SOEN 331/W - winter 2017

Assignment 3 – part 2 (weight 2%)
(Deadline and submission instructions provided in Part 1 of the assignment)

GOAL: practice Model Checking with UPPAAL tool

Below an exercise in modeling and analysis using the model checker Uppaal. Uppaal is free to download and very easy to install and use.

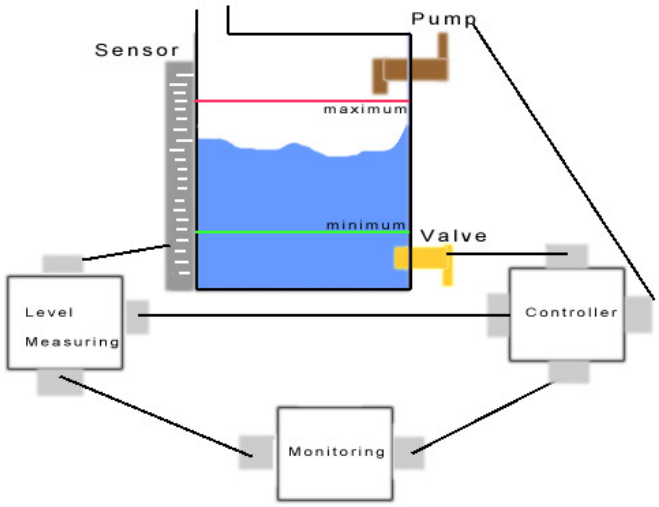
Model checking

Model checking is a technique that can be used in the design and analysis of dynamic systems. A model checker is a computer program that rapidly and cleverly searches through all the possible states of a system to look for problems.

A model checker does not work with the real system, but a *model* of the system - hence the name. Uppaal uses *state diagrams* as models. Apart from a diagram describing the system we want to analyse, we also need to describe some desired properties. These properties are called *queries*.

Exercise: Boiler Plant system

In this assignment, you are required to verify certain properties of a Boiler Plant system using the UPPAAL tool for model checking (see tutorial on UPPAAL).



The Boiler Plant requirements are:

- R1. Every 5 units of time, a new cycle of control is initiated.
- R2. The level measuring component reads the current quantity of water inside the steam boiler as measured by the sensor.
- R3. Then, the level measuring component sends a stimulus parameterized by the current quantity of water inside the boiler to the controller component.
- R4. The controller component should react to the stimulus within 5 units of time.
  - If the value is bigger than the maximum allowed, the controller will send a stimulus to close the pump.
  - if the value is less than the minimum allowed, the controller will send a stimulus to close the valve.
  - If the value is within the safe limit, no reaction is required.
- R5. The monitoring component sends a stimulus to the level measuring component to check its status.
- R6. The level measuring should react to the stimulus by sending the value of the current quantity.
- R7. The monitoring component can send a stimulus to the controller component to shut down the system or switch it on.

Your task:

The properties seen in class are given in the file <Assign3.q>
Import those 4 properties and in addition specify in TL the subsequent properties:

Specify in temporal logic the subsequent properties and complete the Boiler Plant 1 model checking process with UPPAAL following the instructions given in the tutorial:

P1. Eventually the pump will be open in less than 5 units of time when the level measuring sends the level to controller and the quantity is below the safe limit
P2. Invariantly always, in all system executions, the pump is opened when the quantity is below the minimum safe limit
P3. When the level measuring units sends the controlLevel shared event, eventually the controlLevel will happen at the controller in less than 5 units of time
P4. When the controlLevel event happen at the controller and if the quantity is more than the safe limit, the quantity eventually will be in the safe range between max and minimum.

Complete the Boiler Plant 1 model checking process with UPPAAL following the instructions given in the tutorial. If the model checking process fails for a given property, analyze the UPPAAL contra-example and discuss the reason for the failure. Document the results of the Boiler Plant model checking.

Submit the following files:
Boiler Plant **2** model file (.xml)
Your properties file (.q)
Documented results of task 1 and task2