Coursework 1: Rigorous Methods for Software Engineering
F21RS

Introduction:

Many engineering facilities make use of water as a coolant. Storage tanks are typically used in order to maintain a sufficient supply of water. Controlling the amount of water within such water tanks can therefore represent a safety critical component of the facility. All such tanks have physical limits which if exceeded will represent a major hazard to life and/or the environment. Automated subsystems which detect such hazards and invoke corrective actions play a critical role in ensuring the overall safety of a system. The focus of this coursework is the development of Alloy model of a software based Water Tank Protection (WTP) system.

The role of WTP is to ensure that a safe level of water is maintained with the tank. Exceeding the capacity would result in a structural failure in the water tank, which in turn would cause a failure in the water supply.

Conversely, if the water level get too low then the safety of the facilities that it is cooling maybe compromised.

Modelling of WTP in Alloy

Your first task is to develop an Alloy model of the Water Tank Protection system. The WTP system comprises of a central controller and 4 boundary subsystems that manage the console, sensors, alarm, and an emergency drainage valve.

1. Identify the relevant signature for the Alloy specification of WTP system.
2. Model the relationships between the central controller and the boundary subsystems.
3. In order to reduce the effects of component failure 3 sensors are used. How would you express this in Alloy?
4. The range of valid water level valves is divided into 3 categories: **low, normal, and high.** If a **Normal** sensor value is returned to the WTP controller then no action is required. If however a **High** sensor value is returned to the WTP controller then the alarm is enabled. Once the alarm is enabled, if the water-level returns to **Normal** by the next set of sensor readings then the alarm should be disabled. However, if the next time the sensor readings are sampled the value is still **High** then the WTP controller should open the emergency drainage valve. Note that if the emergency drainage valve is opened then the WTP controller ignores all sensor input until the system has been reset. If a **Low** sensor value is returned to the WTP controller then the alarm is enabled. Once the alarm is enabled, if the water-level eventually returns to **Normal** then the alarm should be disabled. The WTP controller should close the emergency drainage valve and/or disable the alarm when the reset mechanism 2 is enabled. However, a reset request should be ignored if the water-level is not below the **High**

threshold. How would you model the relationships between the WTP controller and the sensor readings in Alloy? Describe the behaviour using suitable predicates.

Modelling of the Software Requirements in Alloy

The safety-critical software for the WTP system is distributed across 5 packages (subsystems) as described below (see also CW2):

Console: provides an interface to the WTP controller. Specifically it supports a reset mechanism and is responsible for maintaining the state information on the reset subsystem. In addition it also counts the number of alarm events.

Sensors: responsible for maintaining and providing access to the current values of the sensors.

Alarm: provides control of the WTP alarm and is responsible for maintaining the state information on the alarm subsystem.

Drain: provides control of the vessel's emergency drainage valve and is responsible for maintaining the state information on the Drain subsystem.

WTP: responsible for the overall control provided by the WTP system

Write an Alloy model for each subsystem. The model should contain at least one signature and at least one predicate describing the behaviour of each subsystem. Test your model within a certain scope. Experiment with at least two runs for each predicate. How did you select the scope? Was Alloy useful for this modelling task? Why or Why not? Reflect on your experience (300 words).

Deliverables

1. A model of the hierarchical structure of a WTP system. [2 points]
2. A simple Alloy model of the WTP system, containing suitable signatures and fields. Reflection on and explanation of your design decisions. [3 points]
3. Reflection on using cardinality constraints in Alloy models in the current specification task. [3 points]
4. Alloy model of the relationship between the WTP controller and the sensor readings in Alloy. Reflection on the design decision.[5 points]
5. Modelling of each software requirement in Alloy. Reflection on the use of predicates and scope and the suitability of the tool for this task. [7 points]
6. Reflection on the use of Alloy and on what makes it suitable for this task [5 points]

Submission deadline:

Your submission (report and Alloy models) should be uploaded to VISION by 3.30pm (local time) on Friday, November, 1st , 2019 (end of week 7).

Note that this is an individual project which means that your submission MUST be your own work. This assignment counts for 50% of the coursework marks that are available for this course.