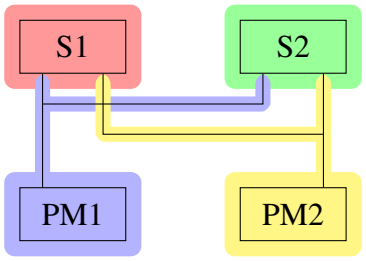
1.

a)

There are four error containment regions with sensor buses included. Each sensor module, PM1 + sensor bus and PM2 + sensor bus, see figure below.



b)

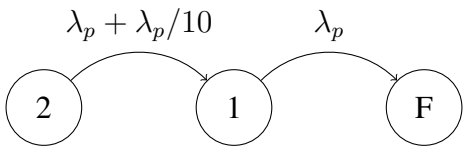
The system consists of two primary independent subsystems, one for the processor modules and one for the sensor modules.

c)

The sensor subsystem can be seen as a parallel system with two components:

$$R_{sensors}(t) = 1 - (1 - R_s(t))^2 = 2R_s(t) - R_s^2(t)$$
$$\Rightarrow R_{sensors}(t) = 2e^{-\lambda_s t} - e^{-2\lambda_s t}$$

The processor subsystem is modeled with the following Markov chain.



We obtain the following equation system:

$$P'(t) = P(t)Q$$
$$P(t) = \begin{bmatrix} P_2(t) & P_1(t) & P_F(t) \end{bmatrix}$$
$$P(0) = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$$
$$Q = \begin{bmatrix} -1.1\lambda_p & 1.1\lambda_p & 0 \\ 0 & -\lambda_p & \lambda_p \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{cases} P_2'(t) &= -1.1\lambda_p P_2(t) \\ P_1'(t) &= 1.1\lambda_p P_2(t) - \lambda_p P_1(t) \\ P_F'(t) &= \lambda_p P_1(t) \end{cases}$$

We solve the equation system using Laplace transform:

$$sP_2(s) - 1 = -1.1\lambda_p P_2(s) \quad (1)$$
$$sP_1(s) = 1.1\lambda_p P_2(s) - \lambda_p P_1(s) \quad (2)$$
$$sP_F(s) = \lambda_p P_1(s) \quad (3)$$

From (1), we get

$$P_2(s) = \frac{1}{s + 1.1\lambda_p} \Rightarrow P_2(t) = e^{-1.1\lambda_p t}$$

From (2), we get

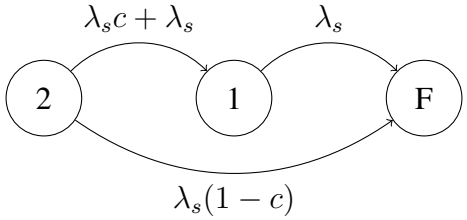
$$P_1(s) = \frac{1.1\lambda_p}{s+\lambda_p} P_2(s) = \frac{1.1\lambda_p}{(s+\lambda_p)(s+1.1\lambda_p)} = \frac{11}{s+\lambda_p} - \frac{11}{s+1.1\lambda_p}$$
$$\Rightarrow P_1(t) = 11\left(e^{-\lambda_p t} - e^{-1.1\lambda_p t}\right).$$

We obtain the following reliability:

$$R_{PMs}(t) = P_2(t) + P_1(t) = 11e^{-\lambda_p t} - 10e^{-1.1\lambda_p t}$$
$$R_{system}(t) = R_{sensors}(t) \cdot R_{PMs}(t)$$
$$= \left(2e^{-\lambda_s t} - e^{-2\lambda_s t}\right)\left(11e^{-\lambda_p t} - 10e^{-1.1\lambda_p t}\right)$$

d)

The reliability of the sensor subsystem is obtained using a Markov chain model:



