

It is assumed that repair always restores the system to a fully functional state.

The Markov Approach - Example

Consider a 2oo3 voted system of identical components.

- Step 2 and 3: Set up the Markov model, and include the transition rates



The failed states of this subsystem are state 2 and state 3.

The Markov approach - example

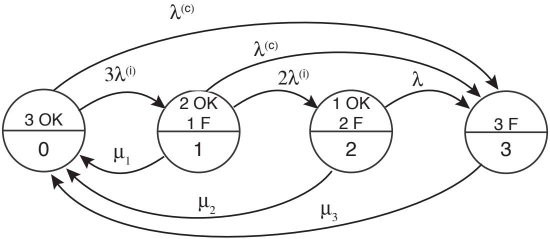
Consider a 2oo3 voted system of identical components.

- Step 4: Set up the transition matrix

$$\mathbb{A} = \begin{pmatrix} -3\lambda & 3\lambda & 0 & 0 \\ \mu_1 & -(\mu_1 + 2\lambda) & 2\lambda & 0 \\ \mu_2 & 0 & -(\mu_2 + \lambda) & \lambda \\ \mu_3 & 0 & & -\mu_3 \end{pmatrix}$$

The Markov Approach - Example

- What if CCFs are included?



$$\mathbb{A} = \begin{pmatrix} -(3\lambda^{(i)} + \lambda^{(c)}) & 3\lambda^{(i)} & 0 & \lambda^{(c)} \\ \mu_1 & -(\mu_1 + 2\lambda^{(i)} + \lambda^{(c)}) & 2\lambda^{(i)} & \lambda^{(c)} \\ \mu_2 & 0 & -(\mu_2 + \lambda) & \lambda \\ \mu_3 & 0 & 0 & -\mu_3 \end{pmatrix}$$

The Markov Approach - What to Calculate?

With basis in the Markov model, it is possible to calculate:

- Time dependent probabilities ("Probability of being in state "i" at time t)
- Steady state probabilities ("Average probability of being in state "i", % of time in state "i")
- Visit frequency to a specific state or a set of states (e.g., into the failed state)
- Mean time to first entry to a specific state (e.g., mean time to failure)

Using Markov to Calculate PFD

Let $\mathcal{D}$ be the set of states where the voted system is down (e.g., in the failed state). Two calculate PFD$_{avg}$, we have two options:

- Option 1: Calculations based on time dependent probabilities:

$$PFD(t) = \sum_{i \in \mathcal{D}} P_i(t)$$

  The PFD$_{avg}$ becomes:

$$PFD_{avg} = \frac{1}{\tau} \int_0^{\tau} PFD(t)\, dt$$

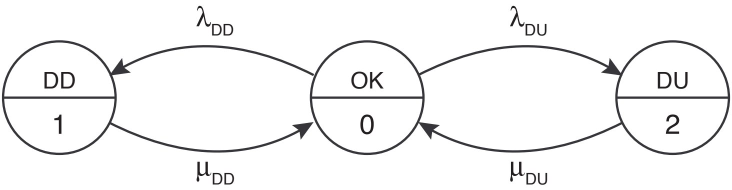
- Option 2: Calculations based on steady state probabilities. In this case:

$$PFD_{avg} = \sum_{i \in \mathcal{D}} P_i$$

Using Steady-State Probabilities

Consider a single system that may fail due to DU or DD failures. The system states are:

State	State description
0	The channel is functioning (no DU or DD failures)
1	The channel has a DD fault
2	The channel has a DU fault



Parameters

The Markov transition matrix becomes:

$$\mathbb{A} = \begin{pmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & -\mu_{DD} & 0 \\ \mu_{DU} & 0 & -\mu_{DU} \end{pmatrix}$$

Parameter	Description	Comments
λ_{DU}	Dangerous undetected (DU) failure rate	
λ_{DD}	Dangerous undetected (DD) failure rate	
μ_{DU}	“Repair” rate of DU failures	$1/(\frac{\tau}{2} + MRT)$
μ_{DD}	Repair rate of DD failures	$1/MTTR$

Solving Steady State Equations

Three states (0,1,2) means that we need three equations to solve for P_0, P_1, and P_2. The approach is:

- Step 1: Set up the steady state equations from $\mathbf{P}\mathbb{A} = \mathbf{0}$

The main approach is to (i) choose two equations (out of the three) from the above equations, preferably the ones with most zeros, plus (ii) the equation $P_0 + P_1 + P_2 = 1$. The equations then becomes:

$$
\begin{aligned}
P_0 + P_1 + P_2 &= 1 \\
\lambda_{DD} P_0 - \mu_{DD} P_1 &= 0 \\
\lambda_{DU} P_0 - \mu_{DU} P_2 &= 0
\end{aligned}
$$

Solving Steady State Equations (cont.)

