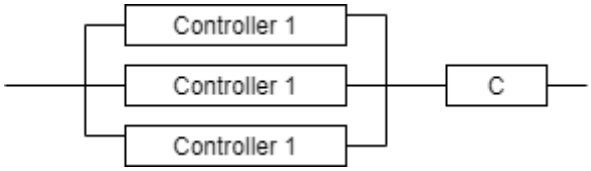
Safety and Reliability of Embedded Systems - SRES (WS 19/20)
Problem Set 3

Problem 1: Reliability estimation by using RBD 's

The safeguarding system of a railroad crossing consists of three heterogeneous controllers and a component "C" that rectifies if any of them has failed. In normal conditions, the three controllers and "C" are functional. For the system to remain functional at least one controller and "C" have to be functional. The three controllers fail independently from each other.

1. Draw the corresponding reliability block diagram for the safeguarding system. To simplify the analysis of the safeguarding system, it is further assumed that C has a reliability R_c of 1 which means that it never fails.

   -



To simplify the analysis of the safeguarding system, it is further assumed that C has a reliability R_c of 1 which means that it never fails.

2. Please calculate the reliability R_{sys} of the safeguarding system if each controller has a reliability $R_{ctrl} = 0.95$

   -

$$R_{series}(t) = \prod_{i=1}^{n} R_{K_i}(t) \qquad R_{parallel}(t) = 1 - \prod_{i=1}^{n} (1 - R_{K_i}(t))$$

Given,

$R_{ctrl} = 0.95$

$R_{sys} = R_{ctrls} * R_c$

$R_{ctrls} = 1 - (1-0.95)^3 = 0.999875$

$R_{sys} = 0.999875*1 = 0.999875$

Now assume that the reliability Rc of C is 0.9.

3. Recalculate the resulting reliability Rsys of the system.

   -

$R_c = 0.9$

$R_{sys} = R_{ctrls} * R_c$

$R_{ctrls\_parallel} = 0.9 - (1 - 0.95)^3 = 0.999875$

$R_{sys\_parallel} = 0.999875*0.9 = 0.899875$

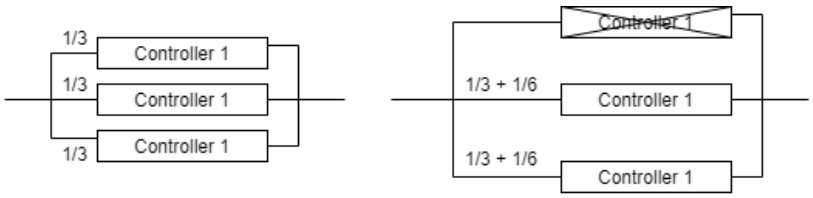
$R_{ctrls\_series} = (0.95)^3 = 0.857375$

$R_{sys\_series} = 0.857375*0.9 = 0.7716375$

$R_{sys\_series} < R_{sys\_parallel}$

Problem 2: Markov Processes

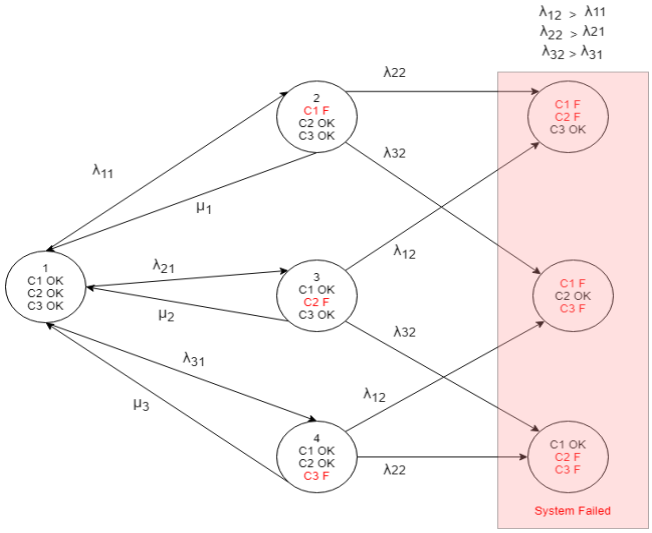
Assume that the configuration of the safeguarding system has undergone some changes. Unlike the old configuration, the new one includes ***three controllers which are identical*** and ***there is no component "C",*** which rectifies if the controllers have failed. In normal operating conditions, the ***total load*** of the safeguarding system is ***distributed equally among its controllers (Each controller runs at 1/3 of their maximum capacity)***. Whenever ***one controller fails***, the ***remaining two take over its load (1/6).*** The system fails if two controllers have failed.



*** If one controller fails then the remaining two take over its load

1. Please draw the corresponding Markov process model under the assumption that if the complete safeguarding system has failed, the system remains in this state (no repair will take place).

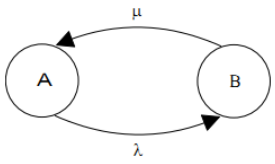
   -



2. For the states of your Markov model, develop the set of related differential equations

   -

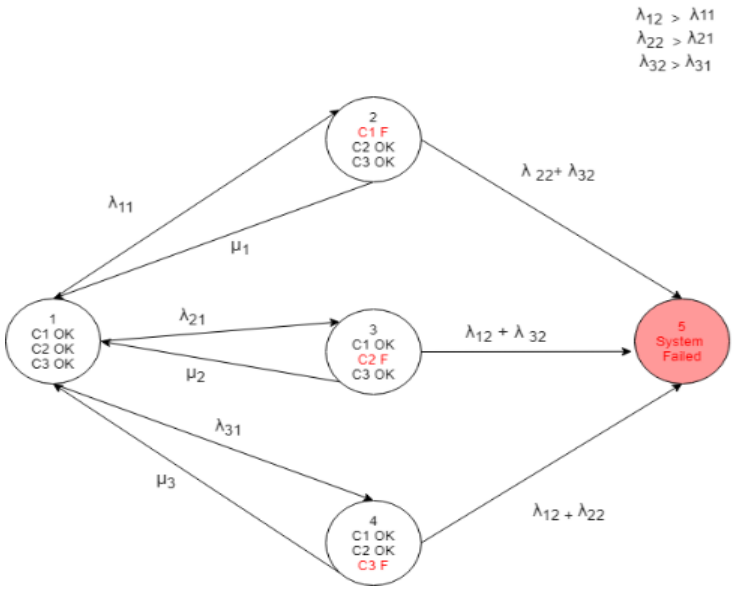
   Basics:



$$\frac{dP_A(t)}{dt} = -\lambda P_A(t) + \mu P_B(t)$$

$$\frac{dP_B(t)}{dt} = \lambda P_A(t) - \mu P_B(t) = -\frac{dP_A(t)}{dt}$$

$$P_A(t) + P_B(t) = 1$$



$$\frac{dS_1(t)}{dt} = -(\lambda_{11} + \lambda_{21} + \lambda_{31}).S_1(t) + \mu_1.S_2(t) + \mu_2.S_3(t) + \mu_3.S_4(t)$$

$$\frac{dS_2(t)}{dt} = \lambda_{11}.S_1(t) - (\mu_1 + \lambda_{22} + \lambda_{32}).S_2(t)$$

$$\frac{dS_3(t)}{dt} = \lambda_{21}.S_1(t) - (\mu_2 + \lambda_{12} + \lambda_{32}).S_3(t)$$

$$\frac{dS_4(t)}{dt} = \lambda_{31}.S_1(t) - (\mu_3 + \lambda_{12} + \lambda_{22}).S_3(t)$$

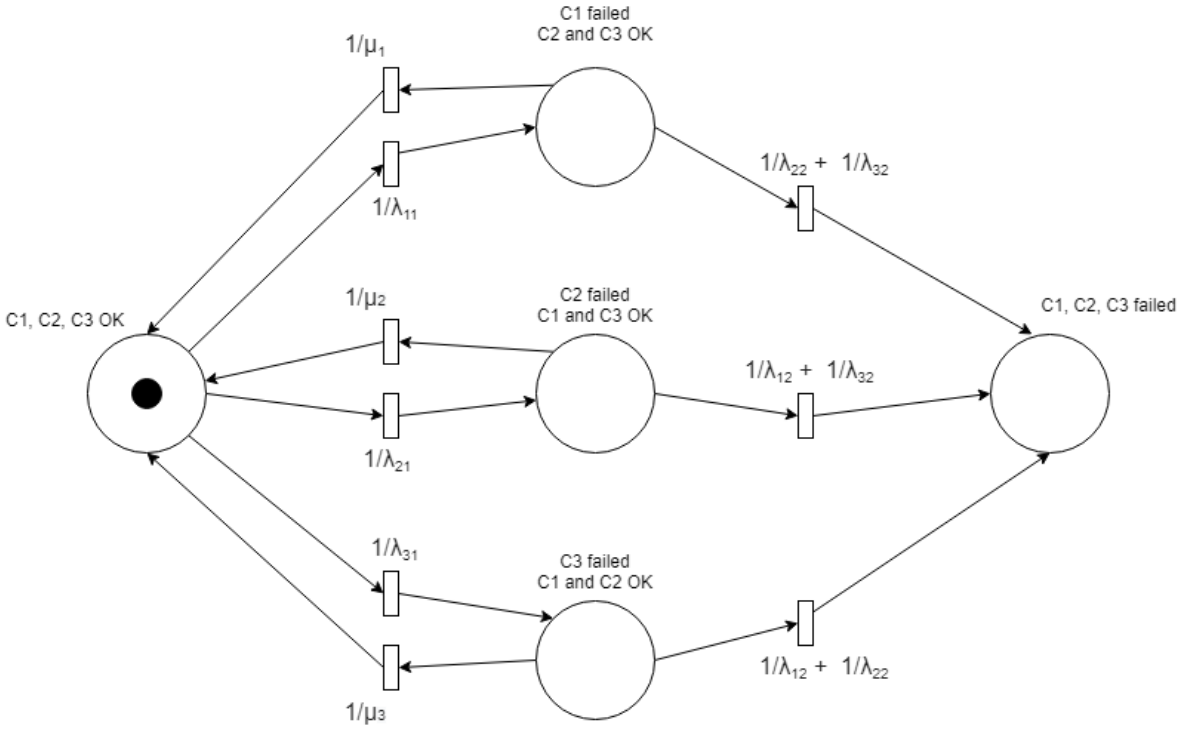
$$\frac{dS_5(t)}{dt} = (\lambda_{22} + \lambda_{32}).S_2(t) + (\lambda_{12} + \lambda_{32}).S_3(t) + (\lambda_{12} + \lambda_{22}).S_4(t)$$

$$S_1(t) + S_2(t) + S_3(t) + S_4(t) + S_5(t) = 1$$

Problem 3: Petri Nets

1. Please draw a Petri Net corresponding to the Markov Process of Problem 2. Which type of Petri Net would this be?

   -



   Type: Stochastic Petri Net (SPN) – Because delay is exponentially distributed

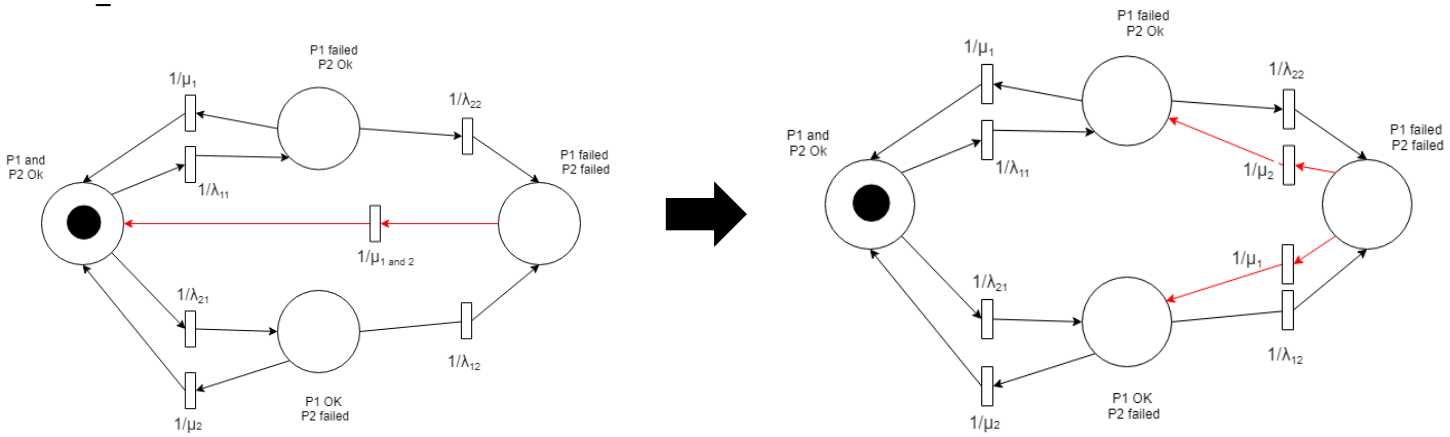
2. Describe briefly the following Petri Net types: C/E Net, P/T Net, Pr/TNet, and SPN. How do they differ from each other?

   -

C/E Net	**P/T Nets** ***(P/T net, Place/Transition Net)***	**Pr/T Nets** ***(Predicate/Transition Net)***	**Timed Petri Net**
Objects, respectively tokens, are **Boolean** data type	Places can obtain **more than one** token (in C/E nets only one token)	Tokens are **colored**: They can be individualized, they do have a description (unlike other tokens)	Similar as in C/E net
Transitions are interpreted as **Events**	Transitions must release or add as many tokens when firing as the **weights** that are given on arcs	Transitions have a **firing condition** and a **firing effect.**	There is **firing delay associated** with each **transition**. This delay specifies the time that the transition has to be enable, before it can actually fire
Places are denoted as **conditions**. **Binary condition**: Each place is allowed to receive exactly one or no token	Places have a **capacity** (maximum number of tokens that may lie in one place): if it is to be bigger than 1, this will be denoted as »K = ...« at the place	Places contain a number of tokens that can be integers or variables	Similar as in C/E nets

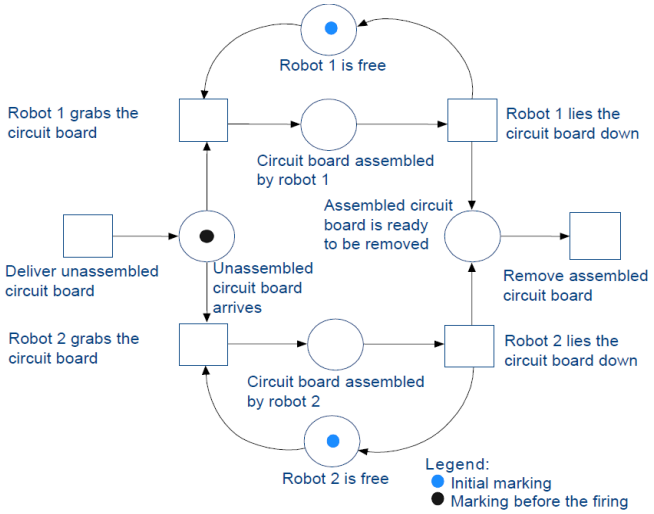
3. Consider the water pump example in the lecture (see chapter 4, page 44). If the repair strategy is changed to repair 2 pumps separately instead of repairing them together, how would you draw your Petri Net to reflect this situation?

–

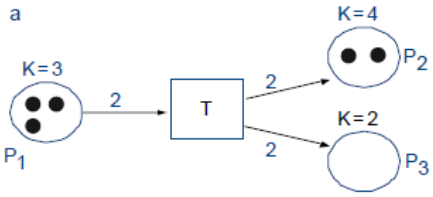


Petri Nets

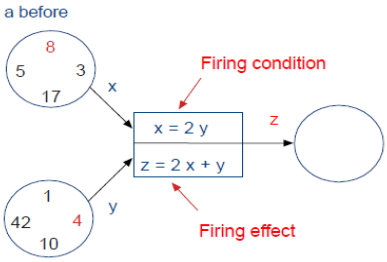
1. Condition/Event Petri nets
    a. State elements hold either one or no token
        i. state elements represent conditions, which can be true or false
        ii. transition elements are representing local events
    b. Event is enabled if and only if
        i. all its pre-conditions (connected by incoming arcs) are true
        ii. all its post-conditions (connected by outgoing arcs) are false
    c. An event occurrence negates its pre- and post-conditions
    d. Events with overlapping pre-conditions are in conflict
    e. Events with overlapping post-conditions are in contact



2. State/Transition Petri nets
    a. Places can obtain more than one token (in C/E nets only one token)
    b. Transitions must release or add as many tokens when firing as the weights that are given on the arrows. (in C/E nets only one token)
    c. If the capacity of a place is to be bigger than 1, this will be denoted as »K = ...« at the place.
    d. The capacity defines the maximum number of tokens that may lie in one place.



3. Predicate/Transistion Petri Nets / Coloured Petri Nets
    a. Apply individual, »colored« tokens
    b. C/E and P/T Nets apply only »black« tokens, which are all the same.



4. Timed Petri Net Types
    a. To study performance and dependability issues of systems it is necessary to include a timing concept into the model.
    b. There are several possibilities to do this for a Petri net; however, the most common way is to associate a firing delay with each transition. This delay specifies the time that the transition has to be enabled, before it can actually fire.