This gives the following equation system:

$$P'(t) = P(t)Q$$
$$P(t) = \begin{bmatrix} P_2(t) & P_1(t) & P_F(t) \end{bmatrix}$$
$$P(0) = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$$
$$Q = \begin{bmatrix} -2\lambda_s & (1+c)\lambda_s & (1-c)\lambda_s \\ 0 & -\lambda_s & \lambda_s \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{cases} P_2'(t) &= -2\lambda_s P_2(t) \\ P_1'(t) &= (1+c)\lambda_p P_2(t) - \lambda_s P_1(t) \\ P_F'(t) &= (1-c)\lambda_s P_2(t) + \lambda_s P_1(t) \end{cases}$$

We solve the equation system using Laplace transform:

$$sP_2(s) - 1 = -2\lambda_s P_2(s) \quad (1)$$
$$sP_1(s) = (1+c)\lambda_s P_2(s) - \lambda_s P_1(s) \quad (2)$$
$$sP_F(s) = (1-c)\lambda_s P_2(s) - \lambda_s P_1(s) \quad (3)$$

From (1), we get:

$$P_2(s) = \frac{1}{s+2\lambda_s} \Rightarrow P_2(t) = e^{-2\lambda_s t}$$

From (2), we get:

$$P_1(s) = \frac{(1+c)\lambda_s}{s+\lambda_s} P_2(s) = \frac{(1+c)\lambda_s}{(s+\lambda_s)(s+2\lambda_s)} = (1+c)\left(\frac{1}{s+\lambda_s} - \frac{1}{s+2\lambda_s}\right)$$
$$\Rightarrow P_1(t) = (1+c)\left(e^{-\lambda_s t} - e^{-2\lambda_s t}\right)$$

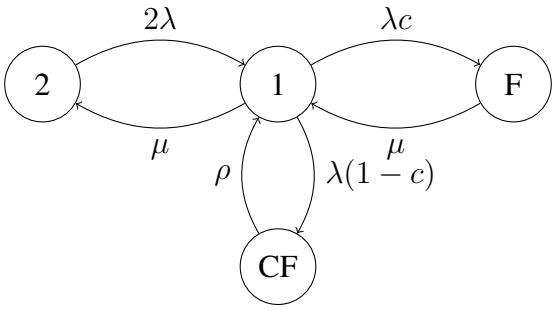
We obtain the following reliability:

$$\begin{aligned} R_{sensors}(t) &= P_2(t) + P_1(t) \\ &= (1+c)e^{-\lambda_s t} - ce^{-2\lambda_s t} \\ R_{system} &= R_{sensors}(t) \cdot R_{PMs}(t) \\ &= \left((1+c)e^{-\lambda_s t} - ce^{-2\lambda_s t}\right)\left(11e^{-\lambda_p t} - 10e^{-1.1\lambda_p t}\right) \end{aligned}$$

2.

a)

The system is modelled by the following Markov model:



State label = # operational modules; F = safe shutdown; CF = unsafe shutdown.

We obtain the following transition rate matrix

$$Q = \begin{bmatrix} -2\lambda & 2\lambda & 0 & 0 \\ \mu & -(\lambda+\mu) & \lambda c & \lambda(1-c) \\ 0 & \mu & -\mu & 0 \\ 0 & \rho & 0 & -\rho \end{bmatrix}$$

and the following equation system

$$\begin{aligned} P'(t) &= P(t)Q \\ P(t) &= \begin{bmatrix} P_2(t) & P_1(t) & P_F(t) & P_{CF}(t) \end{bmatrix} \\ P(0) &= \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}. \end{aligned}$$

This gives the following system of differential equations

$$\begin{cases} P_2'(t) &= -2\lambda P_2(t) + \mu P_1(t) \\ P_1'(t) &= 2\lambda P_2(t) - (\lambda+\mu)P_1(t) + \mu P_F(t) + \rho P_{CF}(t) \\ P_F'(t) &= \lambda c P_1(t) - \mu P_F(t) \\ P_{CF}'(t) &= \lambda(1-c)P_1(t) - \rho P_{CF}(t). \end{cases}$$