- Step 2: Solve for P_0, P_1, and P_2:

By hand-calculations or e.g. MAPLE, we find that:

$$
\begin{aligned}
P_0 &= \frac{1}{\frac{\lambda_{DD}}{\mu_{DD}} + \frac{\lambda_{DU}}{\mu_{DU}} + 1} \\
P_1 &= \frac{\lambda_{DD}}{\mu_{DD}} P_0 \\
P_2 &= \frac{\lambda_{DU}}{\mu_{DU}} P_0
\end{aligned}
$$

Using Maple - Code Example

Solving steady state Markov

#Adjust value of size and insert just
#the non−empty elements of transition matrix
 # Code adapted from
 # http://www.doc.ic.ac.uk/~mjb04/markov.pdf
#The current setup is for figure 3.19 in
 # Fares Innal PhD thesis

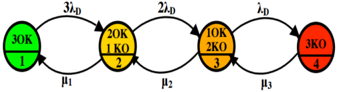


Figure 3.19: Approached Markov model relating to 1oo3 architecture

```
restart;
with(linalg) :
size := 4; #Number of states
A := array(sparse, 1 ..size, 1 ..size); #Transition matrix
e := array(sparse, 1 ..size);

# Entering non-zero transitions (except diagonal values)
A[1, 2] := 3·lambda[D];
A[2, 1] := mu[1];

A[2, 3] := 2·lambda[D];
A[3, 2] := mu[2];

A[3, 4] := 1·lambda[D];
A[4, 3] := mu[3];

#Filling in the diagonal values:
for i to size do
s := 0 :
for j to size do
s := s + A[i, j]
od;
A[i, i] := -s
od;

#Preparing for using linsolve to find steady state
Atran := transpose(A);
for i to size do Atran[size, i] := 1 od;
e[size] := 1;
p := linsolve(Atran, e);
```

Solving Steady State Equations (cont.)

- Step 3: Determine PFD$_{avg}$:

Since the failed states are state 1 and state 2, we find that:

$$PFD_{avg} = P_1 + P_2 = \frac{\lambda_{DD} MTTR + \lambda_{DU}(\frac{\tau}{2} + MRT)}{\lambda_{DD} MTTR + \lambda_{DU}(\frac{\tau}{2} + MRT) + 1}$$

$$\approx \lambda_{DD} MTTR + \lambda_{DU}(\frac{\tau}{2} + MRT)$$

- Note that μ_{DD} and μ_{DU} have been replaced by $1/MTTR$ and $1/(\frac{\tau}{2} + MRT)$
- The approximation is possible because the denominator is close to 1 with λ_{DD} and λ_{DU} being very small

Solving Steady State Equations (cont.)

- Step 4: Insert the values of the parameters and calculate the result:

using input data is table 7.2 in textbook, we get:

- The PFD_{avg} without the approximation becomes $4.418 \cdot 10^{-3}$.
- The PFD_{avg} with the approximation becomes $4.438 \cdot 10^{-3}$.

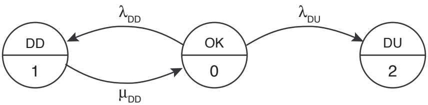
For more examples, visit the textbook.

Using Time-Dependent Probabilities

Consider a single system that may fail due to DU or DD failures. The system states are:

State	State description
0	The channel is functioning (no DU or DD failures)
1	The channel has a DD fault
2	The channel has a DU fault

Note that we do not need a return from the failed state after a DU failure. We assume that the average calculated for the first proof test interval is equal to the long term average.



Solving Time-Dependent Probabilities

With the absorbing state, the new transition matrix becomes:

$$\mathbb{A}^* = \begin{pmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & -\mu_{DD} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

With one of the rows having "just zeros", we see that $\mathrm{P}_2(t)$ and $\dot{\mathbf{P}_2}(\mathbf{t})$ disappears from the equation. To solve the equation, we reduce the transition matrix (now named $\mathbb{A}_t$:) to include only "up-states":

$$\mathbb{A}_t = \begin{pmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} \\ \mu_{DD} & -\mu_{DD} \end{pmatrix}$$

Solving Time-Dependent Probabilities (cont.)

- Step 2: Solve for $P_0(t)$ and $P_1(t)$ ($P_2(t)$ can be found from the two first):
  - The Laplace transform becomes:

$$(P_0^*(s), P_1^*(s))\mathbb{A}_t = \begin{pmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} \\ \mu_{DD} & -\mu_{DD} \end{pmatrix} = (sP_0^*(s) - 1, sP_1^*(s))$$

    The LinearAlgebra (for handling matrix operations) and the inttrans packages (with invlaplace command) may be used in MAPLE to solve the equations.
  - The time-dependent state solution becomes:

$$(P_0(t), P_1(t))\mathbb{A}_t = \begin{pmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} \\ \mu_{DD} & -\mu_{DD} \end{pmatrix} = (P_0\dot{(}t), P_0\dot{(}t))$$

    The dsolve command in MAPLE may be used to solve for the time-dependent state probabilities.

