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

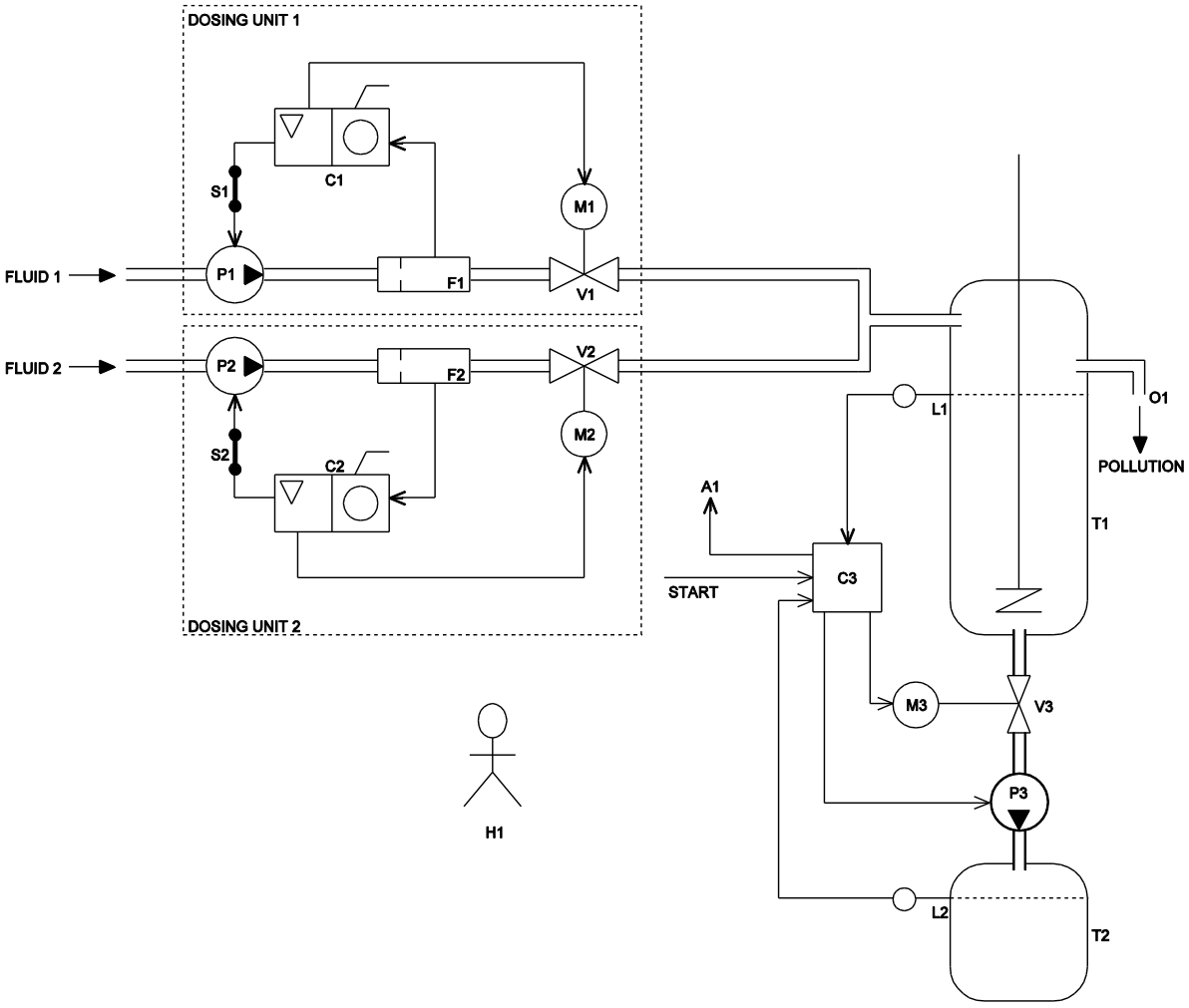
Technical University of Kaiserslautern
Dept. of Computer Sciences
AG Software Engineering: Dependability

Safety and Reliability of Embedded Systems
(WS 14/15)

Problem Set 5

Problem 1: Fault tree analysis

The purpose of the following plant is to mix FLUID 1 and FLUID 2 within tank T1. If a particular mixing time has elapsed, the operator H1 manually sends a START signal to controller C3, which in turn opens valve V3 via an electric motor M3 and initiates the filling process of tank T2. The mixed product is pumped into tank T2 using pump P3 until the level at level sensor L2 is reached. Pump P3 is switched off and valve V3 is closed again automatically by the controller.



In order to exactly dose the amount of fluids mixed, two dosing units (DOSING UNIT 1, DOSING UNIT 2) with mass flow meters (F1, F2) are used. Each flow meter sends electrical impulses to a software counter (C1, C2), using the impulse frequency as a figure for the amount of mass transported per unit time. If a pre-defined impulse count is reached, the software counter switches off the corresponding pump (P1, P2) and shuts the corresponding valve (V1, V2) via an electric motor (M1, M2). It is assumed here that if both dosing units work properly, the amount of mixed fluid within tank T1 is always below level L1.

In order to avoid overfilling, tank T1 is equipped with a safety mechanism. This mechanism is realized by a level sensor L1 built into the tank. If the corresponding level is reached, a signal is sent to controller C3, which immediately starts an emergency filling process of tank T2. In addition, the alarm A1 is triggered, indicating the hazardous condition to the operator. Before tank T2 is completely filled, the operator must switch off pumps P1 and P2 manually by interrupting the emergency switches S1 and S2.

If the safety mechanism fails, the mixed product might exit the tank via pipe O1, thereby causing pollution to the environment.

In the following, a fault tree analysis for the top-event POLLUTION should be performed. For this, please assume that the emergency switches S1 and S2 never fail and that all basic events are stochastically independent.

a) As a first step, draw a high-level fault tree for the top-event p (POLLUTION), thereby only considering the intermediate events d1 (DOSING UNIT 1 FAILS UNSAFE), d2 (DOSING UNIT 2 FAILS UNSAFE) and sm (SAFETY MECHANISM FAILS). Determine the corresponding Boolean function. What does “dosing unit fails unsafe” mean in this example?

b) Refine the intermediate events d1 (DOSING UNIT 1 FAILS UNSAFE) and d2 (DOSING UNIT 2 FAILS UNSAFE) in separate fault tree diagrams. Determine the corresponding Boolean functions. Eliminate repeated events by restructuring your expressions and redraw the diagrams accordingly. For the dosing units we have two intermediate events, the pump not being switched off and the valve not being closed. The pump is dependent on the counter(c1/2) and the mass flow meter (f1/2). The valve is dependent on the motor(m1/2), the counter(c1/2), and a correct working valve(v1/2).

c) Refine the intermediate event sm (SAFETY MECHANISM FAILS) in a separate fault tree diagram. Determine the corresponding Boolean function. (*Hint: the variable order in g) shows the involved events*)

d) Develop the ROBDD for the Boolean expression for p as obtained in question a) using the variable order: d1 → d2 → sm

e) Develop the ROBDD for the Boolean expression for d1 as obtained in question b) using the variable order: c1 → f1 → m1 → v1

f) Develop the ROBDD for the Boolean expression for d2 as obtained in question b) using the variable order: v2 → f2 → c2 → m2

g) Develop the ROBDD for the Boolean expression for sm as obtained in question c) using the variable order: l1 → l2 → p3 → m3 → v3 → c3 → a1 → h1 → t2

h) Assuming the basic event probabilities as given in the table below, now calculate the probability for the top-event p (POLLUTION).

Name	Description of basic event	Probability
t2	TANK T2 FULL	0.1
c1/2	COUNTER C1/2 DEFECTIVE	0.05
a1	ALARM A1 DEFECTIVE	0.03
h1	OPERATOR H1 SLEEPS	0.1
m1/2	MOTOR M1/2 DEFECTIVE	0.06
v1/2	VALVE V1/2 STUCK OPEN	0.08
f1/2	MASS FLOW METER F1/2 DEFECTIVE (NO IMPULSES)	0.05
l1/2	LEVEL SENSOR L1/2 DEFECTIVE	0.05
p3	PUMP P3 DEFECTIVE	0.06
m3	MOTOR M3 DEFECTIVE	0.06
v3	VALVE V3 STUCK CLOSED	0.08
c3	CONTROLLER C3 DEFECTIVE	0.05