Prof. Dr. P. Liggesmeyer
Michael Roth, M.Sc.

Technical University of Kaiserslautern
Dept. of Computer Sciences
AG Software Engineering: Dependability

Safety and Reliability of Embedded Systems
(WS 15/16)

Problem Set 4

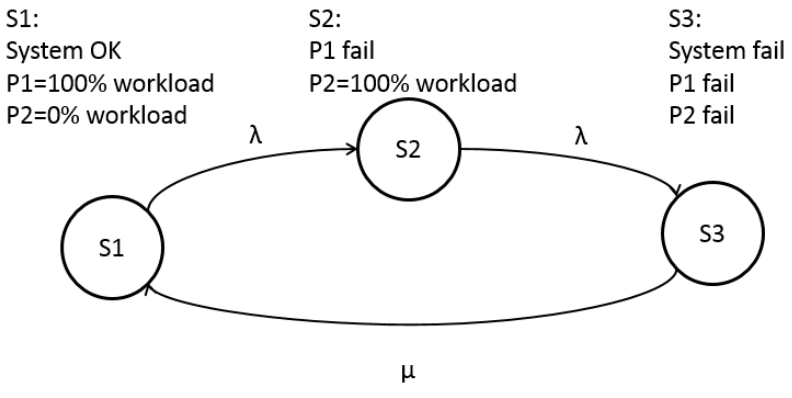
Problem 1: Quantitative Markov Modeling

Consider the two given Markov models below. They depict a pump system with two pumps, P1 and P2, where P2 runs in a **cold** standby (P1 = ON with a workload of 100%, P2 = OFF with a workload of 0%). If P1 fails, P2 will be switched ON and overtake the complete workload immediately. The Pumps are identical and have a failure rate of 0 at a workload of 0% and a failure rate of 2 per year (λ = 2/365 d) at a workload of 100%. If both pumps fail, the whole pump system fails. The two Markov models depict different repair strategies:

1. **Both pumps have to be repaired together**
2. **Each pump has to be repaired separately after a failure**

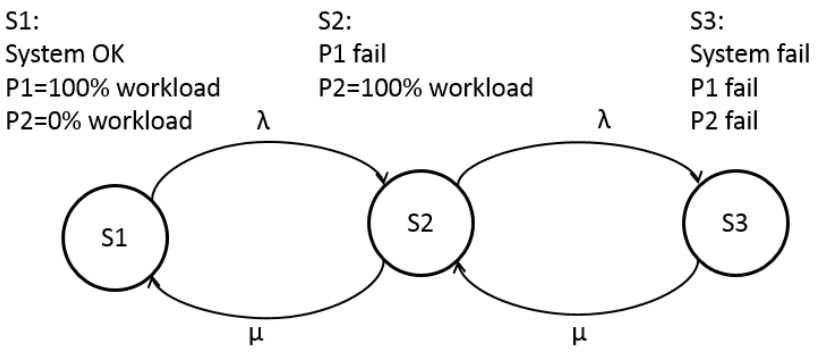
b) **(21 Points)** Derive the differential equations for both Markov models and determine a steady state analysis for both models. Assume λ=2/365 d and μ=1/d. Give a statement which repair strategy is the best w.r.t. a lower probability of the system's fail state.

***Hint**: For calculating the stationary availability t is approximated to infinity. In this case we can set the differential equations to 0 ($dP_{Sx}(t)/dt=0$) and we get constant probability values ($P_{Sx}(t) = P_{Sx}$). So we get a homogeneous linear equation system.*



1.

2.



Problem 2: Fault Tree Analysis – K out of N system

You have to evaluate the failure of a 2 out of 3 system with the help of Fault Tree Analysis. A 2 out of 3 system consists of 3 components and for the system to be operating at least two out of these 3 components have to be operating. Please consider the following events for your analysis:

Event type	Name	Description	Probabilities
Top event	F_{sys}	2 out of 3 system fails	f_{sys}
Intermediate event	F_{12}, F_{13}, F_{23}	Two components fail	f_{12}, f_{13}, f_{23}
Basic event	F_1, F_2, F_3	A single component fails	f_1, f_2, f_3

The probability of failure of each single component is assumed to be $f_c = 0.03$

a) Please draw the corresponding fault tree using the above event names.
b) Try to calculate the probability of failure of the system f_{sys} by applying standard gate formulas known from lecture in a bottom-up fashion.
c) Now determine the minimal cut sets and calculate an approximation for f_{sys}.
d) Finally, draw a binary decision tree for f_{sys} using the variable order $F_1 \rightarrow F_2 \rightarrow F_3$. Convert the tree into a reduced ordered binary decision diagram (ROBDD). Annotate the diagram with probabilities and again calculate the availability f_{sys}.
e) Compare the three results.