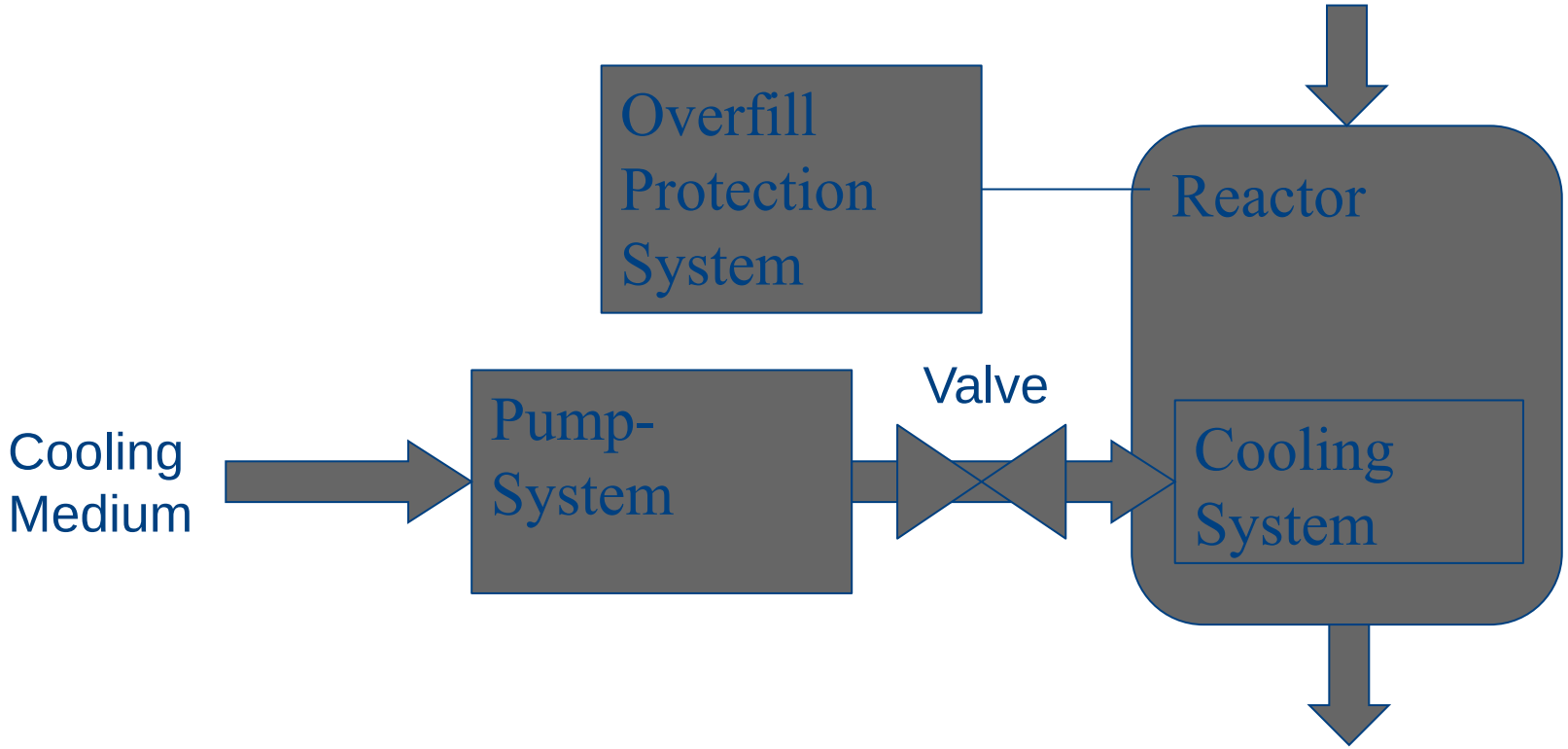
Technische Universität
Kaiserslautern

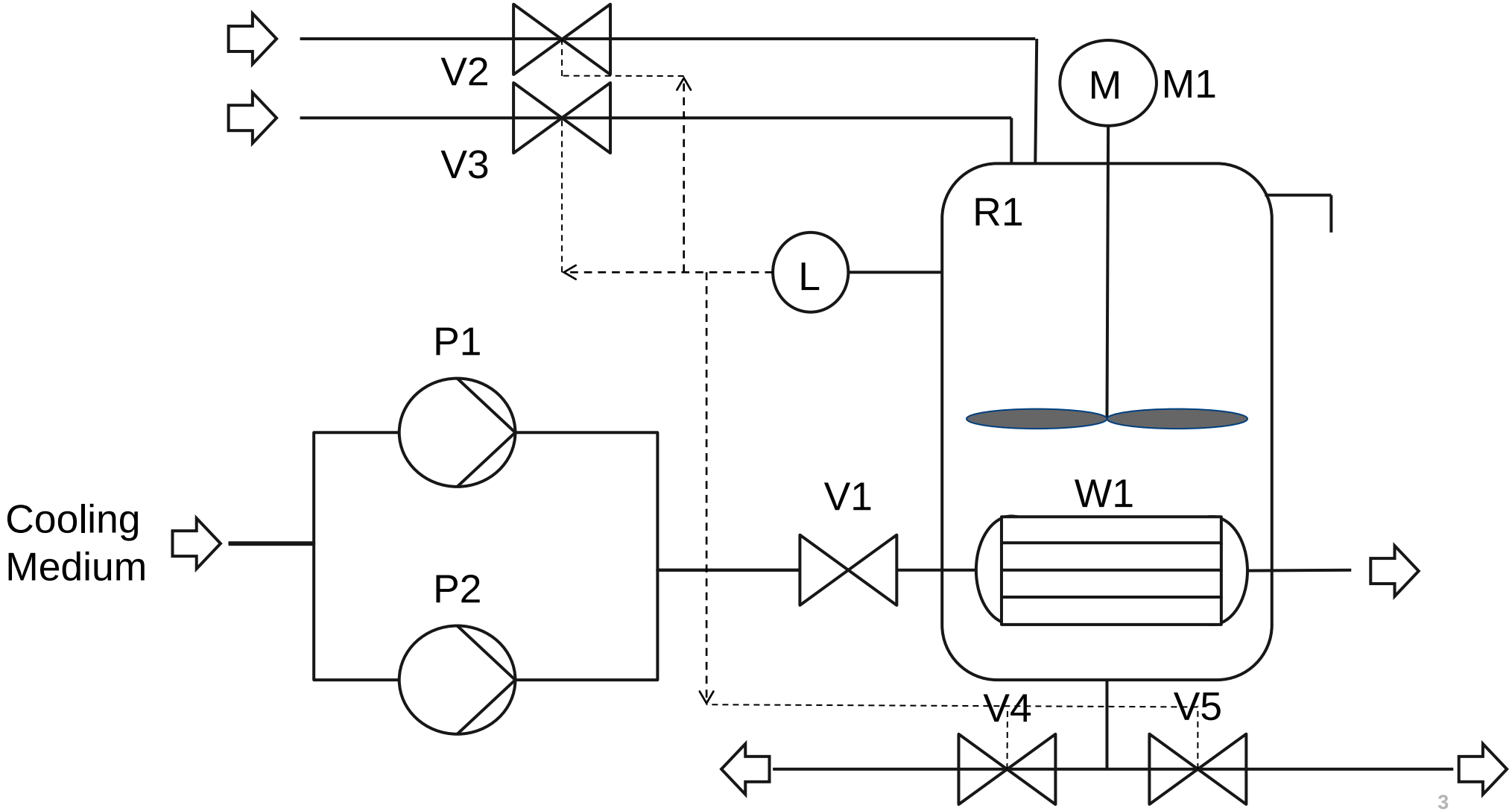
o1o1seda o1o1oo

software engineering dependability

Safety and Reliability of Embedded Systems
(WS 12/13)
Training Fault Tree / Markov Processes

- The system consists of 2 Pumps in a warm standby (each one is working with a 50% load). If one Pump fails the remaining one has to do the compete work (100%). This means also a increasing of their failure rate.





Safety-System

Consists of :

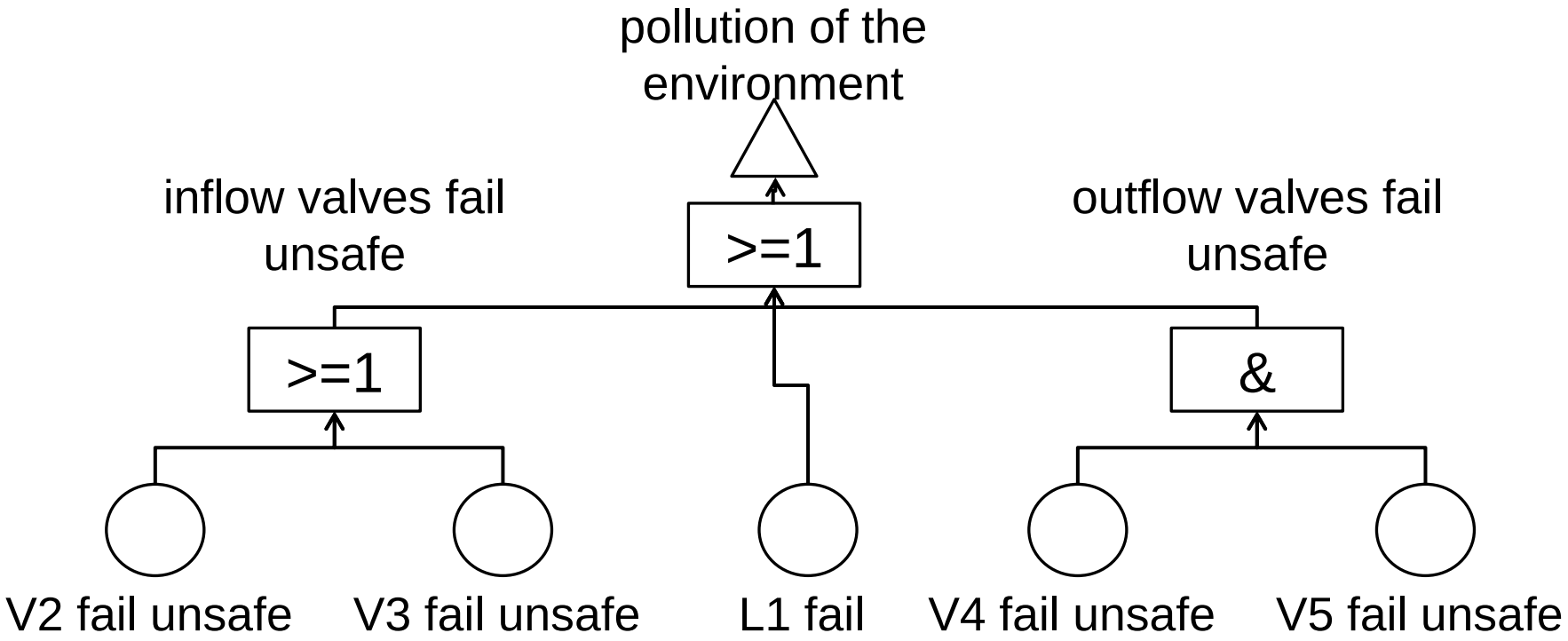
- Cooling-System (P1,P2, V1)
- Stirrer (M1)
- Overfill protection System (L1, V2, V3, C1)

A pollution of the environment is occurs, if the overfill protection system fails in an unsafe way. This system, that consists of the leveling sensor L1, the valves for the products V2 and V3, the outflow valves V4 and V5 and a PLC C1. As one can see that the outflow valves are realized as a redundant system.

Fault Tree for the TLE „Pollution“

Consists of :

- Cooling-System (P1,P2, V1)
- Stirrer (M1)
- Overfill protection System (L1, V2, V3, V4, V5, C1)



Safety-System

Consists of :

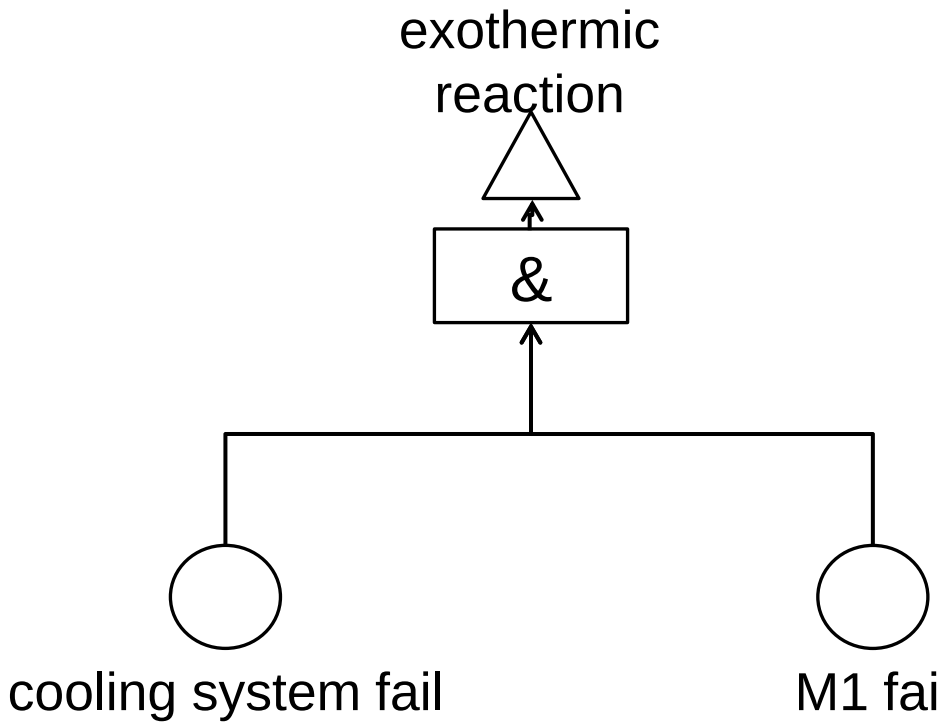
- Cooling-System (P1,P2, V1)
- Stirrer (M1)
- Overfill protection System (L1, V2, V3, C1)

Additionally a exothermic reation is triggerd if the cooling system fails and the stirrer fails.

Fault Tree for the TLE „exothermic reation“

Consists of :

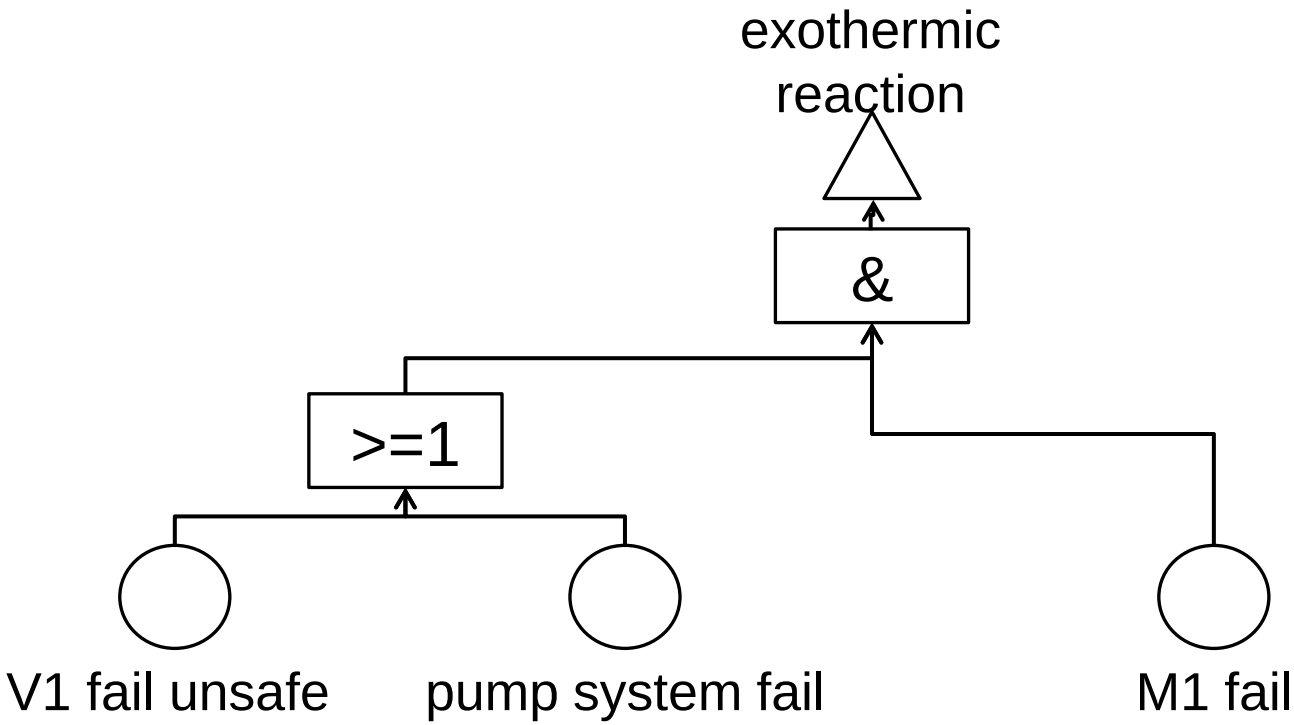
- Cooling-System (P1,P2, V1)
- Stirrer (M1)
- Overfill protection System (L1, V2, V3, V4, V5, C1)



Fault Tree for the TLE „exothermic reation“

Consists of :

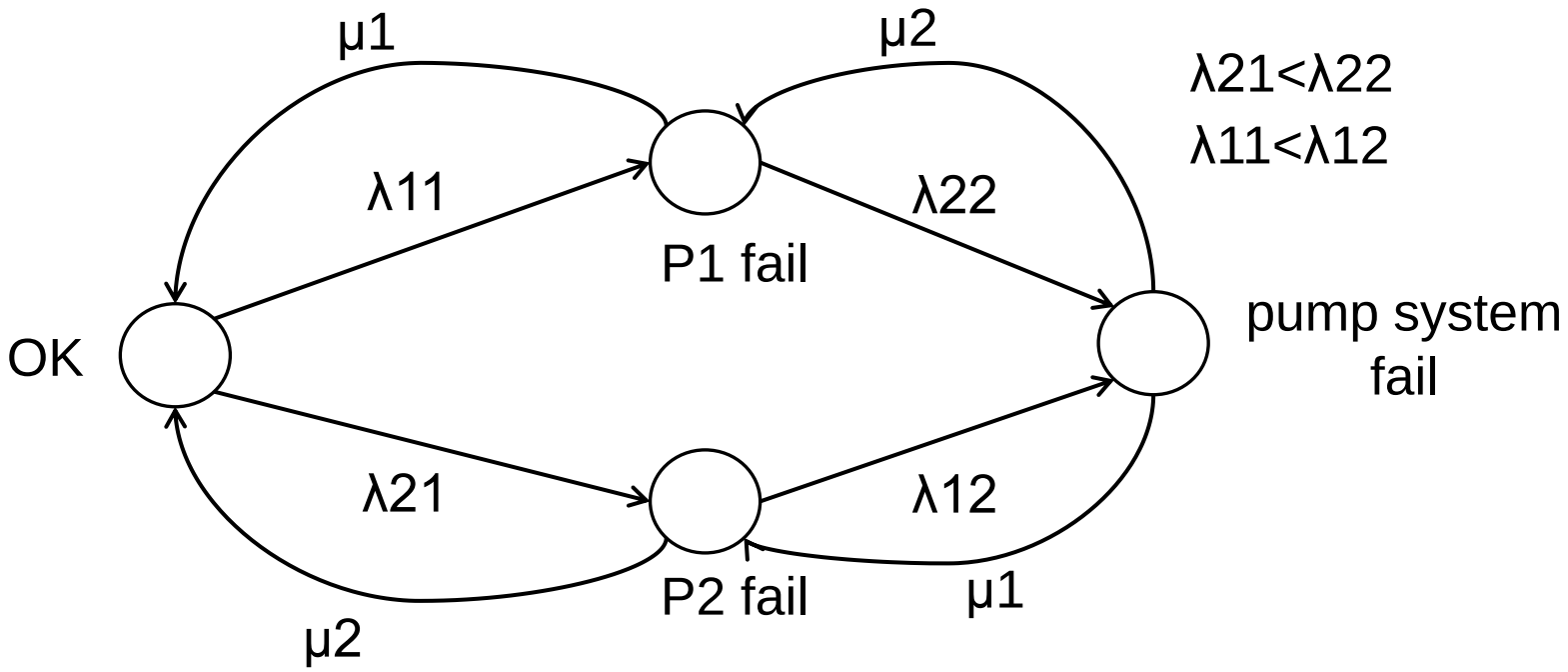
- Cooling-System (P1,P2, V1)
- Stirrer (M1)
- Overfill protection System (L1, V2, V3, V4, V5, C1)



Markov Process for „pump system fail“

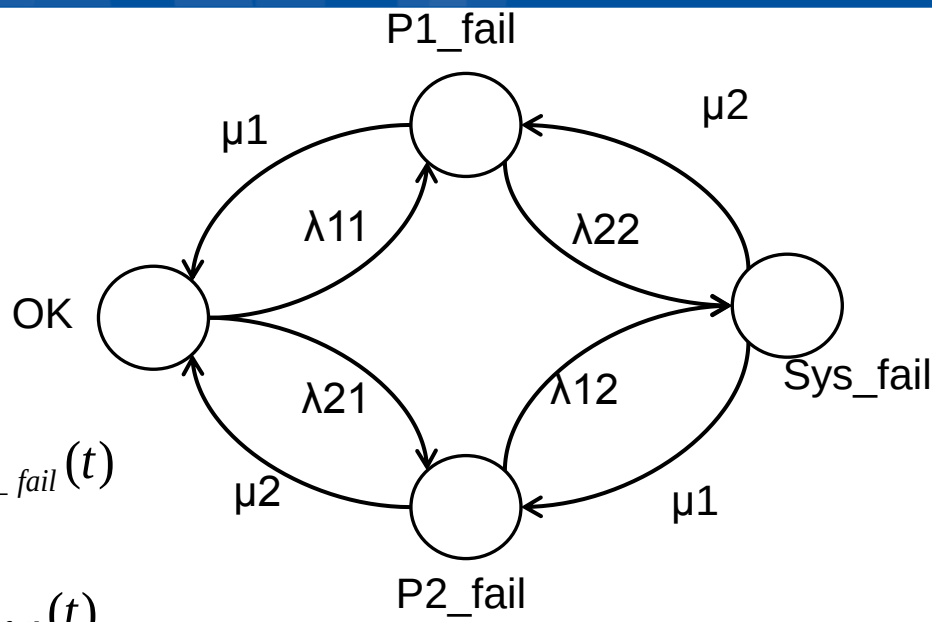
Consists of :

- Cooling-System (P1,P2, V1)
- Stirrer (M1)
- Overfill protection System (L1, V2, V3, V4, V5, C1)



For Markov Process:

- Steady state analysis



$$\frac{dP_{OK}(t)}{dt} = -(\lambda_{11}+\lambda_{21})\cdot P_{OK}(t) + \mu_1 \cdot P_{P1\_fail}(t) + \mu_2 \cdot P_{P2\_fail}(t)$$

$$\frac{dP_{P1\_fail}(t)}{dt} = \lambda_{11}\cdot P_{OK}(t) + \mu_2 \cdot P_{Sys\_fail} - (\lambda_{22}+\mu_1)\cdot P_{P1\_fail}(t)$$

$$\frac{dP_{P2\_fail}(t)}{dt} = \lambda_{21}\cdot P_{OK}(t) + \mu_1 \cdot P_{Sys\_fail} - (\lambda_{12}+\mu_2)\cdot P_{P2\_fail}(t)$$

$$\frac{dP_{Sys\_fail}(t)}{dt} = \lambda_{12}\cdot P_{P2\_fail}(t) + \lambda_{22}\cdot P_{P1\_fail}(t) - (\mu_1+\mu_2)\cdot P_{Sys\_fail}(t)$$

$$P_{OK}(t) + P_{P1\_fail}(t) + P_{P2\_fail}(t) + P_{Sys\_fail}(t) = 1$$

For resulting Fault Tree:

- Fault Tree Analysis

$$[P_{V1}(t)+P_{Sys\_fail}(t)-P_{V1}(t)*P_{Sys\_fail}(t)]*P_{M1}(t)$$