Solving Time-Dependent Probabilities (cont.)

- Step 3 Find PFD$_{avg}$:
  - Once the state probabilities have been found, we can calculate PFD$_{avg}$ as:

$$PFD_{avg} = \frac{1}{\tau}\int_0^{\tau} \sum_{i \in \mathcal{D}} P_i(t)\,dt = 1 - \frac{1}{\tau}\int_0^{\tau} \sum_{i \in \mathcal{U}} P_i(t)\,dt$$

  where $\mathcal{D}$ are the states that are defined as failed state, and $\mathcal{U}$ are the states where the system is functioning (even if degraded).

MAPLE may be used for this purpose using the int-function.

Solving time-dependent state equations (continued)

- Step 4: Insert the values of the parameters and calculate the result:
  - Reference to input data is table 7.2 in textbook.
  - The PFD_{avg} without the approximation becomes $4.418 \cdot 10^{-3}$.
  - The PFD_{avg} with the approximation becomes $4.438 \cdot 10^{-3}$.

For more examples, visit the textbook.

Using Maple - code example

Code:

```
restart; with(DEtools) : with(LinearAlgebra) :
A := Matrix([[-lambda, lambda], [mu,-mu]]);
ATrans := Transpose(A);
Solutions := matrixDE(ATrans, t);
S := Solutions[1];
S0 := eval(S, t=0);
S0Matrix := Matrix([S0]);
P0 := ⟨1, 0⟩; #Alternatively, we could write P0:=Vector([1,0])
C0 := LinearSolve(S0Matrix, P0);
P := S.C0;
```

Result:

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

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

$$Solutions := \left[\begin{bmatrix} 1 & e^{-(\lambda+\mu)t} \\ \frac{\lambda}{\mu} & -e^{-(\lambda+\mu)t} \end{bmatrix}, \begin{bmatrix} 0 & 0 \end{bmatrix} \right]$$

$$S := \begin{bmatrix} 1 & e^{-(\lambda+\mu)t} \\ \frac{\lambda}{\mu} & -e^{-(\lambda+\mu)t} \end{bmatrix}$$

$$S0 := \begin{bmatrix} 1 & 1 \\ \frac{\lambda}{\mu} & -1 \end{bmatrix}$$

$$S0Matrix := \begin{bmatrix} 1 & 1 \\ \frac{\lambda}{\mu} & -1 \end{bmatrix}$$

$$P0 := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$C0 := \begin{bmatrix} \frac{\mu}{\lambda+\mu} \\ \frac{\lambda}{\lambda+\mu} \end{bmatrix}$$

$$P := \begin{bmatrix} \frac{\mu}{\lambda+\mu} + \frac{e^{-(\lambda+\mu)t}\lambda}{\lambda+\mu} \\ \frac{\lambda}{\lambda+\mu} - \frac{e^{-(\lambda+\mu)t}\lambda}{\lambda+\mu} \end{bmatrix}$$

Mean Time to First Failure (MTTF_S)

The mean time to first failure, here called MTTF_S, can be solved by setting $s = 0$ in the Laplace transform equations:

- Consider the single system previously addressed for time-dependent probabilities. With s=0 in the Laplace transform we get:

$$[P_0^*(0), P_1^*(0)]\mathbb{A}_t = [P_0^*(0), P_1^*(0)] \begin{pmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} \\ \mu_{DD} & -\mu_{DD} \end{pmatrix} = [-1, 0]$$

- By using hand-calculation or MAPLE, the result becomes:

$$MTTF_S = {P_0}^*(0) + {P_1}^*(0) = \frac{1}{\lambda_{DU}} + \frac{\lambda_{DD}}{\mu_{DD}\lambda_{DU}} \approx \frac{1}{\lambda_{DU}}$$

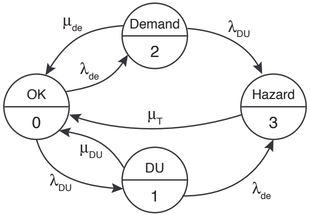
(You may verify the approximation by inserting parameter values from table 7.2 in textbook. See also Chapter 5.5.5)

Including Demand Duration

Consider a safety-critical system (single) that may fail due to DU failure (we omit DD failures). We assume that the system is operating in the low-demand mode, and that a failure to operate on demand may result in a hazardous state. It is further assumed that the SIF is NOT the ultimate safety barrier, so a restoration is possible.