Let $t \to \infty$, and denote $\lim_{t\to\infty} P_i(t)$ as Π_i. We obtain

$$\begin{cases} 0 = -2\lambda\Pi_2(t) + \mu\Pi_1(t) & (1) \\ 0 = 2\lambda\Pi_2(t) - (\lambda+\mu)\Pi_1(t) + \mu\Pi_F(t) + \rho\Pi_{CF}(t) & (2) \\ 0 = \lambda c\Pi_1(t) - \mu\Pi_F(t) & (3) \\ 0 = \lambda(1-c)\Pi_1(t) - \rho\Pi_{CF}(t). & (4) \end{cases}$$

We also know that

$$\Pi_2 + \Pi_1 + \Pi_F + \Pi_{CF} = 1. \tag{5}$$

From (1),(3) and (4), we obtain

$$\Pi_2 = \frac{\mu}{2\lambda}\Pi_1 \tag{6}$$

$$\Pi_F = \frac{\lambda c}{\mu}\Pi_1 \tag{7}$$

$$\Pi_{CF} = \frac{\lambda(1-c)}{\rho}\Pi_1 \tag{8}$$

From (5), (6), (7) and (8), we then obtain

$$\begin{aligned} 1 &= \Pi_1 \left(\frac{\mu}{2\lambda} + 1 + \frac{\lambda c}{\mu} + \frac{\lambda(1-c)}{\rho} \right) \\ &= \frac{2\lambda\mu\rho + \mu^2\rho + 2\lambda^2 c\rho + 2\lambda^2(1-c)\mu}{2\lambda\mu\rho}\Pi_1 \\ \Rightarrow \Pi_1 &= \frac{2\lambda\mu\rho}{2\lambda\mu\rho + \mu^2\rho + 2\lambda^2 c\rho + 2\lambda^2(1-c)\mu} \end{aligned} \tag{9}$$

The steady-state probability of being in the unsafe shutdown state is obtained using (8) and (9):

$$\begin{aligned} \lim_{t\to\infty} P_{CF}(t) = \Pi_{CF} &= \frac{\lambda(1-c)}{\rho}\Pi_1 \\ &= \frac{2\lambda\mu\rho}{2\lambda\mu\rho + \mu^2\rho + 2\lambda^2 c\rho + 2\lambda^2(1-c)\mu}\frac{\lambda(1-c)}{\rho} \\ &= \frac{2\lambda^2\mu(1-c)}{2\lambda\mu\rho + \mu^2\rho + 2\lambda^2 c\rho + 2\lambda^2(1-c)\mu}. \end{aligned}$$

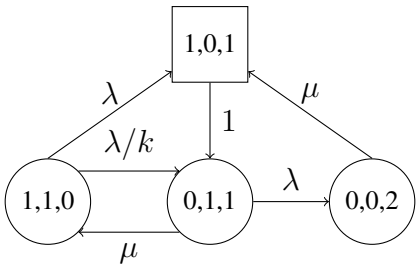
b)

The steady-state availability of the system is

$$\begin{aligned} \lim_{t\to\infty} A(t) = \Pi_2 + \Pi_1 &= \frac{2\lambda\mu\rho}{2\lambda\mu\rho + \mu^2\rho + 2\lambda^2 c\rho + 2\lambda^2(1-c)\mu}\left(\frac{\mu}{2\lambda} + 1\right) \\ &= \frac{2\lambda\mu\rho + \mu^2\rho}{2\lambda\mu\rho + \mu^2\rho + 2\lambda^2 c\rho + 2\lambda^2(1-c)\mu}. \end{aligned}$$

3

We represent possible markings of the GSPN model as {*#pspare*, *#pactive*, *#pdown*}. The reachability set is then {1,1,0}, {1,0,1}, {0,1,1}, {0,0,2}, where {1,0,1} is a vanishing marking. The following extended reachability graph is obtained:



We account for the effects of the vanishing marking by modifying the transition rates, resulting in the following reachability graph: