Exercise 7

In this exercise, we solve Problems 5.9, 5.10 and a problem from an old exam given.

Problem 5.9

A fault tolerant computer system is built from two subsystems, one subsystem consists of three processor modules and the other subsystem consist of two I/O modules. One processor module and one I/O module must be working in order for the system to deliver its service. The two subsystems are connected by a number of buses providing full-connectivity between all modules. Both subsystems use cold stand-by spares. The failure rate is λ_p for an active processor and λ_{io} for an active I/O-module. All modules are assumed to obey the exponential failure law. The failure rate for buses and cold stand-by spares are assumed to be negligible and the coverage is assumed to be ideal. Derive an expression for the system reliability.

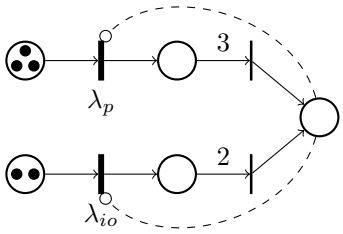

Figure 1: Petri Net for Problem 5.9

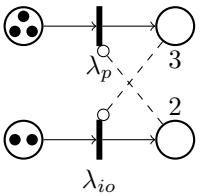

Figure 2: Alternative Petri Net for Problem 5.9

Divide and Conquer

The analysis of large systems can be simplified by dividing the system into a number of independent subsystems. We call these subsystems primary subsystems. A system consists of several of primary subsystems, which all need to function in order for the system to function. At the highest level of abstraction, the system looks at a series system.

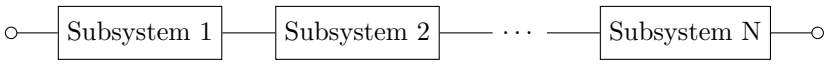

Figure 3: Reliability Block Diagram

Definitions:

- A primary subsystem is one which is essential to the system, i.e., a failure of a primary subsystems always results in a system failure.
- If all failures of a primary subsystem are mutually independent of all failures of all other subsystem, then it is an independent primary subsystem

Solution

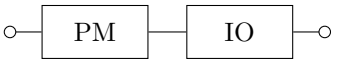

Figure 4: RBD for Problem 5.9

$$R(t) = R_{PM}(t) \times R_{IO}(t)$$

Processor modules – Cold Standby

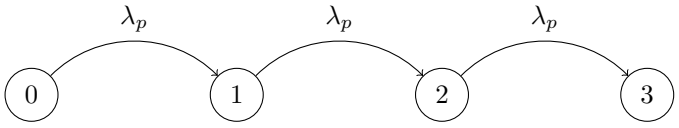

Figure 5: Markov chain for processor modules

State	Primary	Cold stand-by
0	1	2
1	1	1
2	1	0
F	0	0

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

Laplace transform:

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

$$\begin{cases} sP_0 - 1 &= -\lambda_p P_0 \\ sP_1 &= \lambda_p P_0 - \lambda_p P_1 \\ sP_2 &= \lambda_p P_1 - \lambda_p P_2 \\ sP_F &= \lambda_p P_2 \end{cases}$$

$$\begin{aligned} P_0 &= \frac{1}{s+\lambda_p} \\ P_1 &= \frac{\lambda_p}{s+\lambda_p} P_0 = \frac{\lambda_p}{s+\lambda_p}\frac{1}{s+\lambda_p} = \frac{\lambda_p}{(s+\lambda_p)^2} \\ P_2 &= \frac{\lambda_p}{s+\lambda_p} P_1 = \frac{\lambda_p}{s+\lambda_p}\frac{\lambda_p}{(s+\lambda_p)^2} = \frac{\lambda_p^2}{(s+\lambda_p)^3} \\ P_F &= \frac{\lambda_p}{s} P_2 \end{aligned}$$

Inverse Laplace transform:

$$\mathcal{L}^{-1}\left\{\frac{n!}{(s+a)^{n+1}}\right\} = t^n e^{-at}$$

$$\begin{aligned} P_0(t) &= e^{-\lambda_p t} \\ P_1(t) &= \lambda_p t e^{-\lambda_p t} \\ P_2(t) &= \frac{\lambda_p^2 t^2}{2} e^{-\lambda_p t} \\ R_{PM}(t) &= P_0(t) + P_1(t) + P_2(t) = \left(1 + \lambda_p t + \frac{\lambda_p^2 t^2}{2}\right) e^{-\lambda_p t} \end{aligned}$$

IO modules – Cold Standby

State	Primary	Cold standby
0	1	1
1	1	0
2	0	0

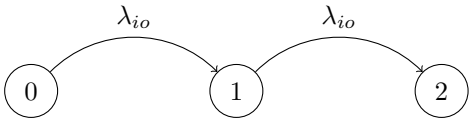

Figure 6: Markov chain for IO modules

$$Q = \begin{bmatrix} -\lambda_{io} & \lambda_{io} & 0 \\ 0 & -\lambda_{io} & \lambda_{io} \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{cases} sP_0 - 1 = -\lambda_{io} P_0 \\ sP_1 = \lambda_{io} P_0 - \lambda io P_1 \\ sP_F = \lambda_{io} P_1 \end{cases}$$

$$\begin{aligned} P_0 &= \frac{1}{s + \lambda_{io}} \\ P_1 &= \frac{\lambda_{io}}{s + \lambda_p} P_0 = \frac{\lambda_{io}}{(s + \lambda_{io})^2} \\ P_F &= \dots \end{aligned}$$

Inverse Laplace transform:

$$\begin{aligned} P_0(t) &= e^{-\lambda_{io} t} \\ P_1(t) &= \lambda_{io} t e^{-\lambda_{io} t} \\ R_{IO}(t) &= P_0(t) + P_1(t) = (1 + \lambda_{io} t)\, e^{-\lambda_{io} t} \end{aligned}$$

System

Reliability for the entire system is

$$\begin{aligned} R_{PM}(t) &= \left(1 + \lambda_p t + \frac{\lambda_p^2 t^2}{2}\right) e^{-\lambda_p t} \\ R_{io}(t) &= (1 + \lambda_{io} t)\, e^{-\lambda_{io} t} \\ R(t) &= R_{PM}(t) \times R_{IO}(t) \end{aligned}$$

Problem 5.10

Derive an expression for the steady-state availability of a system consisting of *two modules operating in active redundancy*. The modules are assumed to be fail-silent and should under normal circumstances produce identical results. *If a fail-silent violation occurs*, which implies that the modules produces non-identical results, then *the system is immediately shut-down by an external unit*. The life time of both modules is exponentially distributed with the failure rate λ. *The assumption coverage for the fail-silent property is c*. The repair time for each of the modules is exponentially distributed with a repair rate μ. If the system crashes due to a fail-silent violation, then the system repair time can be approximated as being exponentially distributed with a repair rate ρ. Only one repair-person is available.

Solution

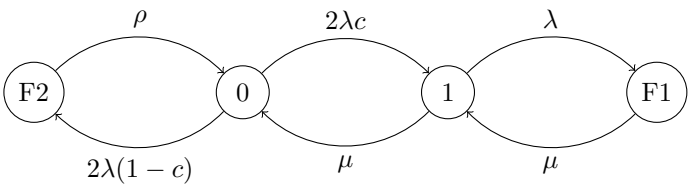

Figure 7: Markov chain for Problem 5.10

This is a birth and death process (see, e.g., Mathematics Handbook, pp. 440-441).

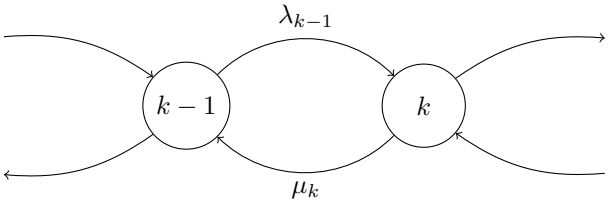

Figure 8: General birth and death process

$$\begin{aligned} \Pi_k &= \frac{\lambda_{k-1}}{\mu_k}\Pi_{k-1} \\ \sum_k \Pi_k &= 1 \end{aligned}$$

Using the formulas above, we get:

$$\Pi_0 = \frac{\rho}{2\lambda(1-c)}\Pi_{F2}$$

$$
\begin{aligned}
\Pi_1 &= \frac{2\lambda c}{\mu}\Pi_0 = \frac{2\lambda c}{\mu}\frac{\rho}{2\lambda(1-c)}\Pi_{F2} = \frac{c\rho}{\mu(1-c)}\Pi_{F2} \\
\Pi_{F1} &= \frac{\lambda}{\mu}\Pi_1 = \frac{\lambda}{\mu}\frac{c\rho}{\mu(1-c)}\Pi_{F2} = \frac{\lambda c\rho}{\mu^2(1-c)}\Pi_{F2} \\
1 &= \Pi_0 + \Pi_1 + \Pi_{F1} + \Pi_{F2} \Rightarrow \\
1 &= \Pi_{F2}\left(1 + \frac{\rho}{2\lambda(1-c)} + \frac{c\rho}{\mu(1-c)} + \frac{c\lambda\rho}{\mu^2(1-c)}\right) \\
&= \Pi_{F2}\left(\frac{2\lambda\mu^2(1-c) + \rho\mu^2 + 2\lambda\mu c\rho + 2\lambda^2 c\rho}{2\lambda\mu^2(1-c)}\right) \\
\Pi_{F2} &= \frac{2\lambda\mu^2(1-c)}{2\lambda\mu^2(1-c) + \rho\mu^2 + 2\lambda\mu c\rho + 2\lambda^2 c\rho} \\
\lim_{t\to\infty} A(t) &= \Pi_0 + \Pi_1 \\
&= \left(\frac{\rho}{2\lambda(1-c)} + \frac{c\rho}{\mu(1-c)}\right)\Pi_{F2} \\
&= \frac{\rho\mu + 2\lambda c\rho}{2\lambda\mu(1-c)}\Pi_{F2} \\
&= \frac{\rho\mu + 2\lambda\rho c}{2\lambda\mu(1-c)}\frac{2\lambda\mu^2(1-c)}{2\lambda\mu^2(1-c) + \rho\mu^2 + 2\lambda\mu c\rho + 2\lambda^2 c\rho} \\
&= \frac{\rho\mu^2 + 2\lambda\rho\mu c}{2\lambda\mu^2(1-c) + \rho\mu^2 + 2\lambda\mu c\rho + 2\lambda^2 c\rho}
\end{aligned}
$$

Exam problem 2004-04-15

A fault-tolerant computer node, intended for use in a satellite, consists of two redundant processor modules (PM1 and PM2) and two redundant sensors (S1 and S2). The system operates in cold stand-by redundancy, where PM1 and S1 are the primary units and PM2 and S2 the backup units.

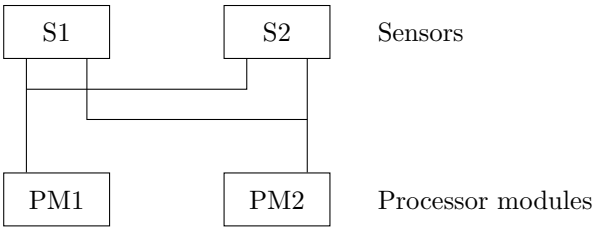

Figure 9: Problem 5.9

1 a

Divide the system into an appropriate number of fault containment regions. Motivate the answer.

Solution

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.

There are four fault containment regions:

- S1
- S2
- PM1 and sensor bus
- PM2 and sensor bus

1 b

Assume that the life times of the processor modules and sensors are exponentially distributed with a failure rate of λ_p for an active (hot) processor module and λ_s for an active sensor. The dormancy factor is 10 for the processor modules and 1 for the sensors. (This means that the failure rate of a cold processor module is ten times lower than the failure rate of an active processor module, while the failure rate is the same for cold and active sensors.) Derive an expression for the reliability of the node. Assume ideal coverage ($c = 1$).

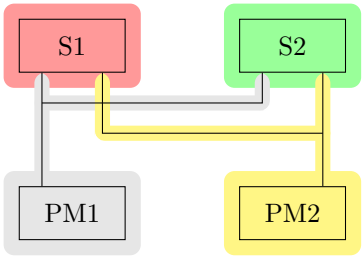

Figure 10: Fault containment regions for Problem 5.9

Solution

The system can be seen as two subsystems connected in serial, one for the processor modules and one for the sensors. The sensor subsystem is two sensors in parallel:

$$\begin{aligned} R_{parallel} &= 1 - F_{parallel} = 1 - \prod_{i=1}^{n} F_i = 1 - \prod_{i=1}^{n} (1 - R_i) \Rightarrow \\ R_{sensor}(t) &= 1 - (1 - R_s(t))^2 = 2R_s(t) - R_s^2(t) \\ \Rightarrow R_{sensor}(t) &= 2e^{-\lambda_s t} - e^{-2\lambda_s t} \end{aligned}$$

The PM subsystem is modeled with the following Markov chain.

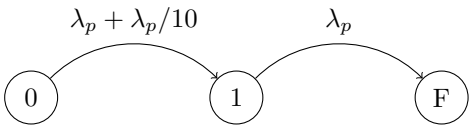

Figure 11: Markov chain for PM subsystem

$$\begin{aligned} P'(t) &= P(t)Q \\ P(0) &= \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \\ Q &= \begin{bmatrix} -1.1\lambda_p & 1.1\lambda_p & 0 \\ 0 & -\lambda_p & \lambda_p \\ 0 & 0 & 0 \end{bmatrix} \end{aligned}$$

Laplace transform:

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

$$\begin{aligned} sP_0 - 1 &= -1.1\lambda_p P_0 \\ sP_1 &= 1.1\lambda_p P_0 - \lambda_p P_1 \\ sP_F &= \lambda_p P_1 \\ P_0 &= \frac{1}{s + 1.1\lambda_p} \end{aligned}$$

$$
\begin{aligned}
P_1 &= \frac{1.1\lambda_p}{s+\lambda_p} P_0 = \frac{1.1\lambda_p}{(s+\lambda_p)(s+1.1\lambda_p)} = \frac{11}{s+\lambda_p} - \frac{11}{s+1.1\lambda_p} \\
P_F &= \frac{\lambda_p}{s} P_1 = \ldots \\
R_{PM}(t) &= P_0(t) + P_1(t) = 11e^{-\lambda_p t} - 10e^{-1.1\lambda_p t}
\end{aligned}
$$

$$
\begin{aligned}
R_{system}(t) &= R_{sensor}(t) \times R_{PM}(t) \\
&= \left(2e^{-\lambda_s t} - e^{-2\lambda_s t}\right)\left(11e^{-\lambda_p t} - 10e^{-1.1\lambda_p t}\right)
\end{aligned}
$$

1 c

Derive an expression for the reliability of the node under the following assumptions: Sensor S1 has a failure mode which cannot be detected by the processor modules. Such a sensor failure will cause the entire system to fail immediately. The probability that a sensor failure will be detected by the processor modules is c. The fault coverage for faults occurring in the processor modules is ideal.
Solution

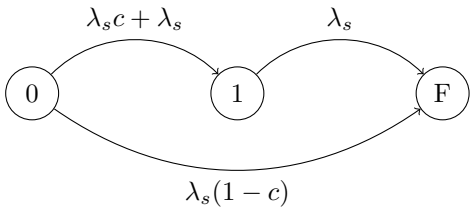

Figure 12: Markov chain

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

$$
\begin{aligned}
sP_0 - 1 &= -2\lambda_s P_0 \\
sP_1 &= (1+c)\lambda_s P_0 - \lambda_s P_1 \\
sP_F &= (1-c)\lambda_s P_0 - \lambda_s P_1 \\
P_0 &= \frac{1}{s+2\lambda_s} \\
P_1 &= \frac{(1+c)\lambda_s}{s+\lambda_s} P_0 = \frac{(1+c)\lambda_s}{(s+\lambda_s)(s+2\lambda_s)} \\
&= (1+c)\left(\frac{1}{s+\lambda_s} - \frac{1}{s+2\lambda_s}\right)
\end{aligned}
$$

$$
\begin{aligned}
P_F &= \dots \\
P_0(t) &= e^{-2\lambda_s t} \\
P_1(t) &= (1+c)\left(e^{-\lambda_s t} - e^{-2\lambda_s t}\right) \\
R_{sensor}(t) &= P_0(t) + P_1(t) \\
&= (1+c)e^{-\lambda_s t} - ce^{-2\lambda_s t} \\
R_{system} &= R_{sensor}(t) \times R_{PM}(t) \\
&= \left((1+c)e^{-\lambda_s t} - ce^{-2\lambda_s t}\right)\left(11e^{-\lambda_p t} - 10e^{-1.1\lambda_p t}\right)
\end{aligned}
$$