The system states are:

State	State description
0	The channel is functioning (no DU failure)
1	The channel has a DU fault
2	A demand has occurred
3	The system is in a hazardous state



Transition Matrix

The Markov transition matrix becomes:

$$\mathbb{A} = \begin{pmatrix} -(\lambda_{\mathrm{DU}} + \lambda_{\mathrm{de}}) & \lambda_{\mathrm{DU}} & \lambda_{\mathrm{de}} & 0 \\ \mu_{\mathrm{DU}} & -(\mu_{\mathrm{DU}} + \lambda_{\mathrm{de}}) & 0 & \lambda_{\mathrm{de}} \\ \mu_{\mathrm{de}} & 0 & -(\mu_{\mathrm{de}} + \lambda_{\mathrm{DU}}) & \lambda_{\mathrm{DU}} \\ \mu_{\mathrm{T}} & 0 & 0 & -\mu_{\mathrm{T}} \end{pmatrix}$$

Parameter	Description
λ_{DU}	Dangerous undetected (DU) failure rate
λ_{de}	Demand rate
μ_{de}	Restoration rate after demand
μ_{T}	Restoration rate for Hazardous event

Solving for PFD_{avg}

It is assumed that the time dependent probabilities have been found using MAPLE (Inverse laplace transforms or integration). Then:

$$PFD_{avg} = \frac{1}{\tau}\int_0^{\tau} P_1(t)\,dt$$

The resulting equation is rather extensive.

For high-reliability channels with short demand duration we have $\lambda_{\mathrm{DU}} \ll \mu_{\mathrm{DU}} \ll \mu_{\mathrm{de}}$. In this case, we get approximately

$$\mathrm{PFD}_{1,\mathrm{avg}} \approx \frac{\lambda_{\mathrm{DU}}\mu_{\mathrm{de}}}{(\lambda_{\mathrm{de}} + \mu_{\mathrm{de}})(\lambda_{\mathrm{de}} + \mu_{\mathrm{DU}})}$$

When $\lambda_{\mathrm{de}} \ll \mu_{\mathrm{de}}$, the following approximation is also adequate

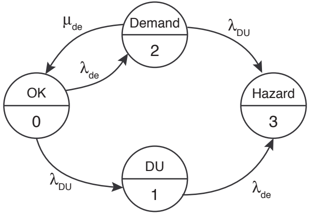
$$\mathrm{PFD}_{2,\mathrm{avg}} \approx \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{de}} + \mu_{\mathrm{DU}}}$$

Including Demand Duration

Consider a safety-critical system (single) that may fail due to DU failure (we omit DD failures). We assume that the system is operating in the low-demand mode, and that a failure to operate on demand may result in a hazardous state. In this case, however, the SIF IS the ultimate safety barrier.

The system states are:

State	State description
0	The channel is functioning (no DU failure)
1	The channel has a DU fault
2	A demand has occurred
3	The system is in a hazardous state



Solving for PFD$_{avg}$

Since the SIF is the ultimiate safety barrier, state 3 is an absorbing state.

- The PFD$_{avg}$ becomes:

$$PFD_{avg} = \frac{1}{\tau}\int_0^{\tau} P_1(t)\,dt$$

The resulting equation is, as for the SIF that was not the ultimate safety barrier, rather extensive.

Solving for HEF(t) and HEF$_{avg}$

For both situations, i.e. that the SIF is the ultimate safety barrier or is not the ultimate safety barrier, we can find the hazardous event frequency (HEF):

- The PFD$_{avg}$ becomes:

$$PFD_{avg} = \frac{1}{\tau}\int_0^{\tau} P_1(t)\,dt$$

The resulting equation is, as for the SIF that was not the ultimate safety barrier, rather extensive.

$$\text{HEF}(t) = P_1(t)\cdot\lambda_{\text{de}} + P_2(t)\cdot\lambda_{\text{DU}}$$

The average HEF in the proof test interval $(0,\tau)$ is

$$\text{HEF} = \frac{1}{\tau}\int_0^{\tau}\text{HEF}(t)\;dt = \frac{1}{\tau}\int_0^{\tau}\left(P_1(t)\cdot\lambda_{\text{de}} + P_2(t)\cdot\lambda_{\text{DU}}\right)\;dt$$

PDS Method and C_{MooN}

If the PDS method is used, it is necessary to address the C_{MooN} factor for the transitions.

- C_{MooN} gives the correction for $N - M + 1..N$ failures in a $MooN$ voted system
- This means that C_{1oo3} includes 3 failures, while C_{2oo4} accounts for 3 and 4 failures
- Consider a CCF transition between two states. Then (C(N-i+1)ooN – C(N-i)ooN) is the correction factor for the case that exactly i out of N components fails

PDS Method and C_{MooN}

Consider a subsystem voted 2oo4. In this case, the possible transitions becomes: