Exercise 9

EDA122/DIT061 Fault-Tolerant Computer Systems
DAT270 Dependable Computer Systems

Autumn 2011

Exam problem 2004-08-23

A fault-tolerant computer node consists of three redundant processor modules (PM 1 to PM 3) and two redundant sensors (S1 and S2). The processor modules operates in active redundancy. The sensors are read by the processor modules via point-to-point connections.

1 a

Fault/error containment aims at preventing faults/errors in one unit from affecting other units.

- Fault/error containment should be maintained at all unit interfaces where fault and error propagation may lead to a reduction of system reliability.
- Fault/error containment is not needed between units that constitute a series system.

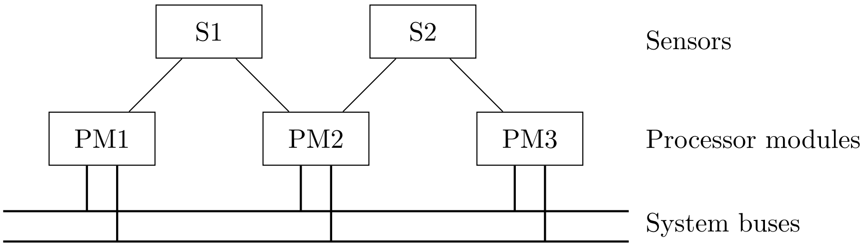


Figure 1: Computer node in Problem 1 from exam 2004-08-23

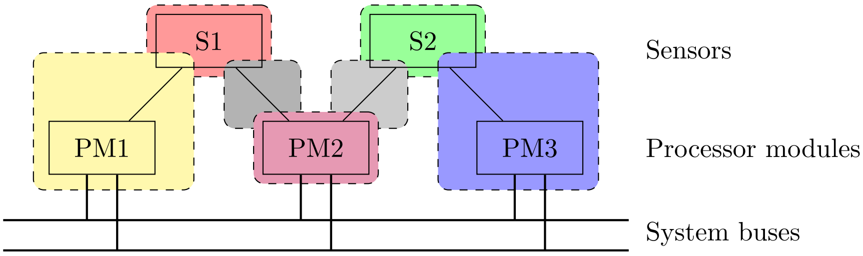


Figure 2: Fault containment regions

There are seven fault containment regions:

- S1
- PM1 + sensor bus
- PM2
- Sensor bus between S1 and PM2
- Sensor bus between S2 and PM2

- S2
- PM3 + sensor bus

1 b

Assume that the failure rates of the sensors and the point-to-point connections are negligible and that the life times of the processor modules are exponentially distributed with the failure rate λ_p. The coverage factor for faults occurring in the processor modules is c. Derive an expression for the reliability of the node. Disregard the system buses.

Solution

The failure rates for the sensors and point-to-point connections are negligible, and the buses are not included ⇒ Only processor failures can occur!

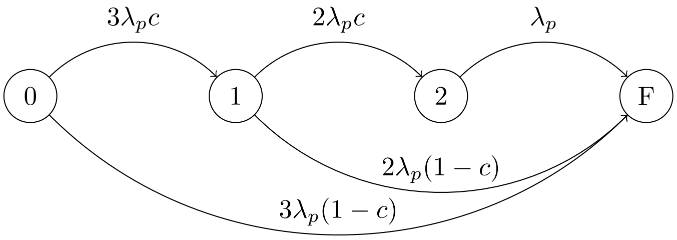


Figure 3: Markov chain model

$$\begin{aligned}
P'(t) &= P(t)Q \\
P(0) &= \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \\
Q &= \begin{bmatrix} -3\lambda_p & 3\lambda_p c & 0 & 3\lambda_p(1-c) \\ 0 & -2\lambda_p & 2\lambda_p c & 2\lambda_p(1-c) \\ 0 & 0 & -\lambda_p & \lambda_p \\ 0 & 0 & 0 & 0 \end{bmatrix}
\end{aligned}$$

Laplace transform:

$$\mathcal{L}\{P'(t) = P(t)Q\} \Rightarrow sP(s) - P(0) = P(s)Q$$

$$\begin{cases} sP_0 - 1 &= -3\lambda_p P_0 \\ sP_1 &= 3\lambda_p c P_0 - 2\lambda_p P_1 \\ sP_2 &= 2\lambda_p c P_1 - \lambda_p P_2 \\ sP_3 &= \dots \end{cases}$$

$$\begin{aligned}
P_0 &= \frac{1}{s+3\lambda_p} \\
P_1 &= \frac{3\lambda_p c}{s+2\lambda_p} P_0 = \frac{3\lambda_p c}{s+2\lambda_p}\frac{1}{s+3\lambda_p} = 3c\left(\frac{1}{s+2\lambda_p} - \frac{1}{s+3\lambda_p}\right)
\end{aligned}$$

$$\begin{aligned}
P_2 &= \frac{2\lambda_p c}{s+\lambda_p}P_1 = \frac{6\lambda_p c^2}{s+\lambda_p}\left(\frac{1}{s+2\lambda_p}-\frac{1}{s+3\lambda_p}\right)\\
&= 6\lambda_p c^2\left(\frac{1}{\lambda_p}\left(\frac{1}{s+\lambda_p}-\frac{1}{s+2\lambda_p}\right)-\frac{1}{2\lambda_p}\left(\frac{1}{s+\lambda_p}-\frac{1}{s+3\lambda_p}\right)\right)\\
&= 3c^2\left(\frac{2}{s+\lambda_p}-\frac{2}{s+2\lambda_p}-\frac{1}{s+\lambda_p}+\frac{1}{s+3\lambda_p}\right)\\
&= 3c^2\left(\frac{1}{s+\lambda_p}-\frac{2}{s+2\lambda_p}+\frac{1}{s+3\lambda_p}\right)\\
P_3 &= \ldots
\end{aligned}$$

$$\begin{aligned}
P_0(t) &= e^{-3\lambda t}\\
P_1(t) &= 3c\left(e^{-2\lambda_p t}-e^{-3\lambda_p t}\right)\\
P_2(t) &= 3c^2\left(e^{-\lambda_p t}-2e^{-2\lambda_p t}+e^{-3\lambda_p t}\right)\\
R(t) &= P_0(t)+P_1(t)+P_2(t)\\
&= e^{-3\lambda_p t}\left(1-3c+3c^2\right)+e^{-2\lambda_p t}\left(3c-6c^2\right)+3c^2e^{-\lambda_p t}
\end{aligned}$$

1 c

Derive an expression for the reliability of the node. Assume ideal coverage (c = 1) and that the failure rate of the point-to-point connections is negligible. Disregard the system buses.

$$\begin{aligned}
R_{PM}(t) &= e^{-\lambda_p t}\\
R_S(t) &= e^{-\lambda_s t}
\end{aligned}$$

$$\begin{array}{lll}
R_{system} & = & \\
 & R_{PM}^3R_S^2 & \text{all modules are ok}\\
 & +3R_{PM}^2(1-R_{PM})R_S^2 & \text{one PMs is broken}\\
 & +3R_{PM}(1-R_{PM})^2R_S^2 & \text{two PMs are broken}\\
 & +R_{PM}^3 2R_S(1-R_S) & \text{one sensors is broken}\\
 & +3R_{PM}^2(1-R_{PM})2R_S(1-R_S) & \text{one PM and one sensor broken}\\
 & +4R_{PM}(1-R_{PM})^2R_S(1-R_S) & \text{two PMs and one sensor broken}\\
 & & \text{(not including PM1+PM2+S2}\\
 & & \text{or PM2+PM3+S1)}
\end{array}$$

Only one PM broken:

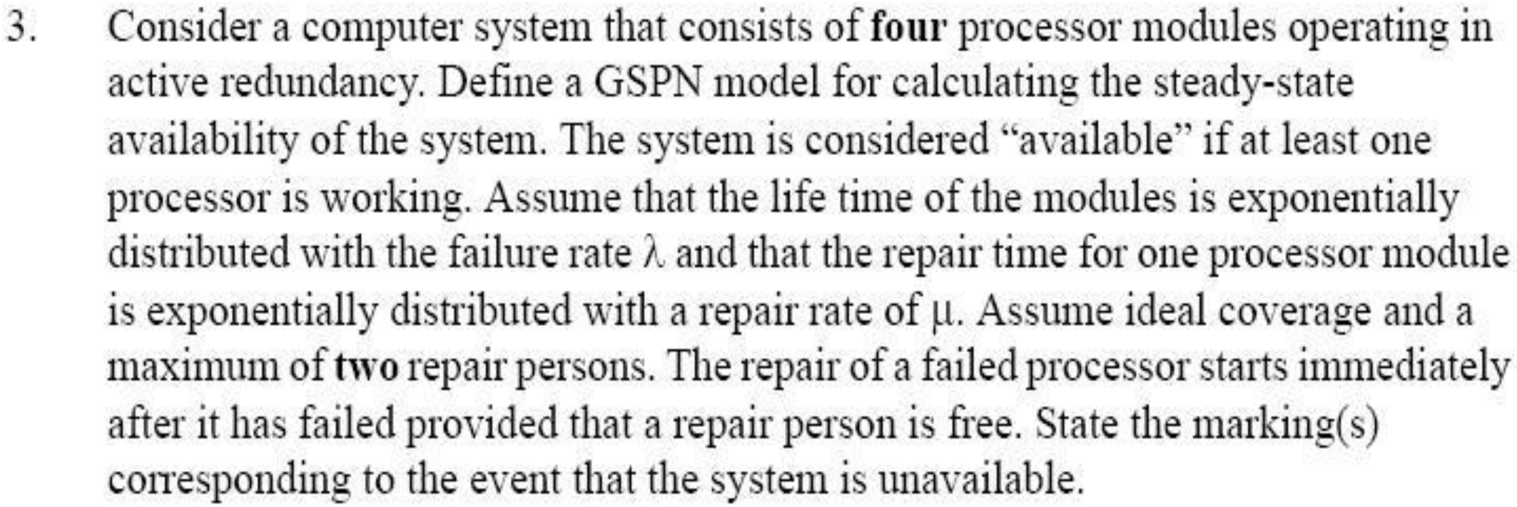
$$\begin{array}{rl}
\text{PM2+PM3 working} & R_{PM}^2(1-R_{PM})\\
\text{PM1+PM3 working} & R_{PM}^2(1-R_{PM})\\
\text{PM1+PM2 working} & R_{PM}^2(1-R_{PM})\\
\Longrightarrow & 3R_{PM}^2(1-R_{PM})
\end{array}$$

Two PMs and one sensor broken:

$$\begin{array}{rl}
\text{PM3+S2 working} & R_{PM}(1-R_{PM})^2R_S(1-R_S)\\
\text{PM1+S1 working} & R_{PM}(1-R_{PM})^2R_S(1-R_S)\\
\text{PM2+S1 working} & R_{PM}(1-R_{PM})^2R_S(1-R_S)\\
\text{PM2+S2 working} & R_{PM}(1-R_{PM})^2R_S(1-R_S)\\
\Longrightarrow & 4R_{PM}(1-R_{PM})^2R_S(1-R_S)
\end{array}$$

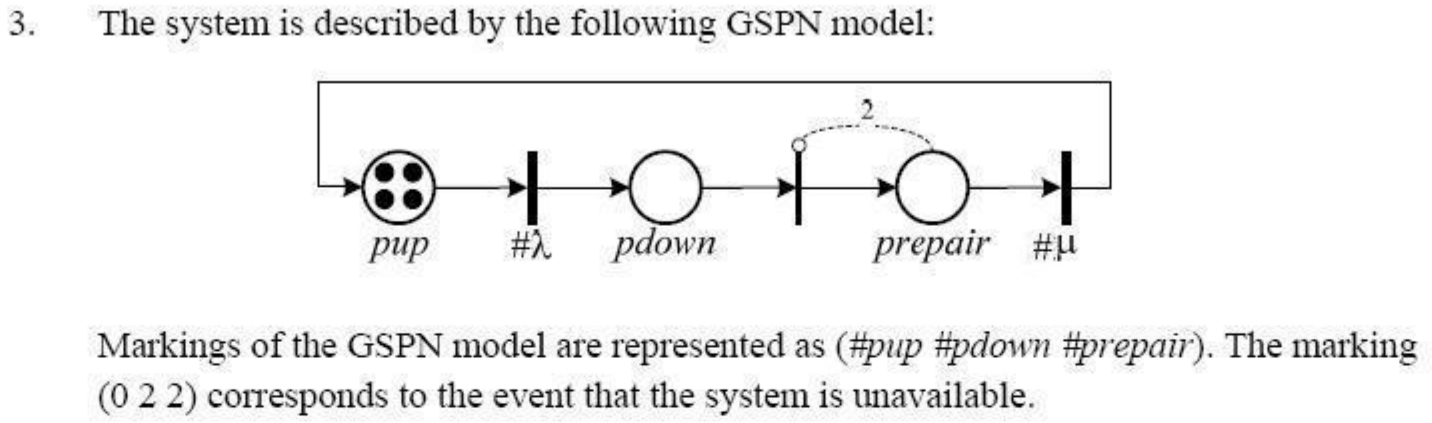
The system does not work if three processor modules or two sensors are broken or if S2+PM1+PM2 or S1+PM2+PM3 are broken.

Exam 2010-01-11
Problem 3



3. Consider a computer system that consists of **four** processor modules operating in active redundancy. Define a GSPN model for calculating the steady-state availability of the system. The system is considered "available" if at least one processor is working. Assume that the life time of the modules is exponentially distributed with the failure rate λ and that the repair time for one processor module is exponentially distributed with a repair rate of μ. Assume ideal coverage and a maximum of **two** repair persons. The repair of a failed processor starts immediately after it has failed provided that a repair person is free. State the marking(s) corresponding to the event that the system is unavailable.

Exam 2010-01-11
Solution 3



3. The system is described by the following GSPN model:

Markings of the GSPN model are represented as (#*pup* #*pdown* #*prepair*). The marking (0 2 2) corresponds to the event that the system is unavailable.

- Exam 2011-08-16 problem 1
  - You can find the problem and the solution on the course homepage under folder named “Old Exams”.